

# Symantec NetBackup™ Security and Encryption Guide

UNIX, Windows, and Linux

Release 7.6



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: 7.6

## Legal Notice

Copyright © 2013 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and 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>

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

# Technical Support

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

Symantec's support offerings include the following:

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

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

[www.symantec.com/business/support/](http://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/](http://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/](http://www.symantec.com/business/support/)

## Customer service

Customer service information is available at the following URL:

[www.symantec.com/business/support/](http://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	<a href="mailto:customercare_apac@symantec.com">customercare_apac@symantec.com</a>
Europe, Middle-East, and Africa	<a href="mailto:semea@symantec.com">semea@symantec.com</a>
North America and Latin America	<a href="mailto:supportsolutions@symantec.com">supportsolutions@symantec.com</a>

# Contents

Technical Support .....	4
Chapter 1      Increasing NetBackup security .....	15
About NetBackup security and encryption .....	16
NetBackup security implementation levels .....	16
World-level security .....	17
Enterprise-level security .....	18
Datacenter-level security overview .....	20
NetBackup Access Control (NBAC) .....	20
Combined world, enterprise, and datacenter levels .....	25
NetBackup security implementation types .....	26
Operating system security .....	28
NetBackup security vulnerabilities .....	28
Standard NetBackup security .....	29
Media Server Encryption Option (MSEO) security .....	30
Client side encryption security .....	31
NBAC on master, media server, and GUI security .....	33
NBAC complete security .....	35
All NetBackup security .....	36
Chapter 2      Security deployment models .....	38
Workgroups .....	39
Single datacenters .....	39
Multi-datacenters .....	39
Workgroup with NetBackup .....	40
Single datacenter with standard NetBackup .....	43
Single datacenter with Media Server Encryption Option (MSEO) .....	46
Single datacenter with client side encryption .....	49
Single datacenter with NBAC on master and media servers .....	51
Single datacenter with NBAC complete .....	55
Single datacenter with all security implemented .....	58
Multi-datacenter with standard NetBackup .....	62
Multi-datacenter with Media Server Encryption Option (MSEO) .....	66
Multi-datacenter with client side encryption .....	71
Multi-datacenter with NBAC on master and media servers .....	76

	Multi-datacenter with NBAC complete .....	82
	Multi-datacenter with all NetBackup security .....	88
Chapter 3	Port security .....	95
	About NetBackup TCP/IP ports .....	95
	About NetBackup daemons, ports, and communication .....	97
	Standard NetBackup ports .....	97
	NetBackup master server outgoing ports .....	98
	NetBackup media server outgoing ports .....	99
	NetBackup enterprise media management (EMM) server outgoing ports .....	100
	Client outgoing ports .....	101
	Windows administration console and Java server outgoing ports .....	101
	Java console outgoing ports .....	102
	About MSDP port usage .....	103
	About Cloud port usage .....	103
	Additional port information for products that interoperate with NetBackup .....	103
	About configuring ports .....	109
	Enabling or disabling random port assignments .....	109
	Specifying firewall connection options on a NetBackup server or client .....	110
	Specifying firewall connection options for destination computers from a source computer .....	113
	Editing port information in configuration files .....	114
	Updating client connection options .....	115
	Updating port settings for the Media Manager in the vm.conf file .....	116
	Port requirements for NDMP backups .....	118
	Known firewall problems encountered when using NetBackup with third-party robotic products .....	118
Chapter 4	Access control security .....	120
	About using NetBackup Access Control (NBAC) .....	123
	NetBackup access management administration .....	126
	About NetBackup Access Control (NBAC) configuration .....	127
	Configuring NetBackup Access Control (NBAC) .....	127
	NBAC configuration overview .....	128
	Configuring NetBackup Access Control (NBAC) on standalone master servers .....	129



Installing the NetBackup 7.6 master server highly available on a cluster .....	130
Configuring NetBackup Access Control (NBAC) on a clustered master server .....	130
Configuring NetBackup Access Control (NBAC) on media servers .....	131
Installing and configuring access control on clients .....	133
Establishing a trust relationship between the broker and the Windows remote console .....	133
NBAC configure commands summary .....	134
Upgrading NetBackup Access Control (NBAC) .....	139
About including authentication and authorization databases in the NetBackup hot catalog backups .....	139
Upgrading NetBackup 7.6 when an older version of NetBackup is using a root broker installed on a remote machine .....	139
Configuring NetBackup Access Control (NBAC) for NetBackup pre-7.0 media server and client computers .....	144
Manually configuring the Access Control host properties .....	145
Unifying NetBackup Management infrastructures with the <code>setuptrust</code> command .....	146
Using the <code>setuptrust</code> command .....	147
Accessing the master server and media server host properties .....	148
Access control host properties .....	148
Network Settings tab .....	149
Authentication Domain tab .....	150
Authorization Service tab .....	151
Accessing the client host properties .....	152
Access control host properties dialog for the client .....	152
Authentication Domain tab for the client .....	153
Network Settings tab for the client .....	154
Access management troubleshooting guidelines .....	155
Troubleshooting topics for NetBackup Authentication and Authorization .....	156
Troubleshooting NBAC issues .....	164
About the UNIX verification procedures .....	165
UNIX master server verification .....	166
UNIX media server verification .....	169
UNIX client verification .....	171
Verification points in a mixed environment with a UNIX master server .....	173
Master server verification points for a mixed UNIX master server .....	175
Media server verification points for a mixed UNIX master server .....	175
Client verification points for a mixed UNIX master server .....	177

Verification points in a mixed environment with a Windows master server .....	178
Master server verification points for a mixed Windows master server .....	181
Media server verification points for a mixed Windows master server .....	181
Client verification points for a mixed Windows master server .....	183
Windows verification points .....	185
Master server verification points for Windows .....	186
Media server verification points for Windows .....	190
Client verification points for Windows .....	192
Using the Access Management utility .....	194
About determining who can access NetBackup .....	195
Individual users .....	195
User groups .....	196
NetBackup default user groups .....	197
Configuring user groups .....	199
Creating a new user group .....	199
Creating a new user group by copying an existing user group .....	200
Renaming a user group .....	200
General tab .....	201
Users tab .....	201
Defined Users pane on the Users tab .....	202
Assigned Users pane on the Users tab .....	203
Adding a new user to the user group .....	203
About defining a user group and users .....	203
Logging on as a new user .....	205
Assigning a user to a user group .....	205
Permissions tab .....	206
About authorization objects and permissions .....	206
Granting permissions .....	208
Viewing specific user permissions for NetBackup user groups .....	209
Authorization objects .....	210
Media authorization object permissions .....	211
Policy authorization object permissions .....	211
Drive authorization object permissions .....	212
Report authorization object permissions .....	213
NBU_Catalog authorization object permissions .....	213
Robot authorization object permissions .....	214
Storage unit authorization object permissions .....	214
DiskPool authorization object permissions .....	215
BUAndRest authorization object permissions .....	216
Job authorization object permissions .....	216

Service authorization object permissions .....	217
HostProperties authorization object permissions .....	218
License authorization object permissions .....	218
Volume group authorization object permissions .....	219
VolumePool authorization object permissions .....	219
DevHost authorization object permissions .....	220
Security authorization object permissions .....	220
Fat server authorization object permissions .....	221
Fat client authorization object permissions .....	221
Vault authorization object permissions .....	222
Server group authorization object permissions .....	222
Key managment system (kms) group authorization object permissions .....	223

Chapter 5	Data at rest encryption security .....	224
	Data at rest encryption terminology .....	226
	Data at rest encryption limitations .....	226
	Encryption security questions to consider .....	229
	NetBackup data at rest encryption options .....	229
	Encryption options comparison .....	229
	Option 1 - NetBackup client encryption .....	230
	About running an encryption backup .....	231
	About choosing encryption for a backup .....	231
	Standard encryption backup process .....	232
	Legacy encryption backup process .....	232
	NetBackup standard encryption restore process .....	233
	NetBackup legacy encryption restore process .....	234
	Installation prerequisites for encryption security .....	235
	Installing encryption on a UNIX NetBackup server .....	235
	Installing encryption on a Windows NetBackup server .....	236
	About installing encryption locally on a NetBackup UNIX client .....	236
	About installing encryption locally on a NetBackup Windows client .....	236
	About configuring standard encryption on clients .....	236
	Managing standard encryption configuration options .....	237
	Managing the NetBackup encryption key file .....	238
	About configuring standard encryption from the server .....	239
	About creating encryption key files on clients notes .....	239
	Creating the key files .....	240
	Best practices for key file restoration .....	241
	Manual retention to protect key file pass phrases .....	241
	Automatic backup of the key file .....	241

Restoring an encrypted backup file to another client .....	242
About configuring standard encryption directly on clients .....	242
Setting standard encryption attribute in policies .....	243
Changing the client encryption settings from the NetBackup server .....	243
About configuring legacy encryption .....	243
About configuring legacy encryption from the server .....	244
Legacy encryption configuration options .....	245
About pushing the legacy encryption configuration to clients .....	246
About pushing the legacy encryption pass phrases to clients .....	247
Managing legacy encryption key files .....	248
Restoring a legacy encrypted backup created on another client .....	251
About setting legacy encryption attribute in policies .....	251
Changing client legacy encryption settings from the server .....	252
Additional legacy key file security for UNIX clients .....	252
Running the bpcd -keyfile command .....	253
Terminating bpcd on UNIX clients .....	254
Option 2 - Media server encryption .....	254
Media server encryption option administration .....	255

Chapter 6	Data at rest key management .....	256
	About the Key Management Service (KMS) .....	259
	KMS considerations .....	259
	KMS principles of operation .....	263
	About writing an encrypted tape .....	264
	About reading an encrypted tape .....	265
	KMS terminology .....	265
	Installing KMS .....	267
	Using KMS with NBAC .....	270
	About installing KMS with HA clustering .....	270
	Enabling cluster use with the KMS service .....	271
	Enabling the monitoring of the KMS service .....	271
	Disabling the monitoring of the KMS service .....	272
	Removing the KMS service from monitored list .....	272
	Configuring KMS .....	272
	Creating the key database .....	273
	About key groups and key records .....	274
	About creating key groups .....	275
	About creating key records .....	275
	Overview of key record states .....	276
	Key record state considerations .....	277
	Prelive key record state .....	278

Active key record state .....	278
Inactive key record state .....	278
Deprecated key record state .....	278
Terminated key record state .....	279
About backing up the KMS database files .....	279
About recovering KMS by restoring all data files .....	280
Recovering KMS by restoring only the KMS data file .....	280
Recovering KMS by regenerating the data encryption key .....	280
Problems backing up the KMS data files .....	281
Solutions for backing up the KMS data files .....	282
Creating a key record .....	282
Listing keys .....	283
Configuring NetBackup to work with KMS .....	283
NetBackup and key records from KMS .....	283
Example of setting up NetBackup to use tape encryption .....	284
About using KMS for encryption .....	286
Example of running an encrypted tape backup .....	287
Example of verifying an encryption backup .....	287
About importing KMS encrypted images .....	288
KMS database constituents .....	288
Creating an empty KMS database .....	289
Importance of the KPK ID and HMK ID .....	289
About periodically updating the HMK and KPK .....	290
Backing up the KMS keystore and administrator keys .....	290
Command line interface (CLI) commands .....	290
CLI usage help .....	291
Create a new key group .....	292
Create a new key .....	292
Modify key group attributes .....	293
Modify key attributes .....	293
Get details of key groups .....	294
Get details of keys .....	294
Delete a key group .....	295
Delete a key .....	295
Recover a key .....	296
Modify host master key (HMK) .....	296
Get host master key (HMK) ID .....	297
Get key protection key (KPK) ID .....	297
Modify key protection key (KPK) .....	297
Get keystore statistics .....	297
Quiesce KMS database .....	298
Unquiesce KMS database .....	298
Key creation options .....	298

- Troubleshooting KMS ..... 299
- Solution for backups not encrypting ..... 300
- Solution for restores not decrypting ..... 300
- Troubleshooting example - backup with no active key record ..... 300
- Troubleshooting example - restore with an improper key record  
state ..... 304
- Index ..... 306

# Increasing NetBackup security

This chapter includes the following topics:

- [About NetBackup security and encryption](#)
- [NetBackup security implementation levels](#)
- [World-level security](#)
- [Enterprise-level security](#)
- [Datacenter-level security overview](#)
- [NetBackup Access Control \(NBAC\)](#)
- [Combined world, enterprise, and 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 on NetBackup master servers, media servers, and attached clients. Also made secure are the operating systems on which the servers and clients are running. The backup data is protected through encryption processes and vaulting. NetBackup data that is sent over the network is protected by dedicated and secure network ports.

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

See “[NetBackup security implementation levels](#)” on page 16.

See “[NetBackup Access Control \(NBAC\)](#)” on page 20.

See “[Operating system security](#)” on page 28.

See “[Standard NetBackup security](#)” on page 29.

See “[Media Server Encryption Option \(MSEO\) security](#)” on page 30.

See “[Client side encryption security](#)” on page 31.

See “[NBAC on master, media server, and GUI security](#)” on page 33.

See “[NBAC complete security](#)” on page 35.

See “[All NetBackup security](#)” on page 36.

## NetBackup security implementation levels

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

[Table 1-1](#) shows how NetBackup security levels can be implemented.

**Table 1-1** NetBackup security implementation levels

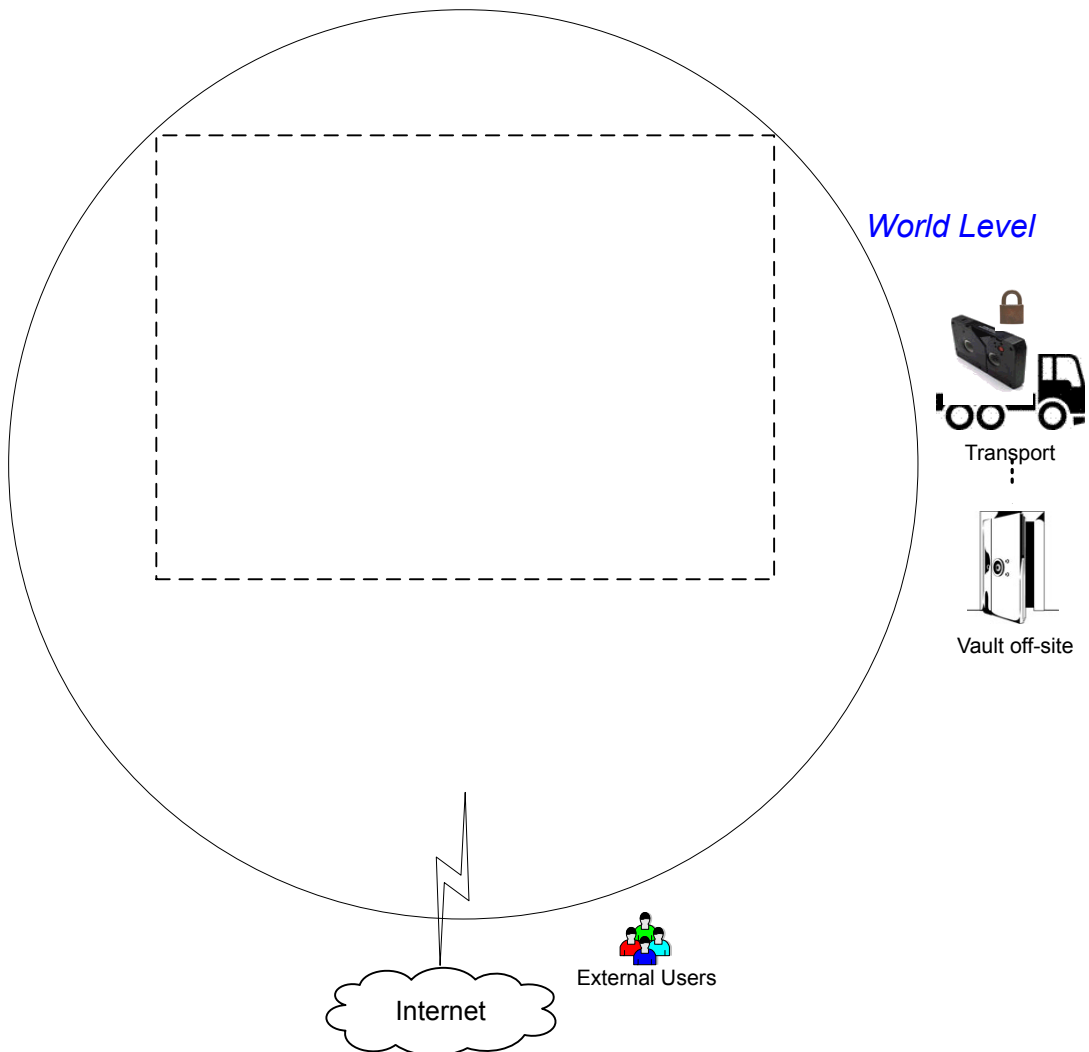
Security level	Description
World level	Specifies the Web server access and the encrypted tapes that are transported and vaulted
Enterprise level	Specifies internal users and security administrators
Datacenter level	Specifies NetBackup operations



# World-level security

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

**Figure 1-1** World-level security scope



**Table 1-2** Types of world-level security

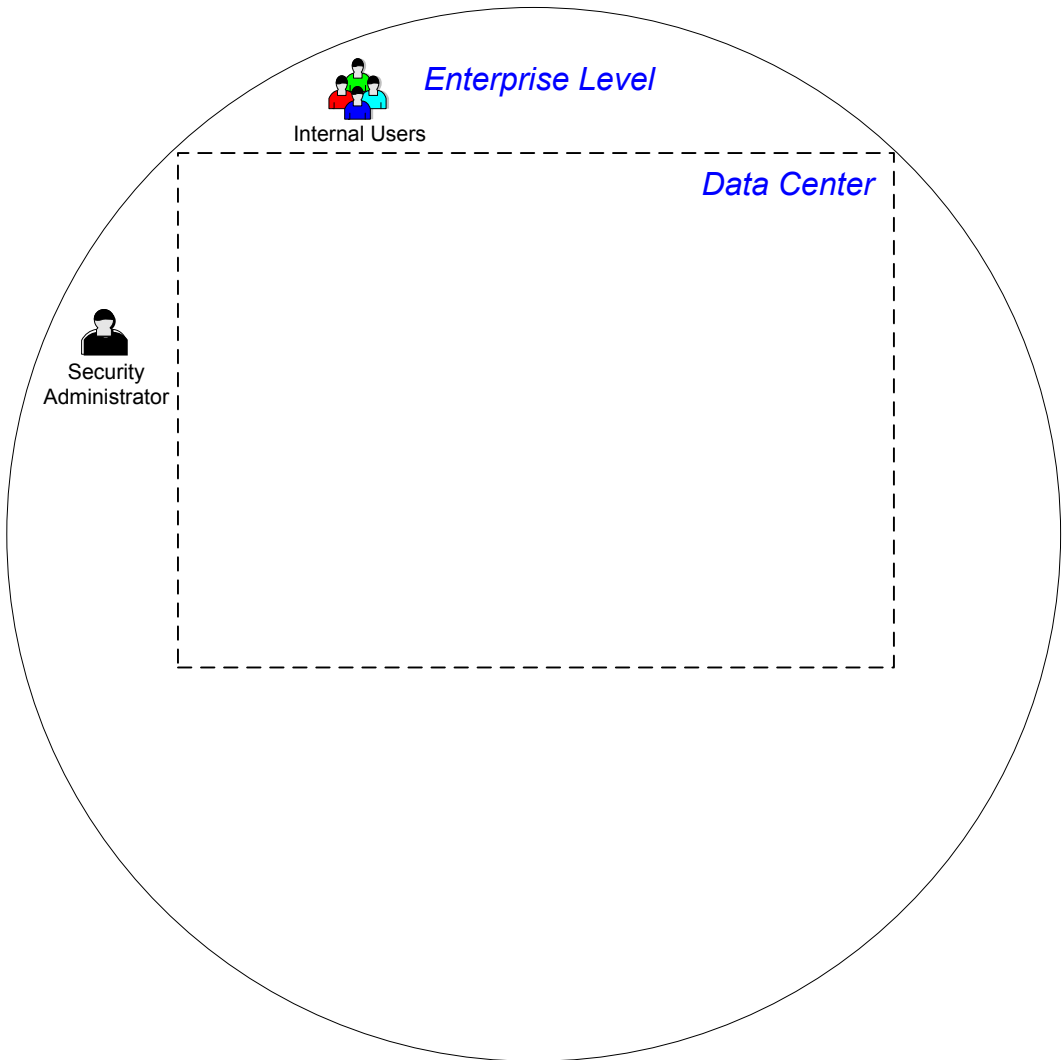
Type	Description
World-level external users	Specifies that external users can access Web servers behind firewalls. External users cannot access or use NetBackup functionality from the internet, because the external firewall prevents NetBackup ports from being accessed.
World-level internet	Specifies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

## Enterprise-level security

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

Figure 1-2 Enterprise-level security scope

## Security Overview



**Table 1-3** Types of enterprise-level security

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

## Datacenter-level security overview

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

[Table 1-4](#) describes the deployment models unique to datacenter-level security.

**Table 1-4** Deployment models for datacenter-level security

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

See “[NetBackup security implementation levels](#)” on page 16.

## NetBackup Access Control (NBAC)

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

See “[About NetBackup security and encryption](#)” on page 16.

Important points about NBAC include:

- Authentication and Authorization are used together

- NBAC uses authentication identities from a trusted source to reliably identify involved parties. Access decisions can then be made for manipulation of NetBackup based on those identities. Note that 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.
- NBAC is now supported with Search. The command `bpbaz - setupindexserver` helps to support NBAC with Search.
- Oracle, Oracle Archiver, DB2, Informix, Sybase, SQL Server, SAP and EV Migrator are not supported with NBAC.
- NBAC is not supported on Appliances.
- The NetBackup catalog backup is supported with NBAC.

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

**Table 1-5** NetBackup components used in security

Component	Description
Root broker	<p>The NetBackup 7.6 master server is the root broker in a datacenter installation. There is no provision to use another root broker. The recommendation is to allow trust between root brokers.</p> <p><b>Note:</b> 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>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>

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

Component	Description
Authorization engine	Communicates with the master server and the media server to determine the permissions of an authenticated user. These permissions determine the functionality available to a given server. The authorization engine also stores user groups and permissions. Only one authorization engine is required in a datacenter installation. The authorization engine also communicates over the WAN to authorize other media servers in a multi-datacenter environment.
GUI	Specifies a Remote Administration Console that receives credentials from the authentication brokers. The GUI then may use the credentials to gain access to functionality on the clients, media, and master servers.
MSEO	Specifies the MSEO (media server Encryption Option) that is a software appliance that encrypts data written to tape by the media server (data at rest encryption). The MSEO is an alternative to the client side encryption that can reduce the CPU processing load on the client.
Master server	Communicates with the root broker and authentication broker, GUI, authorization engine, media server, and clients.
NetBackup administrator	Specifies a user who has been granted administrator permissions to access and manage the NetBackup functionality from within the datacenter.
Media server	Communicates with the master server, root broker and authentication broker, authorization engine, MSEO, and clients 1 through 6. The media server writes unencrypted data to tape for client 5 and encrypted data to tape for client 6.
Clients	Specifies that clients 1 through 4 are standard NetBackup types. Client 5 is a Web server type located in the DMZ. Client 6 is a client side encrypted type also located in the DMZ. All client types are managed by the master server and have their data backed up to tape through the media server. Clients 5 and 6 communicate to NetBackup using NetBackup only ports through the internal firewall. Client 5 also receives connections from the Internet using http only ports through the external firewall.
Tapes	<p>Specifies that the tape security in NetBackup can be increased by adding the following:</p> <ul style="list-style-type: none"> <li>■ Client side encryption</li> <li>■ MSEO (media server Encryption Option)</li> <li>■ Encryption of data at rest</li> </ul> <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 1-5** 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"> <li>■ Greater data confidentiality</li> <li>■ The loss of physical tape is not as critical if all the data is effectively encrypted</li> <li>■ The best risk mitigation strategy</li> </ul> <p>See <a href="#">“Encryption security questions to consider”</a> on page 229. 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 <a href="#">“About NetBackup TCP/IP ports”</a> on page 95. 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"> <li>■ NetBackup Access Control (NBAC)</li> <li>■ Classic NetBackup daemons employ authentication when NBAC is enabled</li> <li>■ CORBA daemons use the fully encrypted channels that support confidentiality, and provide data integrity</li> <li>■ Firewalls</li> <li>■ Disabling the unused ports (see port topic) in NetBackup and in other products See <a href="#">“Enabling or disabling random port assignments”</a> on page 109.</li> <li>■ PBX and VNETD dedicated ports provide increased NetBackup security</li> <li>■ Central set of ports to monitor and open through firewalls</li> </ul>

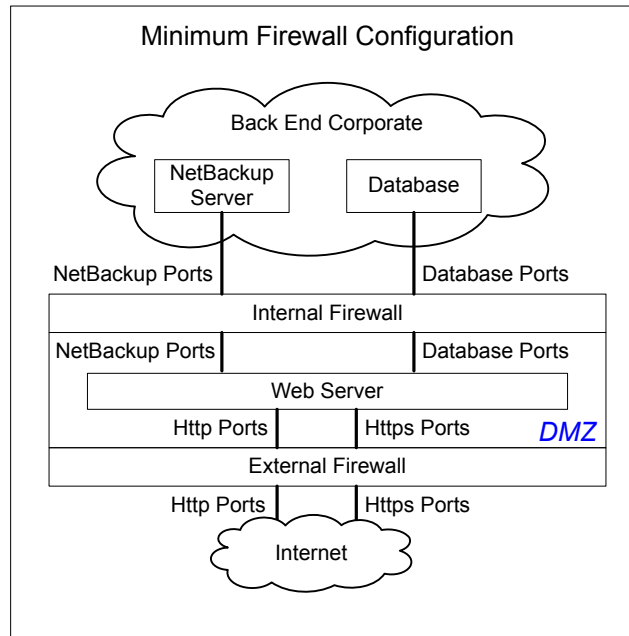
**Table 1-5** NetBackup components used in security (*continued*)

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"> <li>■ Symantec recommends the use of firewall and intrusion detection protection for NetBackup</li> <li>■ 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.</li> <li>■ Secure the master server as much as possible</li> <li>■ Firewalls can include internal firewalls and external firewalls, as follows: <ul style="list-style-type: none"> <li>■ 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.</li> <li>■ 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.</li> </ul> </li> </ul>
Demilitarized zone (DMZ)	<p>Specifies that the demilitarized zone (DMZ) increases security as follows:</p> <ul style="list-style-type: none"> <li>■ The DMZ is a restricted area in which the number of ports that are allowed for specific hosts is highly controlled</li> <li>■ 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.</li> </ul> <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 1-3 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 1-3** Example firewalls and DMZ

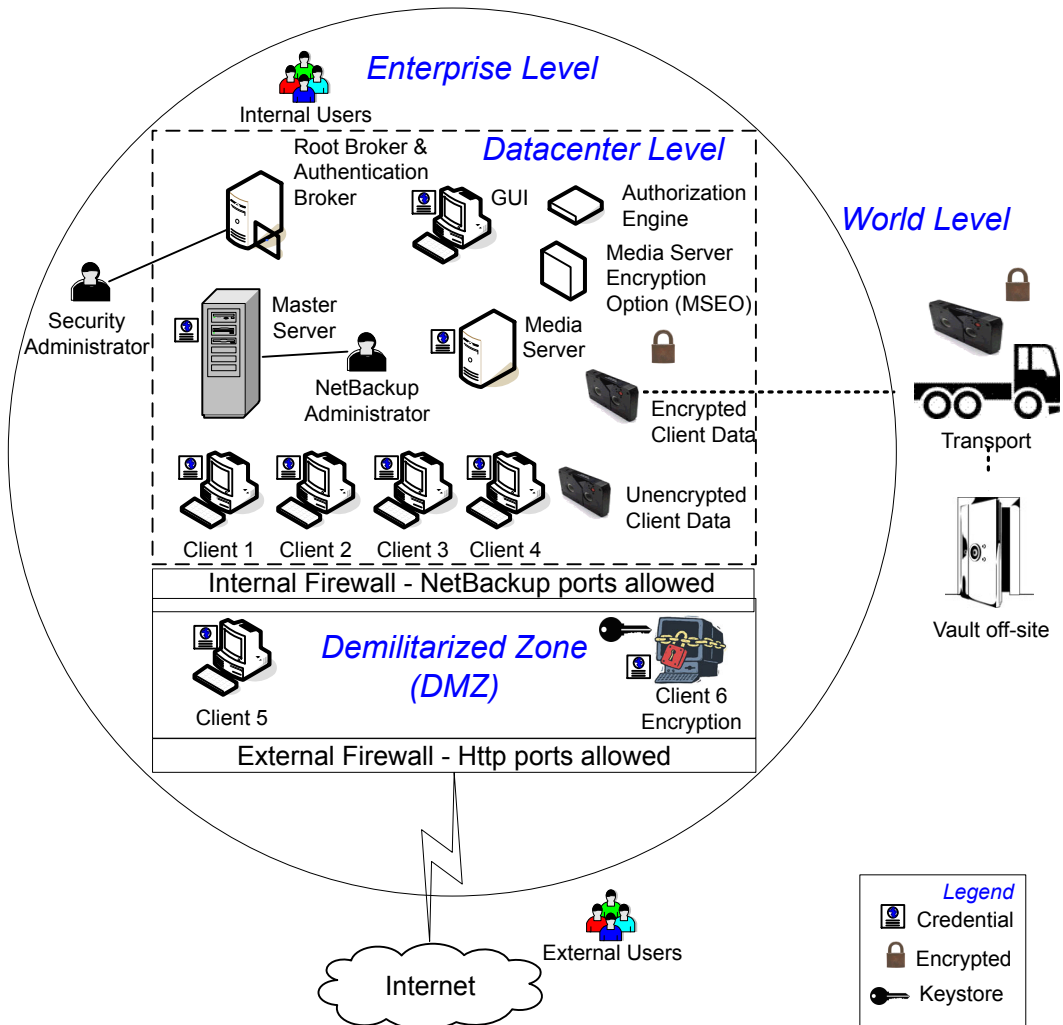


## Combined world, enterprise, and datacenter levels

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

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

**Figure 1-4** Combined world, enterprise, and data level



## NetBackup security implementation types

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

**Table 1-6** Security implementation types

Security implementation type	Characteristics	Complexity	Security deployment models
See <a href="#">“Operating system security”</a> on page 28.	<ul style="list-style-type: none"> <li>Operating system dependent</li> <li>Varies based on system components</li> </ul>	Variable	Workgroup Single datacenter Multi-datacenter
See <a href="#">“Standard NetBackup security”</a> on page 29.	<ul style="list-style-type: none"> <li>Manage as root or administrator</li> <li>Data is not encrypted</li> </ul>	Low	Workgroup with NetBackup Single datacenter with standard NetBackup Multi-datacenter with standard NetBackup
See <a href="#">“Media Server Encryption Option (MSEO) security”</a> on page 30.	<ul style="list-style-type: none"> <li>Media server encryption</li> <li>Client to media server traffic is not encrypted</li> <li>May affect CPU performance on the media server</li> <li>Location of keys</li> </ul>	Low	Single datacenter with media server Encryption Option (MSEO) Multi-datacenter with media server Encryption Option (MSEO)
See <a href="#">“Client side encryption security”</a> on page 31.	<ul style="list-style-type: none"> <li>Data is encrypted on the client</li> <li>Encrypted data is sent over the wire</li> <li>Can affect CPU performance on the client</li> <li>Location of keys</li> </ul>	Medium	Single datacenter with client side encryption Multi-datacenter with client side encryption
See <a href="#">“NBAC on master, media server, and GUI security”</a> on page 33.	<ul style="list-style-type: none"> <li>NBAC gives authorization to access master and media servers</li> <li>Authenticates the system and users to access master and media servers</li> </ul>	Medium	Single datacenter with NBAC on master and media servers Multi-datacenter with NBAC on master and media servers
See <a href="#">“NBAC complete security”</a> on page 35.	<ul style="list-style-type: none"> <li>NBAC gives authorization throughout the system</li> <li>NBAC gives authentication throughout the entire system (servers, clients, and users)</li> </ul>	High	Single datacenter with NBAC complete Multi-datacenter with NBAC complete

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

Security implementation type	Characteristics	Complexity	Security deployment models
See <a href="#">“All NetBackup security”</a> on page 36.	<ul style="list-style-type: none"><li>■ Incorporates all NetBackup security types</li><li>■ The example diagrams and documentation employ all security mechanisms together</li></ul>	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

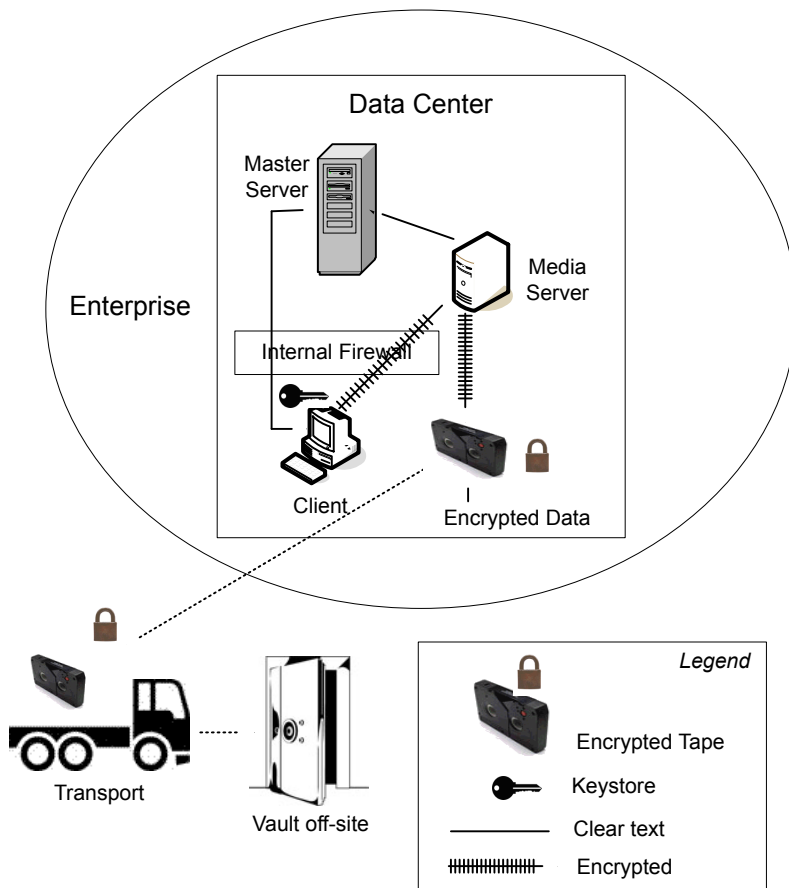
- The importance of accumulative NetBackup updates
- Use the Symantec Web site for information on possible security vulnerability issues:  
[www.symantec.com/avcenter/security/SymantecAdvisories.html](http://www.symantec.com/avcenter/security/SymantecAdvisories.html), or  
[www.symantec.com/security](http://www.symantec.com/security)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

## Standard NetBackup security

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

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

Figure 1-5 Standard NetBackup

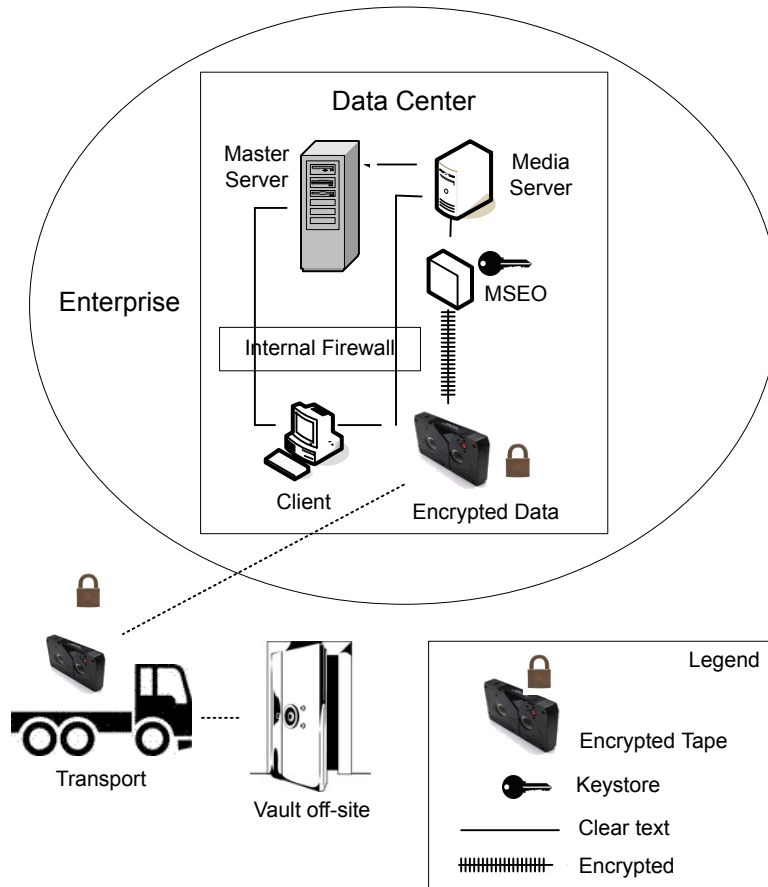


## Media Server Encryption Option (MSEO) security

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

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

**Figure 1-6** Media server encryption option (MSEO)



## Client side encryption security

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

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

- AFS
- DB2
- DataStore
- DataTools-SQL-BackTrack
- Informix-On-BAR
- LOTUS\_NOTES
- MS-Exchange
- MS-SharePoint
- MS-SQL-Server
- MS-Windows
- Oracle
- PureDisk-Export
- SAP
- Split-Mirror
- Standard
- Sybase

The following backup policy types do not support the Client Encryption Option. It is not possible to select the encryption check box in the policy attributes interface for these policy types.

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

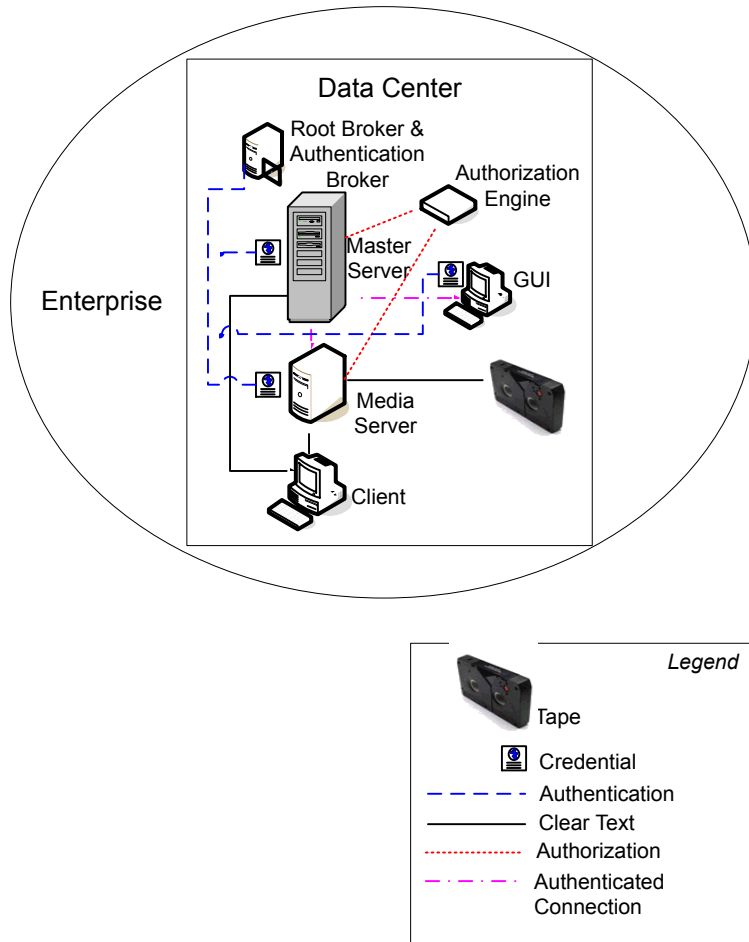
The media server Encryption Option is applied at the point where data is written to tape and can be used with all of the policy types listed. The exceptions are NDMP policies which write data directly from NDMP servers in NDMP format. Media server Encryption Option is supported for Remote NDMP where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

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



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

**Figure 1-7** Client side encryption



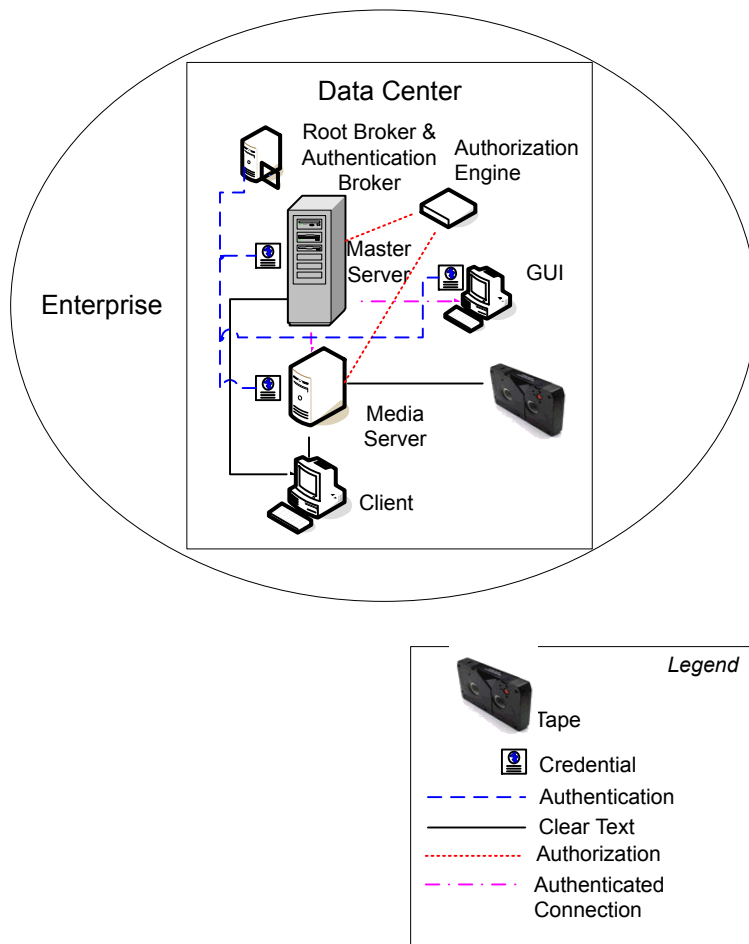
## NBAC on master, media server, and GUI security

The NBAC on master server, media server, and GUI security method uses the authentication broker. The broker provides credentials to the master server, the media server, and the GUI. This datacenter example uses the NetBackup Access Control on the master and the media servers to limit access to portions of NetBackup. Non-root administration of NetBackup can also be done using this example. NBAC is configured for use between the servers and the GUIs. Non-root

users can login to NetBackup using the operating system. Use the UNIX password or the Windows local domain to administer NetBackup. The global user repositories (NIS/NIS+ or Active Directory) can also be used to administer NetBackup. In addition, NBAC can be used to limit the level of access to NetBackup for certain individuals. For example, you can segregate day to day operational control from environmental configuration such as adding new policies, robots, etc.

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

**Figure 1-8** NBAC on master and media server

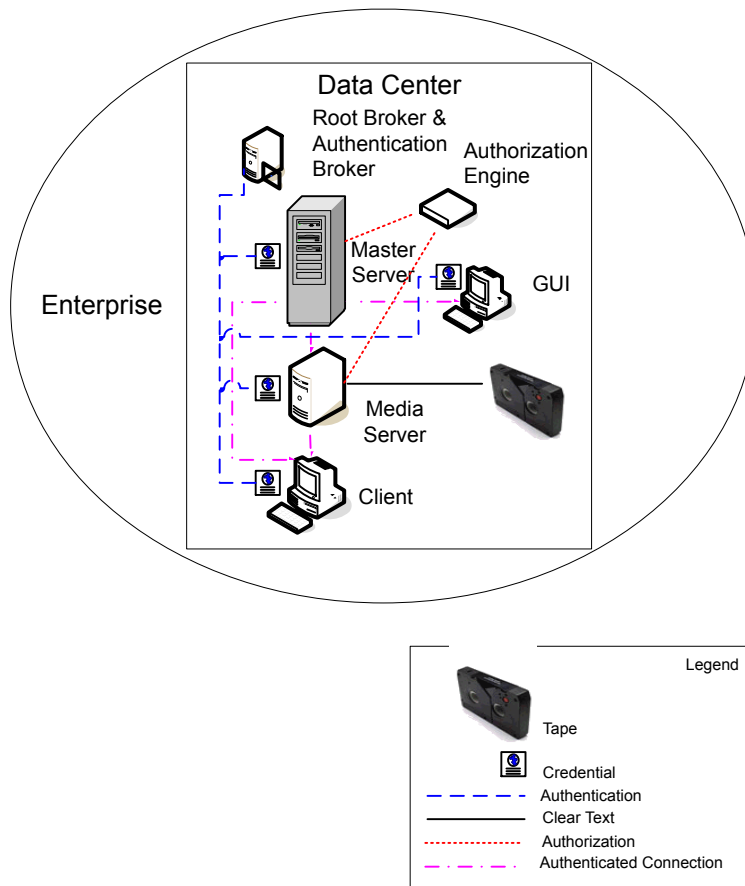


# NBAC complete security

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

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

**Figure 1-9** NBAC complete

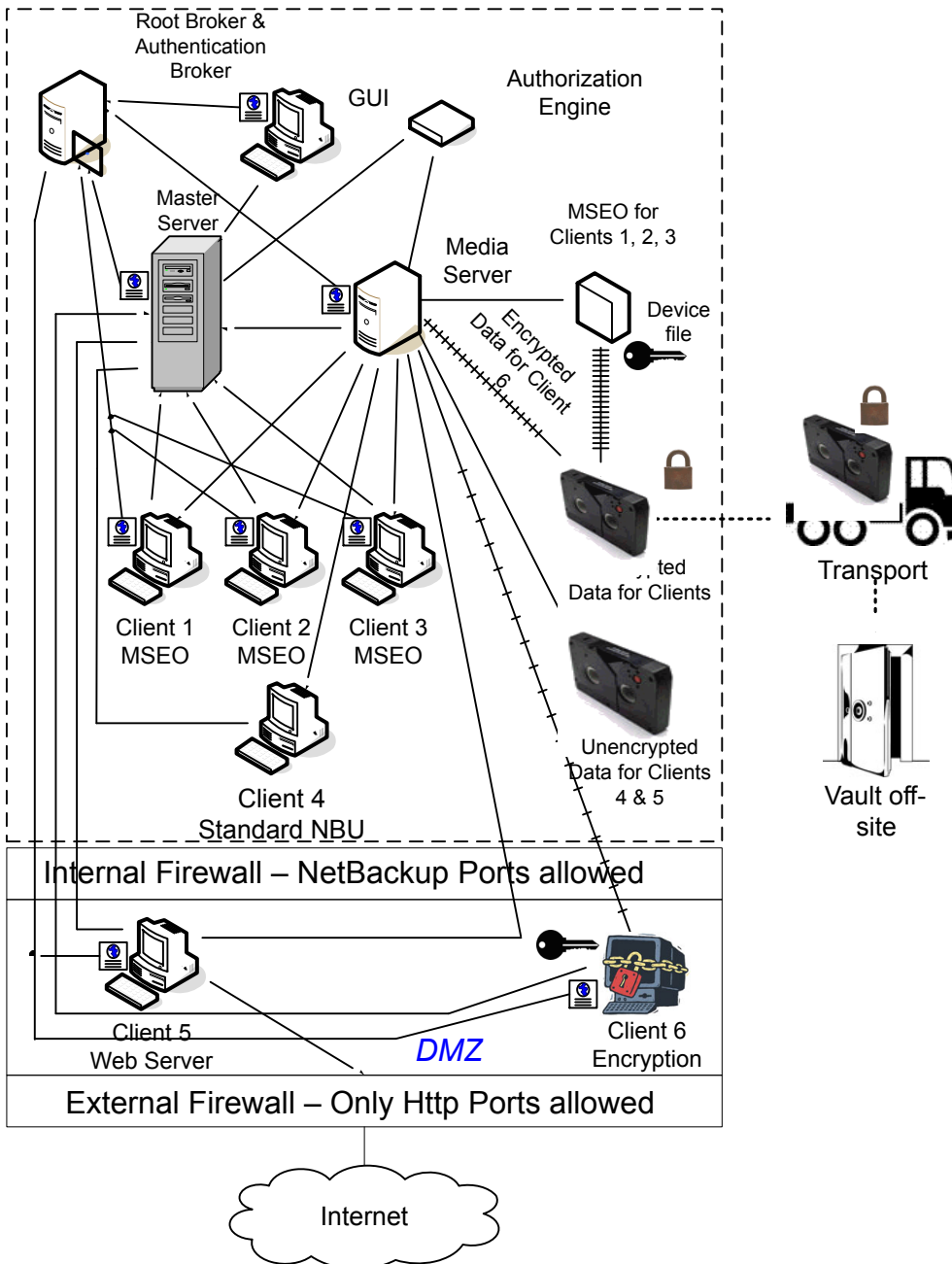


## All NetBackup security

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

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

Figure 1-10 All NetBackup security



# 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 40.

## 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 43.
- See [“Single datacenter with Media Server Encryption Option \(MSEO\)”](#) on page 46.
- See [“Single datacenter with client side encryption”](#) on page 49.
- See [“Single datacenter with NBAC on master and media servers”](#) on page 51.
- See [“Single datacenter with NBAC complete”](#) on page 55.
- See [“Single datacenter with all security implemented”](#) on page 58.

## 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 62.
- See [“Multi-datacenter with Media Server Encryption Option \(MSEO\)”](#) on page 66.
- See [“Multi-datacenter with client side encryption”](#) on page 71.
- See [“Multi-datacenter with NBAC on master and media servers”](#) on page 76.
- See [“Multi-datacenter with NBAC complete”](#) on page 82.
- See [“Multi-datacenter with all NetBackup security”](#) on page 88.

## 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.

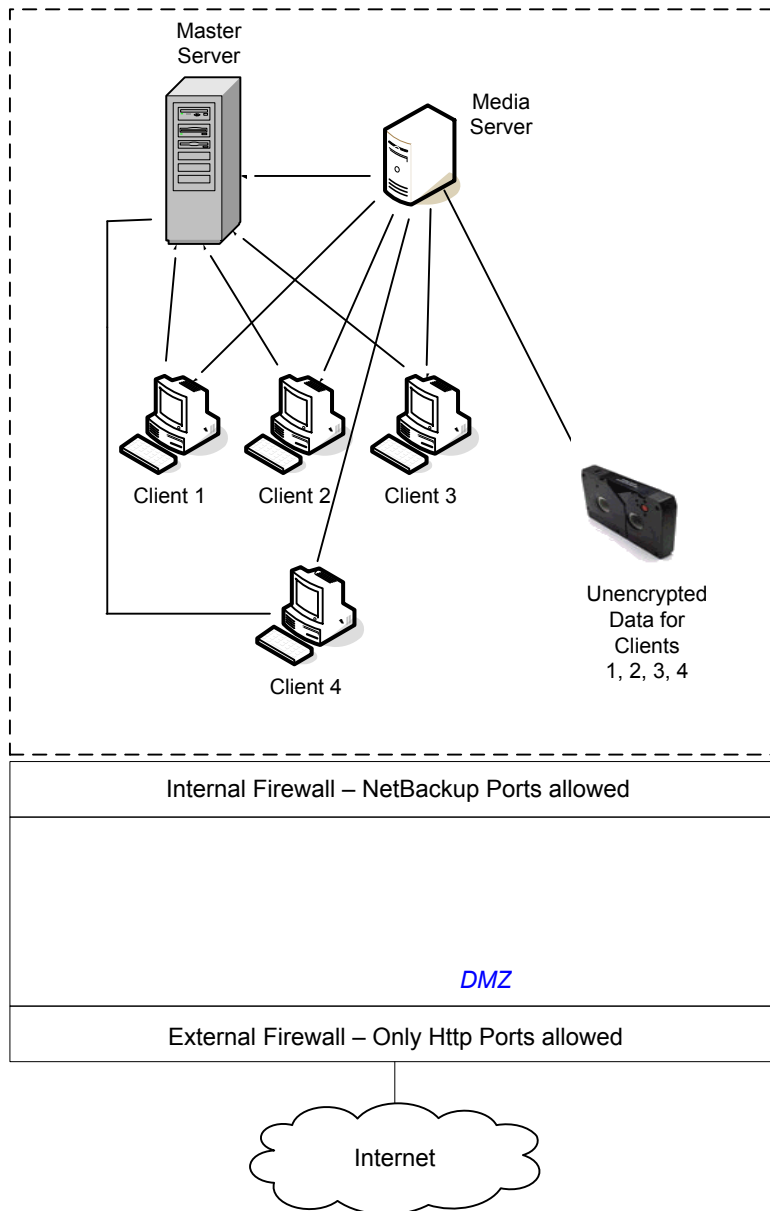
The workgroup with NetBackup includes the following highlights:

- 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><b>Note:</b> 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><b>Caution:</b> 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

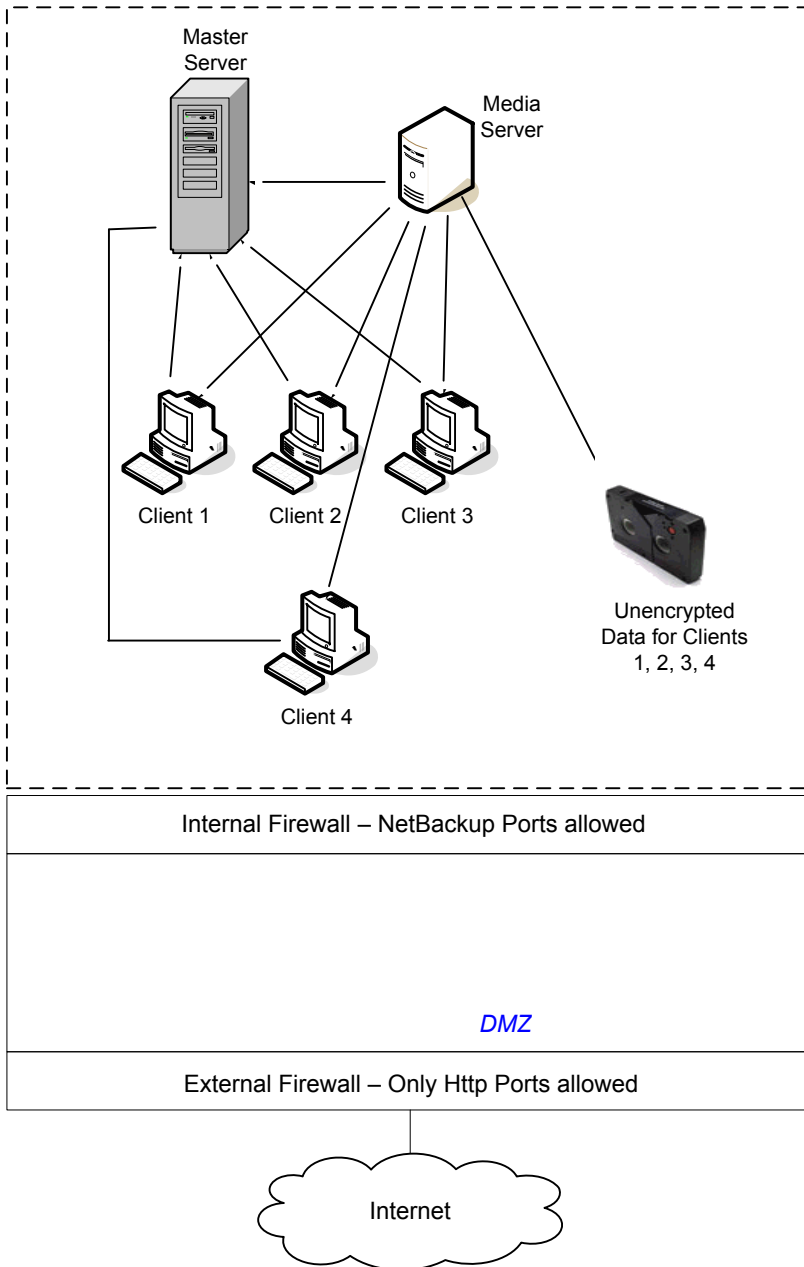
A single datacenter with standard NetBackup is defined as a medium to large group of hosts (greater than 50). It includes the hosts that are both internal only and those that expand through the DMZ to the Internet. This configuration typically has centralized naming service for hosts (such as DNS or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

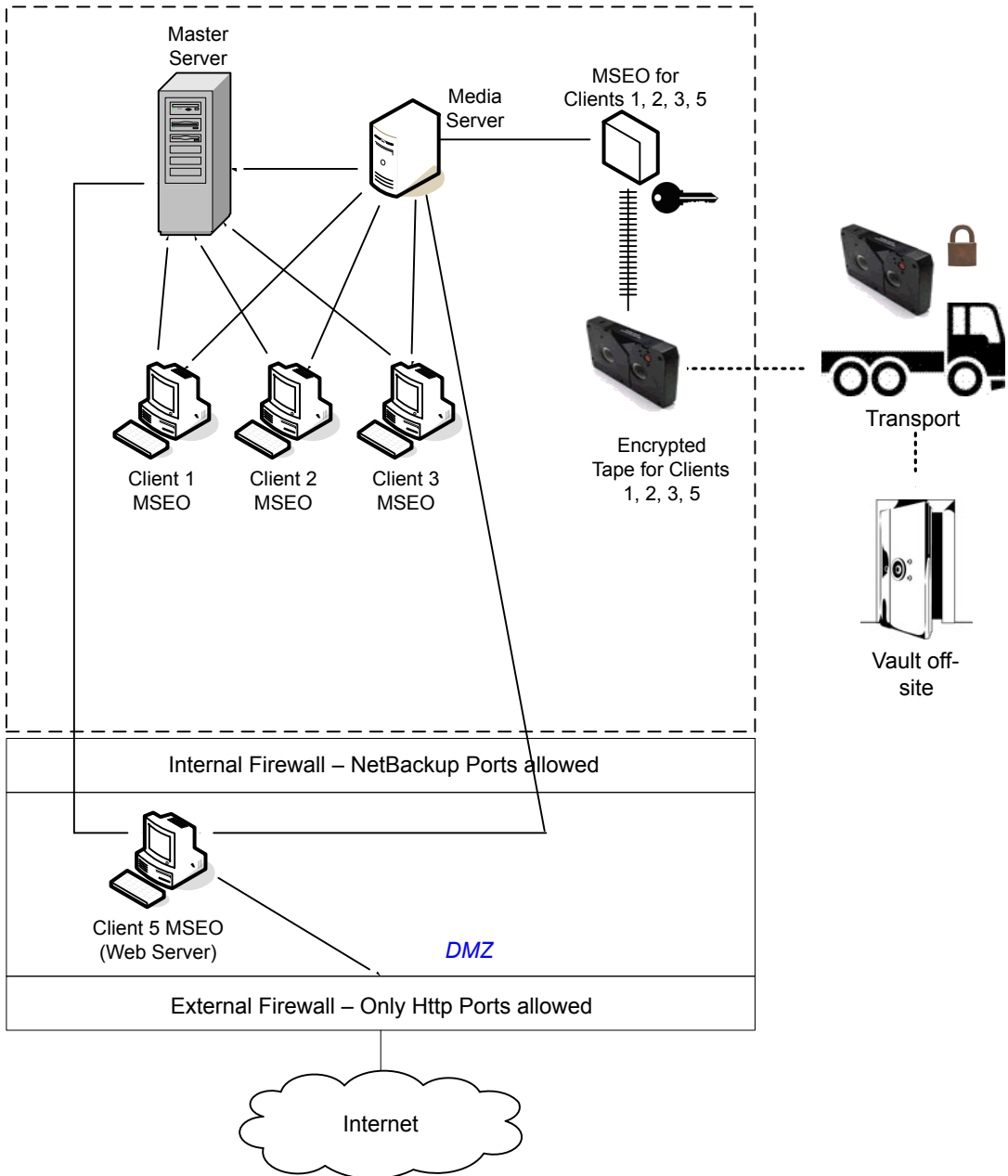
This single datacenter with the Media Server Encryption Option (MSEO) example typically includes more than 50 hosts. All externally facing hosts make use of the Media Server Encryption Option (MSEO). In this example, clients use the MSEO option for all hosts.

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. <b>Note:</b> 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

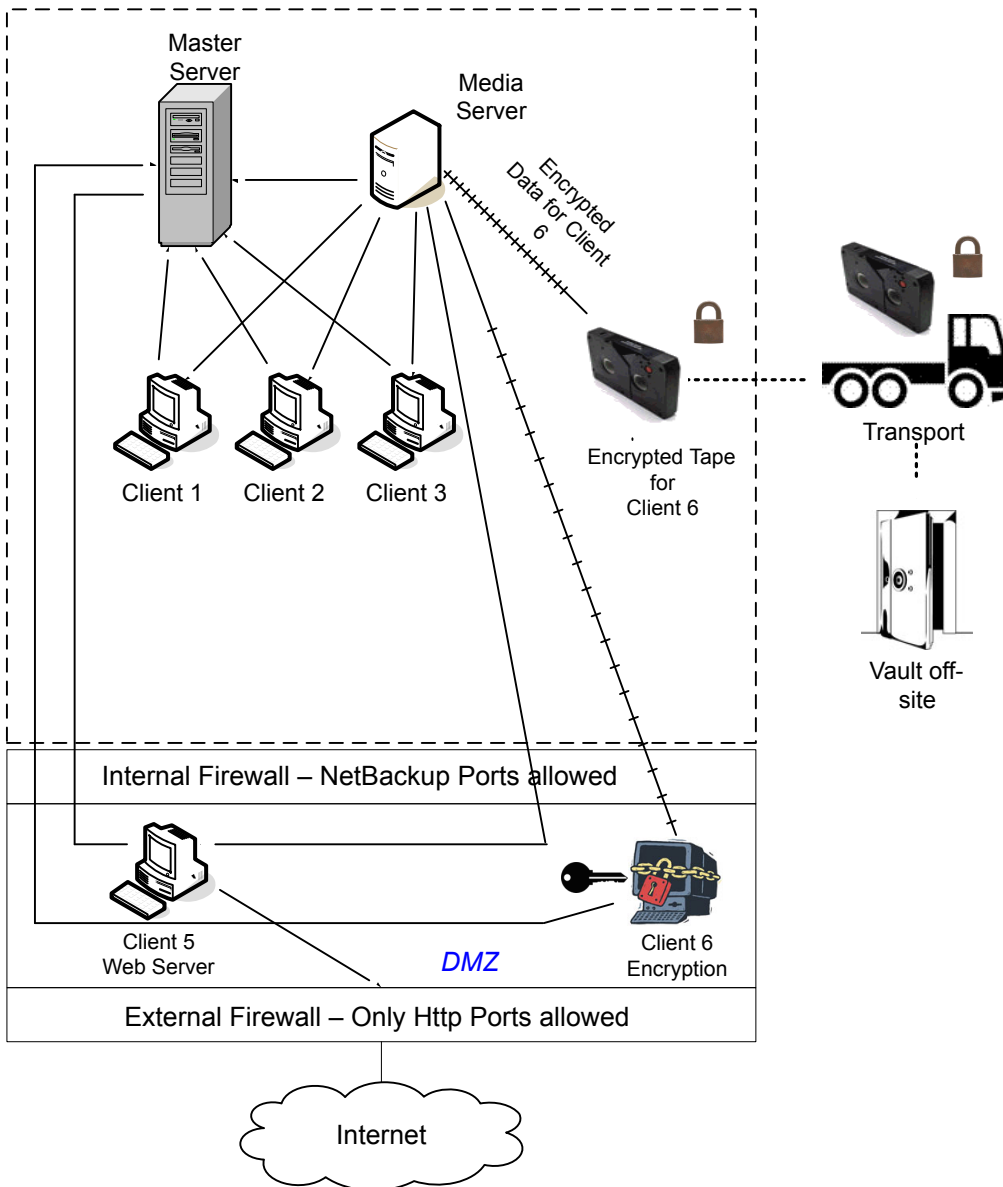
This single datacenter with client side encryption example uses the client side encryption to ensure data confidentiality across the wire as well as on tape. The client side encryption mitigates the risk of passive wire tapping within the organization. The risk of data exposure is reduced as tapes are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

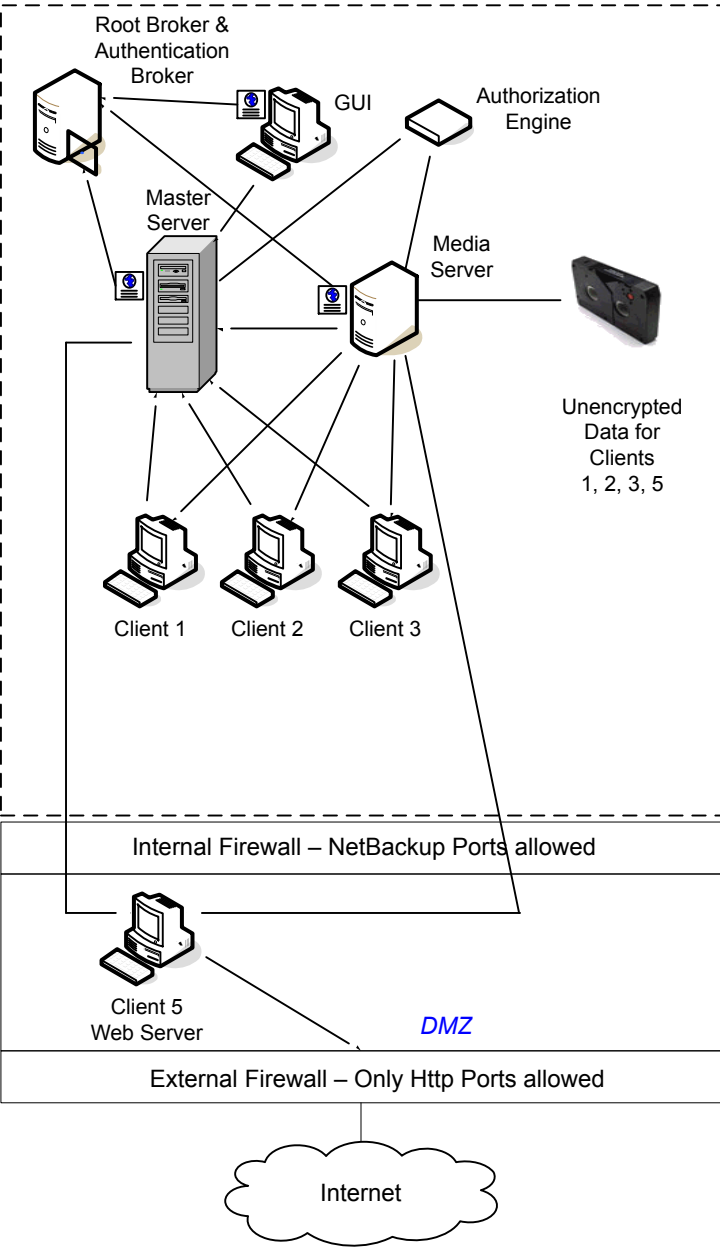
The single datacenter with NBAC on master and media servers includes the following highlights:

- 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><b>Note:</b> 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

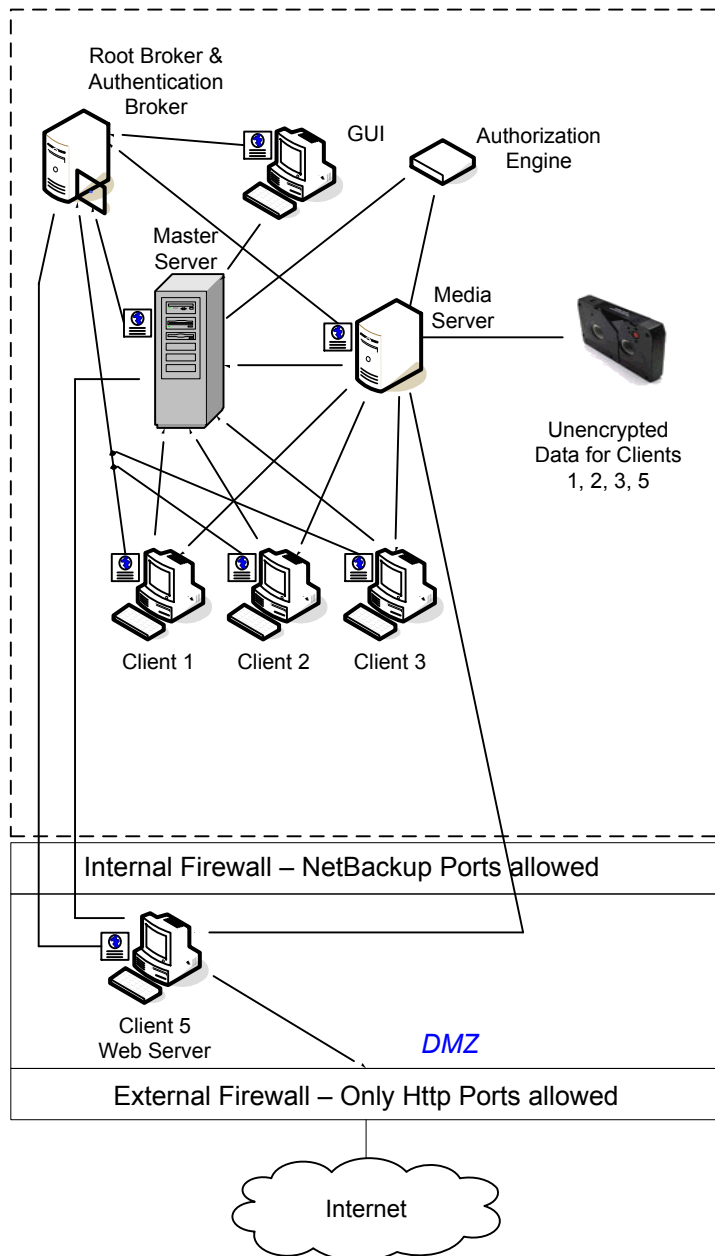
The single datacenter with NBAC complete environment is very similar to the single datacenter with NBAC master and media server. The main differences are that all of the hosts that participate in the NetBackup environment are reliably identified using credentials. And non-root administrators can manage 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. <a href="#">Figure 2-6</a> , 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><b>Note:</b> 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.

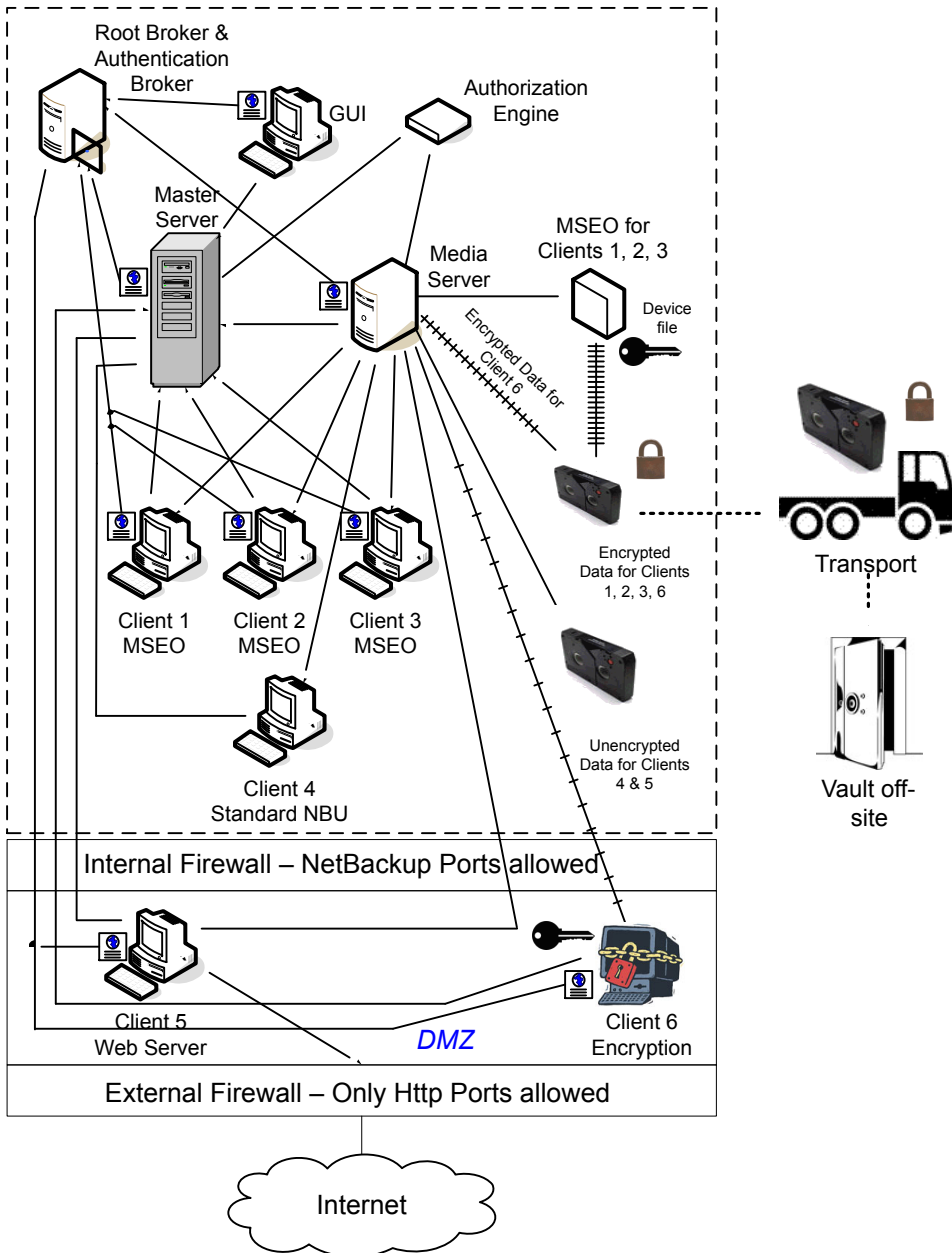
The single datacenter with all security implemented includes the following highlights:

- 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><b>Note:</b> 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 exist 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.

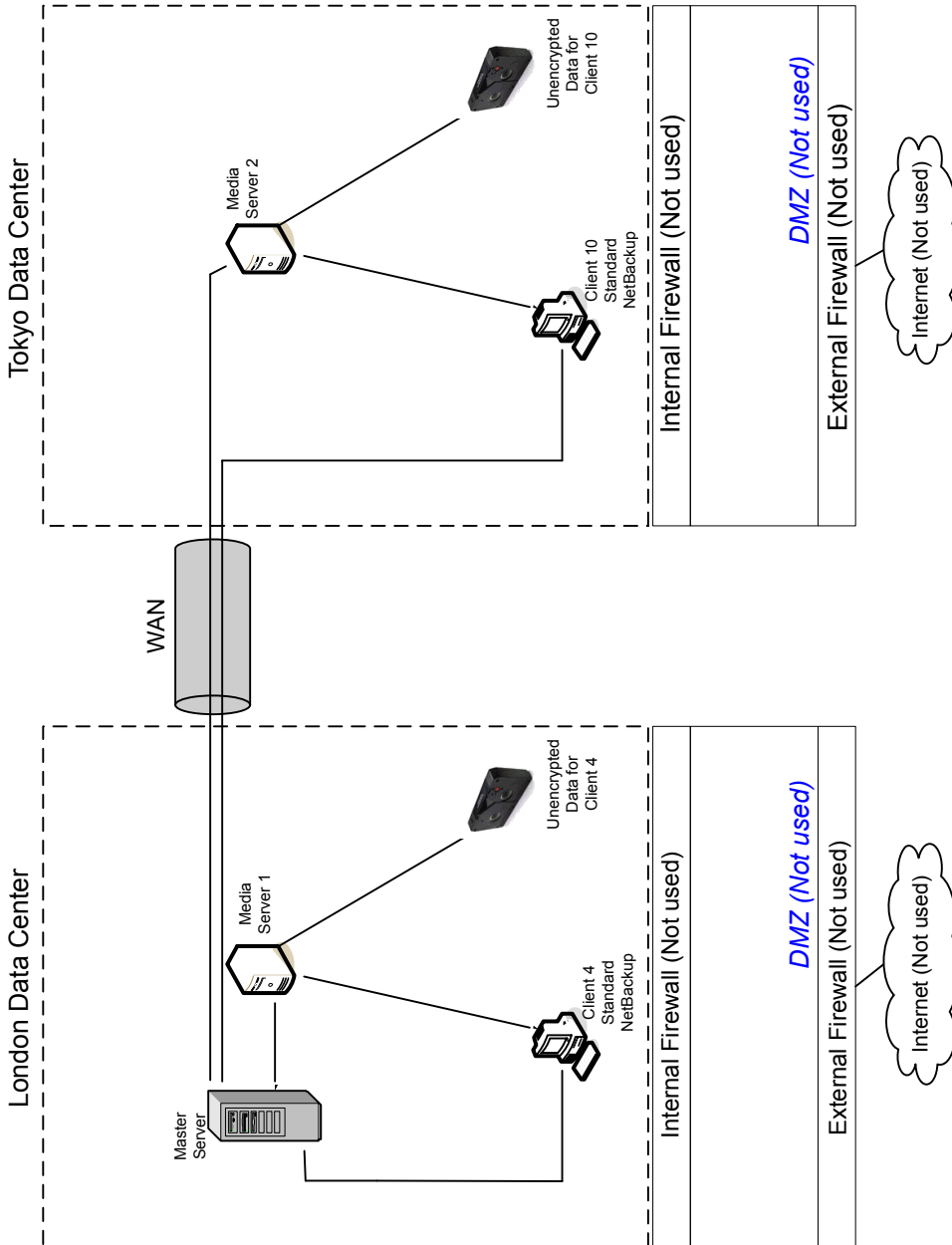
A multi-datacenter includes the hosts that are both internal only and those that expand through the DMZ to the Internet. This configuration typically has centralized naming service for hosts (such as DNS or WINS). It also has a centralized naming service for users (such as NIS or Active Directory).

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.

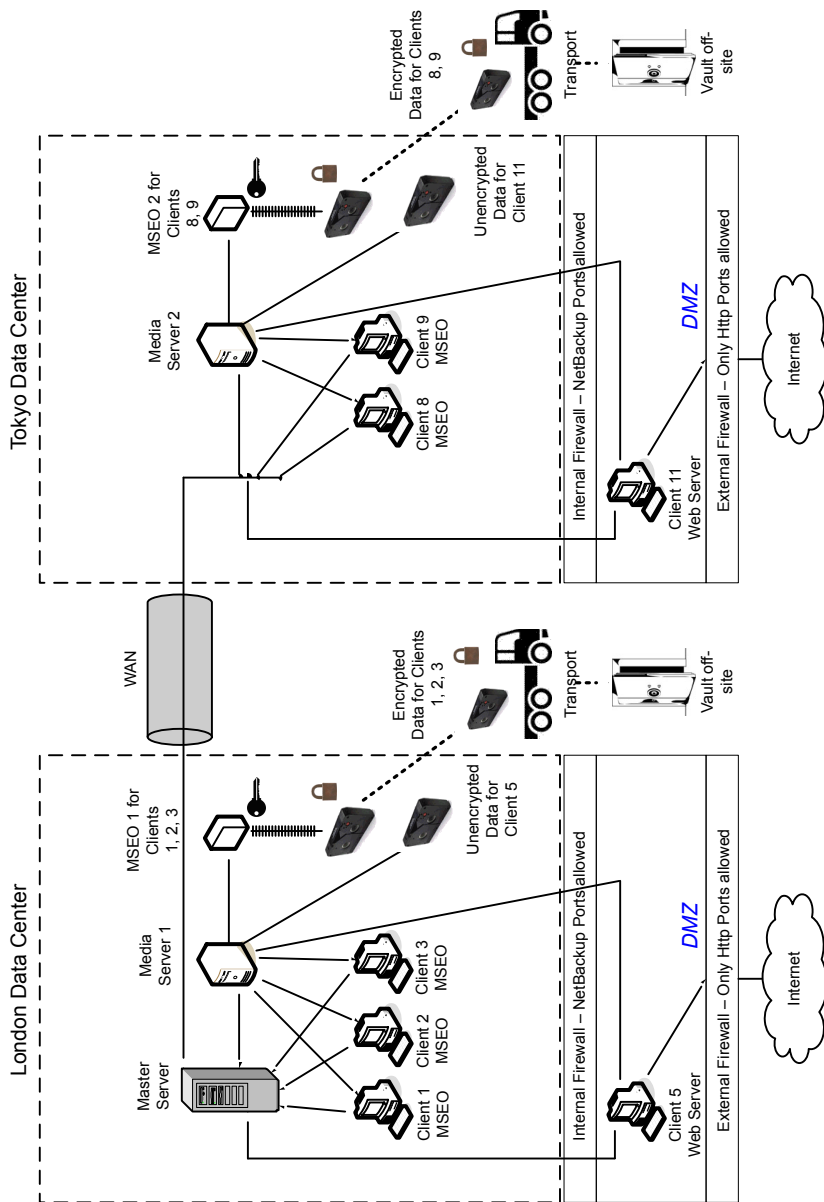
This multi-datacenter example can typically include more than 50 hosts. All externally facing hosts use the Media Server Encryption Option (MSEO). In this example, clients use both encrypted backups for some clients and the MSEO option for other hosts. Data that is too sensitive to be archived off-site 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><b>Note:</b> 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><b>Note:</b> 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><b>Note:</b> 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.

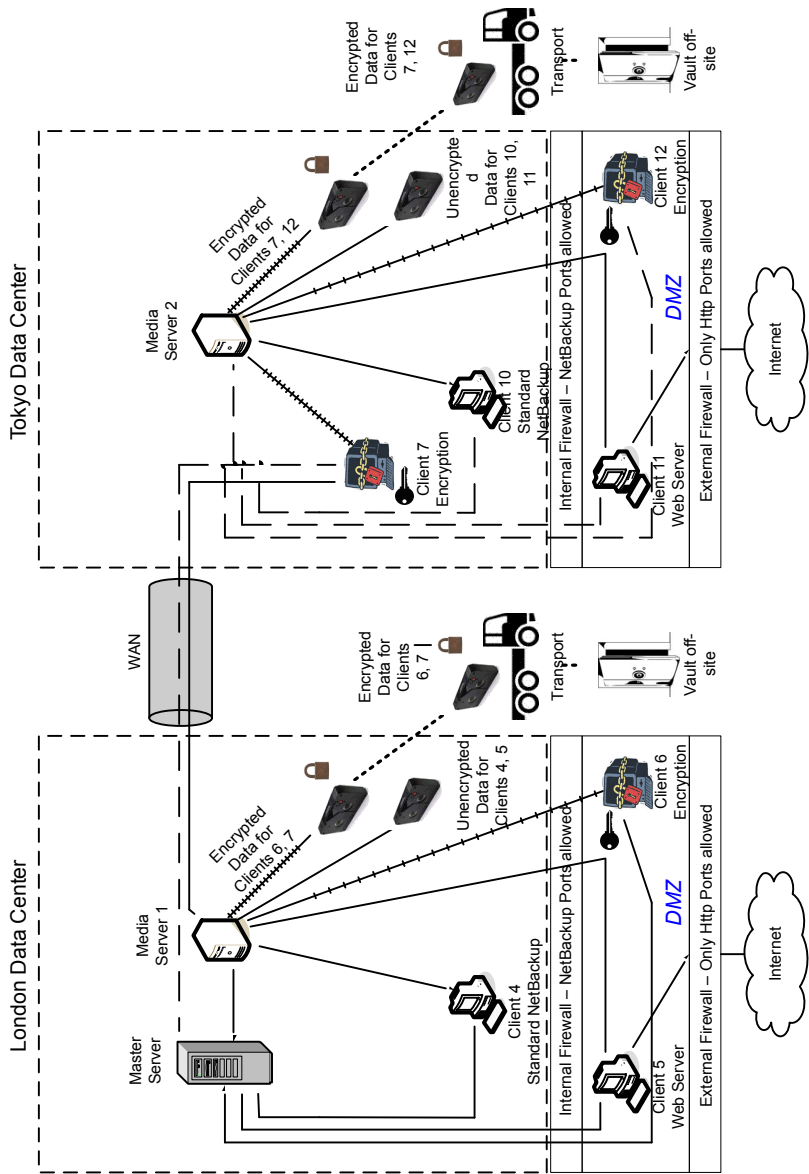
The example multi-datacenter can use client side encryption to ensure data confidentiality across the wire as well as on tape. This encryption helps to mitigate the risk of passive wire tapping within the organization. Risk of data exposure as the tapes are moved off site. This datacenter model assures 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><b>Note:</b> 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><b>Note:</b> 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><b>Note:</b> 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.

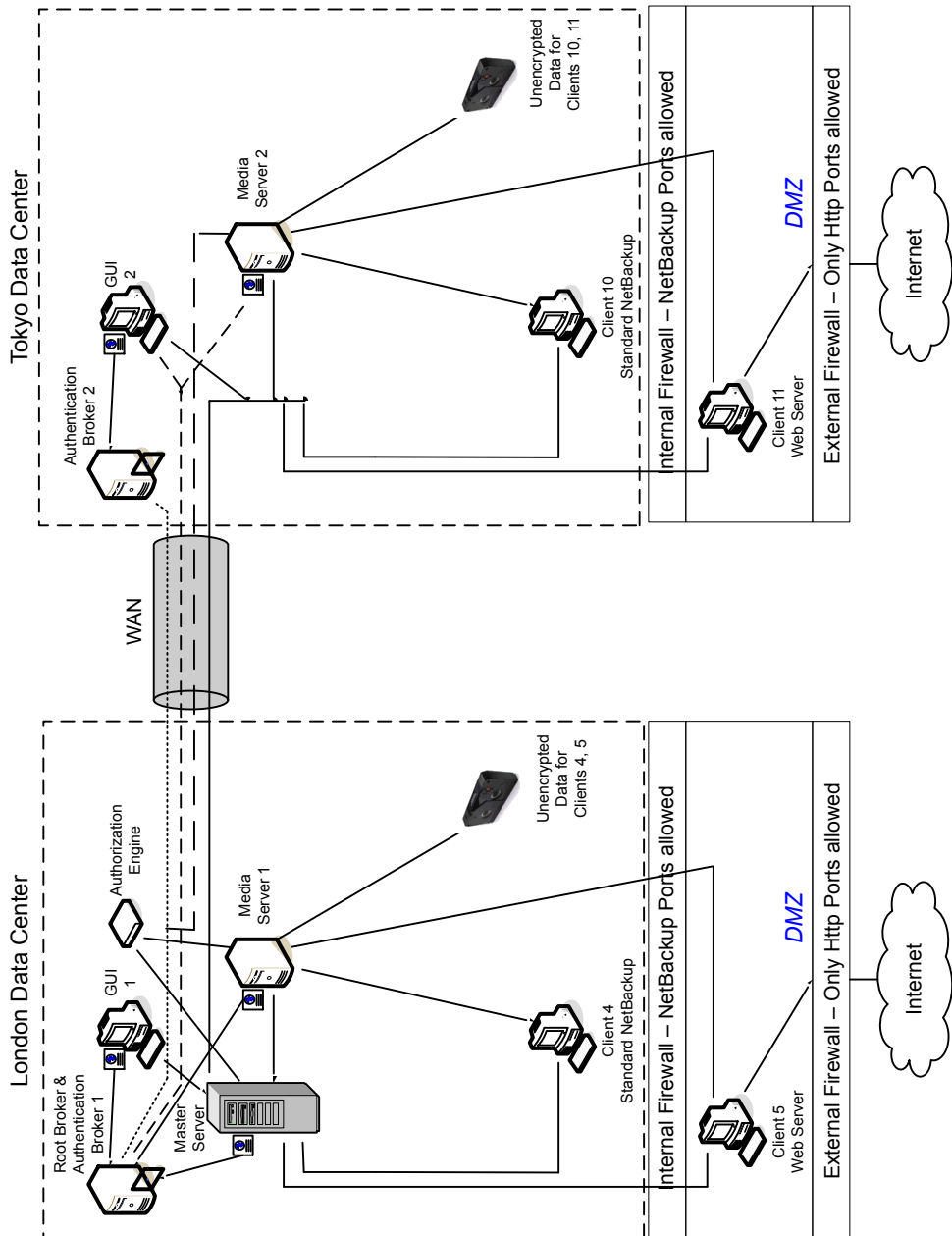
This datacenter example uses NetBackup Access Control on the master servers and media servers. The datacenter limits access to portions of NetBackup and can use non-root administration of NetBackup. Within this environment, NBAC is configured for use between the servers and the GUIs. Non-root users can 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><b>Note:</b> 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, 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 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.

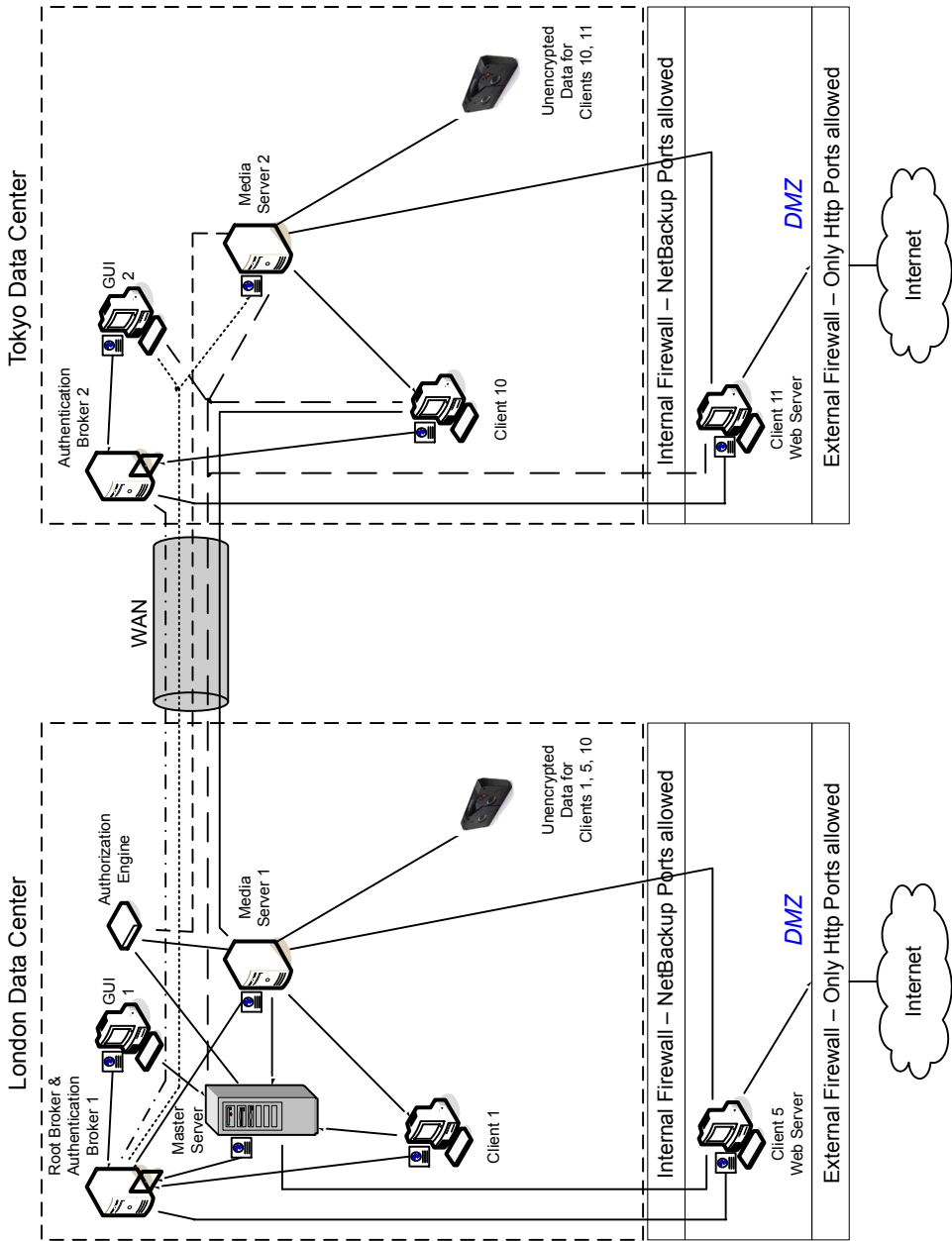
The multi-datacenter with NBAC complete includes the following highlights:

- 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	<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 1, 5, and 10. Media server 1 writes unencrypted data to tape for clients 1, 5, and 10.</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 GUI 2, and clients 10 and 11 in Tokyo. Media server 2 writes unencrypted data to tape for clients 10 and 11.</p>
GUIs	Specifies that in this multi-datacenter example, there are two GUIs. GUI 1 is in London and GUI 2 is in Tokyo. These remote administration console GUIs receive credentials from the authentication brokers. The GUIs then use the credentials to gain access to functionality on the media servers and master servers. In London, GUI 1 receives a credential from authentication broker 1. GUI 1 has access to functionality on the master server and media servers 1 and 2. In Tokyo, GUI 2 receives a credential from the authentication broker 2. GUI 2 has access to functionality on the master server and media servers 1 and 2.

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

Part	Description
Root broker	Specifies that there is only one root broker required in a multi-datacenter installation. Sometimes the root broker is combined with the authentication broker. In this example the root broker and authentication broker are shown as the same component and are located in the London datacenter. In London, the root broker authenticates the authentication broker 1, also in London, and authentication broker 2 in Tokyo. The root broker does not authenticate clients.
Authentication brokers	Specifies that there can be more than one authentication broker in a datacenter installation. Sometimes the authentication broker can be combined with the root broker. In this datacenter installation, there are two authentication brokers. The authentication broker authenticates the master server, media server, GUI, and clients by establishing credentials with each. The authentication broker also authenticates a user through a command prompt. In London, authentication broker 1 authenticates a credential with the master server, media server 1, GUI 1, and clients 1 and 5. All NetBackup servers and clients in Tokyo and London authenticate to authentication broker 1 in London. GUI 1 authenticates to authentication broker 1 in London. GUI 2 authenticates to authentication broker 2 in Tokyo.
Authorization engine	<p>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.</p> <p><b>Note:</b> 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 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:

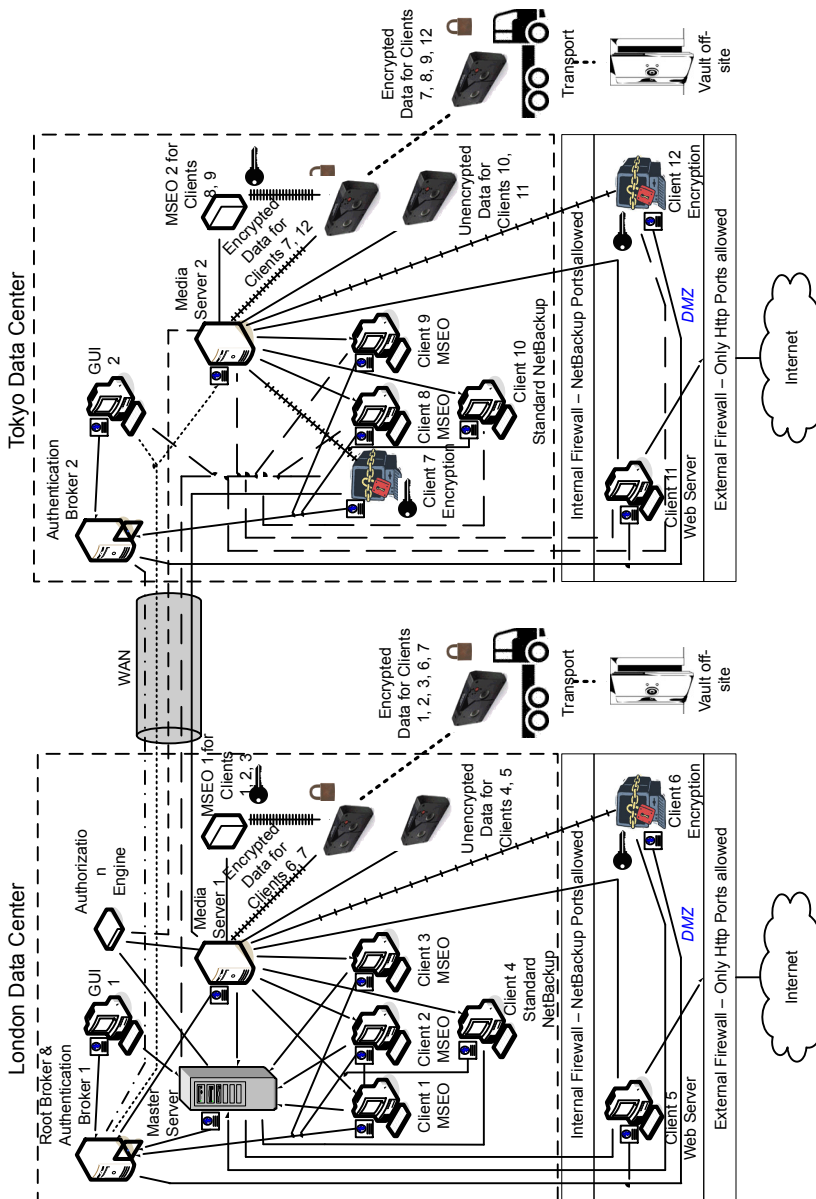
- NetBackup spans two or more geographic regions through a WAN
- Please see the previous multi-datacenter sections for individual option highlights



- 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	<p>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.</p> <p><b>Note:</b> 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>

**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><b>Note:</b> 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><b>Note:</b> 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><b>Note:</b> 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	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 and encrypted client 6 in the DMZ. In Tokyo, the internal firewall lets NetBackup access Web server client 11 and encrypted client 12 in the DMZ. Only selected NetBackup ports and possibly other application ports are enabled for data communication through the internal firewall and into and out of the DMZ. HTTP ports that are open in the external firewall are not allowed to pass through the internal firewall.
Demilitarized Zones (DMZs)	<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 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	Specifies that there can be only one Internet but there are two Internet connections in this multi-datacenter example. One Internet connection is located in London and the other is located in Tokyo. The Internet is a collection of interconnected computer networks that are linked by copper wires, fiber-optic cables and wireless connections. In London, the Web server client 5 can communicate over the Internet using HTTP ports through the external firewall. In Tokyo, the Web server client 11 can communicate over the Internet using HTTP ports through the external firewall.

# Port security

This chapter includes the following topics:

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

## About NetBackup TCP/IP ports

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

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

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

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

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

Port	Description
Registered ports	<p>Specifies ports that are registered with the Internet Assigned Numbers Authority (IANA) and are assigned permanently to specific NetBackup services. For example, the port for the NetBackup client daemon, <code>bpcd</code>, is 13782. You can specify entries in the following files if you need to override the default port numbers:</p> <ul style="list-style-type: none"> <li>■ On UNIX systems, you can specify ports in the <code>/etc/services</code> file.</li> <li>■ On Windows systems, you can specify ports in the <code>%systemroot%\System32\drivers\etc\services</code> file.</li> </ul>
Dynamically allocated ports	<p>Specifies ports that are assigned from the ranges you specify on NetBackup clients and servers.</p> <p>You can configure NetBackup to select a port number at random from the allowed range, or you can configure NetBackup to start at the top of a range and use the first port available.</p>

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

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

The following other guides contain information about NetBackup ports:

- [NetBackup Administrator's Guide, Volume 1](#)
- [NetBackup Administrator's Guide, Volume 2](#)

The following topics contain information about NetBackup ports:

- See [“About NetBackup daemons, ports, and communication”](#) on page 97.
- See [“About configuring ports”](#) on page 109.
- See [“Port requirements for NDMP backups”](#) on page 118.
- See [“Known firewall problems encountered when using NetBackup with third-party robotic products”](#) on page 118.



# About NetBackup daemons, ports, and communication

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

- See [“Standard NetBackup ports”](#) on page 97.
- See [“NetBackup master server outgoing ports”](#) on page 98.
- See [“NetBackup media server outgoing ports”](#) on page 99.
- See [“NetBackup enterprise media management \(EMM\) server outgoing ports”](#) on page 100.
- See [“Client outgoing ports”](#) on page 101.
- See [“Windows administration console and Java server outgoing ports”](#) on page 101.
- See [“Java console outgoing ports”](#) on page 102.
- See [“Additional port information for products that interoperate with NetBackup”](#) on page 103.

## Standard NetBackup ports

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

**Table 3-2** Daemons and ports used in a standard NetBackup environment

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

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

Source	Port name and/or number	Destination	Notes
Client	veritas_pbx 1556	NetBackup master server	Symantec private branch exchange service, VxPBX.
NetBackup master server, media server, or client	vrts-at-port 13783	Master	NetBackup authentication service, VxAT.  The <code>nbatd</code> process listens on port 13783 for back-level media servers and clients. The NetBackup media servers and clients connect using the PBX port.
NetBackup master server or media server	vrts-auth-port 13722	NetBackup master server	NetBackup Authorization Service, VxAZ.  The <code>nbazd</code> process listens on port 13722 for back level media servers and clients. The NetBackup media servers and clients connect using the PBX port.

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

## NetBackup master server outgoing ports

[Table 3-3](#) shows the ports that the master server uses to send data packets.

**Table 3-3** NetBackup master server outbound ports and destinations

Port name and number	Destination	Notes
veritas_pbx 1556	Media server	<p>Connect-back for job information.</p> <p>Connect-back for resource information.</p> <p>Determines the NetBackup software release level on the media server.</p> <p>Starts <code>bpbrm</code> for backups and restores.</p> <p>Starts <code>bptm</code> to manage tape storage units.</p> <p>Starts <code>bpstsinfo</code> to manage disk storage units.</p> <p>Accesses or updates host properties for the media server.</p>
veritas_pbx 1556	Enterprise media management (EMM) server	<p>Determines the NetBackup software release level on the client.</p> <p>Accesses or information about the device, media, and storage databases.</p> <p>Obtains the list of mount points for multistreamed backups.</p> <p>Accesses or updates host properties for the client.</p>
veritas_pbx 1556	Administrative console or Java server	Connect-back for activity monitor.
veritas_pbx 1556	Java console	Connect-back for job monitor.
vrts-at-port 13783	Authentication server	<p>Authenticates users and machines.</p> <p>Used only when the following are both true:</p> <ul style="list-style-type: none"> <li>NetBackup access control (NBAC) is enabled.</li> <li>Media servers and clients in the NetBackup environment host a NetBackup software release level that is lower than the release level on the master server.</li> </ul>
vrts-auth-port 13722	Authorization server	<p>Authorizes a user for system administration.</p> <p>Used only when NBAC is enabled.</p>

## NetBackup media server outgoing ports

[Table 3-4](#) shows the ports that the media server uses to send data packets. The table shows the port name, port number, the destination, and additional information.

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

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

## NetBackup enterprise media management (EMM) server outgoing ports

[Table 3-5](#) shows the ports that the EMM server uses to send data packets.

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

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

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

Port name and number	Destination	Notes
veritas_pbx 1556	Administrative console or Java server	Connect-back for information about device, media, and storage databases.
vrts-at-port 13783	Authentication server	Authenticates users and machines.  Used only when the following are both true: <ul style="list-style-type: none"> <li>■ NetBackup access control (NBAC) is enabled.</li> <li>■ Media servers and clients in the NetBackup environment host a NetBackup software release level that is lower than the release level on the master server.</li> </ul>
vrts-auth-port 13722	Authorization server	Authorizes a user for system administration.

## Client outgoing ports

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

**Table 3-6** NetBackup client outbound ports and destinations

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

## Windows administration console and Java server outgoing ports

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

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

**Table 3-7** Windows administration console and Java server outbound ports and destinations

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

## Java console outgoing ports

[Table 3-8](#) shows the ports that the Java console uses to send data packets.

**Table 3-8** Java console outbound ports and destinations

Port name and number	Destination	Notes
veritas_pbx 1556	Master server	Establishes sockets with the job manager, nbjm.
vnetd 13724	Master server	Establishes sockets with the legacy job manager, bpjobd. Used only when the Java console's NetBackup software level is less than NetBackup 7.6.
vnetd 13724	Java server	Establishes sockets with the legacy Java server, bpjava. Used only when the Java console's NetBackup software level is less than NetBackup 7.6.

## About MSDP port usage

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

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

**Table 3-9** Deduplication ports

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

## About Cloud port usage

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

## Additional port information for products that interoperate with NetBackup

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

- See [“About communication and firewall considerations”](#) on page 104.
- See [“Ports required to communicate with backup products”](#) on page 105.
- See [“Web browser to NetBackup Web GUI connection”](#) on page 106.
- See [“About NetBackup Web GUI to NetBackup server software communication”](#) on page 107.
- See [“About NetBackup server to NetBackup master server \(NBSL\) communication”](#) on page 108.
- See [“About SNMP traps”](#) on page 108.

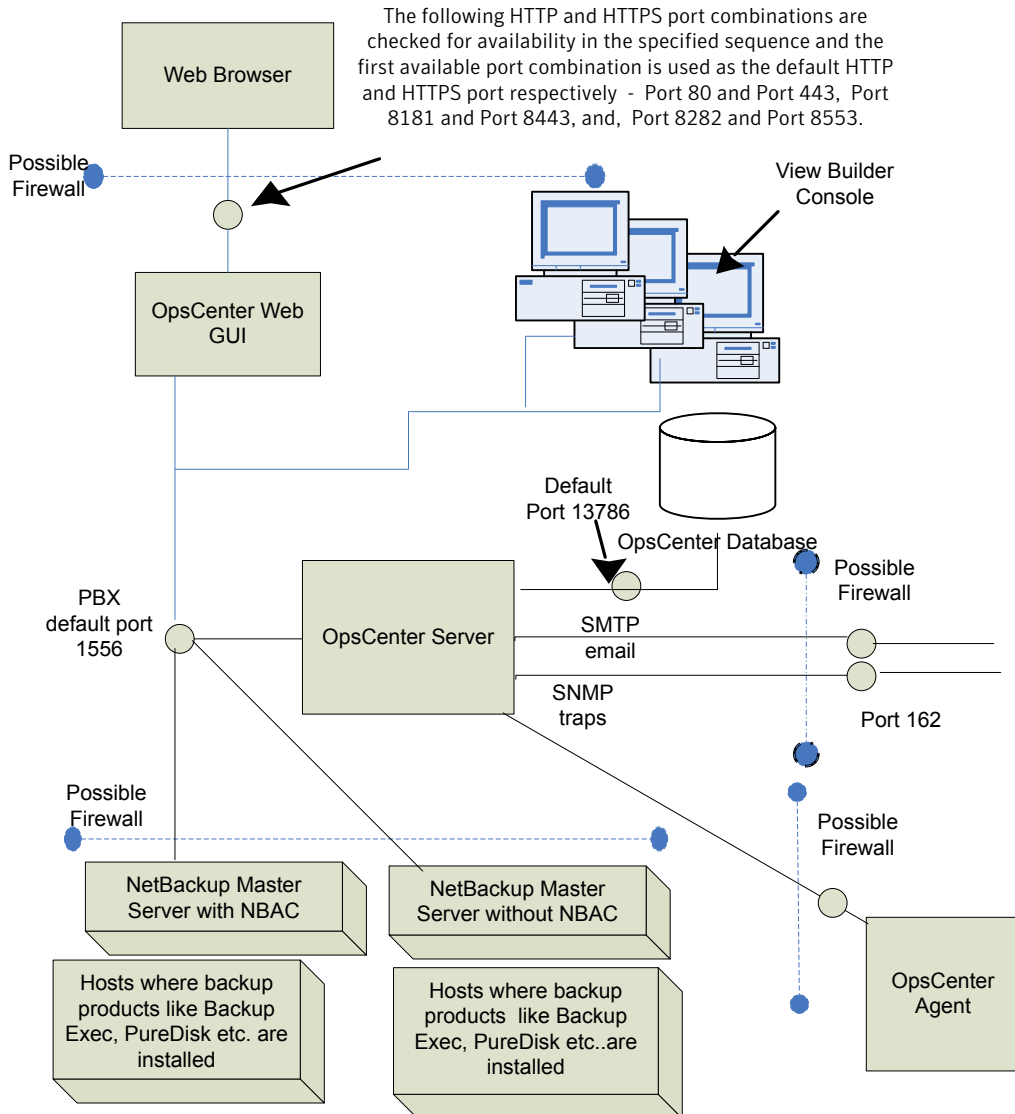
- See [“About NetBackup Web GUI/NetBackup server to Sybase database communication”](#) on page 108.
- See [“About NetBackup Web GUI to NetBackup server email communication”](#) on page 108.

## About communication and firewall considerations

[Figure 3-1](#) shows the key NetBackup components and the communication ports that are used.



**Figure 3-1** Key NetBackup components and how they communicate



## Ports required to communicate with backup products

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

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

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

Backup product	Communication	t r	e b
NetBackup	<p>NetBackup (NetBackup data collector) communicates with the NetBackup master server. The NetBackup master server should be used to connect to the NetBackup master server and should be used to respond to the Agent host. The response is sent on a port in the 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"><li>■ <code>bpererror.exe</code></li><li>■ <code>bpretlevel.exe</code></li><li>■ <code>bpimagelist.exe</code></li></ul>	2	2
Backup Exec	NetBackup (Backup Exec data collector) communicates with Backup Exec Backup Exec API	6	6
PureDisk	NetBackup (PureDisk data collector) communicates with PureDisk SPA using the PureDisk SPA API	1	2

### Web browser to NetBackup Web GUI connection

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

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

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

**Table 3-11** Default HTTP and HTTPS ports

Sr. No.	HTTP port number	HTTPS port number	Description
1.	80	443	<p>Port 80 and Port 443 are checked for availability.</p> <ul style="list-style-type: none"> <li>■ 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.</li> <li>■ In case, some other application like a Web server uses one or both ports, then the next port combination is checked for availability.</li> </ul>
2.	8181	8443	<p>Port 8181 and Port 8443 are checked for availability.</p> <ul style="list-style-type: none"> <li>■ 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.</li> <li>■ 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.</li> </ul>
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.

## About NetBackup Web GUI/NetBackup server to Sybase database communication

The NetBackup Web GUI communicates with the NetBackup Sybase SQL Anywhere database server by using the default port 13786.

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

## About NetBackup Web GUI to NetBackup server email communication

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

## About configuring ports

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

The following topics explain how to set port configuration options:

- See [“Enabling or disabling random port assignments”](#) on page 109.
- See [“Specifying firewall connection options on a NetBackup server or client”](#) on page 110.
- See [“Specifying firewall connection options for destination computers from a source computer”](#) on page 113.
- See [“Editing port information in configuration files”](#) on page 114.
- See [“Updating client connection options”](#) on page 115.
- See [“Updating port settings for the Media Manager in the vm.conf file”](#) on page 116.

## Enabling or disabling random port assignments

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

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

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

The following procedure explains how to specify port assignments.

### To specify port assignments from the Java or Windows interface

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

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

- To specify a media server's port assignments, expand **NetBackup Management > Host Properties > Media Servers**
- 2 Double click the host you want to configure.
  - 3 Click **Port Ranges**.
  - 4 Check or clear **Use random port assignments**.
- Make sure that the master server and the media servers in your environment are set identically. That is, make sure that **Use random port assignments** is cleared on both systems or that **Use random port assignments** is checked on both systems.

## Specifying firewall connection options on a NetBackup server or client

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

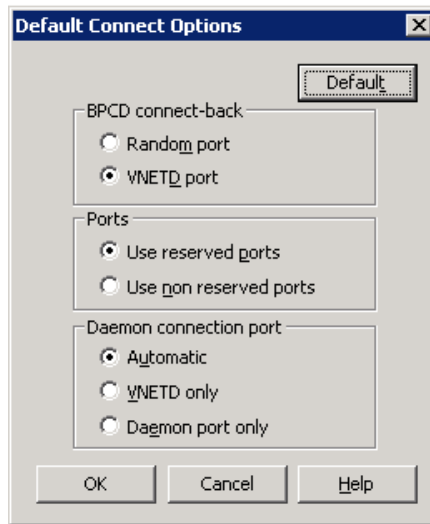
In addition, you can set the default connection options for all of the other destination computers from the source computer. For example, if there is a firewall between the master server and the media servers, you can specify all the connection options from the NetBackup master server.

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

### To specify Firewall connection options from a source computer

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

A display similar to the following appears:



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

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

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

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

Choose one of the following:

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

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

Choose one of the following:

- **Use reserved ports.** Default.  
When in effect, the source computer connects to `bpcd` on the destination computers that use a reserved port number.

- **Use nonreserved ports.**

When in effect, the source computer connects to `bpcd` on destination computers using a nonreserved port number.

Make sure to perform step 8 of this procedure, which ensures that other computers in the NetBackup environment also are configured for nonreserved ports.

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

Choose one of the following:

- **Automatic.** Default for NetBackup 5.0 and later.

Specifies that other computers connect to this host by using the `vnetd` daemon, if possible. If a connection via `vnetd` is not possible, use the daemon's legacy port number.

- **VNETD only.**

Specifies that other computers connect to this host by using only the `vnetd` daemon. If your site's firewall rules prevent connections to this host through the legacy port number, make sure that this setting is in effect.

- **Daemon port only.** Default for releases earlier than NetBackup 5.0.

Specifies that other computers use the legacy port number to connect to this host.

For releases earlier than NetBackup 5.0, connections to `bpcd` always use the legacy `bpcd` port number.

For NetBackup release 5.0 and later, connections to `bpcd` can be made with the `vnetd` port number if both the source and the destination computers use NetBackup 5.0 or later.

When `bpcd` connections are made using the `vnetd` port number, the **Ports** and **BPCD connect-back** options are ignored. In this case, NetBackup uses nonreserved source port numbers, the `vnetd` destination port number, and no callback.



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

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

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

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

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

## Specifying firewall connection options for destination computers from a source computer

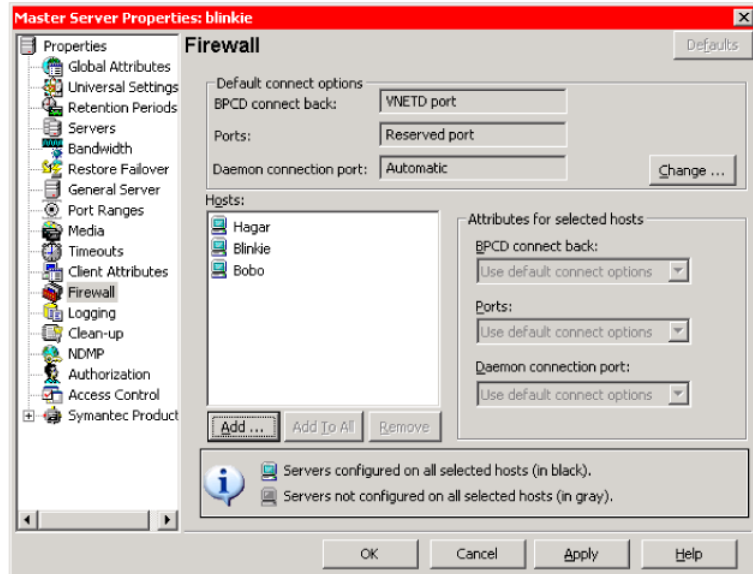
The following procedure describes how to specify Firewall connect options on a source computer that apply to specific destination computers. For example, you can perform this procedure from a master server and specify connect options for clients.

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

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

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

The host list is shown in the following figure:



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

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

See [“Specifying firewall connection options on a NetBackup server or client”](#) on page 110.

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

## Editing port information in configuration files

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

- `ALLOW_NON_RESERVED_PORTS`
- `CLIENT_PORT_WINDOW`
- `CLIENT_RESERVED_PORT_WINDOW`

- `CONNECT_OPTIONS`
- `DEFAULT_CONNECT_OPTIONS`
- `RANDOM_PORTS`
- `SERVER_RESERVED_PORT_WINDOW`
- `SERVER_PORT_WINDOW`

For information about the preceding settings, see the [NetBackup Administrator's Guide, Volume 1](#).

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

#### To change port settings in the `bp.conf` file

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

```
bpgetconfig options > outputfile
```

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

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

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

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

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

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

- [NetBackup Administrator's Guide, Volume I](#)
- *NetBackup Commands*

## Updating client connection options

These settings can also be configured in the **NetBackup Administration Console** by .

NetBackup provides the following ways to specify client connection options:

- From the NetBackup administration console. Expand **Host Properties > Master Servers > Client Attributes > Connect Options**.
- From the command line. You can use the `bpclient` command to update a variety of client attributes.

For example, you can use the `-connect_options` argument to the `bpcclient` command to specify client port connection options.

For more information about the command, see the *NetBackup Commands* manual.

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

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

- On Linux or UNIX, the path is as follows:

```
/usr/opensv/volmgr/vm.conf
```

- On Windows systems, the path is as follows:

```
install_path\volmgr\vm.conf
```

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

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

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

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

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

Setting	Description
CONNECT_OPTIONS	<p><b>Note:</b> The <code>CONNECT_OPTIONS</code> setting affects only connections to hosts that run NetBackup 7.0 and earlier. When NetBackup connects to hosts that run NetBackup 7.0.1 and later, NetBackup uses the <code>veritas_pbx</code> port.</p> <p>Specifies the destination port number that can be used to connect to the Media Manager services. The format is as follows:</p> <pre>CONNECT_OPTIONS = host 0 0 0 1 2</pre> <p>This setting accepts four space-separated arguments. The arguments are as follows.</p> <p>For <i>host</i>, specify the name of the media server to which other computers need to connect.</p> <p>After the <i>host</i> name, type <code>0 0</code>. The arguments in these positions are not used.</p> <p>After <code>0 0</code>, type <code>0</code>, <code>1</code>, or <code>2</code> to specify the connection method to the Media Manager service on the target computer. The connection method specifications are as follows:</p> <ul style="list-style-type: none"> <li>■ If <code>0</code>, the host uses the <code>vnetd</code> port. If that attempt fails, the hosts uses the legacy port number.</li> <li>■ If <code>1</code>, the host uses only <code>vnetd</code> to connect to the server.</li> <li>■ If <code>2</code>, the host uses the legacy Media Manager port.</li> </ul> <p>Default for 5.1 and earlier servers.</p> <p>You can specify multiple <code>CONNECT_OPTIONS</code> settings in the <code>vm.conf</code> file.</p> <p>For NetBackup 6.0 and later, if the <code>vm.conf</code> file does not contain any <code>CONNECT_OPTIONS</code> entries, the Media Manager selects the port based on the <code>bp.conf</code> file settings for <code>DEFAULT_CONNECT_OPTIONS</code> and <code>CONNECT_OPTIONS</code>.</p> <p>For example, the following settings specify that the Media Manager connections to <code>server3</code> use <code>vnetd</code> as the destination port:</p> <pre>CONNECT_OPTIONS = server3 0 0 1</pre>
RANDOM_PORTS	<p>Specifies whether NetBackup chooses ports randomly or sequentially when it communicates with other NetBackup servers. The format is as follows:</p> <pre>RANDOM_PORTS = YES   NO</pre> <p>If <code>RANDOM_PORTS = YES</code>, or if there is no <code>RANDOM_PORT</code> entry, NetBackup selects a random port from the range specified by the <code>CLIENT_PORT_WINDOW</code> setting in the <code>vm.conf</code> file.</p> <p>If <code>RANDOM_PORTS = NO</code>, the NetBackup attempts the connection with the highest source port number in the range. If the source port does not work, NetBackup tries the next highest source port number. The port number is chosen from the list until it finds a source port number that works.</p>

## Port requirements for NDMP backups

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

The following table explains the ports requirements for NDMP backups.

**Table 3-13** Ports requirements for NDMP backups

Backup type	Description
Local	For local operations, the Data Management Application (DMA) needs access to port 10000 on the NDMP server. In this case, the one NDMP server is both the NDMP tape server and the NDMP data server.
Three-way and remote NDMP	For three-way and remote NDMP, the DMA needs access to port 10000 on the NDMP tape server and the NDMP data server. There cannot be a firewall between the NDMP tape server and the NDMP data server. No firewall is needed because control is not required over the TCP/IP ports that are used for the data movement.
Remote NDMP (5.0 / 5.1)	For remote NDMP (5.0 / 5.1), a firewall is not suggested between the DMA and the NDMP hosts because the DMA can be on the same computer as the NDMP tape server. You need an unlimited number of ports available to perform the data movement between the NDMP tape server and the NDMP data server.

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

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

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

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

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

- An automated cartridge system (ACS) server. A remote procedure call enables this communication. There is no common port.
- A Fujitsu library management facility (LMF) server.
- A tape library half-inch (TLH) IBM library manager server.
- A tape library multimedia (TLM) ADIC DAS/SDLC server.

# 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 7.6 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 access control 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 7.6 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
- Troubleshooting NBAC issues
- 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 (and AZ version 4.3.19.2) cannot be upgraded to NetBackup 7.5 or a later version. You must first upgrade to version AZ 6.5.4 (4.3.24.4) before the NBAC upgrade from NetBackup 6.5 to NetBackup 7.5 or a later version 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"> <li>■ User name or password for master server (root or administrator permission).</li> <li>■ Name of master server</li> <li>■ Name of all media servers that are connected to the master server</li> <li>■ Name of all clients to be backed up</li> <li>■ Host name or IP address</li> </ul> <p><b>Note:</b> Host names should be resolvable to a valid IP address.</p> <ul style="list-style-type: none"> <li>■ 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.</li> </ul>

**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"> <li>Some features are provided by upgrading master servers, some by media servers, and some from upgrading clients.</li> <li>NetBackup works with a higher revision master server and lower revision clients and media servers.</li> <li>Feature content determines what is deployed.</li> <li>Deployment can be step wise if required.</li> </ul>
Information about roles	<p>Determine the roles in the configuration as follows:</p> <ul style="list-style-type: none"> <li>Who administers the hosts (root permission on master server equals head administrator).</li> <li>Determine roles to start and then add on the roles as required.</li> </ul>
NBAC license key requirements	No license is required to turn on the access controls.
NBAC and KMS permissions	<p>Typically when using NBAC and when 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.</p>
MSCS Error messages while unhooking shared security services from PBX	<p>In MSCS environments running the <code>bpnbaz -UnhookSharedSecSvcsWithPBX &lt;virtualhostname&gt;</code> command can trigger error messages. However the shared Authentication and Authorization services are successfully unhooked from PBX and the errors can be ignored.</p>
Possible cluster node errors	<p>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.</p>
Catalog recovery fails when NBAC is set to <b>REQUIRED</b> mode	<p>If NBAC is running in <b>REQUIRED</b> mode and a catalog recovery was preformed, NBAC needs to be reset back from <b>PROHIBITED</b> mode to <b>REQUIRED</b> mode.</p>

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"><li>■ Authenticated Principle is removed from the NBAC group: NBU_Users group</li><li>■ Back up and restore permissions of NBU_User group have been removed</li></ul>
The bpnbaz -setupmaster command fails with an error "Unable to contact Authorization Service"	<p>If a user other than an Administrator tries to modify NetBackup security, the bpnbaz -setupmaster fails.</p> <p>Only a user 'Administrator' who is a part of the Administrator's group has permissions to modify the NetBackup security and enable NBAC.</p>
Failure of authentication broker configuration during installation.	<p>Invalid domain name configuration of the system causes failure during configuration of authentication broker.</p> <p>To correct this problem, use the <code>bpnbaz -configureauth</code> command to configure the authentication broker.</p> <p>For more information about the <code>bpnbaz -configureauth</code> command refer to the <a href="#">NetBackup Commands Reference Guide</a>.</p>

## 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 127. 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 129.

---

**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 131.

- 3 Configure clients for NBAC.

See [“Installing and configuring access control on clients”](#) on page 133.

# 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 134. 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 123. 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 156. 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 `bpbaz -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 `bpbaz -setupmaster` command completes successfully.
- 4 Proceed to set up the media servers. See [“Configuring NetBackup Access Control \(NBAC\) on media servers”](#) on page 131.

# Installing the NetBackup 7.6 master server highly available on a cluster

You can use the following procedure to install the NetBackup 7.6 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 7.6 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 Run the `bpnbat -login` command.

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

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

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

See “NBAC configure commands summary” on page 134.

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

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

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

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

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

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

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

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

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

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

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

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

See [“Installing and configuring access control on clients”](#) on page 133.

## Installing and configuring access control on clients

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

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

- 1 Make sure that no backups are currently running.
- 2 To set up the client, run the following command on the master server:

```
bpnbaz -setupClient
```

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

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

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

- 1 Run the following command from the master server:

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

**Sample output of VXSS\_SETTINGS.txt:**

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

- 2 Copy VXSS\_SETTINGS.txt to the administration client.

- 3 Run the following command from the administration client:

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

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

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

## NBAC configure commands summary

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

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

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

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

Table 4-3 NBAC configure commands summary

Command	Description
<code>bpnbaz -GetConfiguredHosts [target.server.com [-out file]   -all [-outfile]   -file progress.file]</code>	<p>The <code>bpnbaz -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"><li>■ <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.</li><li>■ <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.</li><li>■ <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.</li><li>■ <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 # after hostname followed by the NBAC status.</li><li>■ 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.</li></ul>

Table 4-3 NBAC configure commands summary (continued)

Command	Description
<code>bpbaz -SetupMaster [-fsa [&lt;domain type&gt;:&lt;domain name&gt;:]&lt;user name&gt;]</code>	<p>The <code>bpbaz -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>bpbaz -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"><li>■ <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.</li><li>■ <code>domain type</code> is the type of network domain you are using. For example the <code>bpbaz -SetupMaster -fsa nt:ENTERPRISE:jdoe</code> command provisions the Windows enterprise domain user <code>jdoe</code> as NBU Administer.</li><li>■ <code>domain name</code> is the name of the particular domain you are using. For example the <code>bpbaz -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.</li><li>■ <code>user name</code> is the particular OS user name you are designating as an NBU Administrator.</li></ul> <p><b>Note:</b> 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>bpnbaz -SetupMedia [ media.server.com [-out file]   -all [-out file]   -file progress.file ] [-dryrun] [-disable]</code>	<p>The <code>bpnbaz -SetupMedia</code> command is run by an NBU_Administrator group member on the master server. It should not be run until a <code>bpnbaz -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"><li>■ <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.</li><li>■ <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.</li><li>■ <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.</li><li>■ <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.</li><li>■ <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.</li><li>■ <code>-disable</code> option can disable NBAC (USE_VXSS = PROHIBITED ) on targeted hosts.</li></ul>

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

Command	Description
<pre>bpbaz -SetupClient [ client.server.com [-out file]   -all [-images] [-out file]   -file progress.file ] [-dryrun] [-disable]</pre>	<p>The <code>bpbaz -SetupClient</code> command is used for setting up NBAC on the clients. It should not be run until the <code>bpbaz -SetupMaster</code> command has been completed successfully. The <code>bpbaz -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"> <li>■ <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.</li> <li>■ <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.</li> <li>■ <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.</li> <li>■ <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.</li> <li>■ <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.</li> <li>■ <code>-disable</code> is an option that disables NBAC (USE_VXSS = PROHIBITED) on targeted hosts.</li> <li>■ <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 [# separated value]. 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.</li> </ul>

# Upgrading NetBackup Access Control (NBAC)

---

**Note:** If NBAC is enabled, it is upgraded as part of the NetBackup upgrade. Refer to the [NetBackup Upgrade Guide](#) for instructions about how to upgrade NetBackup. Make sure that current AT and AZ services are running when the upgrade is performed. If NetBackup is running in a cluster server, make sure that both services are running in the active node where NetBackup is running and the upgrade is performed.

---

The following procedure describes how to upgrade NetBackup Access Control (NBAC).

## Upgrading NetBackup Access Control (NBAC)

- 1 On the master server, stop NetBackup.
- 2 Upgrade NetBackup.

On the media servers and client computers, first stop NetBackup and then upgrade NetBackup. Note that the shared authentication and authorization packages are no longer used on media servers and client computers. These products can be removed if no other Symantec product 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 7.6 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 7.6 when an older version of NetBackup is using a root broker installed on a remote machine.

### Upgrading NetBackup 7.6 when an older version of NetBackup is using a root broker installed on a remote machine

- 1 Before upgrading to NetBackup 7.6, 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 7.6 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 7.6 upgrade is completed then migrates the remote root broker (RB) and local shared authentication broker (AB) into NetBackup 7.6 by using the `atutil` tool which is shipped with NetBackup 7.6.
- 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 7.6 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 7.6 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 7.6 authorization service by executing the following commands.

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

On Windows, run `net start nbazd`.

### 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 7.6 AZ using the following command.**

On UNIX platforms, run `/usr/opensv/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 7.6 using the following command.**

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

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

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

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

**20 Run the `setupmaster` command.**

**21 Restart the NetBackup service.**

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

---

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

---

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



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

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

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

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

On UNIX platforms, use the `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 148. for the media servers. See [“Accessing the client host properties”](#) on page 152. 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 7.6 and OpsCenter 7.6 establish trust automatically. You may need to do these `setuptrust` operations manually with older NetBackup master servers. At the end of the NetBackup master server 7.6 installation, there is a question on the OpsCenter host name. With that, the master server can initiate a two-way trust setup.

---

Details on the `setuptrust` command are described in the [NetBackup Commands Reference Guide](#). See “Using the `setuptrust` command” on page 147. 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

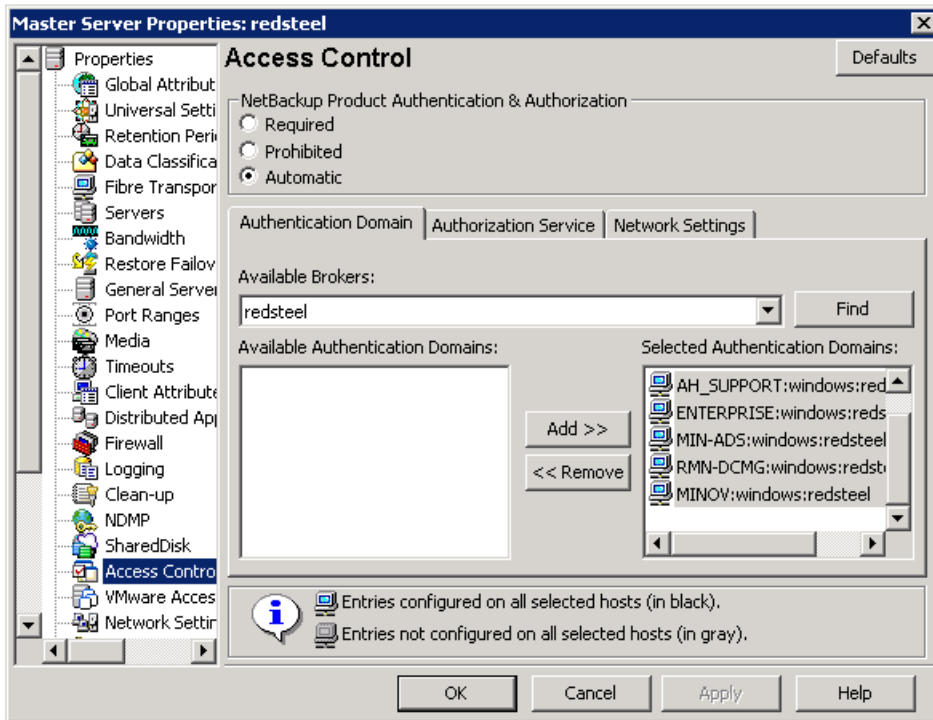
To access the master server and media server host properties in the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > master server or media server > Select server > Access Control**.

## 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



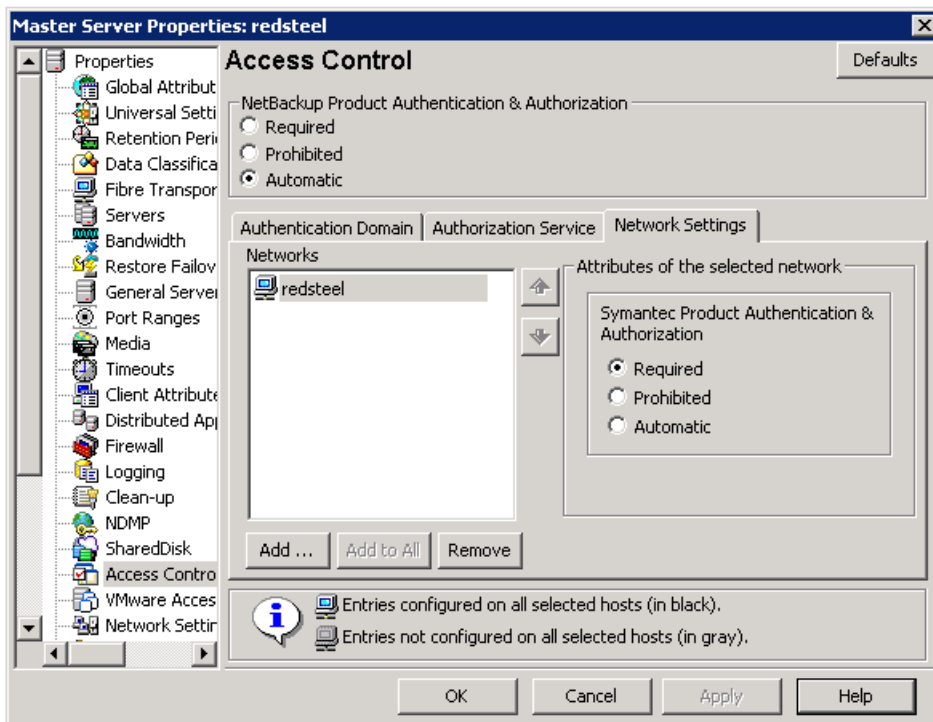
When **Automatic** is selected, you can specify computers or domains required to use **NetBackup Product Authentication and Authorization**. Otherwise you can specify computers that are prohibited from using the **NetBackup Product Authentication and Authorization**.

## 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:

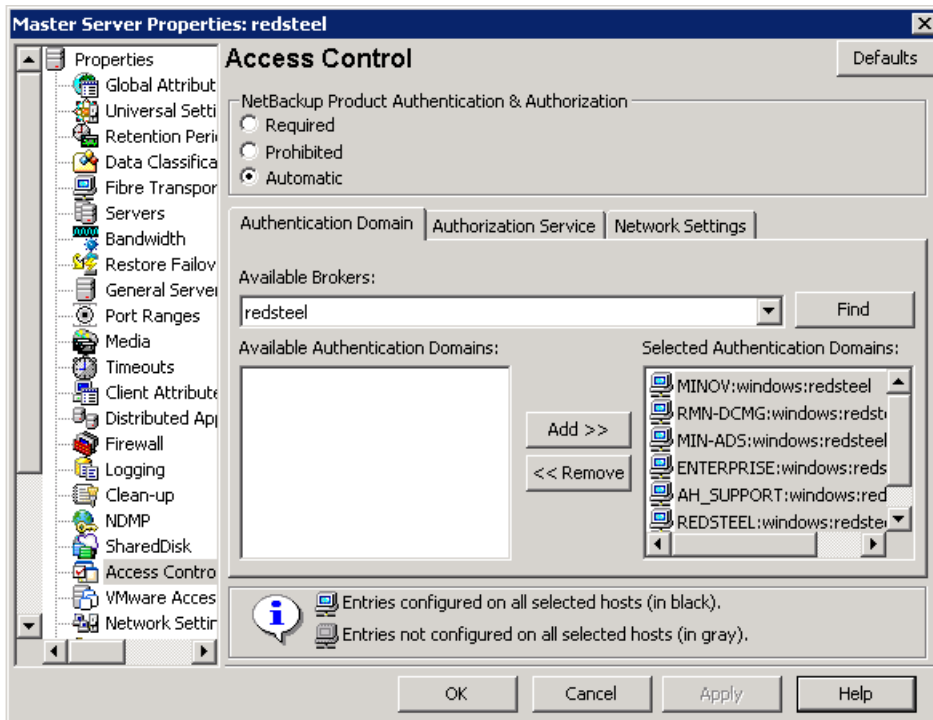
- Which authentication servers support which authentication mechanisms
- What domains each supports.

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

---

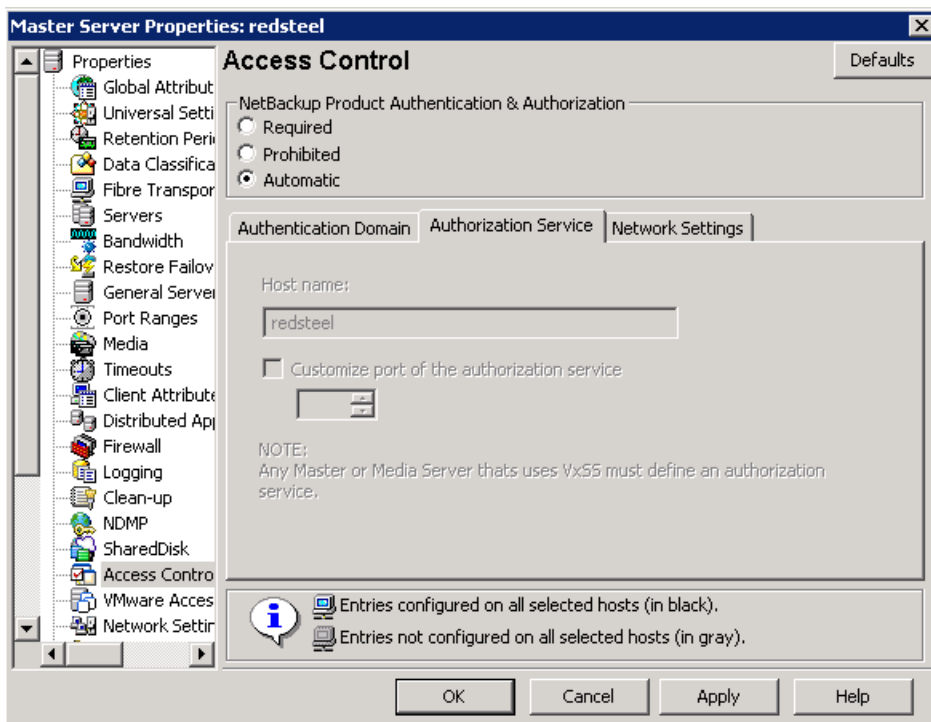
**Note:** No changes are allowed from this tab. It is read only.

---

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**.

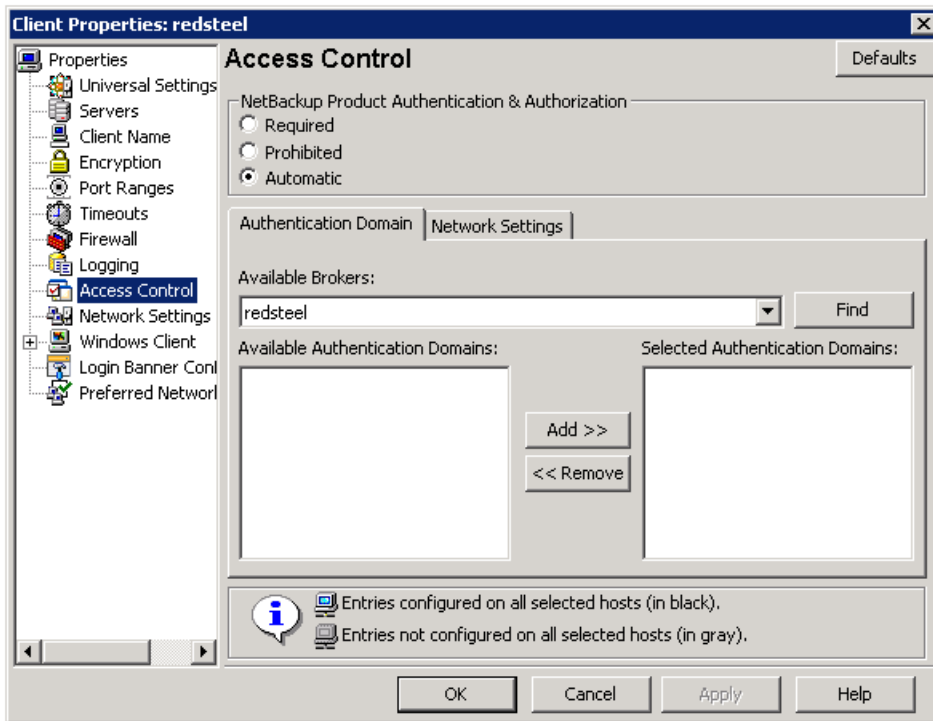
## Access control host properties dialog for the client

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.

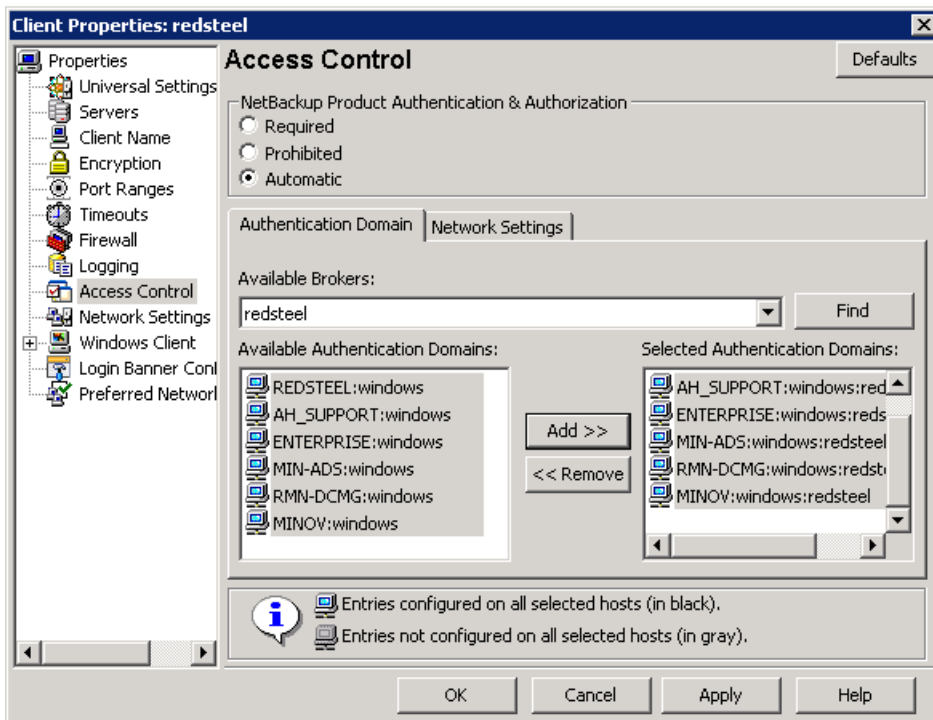
## Authentication Domain tab for the client

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

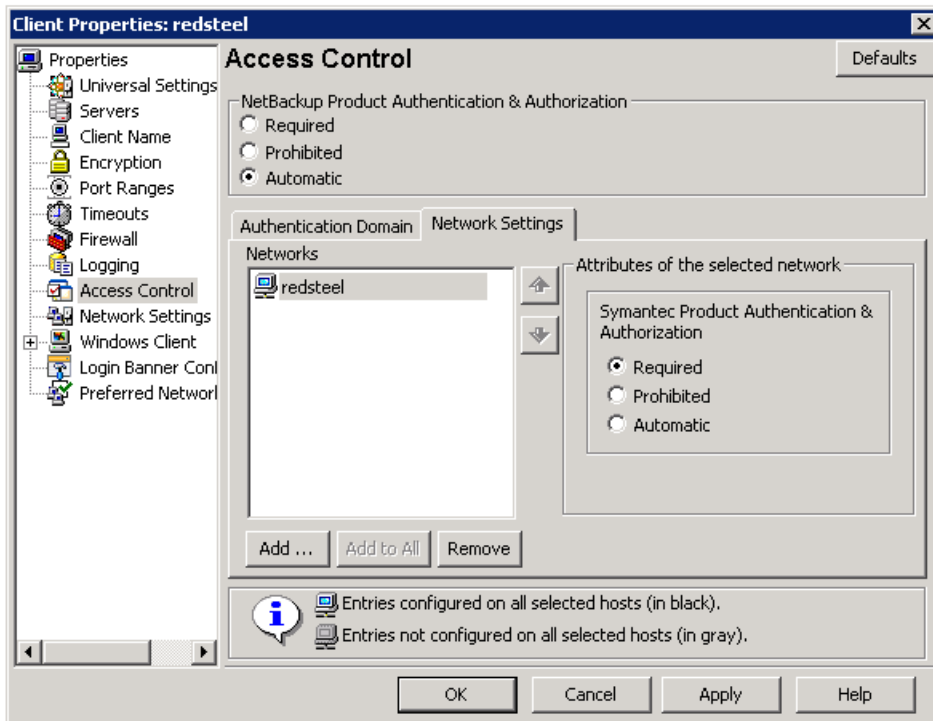


## Network Settings tab for the client

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 156, 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 185.
- UNIX verification points  
See [“About the UNIX verification procedures”](#) on page 165.
- 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 173.
- 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 178.

## 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>bpbaz</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>bpdbm</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 <a href="#">NetBackup Troubleshooting Guide</a> 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>installlics</code>, select the option for uninstalling authentication and authorization. The following directories should be empty after uninstalling:</p> <p><code>/opt/VRTSsat</code> and <code>/opt/VRTSaz</code></p> <p><code>/etc/vx/vss</code>  <code>/var/VRTSsat</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/VRTSsat/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/openv/var/vxss/credentials/</code></p> <p>Windows:</p> <p><code>&lt;user_home_dir&gt;\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 and later 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 <b>NetBackup Administration Console</b> 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 <code>nbac_cron</code> 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"> <li>■ <code>-SetupAt [-Port #]</code>  <code>-SetupCron [-Port #]</code></li> </ul> <p>Either option sets up an authentication account. Optionally, specify a port number to use for authentication.</p> <ul style="list-style-type: none"> <li>■ <code>-AddAt</code></li> </ul> <p>Create an authorization account for a user.</p> <ul style="list-style-type: none"> <li>■ <code>-AddCron</code></li> </ul> <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"> <li>■ Add <code>AUTHENTICATION_DOMAIN</code>, <code>AUTHORIZATION_SERVICE</code> and <code>USE_VXSS</code> entries in Registry.</li> <li>■ Change the service type of NetBackup Authentication and Authorization services to <code>AUTOMATIC</code>.</li> <li>■ Restart the NetBackup services.</li> <li>■ Verify that the <code>nbatd</code> and <code>nbazd</code> services are running.</li> </ul> <p><b>Note:</b> 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>bpnbaz -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 __lch_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 <a href="http://support.microsoft.com/">http://support.microsoft.com/</a> .
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	<p>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.</p>
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.

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

Topic	Configuration tips
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>bpnbaz -SetupMaster</code> to manage remote broker parts fail. You will have to manually configure passive nodes. Run <code>bpnbaz -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>

## Troubleshooting NBAC issues

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

**Table 4-5** NBAC issues

Issue and Cause	Solution
<p><b>A user directed backup or restore fails</b></p> <p>A user directed backup or restore fails with NBAC in the automated mode. The BAR GUI shows some errors on the Windows UI when NBAC is configured.</p> <p>A backup or restore failure can happen when a NetBackup setup on a UNIX master server is configured with NBAC and you try to use the Windows UI without first configuring the UI for such a kind of setup. Another reason is that there can be an expired certificate in the home directory.</p>	<p>Configure the Windows UI to support the setup.</p> <p>There should be at least one Microsoft Windows system that acts as an Authentication Broker to authenticate users from the Active Directory domain.</p> <p>Refer to the <a href="#">TECH199281</a> for steps to configure the Windows UI to make use of existing users from Active Directory to manage or operate or use a NetBackup environment that is primarily on UNIX/Linux platforms.</p> <p>After you correctly configure the setup run the 'bpnbat -logout' command to log out from the setup before you restart the UI.</p>

Table 4-5 NBAC issues (*continued*)

Issue and Cause	Solution
<b>Authentication failure with error 116</b>  The authentication fails with 'error 116-VxSS authentication' when you try to set up NBAC on a target host.	Check whether NBAC authentication is configured correctly and also if you have a valid usable credential for the target host.
<b>Error when a non-admin user from the NBU_Operator group tries to use Access Management</b>  A non-admin user is added to the NBU_Operator group. Read, Browse, and Configure permissions are assigned along with the permission to configure the Host Properties. However, when the user tries to open the Access Management utility, it gives an error.	<p>The users from the NBU_Operator group have limited permissions.</p> <p>The user would require a different set of permissions to use the Access Management utility. For the required permissions, add the user to the NBU_Security_Admin group.</p> <p>For more information about user groups, See <a href="#">"NetBackup default user groups"</a> on page 197.</p>

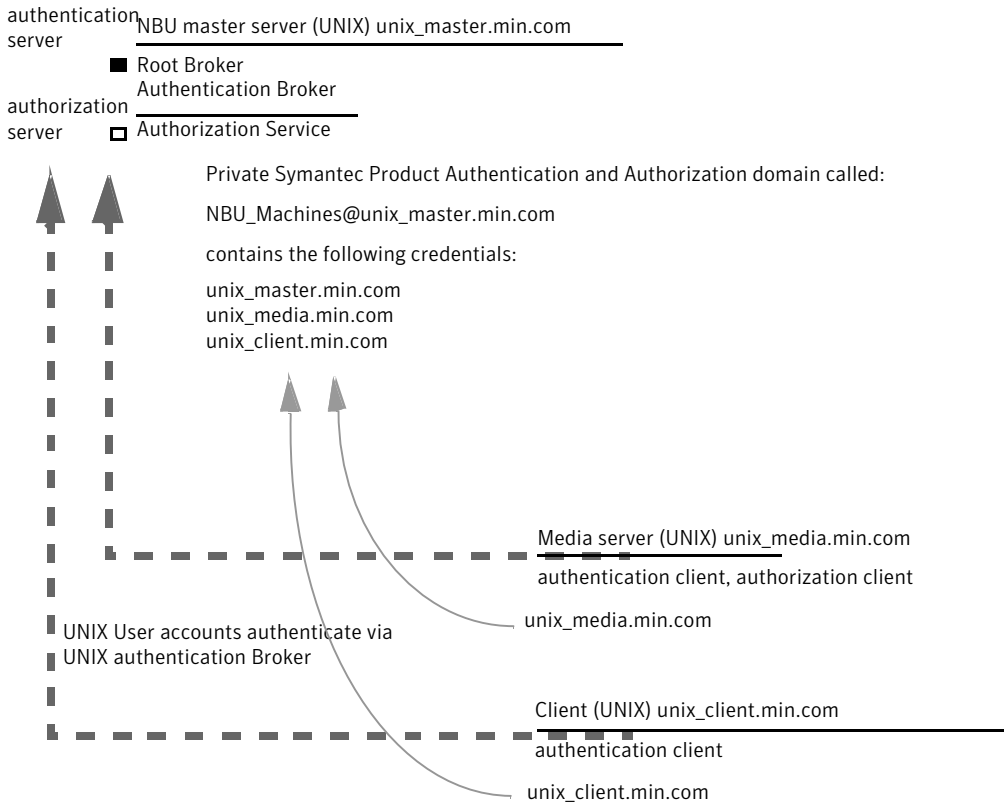
## About the UNIX verification procedures

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 166.
- UNIX media server verification  
See ["UNIX media server verification"](#) on page 169.
- UNIX client verification  
See ["UNIX client verification"](#) on page 171.

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

**Figure 4-8** Example configuration containing UNIX systems only



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

## UNIX master server verification

Use the following procedures to verify the UNIX master server:

- Verify UNIX master server settings.
- Verify which computers are permitted to perform authorization lookups.
- Verify that the database is configured correctly.
- Verify that the `nbatd` and `nbazd` processes are running.
- Verify that the host properties are configured correctly.

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

**Table 4-6** 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><b>Note:</b> When determining if a credential has expired, remember that the output displays the expiration time in GMT, not local time.</p> <p><b>Note:</b> 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 4-6** 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 <code>vx</code> (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 &lt;server_name&gt;</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 4-6** Verification process for the UNIX master server (*continued*)

Process	Description
Verify that the <code>nbatd</code> and <code>nbazd</code> 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 <b>Access Control</b> host properties, verify that the <b>NetBackup Authentication and Authorization</b> property is set correctly. (The setting should be either <b>Automatic</b> or <b>Required</b>, depending on whether all of the computers use <b>NetBackup Authentication and Authorization</b> or not. If all computers do not use <b>NetBackup Authentication and Authorization</b>, set it to <b>Automatic</b>.)</p> <p>In the <b>Access Control</b> 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 4-7** 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/opensv/var/vxss/credentials/</code> directory.</p> <p>For example:</p> <pre>bpnbat -whoami -cf /usr/opensv/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/opensv/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 4-7** 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 4-8** 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/opensv/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 4-8** 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 <b>Access Control</b> 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>

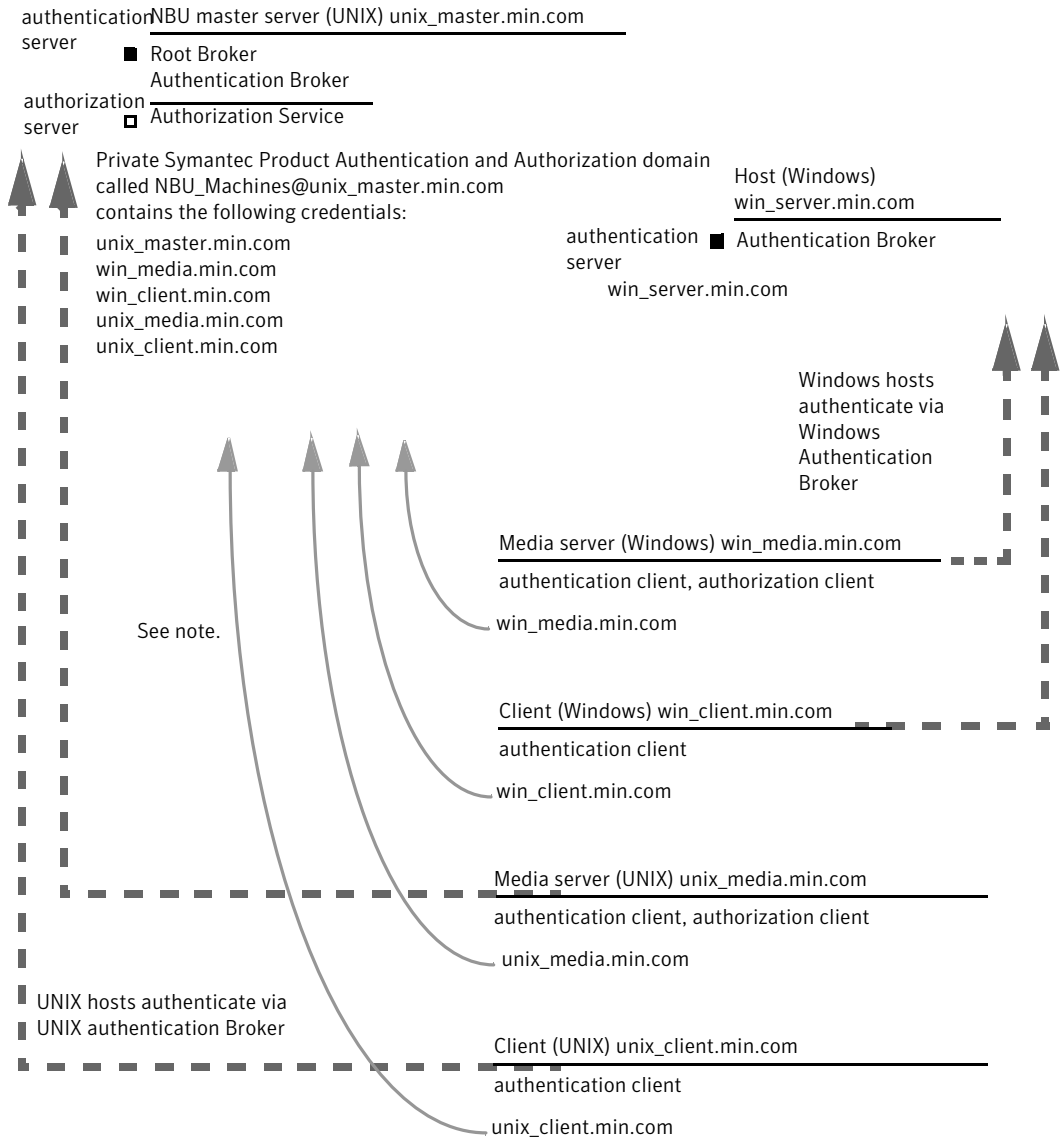
Verification points in a mixed environment with a UNIX master server

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 174. 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 166. 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 4-9                      Verification procedures for a mixed UNIX master server

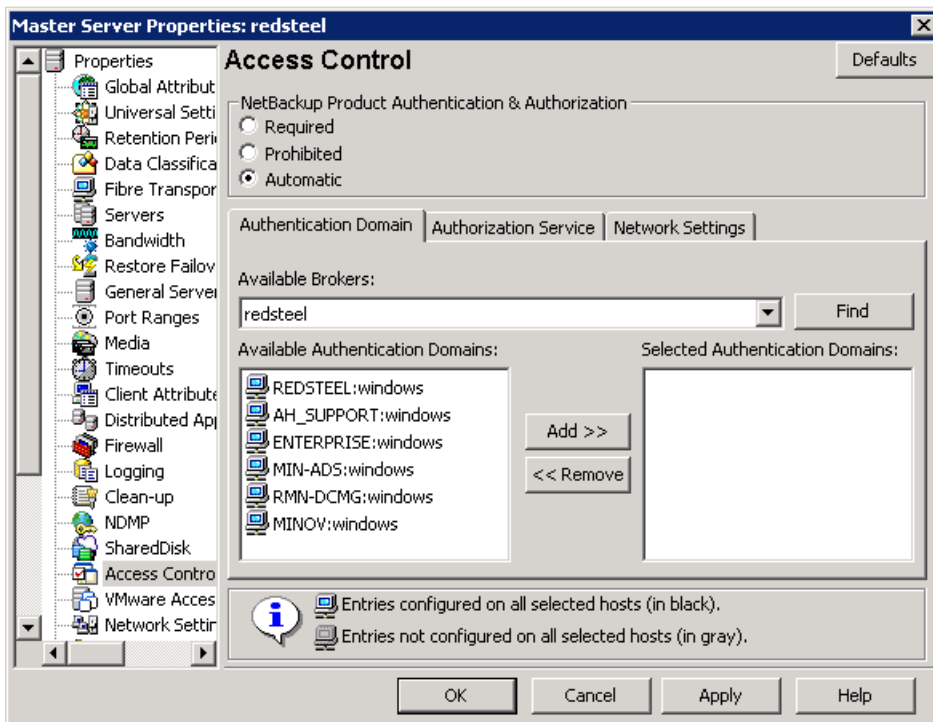
Procedure	Description
Verify the UNIX media server	See <a href="#">“UNIX media server verification”</a> on page 169. for the verification procedure for a UNIX media server.
Verify the Windows media server	<p>Check that the computer certificate comes from the root authentication broker, which is found 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"><li>■ <code>bpnbat -addmachine</code> on the root authentication broker (in this example, <code>unix_master</code>)</li><li>■ <code>bpnbat -loginmachine</code> (in this example, <code>win_media</code>)</li></ul> <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 4-9** 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 <b>NetBackup Authentication and Authorization</b> 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 <a href="#">Figure 4-10</a> on page 177. for a display on how to match the platform to the most useful authentication domains.</p>



Figure 4-10 Cross platform authentication domains



## Client verification points for a mixed UNIX master server

See [“UNIX client verification”](#) on page 171. for the procedures to verify the UNIX client computers.

The following table describes the procedures to verify Windows clients.

**Table 4-10** 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

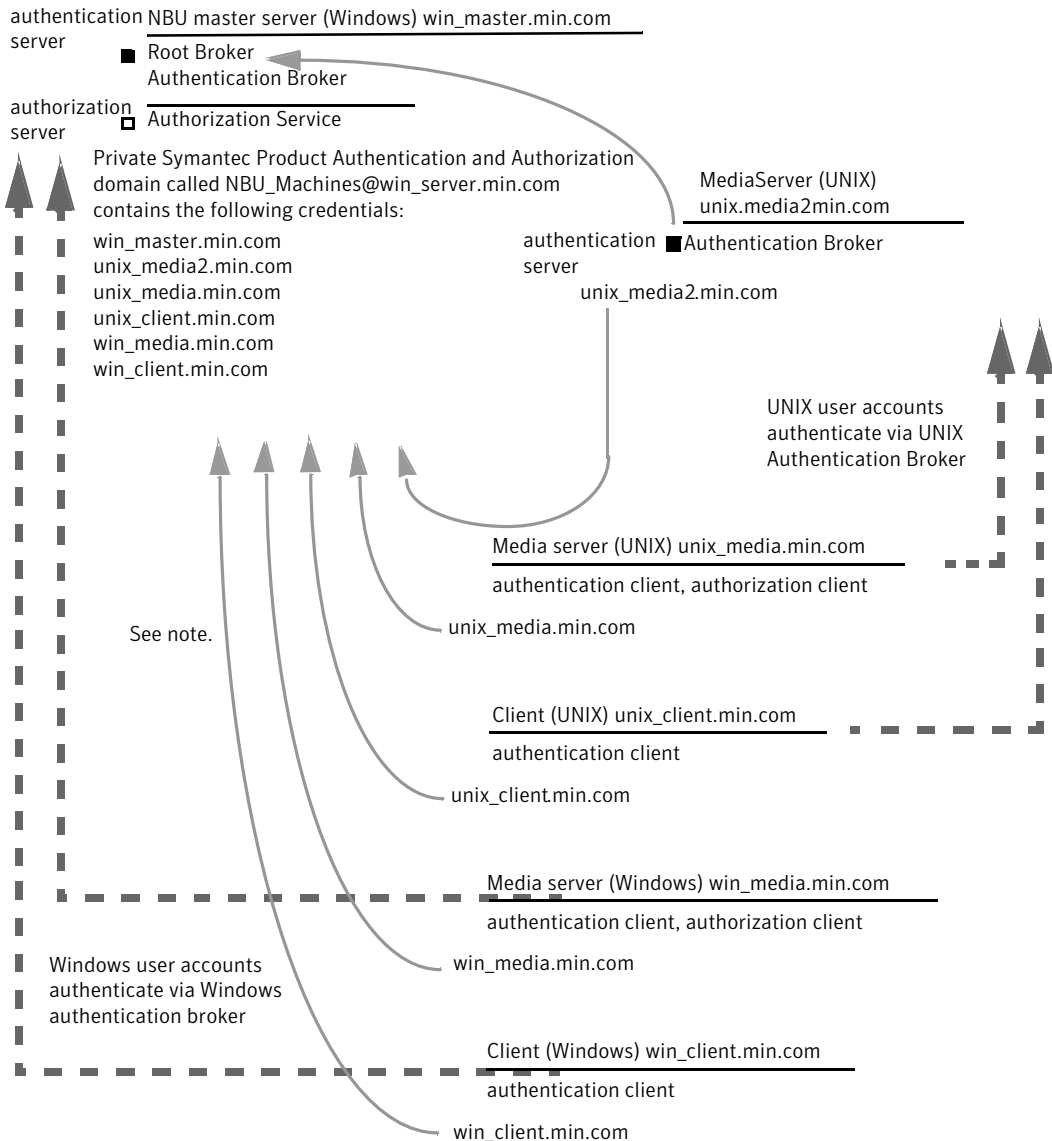
The following procedures can help you verify that the master server, media server, and client are configured correctly. They should be configured for a heterogeneous NetBackup Access Control environment. The master server is a Windows computer.

- Master server verification points for mixed Windows master  
See [“Master server verification points for a mixed Windows master server”](#) on page 181.
- Media server verification points for mixed Windows master  
See [“Media server verification points for a mixed Windows master server”](#) on page 181.
- Client verification points for mixed Windows master

See [“Client verification points for a mixed Windows master server”](#) on page 183.

See [Figure 4-11](#) on page 180. 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 186. 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 4-11** Media server verification procedures for a mixed Windows master server

Procedure	Description
Verify the Windows media server for a mixed Windows master server	See “ <a href="#">Media server verification points for Windows</a> ” on page 190. 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/opensw/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 4-11** 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>bpnbaz -ListGroup -CredFile "/usr/opensv/var/vxss/credentials/&lt;hostname&gt;"</code></p> <p>For example:</p> <pre>bpnbaz -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>bpnbaz -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 4-11** 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 cat(1)ing the bp.conf 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 PASSWD domains and NIS domains point to unix_media2.company.com, 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 4-12** Verification procedures for a mixed Windows master server

Procedure	Description
Verify the credential for the Windows client	See <a href="#">“Client verification points for Windows”</a> on page 192. for the verification procedures for Windows clients.

**Table 4-12**      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>bnpbat -whoami</code> with <code>-cf</code> for the client's credential file.</p> <p>For example:</p> <pre>bnpbat -whoami -cf \ "/usr/openv/var/vxss/credentials/ unix_client.company.com" Name: unix_client.company.com Domain: NBU_Machines@win_master.company.com Issued by: /CN=broker/OU=root@ win_master.company.com/O=vx Expiry Date: Oct 31 21:16:01 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.</pre>
Verify that the authentication client libraries are installed	<p>Run <code>bnpbat -login</code> on the client to verify that the authentication client libraries are installed.</p> <pre>bnpbat -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

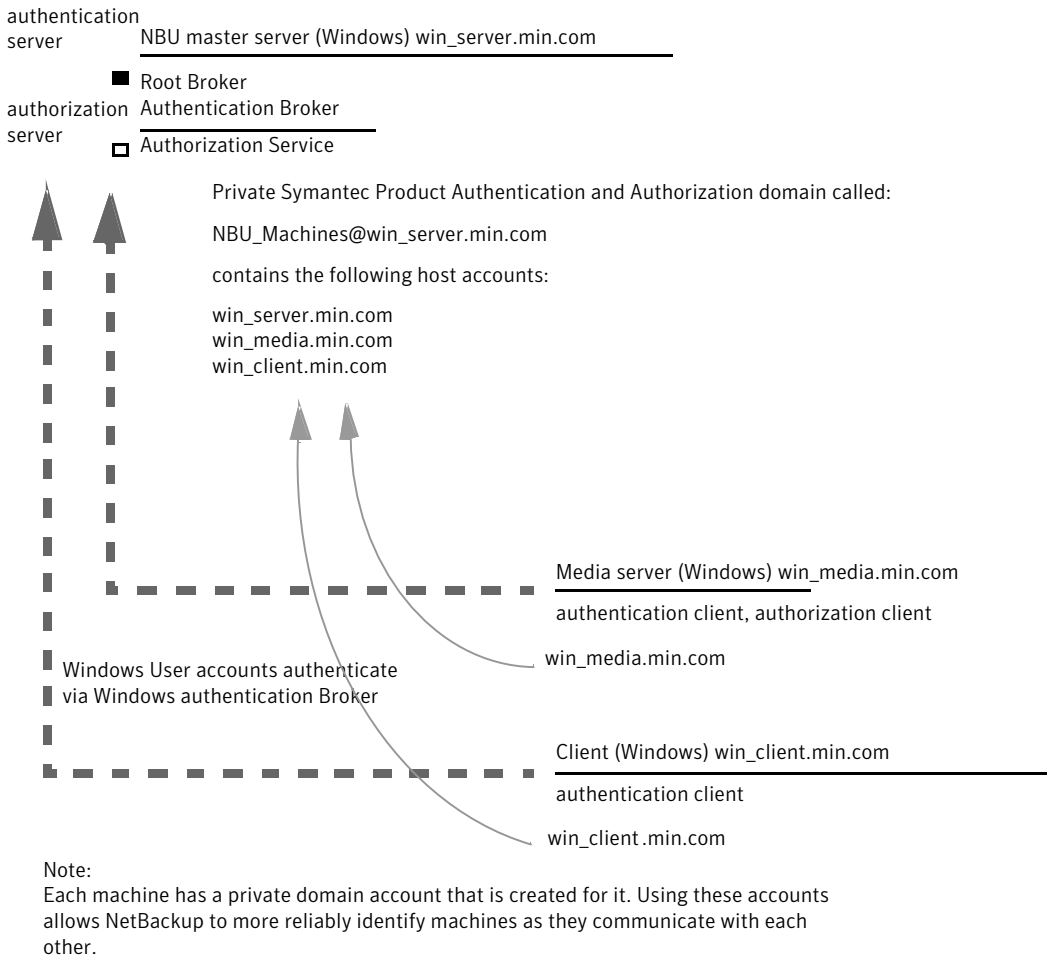
The following configuration procedures can help you verify that the master server, media server, and client are configured correctly for access control.

These Windows verification points include:

- See [“Master server verification points for Windows”](#) on page 186.
- See [“Media server verification points for Windows”](#) on page 190.
- See [“Client verification points for Windows”](#) on page 192.

[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 4-13** 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><b>Note:</b> 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><b>Note:</b> 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 4-13** 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><b>Note:</b> 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 <code>vx</code>), <code>NBU_Machines@win_master.company.com</code>.</p> <p><b>Note:</b> 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 4-13** 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	<p>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.</p>
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 <a href="#">Figure 4-13</a> on page 190. for an example of the host properties settings on the <b>Authentication</b> domain tab.</p> <p>In the <b>Access Control</b> 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
ab (Default)	REG_SZ	(value not set)
ab AUTHORIZATION_SERVICE	REG_SZ	redsteel 0
ab Browser	REG_SZ	redsteel
ab Client_Name	REG_SZ	redsteel
ab EMMPORT	REG_DWORD	0x00000614 (1556)
ab EMMSERVER	REG_SZ	redsteel
ab Exclude	REG_MULTI_SZ	C:\Program Files\Veritas\NetBackup\bin\*.lock C:\Prog...
ab HOST_CACHE_TTL	REG_DWORD	0x00000e10 (3600)
ab IP_ADDRESS_FAMILY	REG_SZ	AF_UNSPEC
ab Port_BPCD	REG_DWORD	0x000035d6 (13782)
ab Port_BPRD	REG_DWORD	0x00003598 (13720)
ab Server	REG_MULTI_SZ	redsteel
ab USE_VXSS	REG_SZ	AUTOMATIC
ab VXDBMS_NB_CONF	REG_SZ	C:\Program Files\Veritas\NetBackupDB\conf
ab VXDBMS_NB_DATA	REG_SZ	C:\Program Files\Veritas\NetBackupDB\data
ab VXSS_NETWORK	REG_MULTI_SZ	redsteel REQUIRED
ab 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 4-14** 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</code> with <code>-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 4-14 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 -ListGroups -CredFile "machine_credential_file"</code></p> <p>For example:</p> <pre>bpnbaz -ListGroups -CredFile "C:\Program Files\Veritas\NetBackup\var\vxss\credentials\ win_media.company.com" NBU_Operator NBU_Admin NBU_SAN Admin NBU_User NBU_Security Admin Vault_Operator Operation completed successfully.</pre> <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 <b>NetBackup Authentication and Authorization</b> 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 4-15** 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: <code>bpnbat -loginmachine</code></p>
Verify that the authentication client libraries are installed	<p><b>Note:</b></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 4-15 Client verification procedures for Windows (*continued*)

Procedure	Description
Verify correct authentication domains	Check that any defined authentication domains for the client are correct either in the <b>Access Control</b> 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 195.
- The creation of user groups.  
See [“User groups”](#) on page 196.

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

See [“Viewing specific user permissions for NetBackup user groups”](#) on page 209. 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.

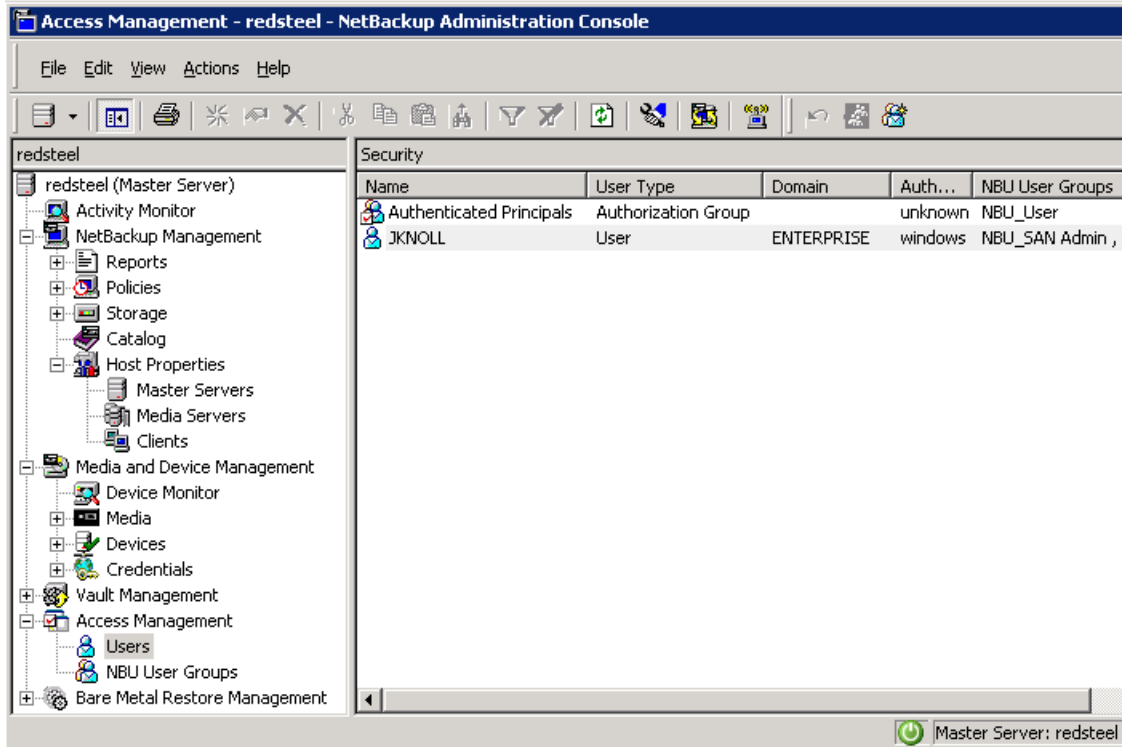
## Individual users

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 196. for a display of the individual authenticated users.

**Figure 4-14** Individual users



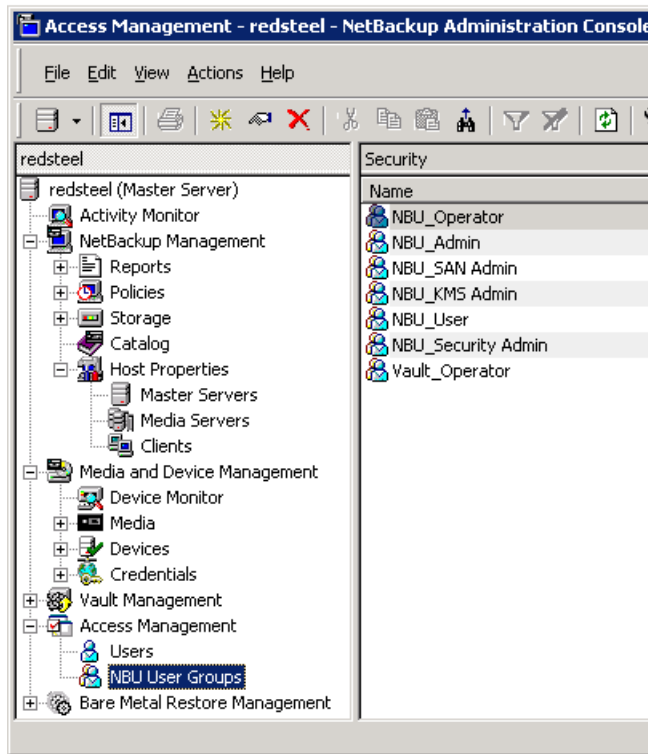
All authenticated users are implicit members of the NBU\_Users user group. All other groups must have members defined explicitly. The NetBackup Security Administrator can delete a manually added member to other groups. However, the Security Administrator may not delete the predefined implicit members 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 197. 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 4-16 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><b>Note:</b> 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 <b>Access Management</b>. Configuring access control includes the following abilities:</p> <ul style="list-style-type: none"> <li>■ To see the contents of <b>Access Management</b> in the <b>NetBackup Administration Console</b></li> <li>■ To create, modify, and delete users and user groups</li> <li>■ To assign users to user groups</li> <li>■ To assign permissions to user groups</li> </ul>

Table 4-16 NetBackup default user groups (*continued*)

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

## Configuring user groups

The Security Administrator can create new user groups. 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 201. 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 206.

- 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.

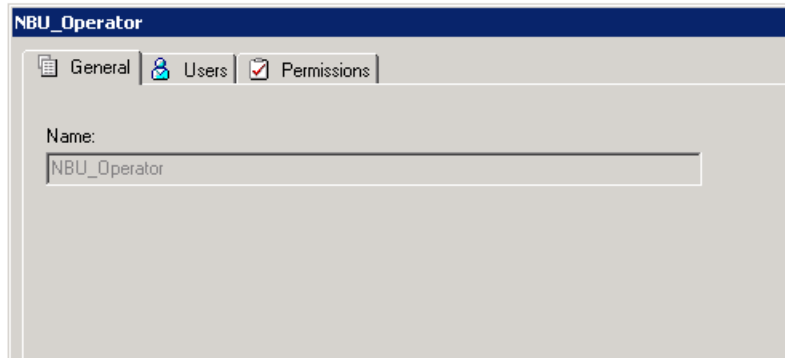


## General tab

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

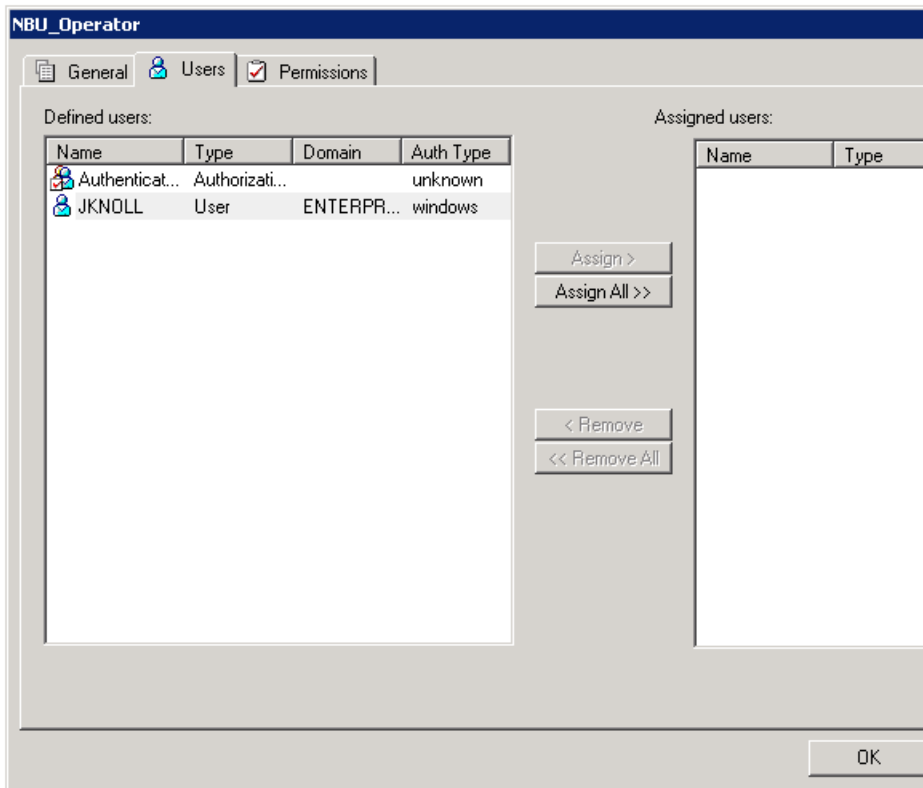


## Users tab

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 205.

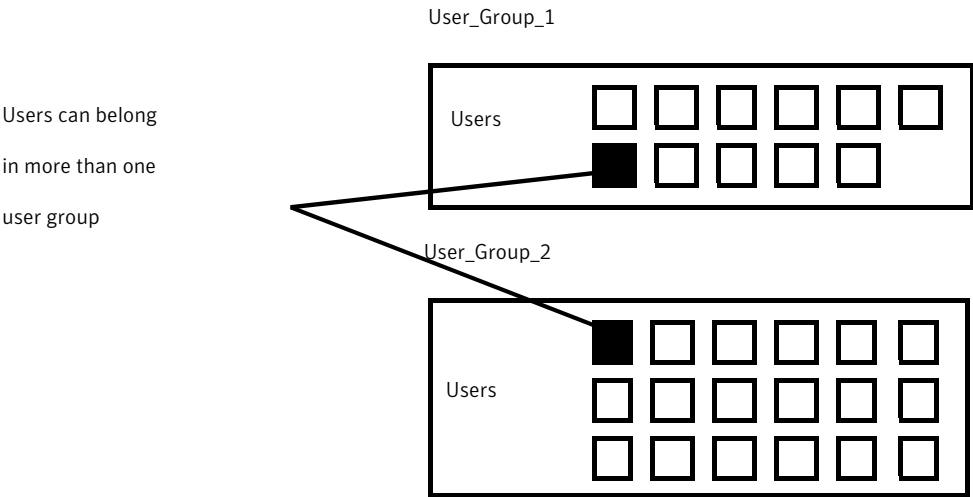
## About defining a user group and users

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.

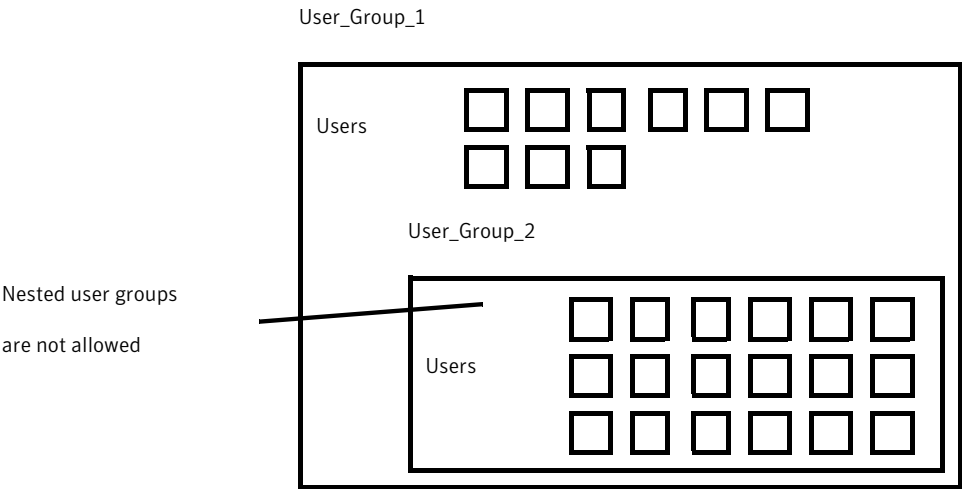
Figure 4-18 Defining a user group



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



## 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.

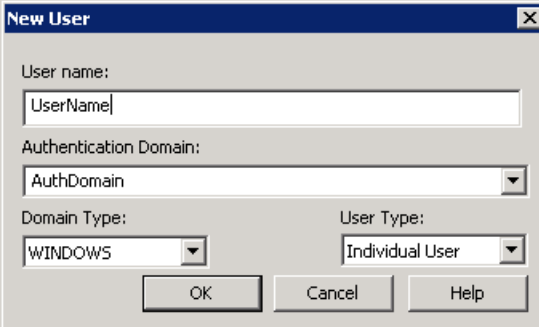
## Assigning a user to a user group

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

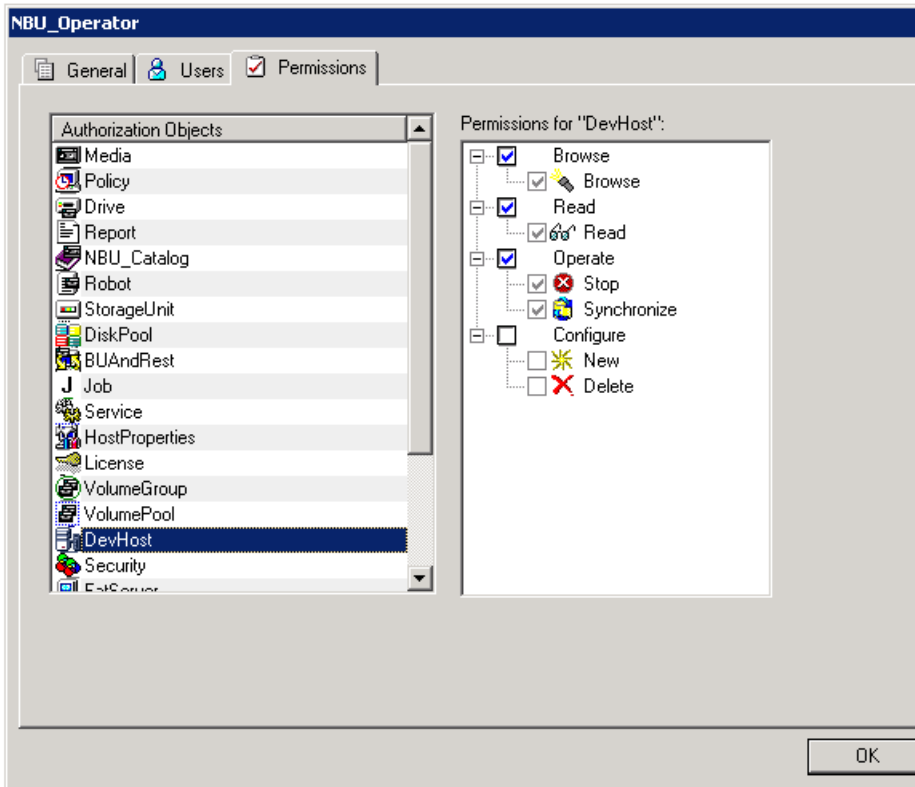
The **Permissions** tab contains a list of the NetBackup authorization objects and configurable permissions that are associated with each object.

## 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.

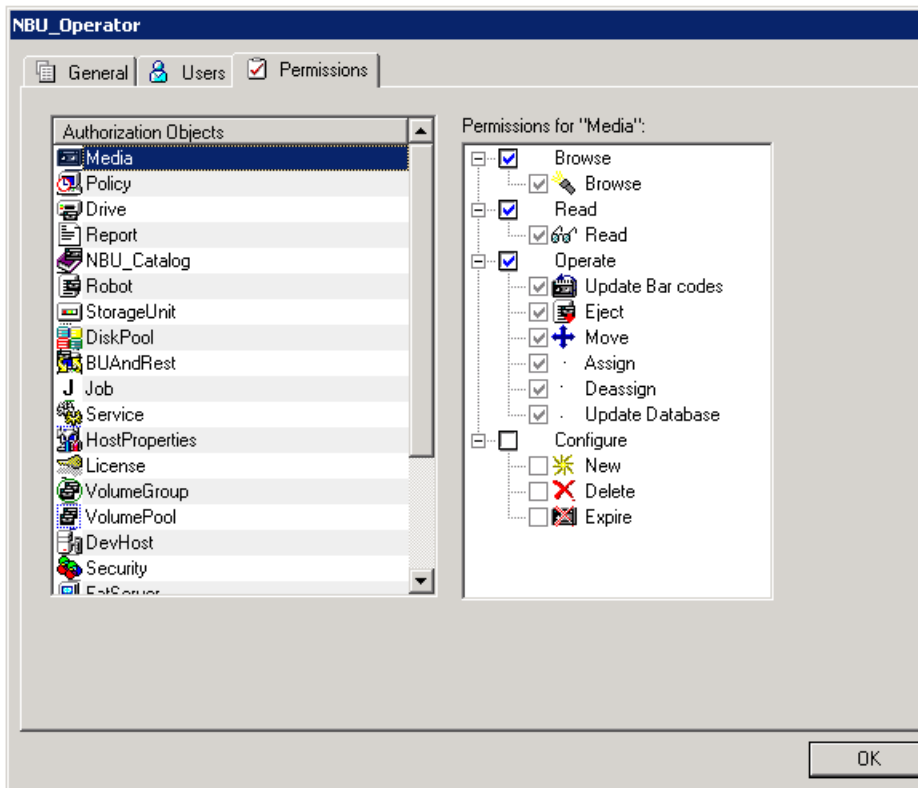
## To grant a permission to the members of a user group

- 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 211.
- See ["Policy authorization object permissions"](#) on page 211.
- See ["Drive authorization object permissions"](#) on page 212.
- See ["Report authorization object permissions"](#) on page 213.
- See ["NBU\\_Catalog authorization object permissions"](#) on page 213.
- See ["Robot authorization object permissions"](#) on page 214.
- See ["Storage unit authorization object permissions"](#) on page 214.
- See ["DiskPool authorization object permissions"](#) on page 215.
- See ["BUAndRest authorization object permissions"](#) on page 216.
- See ["Job authorization object permissions"](#) on page 216.
- See ["Service authorization object permissions"](#) on page 217.
- See ["HostProperties authorization object permissions"](#) on page 218.
- See ["License authorization object permissions"](#) on page 218.
- See ["Volume group authorization object permissions"](#) on page 219.
- See ["VolumePool authorization object permissions"](#) on page 219.
- See ["DevHost authorization object permissions"](#) on page 220.
- See ["Security authorization object permissions"](#) on page 220.
- See ["Fat server authorization object permissions"](#) on page 221.
- See ["Fat client authorization object permissions"](#) on page 221.
- See ["Vault authorization object permissions"](#) on page 222.
- See ["Server group authorization object permissions"](#) on page 222.

- See [“Key management system \(kms\) group authorization object permissions”](#) on page 223.

## Media authorization object permissions

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

**Table 4-17** Media authorization object permissions

Set	Activity	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	X	---
Read	Read	X	X	---	---	---	X	---
Operate	Update barcodes	X	X	---	---	---	X	---
	Eject	X	X	---	---	---	X	---
	Move	X	X	---	---	---	X	---
	Assign	X	X	---	---	---	X	---
	Deassign	X	X	---	---	---	X	---
	Update Database							
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 4-18** Policy authorization object permissions

Set	Activity	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	---	---

**Table 4-18** Policy authorization object permissions (*continued*)

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_SAN Admin	NBU_User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Read	Read	X	X	---	---	---	---	---
Operate	Back up	X	X	---	---	---	---	---
Configure	Activate	---	X	---	---	---	---	---
	Deactivate	---	X	---	---	---	---	---
	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---

## Drive authorization object permissions

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

**Table 4-19** Drive authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_SAN Admin	NBU_User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	X	---	---	X	---
Read	Read	X	X	X	---	---	X	---
Operate	Up	X	X	---	---	---	---	---
	Down	X	X	---	---	---	---	---
	Reset	X	X	---	---	---	---	---
	Assign	X	---	---	---	---	---	---
	Deassign	X	---	---	---	---	---	---
Configure	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---

## Report authorization object permissions

The following table shows the permissions that are associated with the Report authorization object. Reports include only the Access permission set, and do not include a Configure or Operate permission set.

**Table 4-20** Report authorization object permissions

Set	Activity	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Browse	Browse	---	X	---	---	---	X	---
Read	Read	---	X	---	---	---	X	---

## NBU\_Catalog authorization object permissions

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

**Table 4-21** NBU\_Catalog authorization object permissions

Set	Activity	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Browse	Browse	---	X	---	---	---	X	---
Read	Read	---	X	---	---	---	X	---
Operate	Back up	---	X	---	---	---	---	---
	Restore	---	X	---	---	---	---	---
	Verify	---	X	---	---	---	---	---
	Duplicate	---	X	---	---	---	---	---
	Import	---	X	---	---	---	---	---
	Expire	---	X	---	---	---	---	---

**Table 4-21** NBU\_Catalog authorization object permissions (*continued*)

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_SAN Admin	NBU_User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Configure	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---
	Read	---	X	---	---	---	---	---
	Configuration	---	X	---	---	---	---	---
	Set Configuration							

## Robot authorization object permissions

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

**Table 4-22** Robot authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_SAN Admin	NBU_User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	X	---	---	X	---
Read	Read	X	X	X	---	---	X	---
Operate	Inventory	X	X	---	---	---	X	---
Configure	New	---	X	---	---	---	X	---
	Delete	---	X	---	---	---	X	--

## Storage unit authorization object permissions

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

**Table 4-23** Storage unit authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_SAN Admin	NBU_User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	---	---
Read	Read	X	X	---	---	---	---	---
Configure	Assign	---	X	---	---	---	---	---
	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---

## DiskPool authorization object permissions

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

**Table 4-24** DiskPool authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_SAN Admin	NBU_User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	X	---	---	---	---
Read	Read	X	X	X	---	---	---	---
Operate	New	---	X	X	---	---	---	---
	Delete	---	X	X	---	---	---	---
	Modify	---	X	X	---	---	---	---
	Mount	---	X	X	---	---	---	---
	Unmount	---	X	X	---	---	---	---
Configure	Read Configuration	---	X	X	---	---	---	---
		---	---	X	---	---	---	---
	Set Configuration							

## BUAndRest authorization object permissions

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

**Table 4-25** BUAndRest authorization object permissions

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

## Job authorization object permissions

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

**Table 4-26** Job authorization object permissions

Set	Activity	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	X	---
Read	Read	X	X	---	---	---	X	---



**Table 4-26** Job authorization object permissions (*continued*)

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_SAN Admin	NBU_User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Operate	Suspend	X	X	---	---	---	X	---
	Resume	X	X	---	---	---	X	---
	Cancel	X	X	---	---	---	X	---
	Delete	X	X	---	---	---	X	---
	Restart	X	X	---	---	---	X	---
	New	X	X	---	---	---	X	---

## Service authorization object permissions

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

**Table 4-27** Service authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_SAN Admin	NBU_User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	X	---
Read	Read	X	X	---	---	---	X	---
Operate	Stop	X	X	---	---	---	---	---

The Read and Browse permissions do not have an effect on the Services/Daemons tab. This information is harvested from the server using user level calls. The calls are used to access the process task list and is displayed to all users for informational purposes.

If a user is not a member of the NBU\_Admin user group, but is logged on as an OS administrator (Administrator or root), then:

- The user is able to restart a service from within the **NetBackup Administration Console** or from the command line.
- The user is able to stop a service from within the **NetBackup Administration Console** but not from the command line.

If a user is not a member of the NBU\_Admin user group, but is logged on as an OS administrator (`root`). That user is able to restart a daemon from the command line only:

```
/etc/init.d/netbackup start
```

If a user is a member of the NBU\_Admin user group, but is not logged on as an OS administrator (Administrator), then:

- The user is not able to restart a service from within the **NetBackup Administration Console** or from the command line.
- The user is not able to stop a service from within the **NetBackup Administration Console** but the user can use the command line.

(For example, `bprdreq -terminate`, `bpdgm -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 4-28** HostProperties authorization object permissions

Set	Activity	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Browse	Browse	X	X	X	X	X	X	X
Read	Read	X	X	X	X	X	X	X
Configure	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	--

## License authorization object permissions

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

**Table 4-29** License authorization object permissions

Set	Activity	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Browse	Browse	X	X	X	X	X	X	X
Read	Read	X	X	X	X	X	X	X
Configure	Assign	---	X	---	---	---	---	---
	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---

## Volume group authorization object permissions

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

**Table 4-30** Volume group authorization object permissions

Set	Activity	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	X	---
Read	Read	X	X	---	---	---	X	---
Configure	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---

## VolumePool authorization object permissions

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

**Table 4-31** VolumePool authorization object permissions

Set	Activity	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	X	---

**Table 4-31** VolumePool authorization object permissions (*continued*)

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_SAN Admin	NBU_User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Read	Read	X	X	---	---	---	X	---
Configure	Assign	---	X	---	---	---	---	---
	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---

## DevHost authorization object permissions

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

---

**Note:** Access to the "Media and Device Management --> Credentials" node in the GUI is controlled by the DevHost object.

---

**Table 4-32** DevHost authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_SAN Admin	NBU_User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	X	---	---	X	---
Read	Read	X	X	X	---	---	X	---
Operate	Stop	X	X	---	---	---	---	---
	Synchronize	X	X	---	---	---	---	---
Configure	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---

## Security authorization object permissions

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

**Table 4-33** Security authorization object permissions

Set	Activity	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Browse	Browse	---	---	---	---	X	---	---
Read	Read	---	---	---	---	X	---	---
Configure	Security	---	---	---	---	X	---	---

## Fat server authorization object permissions

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

**Table 4-34** Fat server authorization object permissions

Set	Activity	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Browse	Browse	X	X	X	---	---	---	---
Read	Read	X	X	X	---	---	---	---
Configure	Modify	---	X	X	---	---	---	---
	Modify SAN Configuration	---	---	X	---	---	---	---

## Fat client authorization object permissions

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

**Table 4-35** Fat client authorization object permissions

Set	Activity	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Browse	Browse	X	X	X	---	---	---	---
Read	Read	X	X	X	---	---	---	--

**Table 4-35** Fat client authorization object permissions (*continued*)

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_SAN Admin	NBU_User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Operate	Discover	---	X	X	---	---	---	---
Configure	Modify	---	X	X	---	---	---	---

## Vault authorization object permissions

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

**Table 4-36** Vault authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_SAN Admin	NBU_User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	---	X	---	---	---	X	---
Read	Read	---	X	---	---	---	X	---
Operate	Manage Containers	---	X	---	---	---	X	---
	Run Reports	---	X	---	---	---	X	---
Configure	Modify	---	X	---	---	---	---	---
	Run Sessions	---	X	---	---	---	---	---

## Server group authorization object permissions

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

**Table 4-37** Server group authorization object permissions

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

**Table 4-37** Server group authorization object permissions (*continued*)

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_SAN Admin	NBU_User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Read	Read	X	X	---	---	---	X	---
Configure	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---
	Modify	---	X	---	---	---	---	---

## Key management system (kms) group authorization object permissions

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

**Table 4-38** Key management system group authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_SAN Admin	NBU_User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	---	X	---	---	---	---	X
Read	Read	---	X	---	---	---	---	X
Configure	New	---	---	---	---	---	---	X
	Delete	---	---	---	---	---	---	X
	Modify	---	---	---	---	---	---	X

# 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 : <a href="http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf">http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf</a>.</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"><li>■ 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.</li><li>■ 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.</li><li>■ Data encryption is much like automobile security. Most problems are related to lost / misplaced keys and not related to malfunctioning locks.</li><li>■ Since misuse is more likely to lead to problems, the usability of an encryption product should be part of the consideration.</li></ul> <p>Usability considerations include the following:</p> <ul style="list-style-type: none"><li>■ Encryption integration with the product</li><li>■ Encryption integration with business processes.</li><li>■ Appropriate encryption key granularity</li><li>■ Recoverability</li></ul>
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 230. 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 230.
- Option 2 - Media server encryption  
See [“Option 2 - Media server encryption”](#) on page 254.
- 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 230.	<ul style="list-style-type: none"><li>■ The encryption key is on the client computer and not controlled by the NetBackup administrator</li><li>■ Can be deployed without affecting the NetBackup master and media servers</li><li>■ Can be deployed on a per client basis</li></ul>	<ul style="list-style-type: none"><li>■ 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</li><li>■ Encryption and compression taking place on the client can affect client performance</li></ul>
See "Option 2 - Media server encryption" on page 254.	<ul style="list-style-type: none"><li>■ Will not affect client computer performance</li><li>■ Master / Media server centralized keys</li></ul>	<ul style="list-style-type: none"><li>■ Master / Media server centralized keys</li><li>■ Limited options for detailed Key Granularity</li><li>■ Not tightly integrated with NetBackup configuration and operation</li><li>■ Encryption and compression taking place on the media server can affect media server performance</li></ul>
Option 3 - third-party encryption appliances and hardware devices	<ul style="list-style-type: none"><li>■ Generally little (or no performance) affect due to added hardware.</li><li>■ Generally NIST FIPS 140 certified.</li></ul>	<ul style="list-style-type: none"><li>■ 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.</li><li>■ No integration with NetBackup configuration, operation, or diagnostics.</li><li>■ Disaster recovery scenario that is provided by the Appliance or Device.</li></ul>

## 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 231.
- Standard encryption backup process  
See [“Standard encryption backup process”](#) on page 232.
- Legacy encryption backup process  
See [“Legacy encryption backup process”](#) on page 232.

## 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 232. for a description of the backup process for standard encryption. See [“NetBackup standard encryption](#)

[restore process](#)” on page 233. for a description of the restore process for standard encryption.

See “[Legacy encryption backup process](#)” on page 232. for a description of the backup process for legacy encryption. See “[NetBackup legacy encryption restore process](#)” on page 234. 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 and later versions, the encryption software is automatically installed with the NetBackup UNIX server and client installations.

A key file must exist. The key file is created when you run the `bpkeyutil` command from the server or from the client.

- The **Encryption** attribute must be selected on the NetBackup policy that includes the client.

If the prerequisites are met, the backup takes place as follows:

- The client takes the latest key from the key file.

For each file that is backed up, the following occurs:

- The client creates an encryption `tar` header. The `tar` header contains a checksum of the key and the cipher that NetBackup used for encryption.
- To write the file data that was encrypted with the key, the client uses the cipher that the `CRYPT_CIPHER` configuration entry defines. (The default cipher is AES-128-CFB.)

---

**Note:** Only file data is encrypted. File names and attributes are not encrypted.

---

- The backup image on the server includes a flag that indicates whether the backup was encrypted.

## Legacy encryption backup process

The prerequisites for encrypting a legacy backup are as follows:

- The encryption software must include the appropriate DES library, as follows:
  - For 40-bit DES encryption, `libvdes40.suffix`; the suffix is `so`, `sl`, or `dll`, depending on the client platform.



- For 56-bit DES encryption, `libvdes56.suffix`; the suffix is `so`, `sl`, or `dll`, depending on the client platform.

---

**Note:** In NetBackup 7.5 and later versions the encryption software is automatically installed with the NetBackup UNIX server and client installations.

---

- A key file must exist as specified with the `CRYPT_KEYFILE` configuration option. You create the key file when you specify a NetBackup pass phrase with the server `bpinst` command or the client `bpkeyfile` command.
- You must select the **Encryption** attribute on the NetBackup policy that includes the client.

If the prerequisites are met and the backup is to be encrypted, the following occurs:

- The client takes the latest data from its key file and merges it with the current time (the backup time) to generate a DES key. For 40-bit DES, 16 bits of the key are always set to zero.

For each backed-up file, the following occurs:

- The client creates an encryption `tar` header. The `tar` header contains a checksum of the DES that NetBackup used for encryption.
- The client writes the file data that was encrypted with the DES key. Note that only file data is encrypted. File names and attributes are not encrypted.
- The server reads the file names, attributes, and data from the client and writes them to a backup image on the server. The server DOES NOT perform any encryption or decryption of the data. The backup image on the server includes the backup time and a flag that indicates whether the backup was encrypted.

## NetBackup standard encryption restore process

The prerequisites for restoring a standard encrypted backup are as follows:

- The encryption software must be loaded onto the client.

---

**Note:** In NetBackup 7.5 and later versions, the encryption software is automatically installed with the NetBackup UNIX server and client installations.

---

- A key file must exist. The key file is created when you run the `bpkeyutil` command from the server or from the client.

When the restore occurs, the server determines from the backup image whether the backup was encrypted. The server then connects to `bpcd` on the client to initiate the restore. The server sends to the client an encryption flag on the restore request.

When a backup takes place properly, the restore occurs as follows:

- The server sends file names, attributes, and encrypted file data to the client to be restored.
- If the client reads an encryption `tar` header, the client compares the checksum in the header with the checksums of the keys in the key file. If the one of the keys' checksum matches the header's checksum, NetBackup uses that key to decrypt the file data. It uses the cipher that is defined in the header.
- The file is decrypted and restored if a key and cipher are available. If the key or cipher is not available, the file is not restored and an error message is generated.

## NetBackup legacy encryption restore process

The prerequisites for restoring a legacy encrypted backup are as follows:

- The legacy encryption software must be loaded on the client.

---

**Note:** In NetBackup 7.5 and later versions, the encryption software is automatically installed with the NetBackup UNIX server and client installations.

---

- The encryption software must include the 40-bit DES library. The name of the 40-bit DES library is `libvdes40.suffix`; the suffix is `so`, `sl`, or `dll` depending on the client platform.
- If the `CRYPT_STRENGTH` configuration option is set to `DES_56`, the encryption software must also include the 56-bit DES library. The name of the 56-bit DES library is `libvdes56.suffix`; the suffix is `so`, `sl`, or `dll` depending on the client platform.
- A key file must exist as specified with the `CRYPT_KEYFILE` configuration option. You create the key file when you specify a NetBackup pass phrase with the server `bpinst` command or the client `bpkeyfile` command.

The server determines from the backup image whether the backup was encrypted. The server then connects to `bpcd` on the client to initiate the restore. The server sends to the client an encryption flag and backup time from the backup image on the restore request.

If the prerequisites are met, the following occurs:

- The server sends file names, attributes, and encrypted file data to the client to be restored.
- The client takes its key file data and merges it with the backup time to generate one or more 40-bit DES keys. If the 56-bit DES library is available, the client also generates one or more 56-bit DES keys.
- If the client reads an encryption `tar` header, the client compares the checksum in the header with the checksums of its DES keys. If the checksum of a DES key matches the checksum in the header, NetBackup uses that DES key to decrypt the file data.

The file is decrypted and restored if a DES key is available. If the DES key is not available, the file is not restored and an error message is generated.

## Installation prerequisites for encryption security

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

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

## Installing encryption on a UNIX NetBackup server

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

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

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

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

```
/usr/opensv/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 236. 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 236. 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, Volume I](#) for details.

## Managing standard encryption configuration options

The following table describes the three encryption-related configuration options for the standard encryption that can exist on a NetBackup client.

Ensure that the options are set to the appropriate values for your client.

**Table 5-5** Three encryption-related 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:
	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.
<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.

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

Option	Value	Description
<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/opensv/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, Volume 1](#) 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 243.
- Changing client encryption settings from the server  
See "[Changing the client encryption settings from the NetBackup server](#)" on page 243.

## 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 237. 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, Volume I](#) for details.

You can set the CRYPT\_OPTION and CRYPT\_STRENGTH options on the `bpinst -LEGACY_CRYPT` command. The equivalent option settings are `-crypt_option`, `-crypt_strength`, respectively.

## About configuring legacy encryption from the server

You can configure most NetBackup clients for encryption by using the `bpinst` command from the server.

Prerequisites for this method include the following:

- The NetBackup client software must be running on a platform that supports NetBackup encryption.  
Refer to the *NetBackup Release Notes* for details on supported platforms.
- The NetBackup clients must be running NetBackup 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/opensv/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 246. and See

[“About pushing the legacy encryption pass phrases to clients”](#) on page 247. 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.
	<code>required REQUIRED</code>	Specifies that the client requires encrypted backups. If the server requests an unencrypted backup, it is considered an error.
<code>CRYPT_KIND = kind</code>		Defines the encryption type on NetBackup clients. The possible values for <i>kind</i> follow:
	<code>NONE</code>	Neither standard encryption nor legacy encryption is configured on the client.
	<code>LEGACY</code>	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.
	<code>STANDARD</code>	Specifies the cipher encryption type, which can be either 128-bit encryption or 256-bit encryption.
<code>CRYPT_STRENGTH = strength</code>		Defines the encryption strength on NetBackup clients. The possible values for <i>strength</i> follow:

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

Option	Value	Description
	<code>des_40 DES_40</code>	(The default value) Specifies 40-bit DES encryption.
	<code>des_56 DES_56</code>	Specifies the 56-bit DES encryption.
<code>CRYPT_LIBPATH = directory_path</code>		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 <code>C:\VERITAS</code> .
	<code>/usr/opensv/lib/</code>	The default value on UNIX systems.
	<code>install_path\NetBackup\ bin\</code>	The default value on Windows systems
<code>CRYPT_KEYFILE = file_path</code>		Defines the file that contains the encryption keys on NetBackup clients.
	<code>/usr/opensv/netbackup/ keyfile</code>	The default value on UNIX systems.
	<code>install_path\NetBackup\ bin\keyfile.dat</code>	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 phrase 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 252. 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, Volume 1](#) 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 253., 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

## 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](http://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 `nbmkmsutil`.

KMS has a minimal effect on existing NetBackup operation system management and yet provides a foundation for future Key Management Service enhancements.

## KMS considerations

The following table describes the considerations that relate to the functionality and use of KMS.

Table 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"><li>■ To allow for the <code>ENCR_</code> prefix on the volume pool names.</li><li>■ To communicate with the key Management Service.</li><li>■ To provide support for the T10 / SCSI standard tape drives with embedded (LT04 and equivalent) encryption.</li><li>■ 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.</li><li>■ 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.</li></ul>
KMS installation and deployment decisions	<p>Following are decisions you must make for KMS deployment:</p> <ul style="list-style-type: none"><li>■ Whether to choose KMS random generated keys or passphrase generated keys</li><li>■ Whether to include NBAC deployment</li></ul>
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"><li>■ AES_128</li><li>■ AES_192</li><li>■ AES_256 (default cipher)</li></ul>
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"><li>■ Key file or key database Contains the data encryption keys. The key file is located at /opt/opensv/kms/db/KMS_DATA.dat.</li><li>■ 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/opensv/kms/key/KMS_HMKF.dat</li><li>■ 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/opensv/kms/key/KMS_KPKF.dat. Currently the same key protection key is used to encrypt all of the records.</li><li>■ 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.</li></ul>

**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"><li>■ Encryption key This key is given to the tape drive.</li><li>■ Encryption key Tag This tag is the identifier for the encryption key.</li><li>■ Record state Each of the key records has a state. The states are prelive, active, inactive, deprecated, and terminated.</li><li>■ Metadata Metadata includes logical name, creation date, modification date, and description.</li></ul>
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"><li>■ LTO4 drives can read LTO2, LTO3, and LTO4 media</li><li>■ LTO4 drives can write LTO3 and LTO4 media</li><li>■ LTO4 drives can only encrypt LTO4 media</li><li>■ LTO4 encrypted and decrypted media only works in LTO4 drives</li></ul>

**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/openv/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 <a href="#">NetBackup Cloud Administrator's Guide</a> .
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 <a href="#">NetBackup AdvancedDisk Storage Solutions Guide</a> .
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.

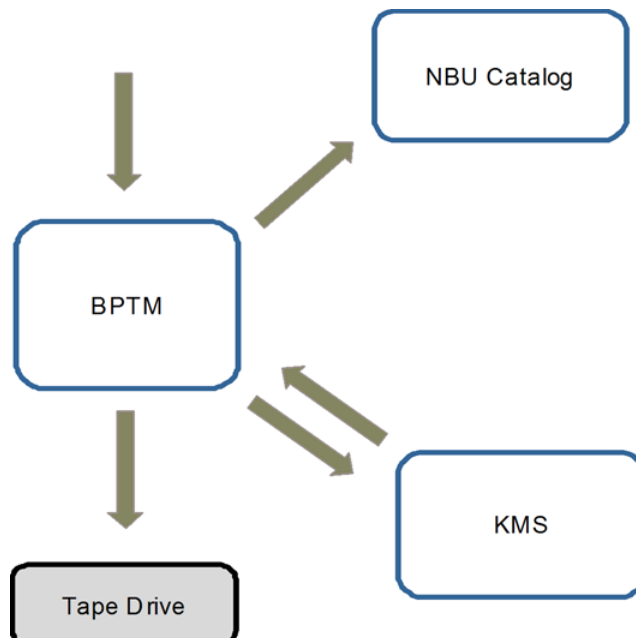
The backup then proceeds as normal.

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/openssl/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"> <li>■ Preive, which means that the key record has been created, but has never been used.</li> <li>■ Active, which means that the key record can be used for encryption and decryption in both backup and restore.</li> <li>■ Inactive, which means that the key record cannot be used for encryption, but can be used for decryption only during restore.</li> <li>■ Deprecated, which means that the key record cannot be used for encryption or decryption.</li> <li>■ Terminated, which means that the key record is not available for use but it can be deleted.</li> <li>■ Keystore , which means that the keystore is the file that keeps the data encryption keys.</li> <li>■ 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.</li> </ul> <p><b>Note:</b> 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 the key records:

```
nbkmsutil -createkey -kgname ENCR_pool1 -keyname Q2_2008_key -activate -desc "key for Apr, May, & Jun"
```

---

**Note:** If you create more than one key record by using the command `nbkmsutil -kgname name -activate`, only the last key remains active.

---

- 12 To list all of the keys that belong to a key group name, use the following command:

```
nbkmsutil -listkeys -kgname keyname
```

---

**Note:** Symantec recommends that you keep a record of the output of the `nbkmsutil -listkeys` command. The key tag that is listed in the output is necessary if you need to recover keys.

---

The following command and output use the examples in this procedure.

```
# nbkmsutil -listkeys -kgname ENCR_pool1
Key Group Name      : ENCR_pool1
Supported Cipher    : AES_256
Number of Keys      : 2
Has Active Key      : Yes
Creation Time       : Thu Aug  8 16:23:06 2013
Last Modification Time: Thu Aug  8 16:23:06 2013
Description         : -
  Key Tag          : 825784185f87145c368c54e919908905a45f79927cb733337a53e9b174bbe046
  Key Name         : Q2_2013_key
  Current State    : ACTIVE
  Creation Time    : Thu Aug  8 16:25:19 2013
  Last Modification Time: Thu Aug  8 16:25:19 2013
  Description      : key for Apr, May, & Jun
  FIPS Approved Key : No
  Key Tag          : f63af53ead99920e98f3e0f4a586afccf32e79e75240e65499d1cd0cbd7c7fdd
  Key Name         : Q1_2013_key
  Current State    : INACTIVE
  Creation Time    : Thu Aug  8 16:25:03 2013
  Last Modification Time: Thu Aug  8 16:25:19 2013
  Description      : key for Jan, Feb, & March
  FIPS Approved Key : No
Number of Keys: 2
```

See [“About installing KMS with HA clustering”](#) on page 270.

See [“Using KMS with NBAC”](#) on page 270.

## 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/openv/netbackup/bin`

- 3 Run the following command:

On Windows: `bpclusterutil -disableSvc "NetBackup Key Management Service"`

On UNIX: `bpclusterutil -disableSvc nbkms`

## Removing the KMS service from monitored list

You can remove the KMS service from the list of services that can be monitored.

### To remove the KMS service from the list of monitored services

- 1 Disable monitoring of the optional product service using the previous procedure
- 2 Follow the optional product-specific steps to remove the product
- 3 Open the command prompt on the active node of the cluster
- 4 Change the directory, as follows:

On Windows: `<NetBackup_install_path>\NetBackup\bin`

On UNIX: `/usr/openv/netbackup/bin`

- 5 Run the following command:

On Windows: `bpclusterutil -deleteSvc "NetBackup Key Management Service"`

On UNIX: `bpclusterutil -deleteSvc nbkms`

## Configuring KMS

The configuration of KMS is done by creating the key database, key groups, and key records. Then NetBackup is configured to work with KMS.



**To configure and initialize KMS**

- 1 Create the key database, the host master key (HMK), and the key protection key (KPK).
- 2 Create a key group that matches the volume pool.
- 3 Create an active key record.

## Creating the key database

Use the following procedure to create an empty key database. A key database is created by invoking the service name with the `-createemptydb` option. This process checks and ensures that an existing key database does not already exist, and then proceeds with the creation. Two protection keys need to be created when the KMS is initialized. They are the Host Master Key (HMK) and the Key Protection Key (KPK).

As with all KMS key creation activities, the user is presented with the following options for creating these keys:

- Keys are generated by 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.

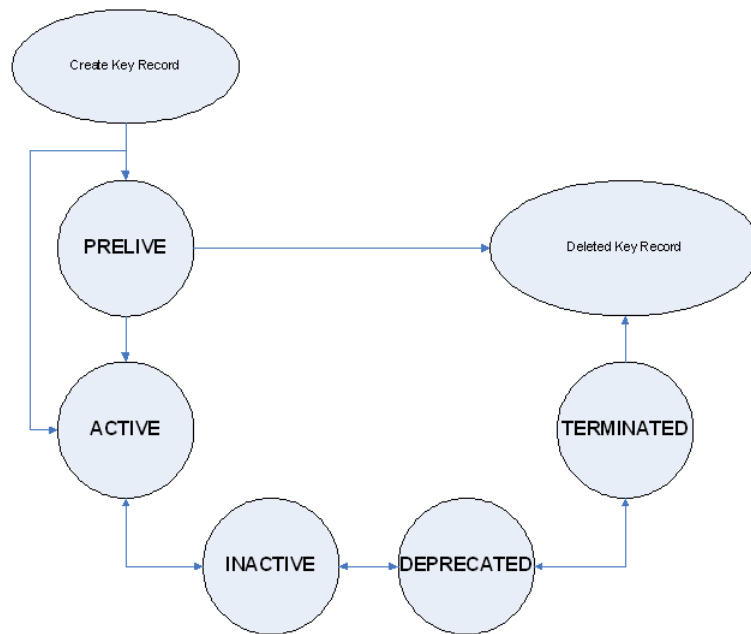
Between the active state and terminated state, the record can move one state at a time in either direction. Outside of this state range, the transitions are one directional. Deleted key records cannot be recovered (unless they were created using a passphrase), and active keys cannot be moved back to 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 134220503860000000  
  
134220503860000000 -  
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 283.
- Setting up NetBackup to use encryption  
See [“Example of setting up NetBackup to use tape encryption”](#) on page 284.

## 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

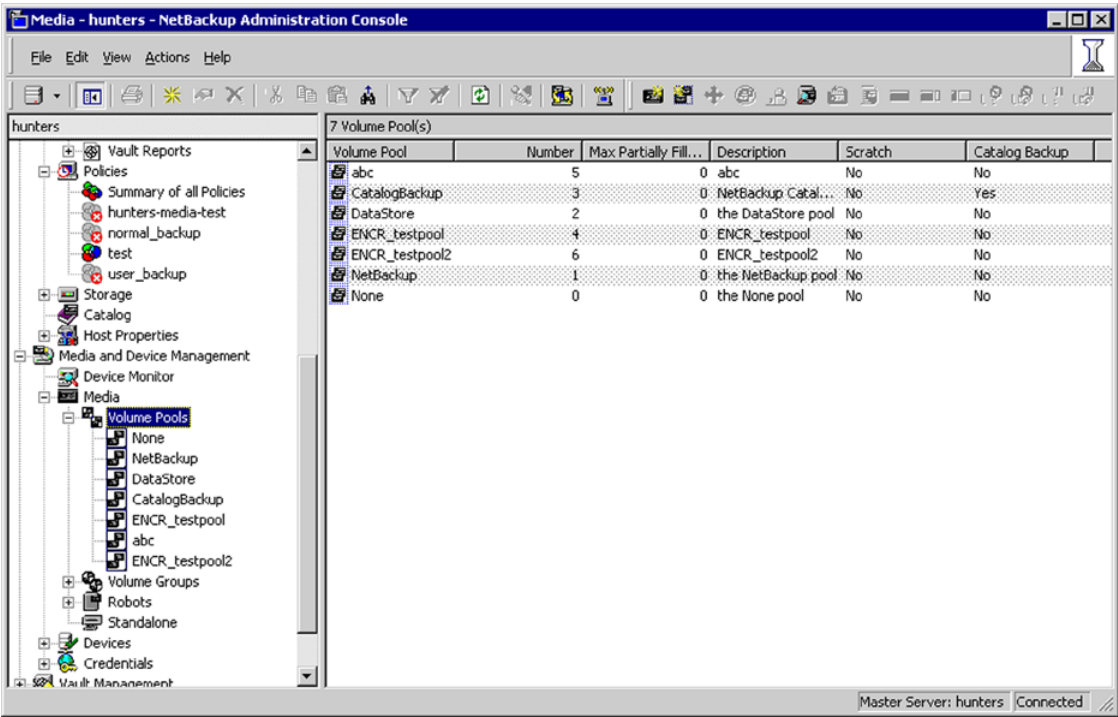
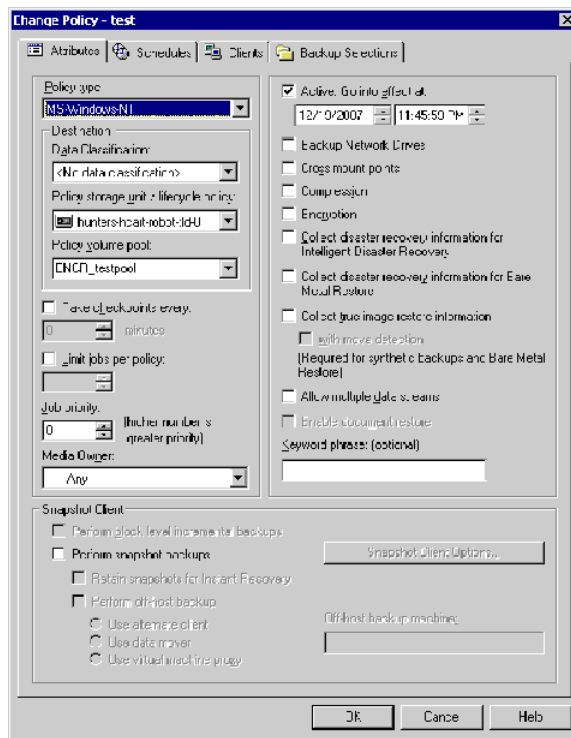


Figure 6-4 shows a NetBackup Policy that is configured to use the volume pool ENCR\_testpool, which is the same name as the key group that you configured earlier.

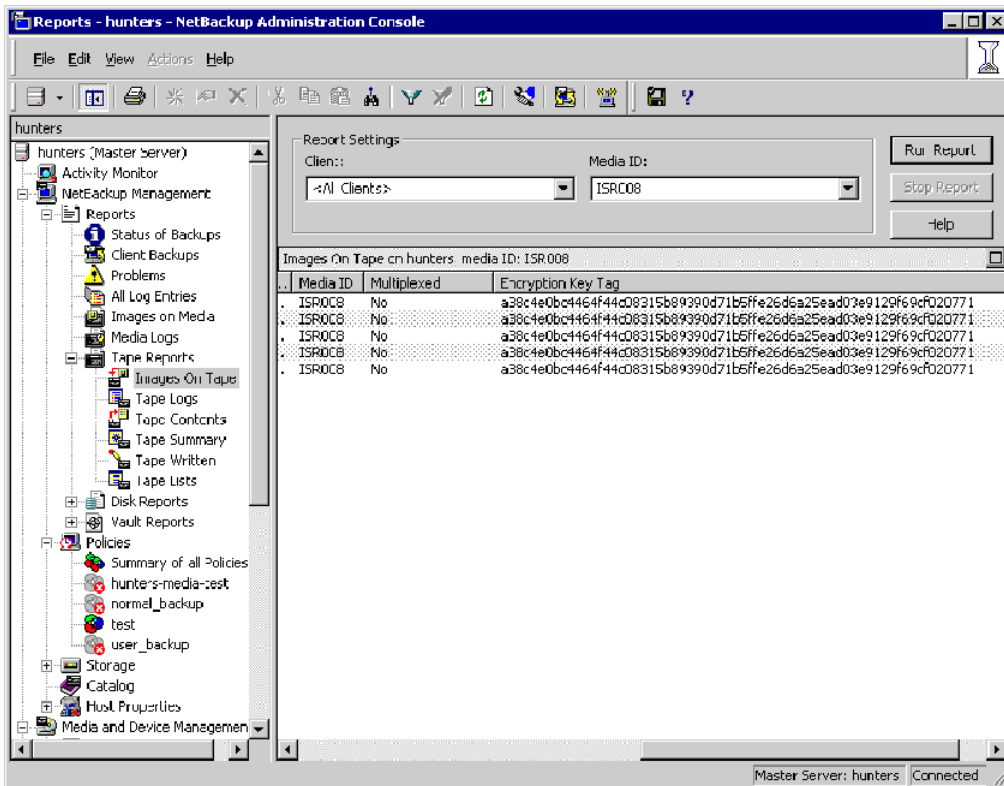
**Figure 6-4** NetBackup Change Policy dialog box with KMS volume pool



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:

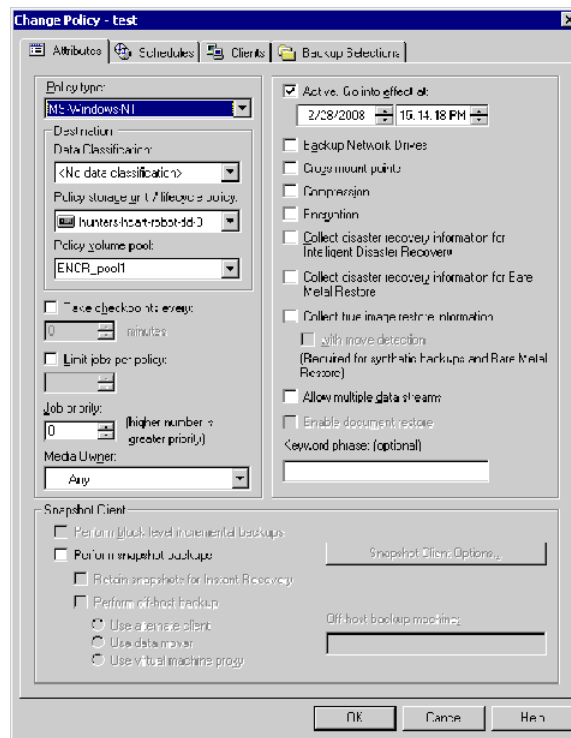
- Example of running an encrypted tape backup  
See [“Example of running an encrypted tape backup”](#) on page 287.
- Example of verifying an encryption backup  
See [“Example of verifying an encryption backup”](#) on page 287.
- About importing KMS encrypted images  
See [“About importing KMS encrypted images”](#) on page 288.

## 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 Change Policy dialog box 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



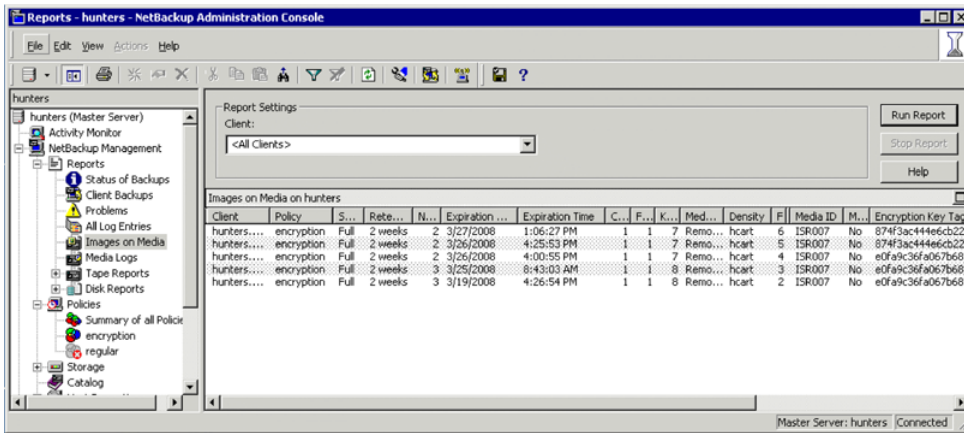
## Example of verifying an encryption backup

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 286.

**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 291.
- Create a new key group  
See [“Create a new key group”](#) on page 292.
- Create a new key  
See [“Create a new key”](#) on page 292.
- Modify key group attributes  
See [“Modify key group attributes”](#) on page 293.

- Modify key attributes  
See [“Modify key attributes”](#) on page 293.
- Get details of key groups  
See [“Get details of key groups”](#) on page 294.
- Get details of keys  
See [“Get details of keys”](#) on page 294.
- Delete a key group  
See [“Delete a key group”](#) on page 295.
- Delete a key  
See [“Delete a key”](#) on page 295.
- Recover a key  
See [“Recover a key”](#) on page 296.
- Modify host master key (HMK)  
See [“Modify host master key \(HMK\)”](#) on page 296.
- Get host master key (HMK) ID  
See [“Get host master key \(HMK\) ID”](#) on page 297.
- Modify key protection key (KPK)  
See [“Modify key protection key \(KPK\)”](#) on page 297.
- Get key protection key (KPK) ID  
See [“Get key protection key \(KPK\) ID”](#) on page 297.
- Get keystore statistics  
See [“Get keystore statistics”](#) on page 297.
- Quiesce KMS database  
See [“Quiesce KMS database”](#) on page 298.
- Unquiesce KMS database  
See [“Unquiesce KMS database”](#) on page 298.

## 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>
-kgname <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>
-kgroup <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).
<code>-kgname</code>	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>
-kgroup <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>-kgroup</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 -kname 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 status: nexus scope 0, key scope 0
14:29:16.384 [19978] <2> manage_drive_attributes: encryp mode 0x0, decryp mode 0x0, algorithm index 0, key instance 0
14:29:16.384 [19978] <2> KMCLIB::kmsGetKeyAndKad: Entering function...(KMCLib.cpp:583)
14:29:16.384 [19978] <2> KMCLIB::GetQueryableFacetInstance: Entering function...(KMCLib.cpp:207)
14:29:16.384 [19978] <2> KMCLIB::InitOrb: Entering function...(KMCLib.cpp:158)
14:29:16.385 [19978] <2> Orb::init: Created anon service name: NB 19978 1536015948517350 (Orb.cpp:600)
14:29:16.385 [19978] <2> Orb::init: endpointvalue is : pbxiop://1556:NB 19978 1536015948517350 (Orb.cpp:618)
14:29:16.385 [19978] <2> Orb::init: initializing ORB kmslib with: kmslib -ORBSvcConfDirective "-ORB DottedDecimalAddresses 0" -ORBSvcConfDirective "static PBXIOP_Factory" -ORBSvcConfDirective "static EndpointSelectorFactory" -ORBSvcConfDirective "static Resource_Factory -ORBPProtocolFactory PBXIOP_Factory" -ORBSvcConfDirective "static Resource_Factory -ORBPProtocolFactory IIOP_Factory" -ORBSvcConfDirective "static PBXIOP_Evaluator_Factory -orb kmslib" -ORBSvcConfDirective "static Resource_Factory -ORBConnectionCacheMax 1024" -ORBEndpoint pbxiop://1556:NB 19978 1536015948517350 -ORBSvcConf /dev/null -ORBSvcConfDirective "static Server Strategy Factory -ORBMaxRecvGIOPPayloadSize 268435456" (Orb.cpp:725)
14:29:16.406 [19978] <2> vnet_cached_gethostbyname: vnet hosts.c.307: found host in cache: felix.min.veritas.com
14:29:16.406 [19978] <2> vnet_cached_gethostbyaddr_rnl: vnet hosts.c.506: found IP in cache: 127.0.0.1
14:29:16.460 [19978] <2> db_error_add_to_file: dberror.c:midnite = 1205730000
14:29:16.461 [19978] <16> get_encryption_key: NBKMS failed with error status: Key group does not have an active key (1227)
14:29:16.462 [19978] <2> send_MDS_msg: MEDIADB 1 42 JRO111 4000007 *NULL* 6 1205781805 1205782033 1206991633 0 64 2 2 1 4 0 8193 1024 0 8 0

```

What does this error look like in the activity monitor?

Figure 6-11 shows that a status code 83 - media open error message returned.

Figure 6-11 Activity monitor with status code 83

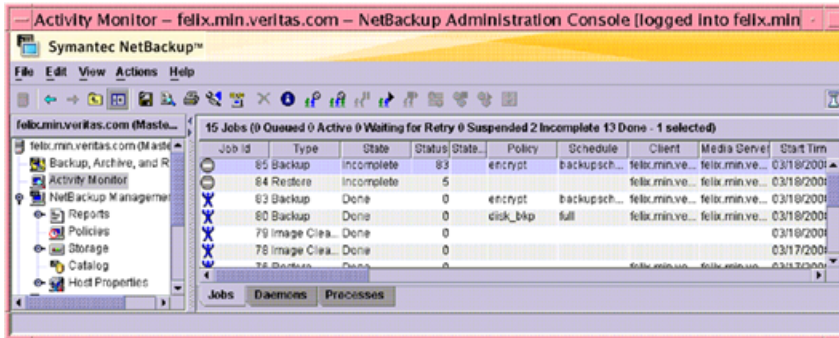


Figure 6-12 shows the detailed status. You can see a message stating that nbk<sub>sm</sub> failed with error status key group does not have an active key (1227). With the information in the previous diagnostics, you can determine the particular problem or to identify what a given problem is related to.

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

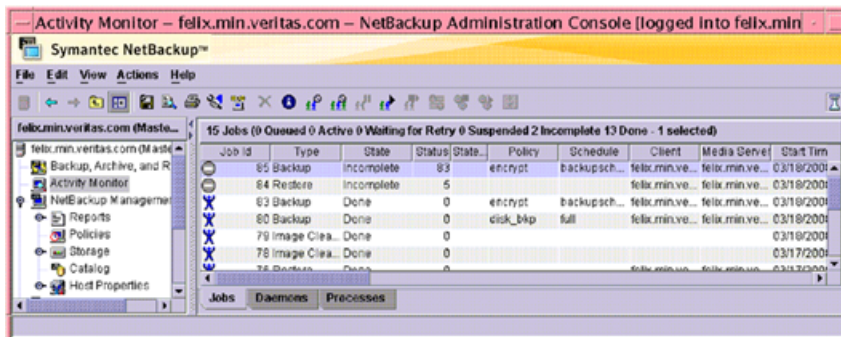
```

14:53:48.782 [21109] <2> io_read_backup_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
[c7fac3d0d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d]
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 : pbxiopt://1556:NB_21109_1537488329610200.(Orb.cpp:618)
14:53:48.798 [21109] <2> Orb::init: initializing ORB kmslib with: kmslib -ORBSvcConfDirective "-"
ORB DottedDecimalAddresses "" -ORBSvcConfDirective "static PBXIOF_Factory" -ORBSvcConfDirective "static
EndpointSelectorFactory" -ORBSvcConfDirective "static Resource_Factory" -ORBProtocolFactory PBXIOF_Factory" -
ORBSvcConfDirective "static Resource_Factory" -ORBProtocolFactory IOF_Factory" -ORBSvcConfDirective "static
PBXIOF_Evaluator_Factory" -orb kmslib" -ORBSvcConfDirective "static Resource_Factory" -ORBConnectionCacheMax 1024
" -ORBEndpoint pbxiopt://1556:NB_21109_1537488329610200 -ORBSvcConf /dev/null -ORBSvcConfDirective "static
Server_Strategy_Factory" -ORBMaxRecvGPOPayloadSize 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:midnote = 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 232, 234
- 56-bit DES key
  - library 235

## A

- About
  - KMS 259
- about
  - ports 95
- Access Control
  - nbac\_cron.exe 162
- access control
  - host properties 148
  - individual users
    - description 195
  - nbac\_cron utility 162
  - user groups
    - Administrator 198
    - configuring 199
    - Default User 198
    - description 196
    - KMS Administrator 199
    - Operator 198
    - renaming user groups 200
    - SAN Administrator 198
    - Security Administrator 198
    - Vault Operator 199
- access control host properties dialog
  - for client 152
- Access Management
  - utility 194
- access management
  - troubleshooting guidelines 155
- accessing
  - client host properties 152
- active
  - key record state 278
- adding a new user
  - to the user group 203

- administration
  - media server encryption 255
  - NetBackup access management 126
- Administrator Access Control user group 198
- all NetBackup security
  - multi-datacenter 88
- all security implemented
  - single datacenter 58
- ALLOWED (encryption option) 237, 245
- alternate client restore (see redirected restore) 242, 251
- Assigned Users pane
  - on the Users tab 203
- assigning a user
  - to a user group 205
- attribute for encryption 231, 243, 251
- authentication
  - port 160
- Authentication Domain
  - tab 150
  - tab for client 153
- authorization objects
  - in NetBackup Administration Console 210
- authorization objects and permissions
  - in the NetBackup Administration Console 206
- authorization port 160
- Authorization Service
  - tab 151
- automatic backup
  - key file 241

## B

- backing up
  - KMS database files 279
- backing up problems
  - KMS data files 281
- backup
  - choosing encryption 231
- backup with no active key record
  - troubleshooting example 300

- backups
  - KMS keystore and administrator keys 290
- backups not encrypting
  - solution 300
- best practices
  - for key file restoration 241
- bp.conf
  - port usage settings in the NetBackup configuration 114
- bpcd 234
  - terminating 254
- BPCD connect-back
  - options 110
- bpclient command
  - specifying 115
- bpinst command 233–234
  - for setting encryption attribute (legacy) 252
  - pushing configuration to clients (legacy) 246
- bpkeyfile command
  - change\_netbackup\_pass\_phrase option 250
  - changing key file pass phrase 254
  - introduction (standard) 233–234
  - managing the key file (legacy) 249
- bpkeyutil command
  - adding pass phrases 238
  - creating the key file 240
  - introduction 232
  - managing the key file 238
  - redirected restore 242, 251
  - standard restore introduction 233
- BUAndRest authorization object
  - permissions 216

## C

- changing
  - client encryption settings from the server 243
  - client legacy encryption settings 252
- checksum of DES key
  - explanation
    - legacy encryption 233
    - legacy restore 235
    - standard encryption 232
    - standard restore 234
- choosing encryption
  - for a backup 231
- cipher types 260
- class
  - see policy 243, 251
- CLI
  - usage help 291
- client
  - access control host properties dialog 152
  - outgoing ports 101
- client encryption settings
  - changing 243
- client legacy encryption settings
  - changing 252
- client side encryption
  - multi-datacenter 71
  - security 31
  - single datacenter 49
- client verification points
  - for a mixed Windows master server 183
  - for Windows 192
- clients
  - configuring standard encryption 236
- clustered environments
  - additional key file security (legacy) 253
  - managing the key file (legacy) 249
  - managing the key file (standard) 238
  - pushing configuration (legacy) 247
  - pushing software (standard) 248
- cnpp option 250
- Combined world, enterprise, and data center levels 25
- command line interface (CLI)
  - commands 290
- command usage
  - conventions 134
- commands
  - command line interface (CLI) 290
- comparison
  - encryption options 229
- configuration
  - and clustering (legacy) 244
  - and clustering (standard) 239
  - options (legacy) 245
  - pushing to clients (legacy) 246
- configuring
  - clients for encryption
    - from client (standard) 242
    - from server (legacy) 246
    - from server (standard) 239
  - KMS 272
  - legacy encryption 243
  - legacy encryption from the server 244
  - ports 109

- configuring (*continued*)
  - standard encryption
    - on clients 236
  - standard encryption from the server 239
- configuring access control
  - for NetBackup pre-7.0 media server and client machines 144
- configuring access control host properties
  - manually 145
- configuring NetBackup
  - to work with KMS 283
- configuring port usage client attribute settings
  - bpclient command 115
- considerations
  - key record state 277
- controls users in user groups
  - Users tab 201
- create
  - new key 292
  - new key group 292
- creating
  - empty KMS database 289
  - encryption key files
    - on clients notes 239
  - key database 273
  - key file 240
  - key groups 275
  - key record 282
  - key records 275
  - new user group 199
    - by copying an existing user group 200
- CRYPT option 252
- CRYPT\_CIPHER option 238
- CRYPT\_KEYFILE option 233–234, 246, 249
- CRYPT\_KIND option 237, 245
- CRYPT\_LIBPATH option 246
- CRYPT\_OPTION 231, 237, 245–246
- CRYPT\_STRENGTH option 234, 245–246

## D

- Daemon connection port
  - options 110
- data at rest encryption
  - limitations 226
  - options 229
  - terminology 226
- database constituents
  - KMS 288

- datacenter
  - multi 39
  - single 39
- datacenter-level
  - security 20
- decryption
  - of key file (legacy) 253
  - overview (legacy) 234
  - overview (standard) 233
- deduplication hosts
  - and firewalls 103
- deduplication port usage
  - about 103
- default
  - port numbers
    - NetBackup 97
- Default User Access Control user group 198
- default user groups
  - NetBackup 197
- Defined Users pane
  - on the Users tab 202
- defining
  - user group and users 203
- definition
  - key groups and key records 274
- delete
  - key 295
  - key group 295
- DENIED (encryption option) 237, 245
- deprecated
  - key record state 278
- DES
  - key checksum 233–235
  - key checksum for standard encryption 232
- details
  - key groups 294
  - keys 294
- DevHost authorization object
  - permissions 220
- disable
  - random port assignments 109
- disabling the monitoring
  - KMS service 272
- DiskPool authorization object
  - permissions 215
- display
  - HMK ID 297
  - KPK ID 297

- drive authorization object
  - permissions 212

## E

- EMM server
  - outgoing ports 100
- enabling cluster use
  - KMS service 271
- enabling the monitoring
  - KMS service 271
- encrypted backup
  - restoring (legacy) 251
  - restoring (standard) 242
- encrypted backup file
  - restoring to another client 242
- encrypted tape
  - reading 265
  - writing 264
- encryption
  - allow
    - deny. *See* require
  - attribute
    - setting 243
  - configuration options (legacy) 245
  - configuring from client (standard) 242
  - file containing keys for (legacy) 246
  - kind
    - defining (legacy) 245
    - defining (standard) 237
  - legacy
    - prerequisites 232
    - prerequisites for restoring 234
    - tar header 235
  - libraries
    - defining (legacy) 246
  - managing from client (standard) 237
  - of key file (legacy) 253
  - overview (legacy) 234
  - overview (standard) 233
  - policy attribute for
    - how to set 231, 243, 251
  - security questions 229
  - standard
    - prerequisites for restoring 233
    - tar header 234
  - strength
    - defining (legacy) 245
  - tar header
    - legacy 233

- encryption (*continued*)
  - tar header (*continued*)
    - standard 232
    - using KMS 286
    - what is and isn't encrypted (legacy) 233
    - what is and isn't encrypted (standard) 232
- Encryption attribute
  - in policies 251
- encryption backup
  - running 231
- encryption options
  - comparison 229
- encryption security
  - installation prerequisites 235
- enterprise level
  - security 18
- example
  - running an encrypted tape backup 287
  - setting up NetBackup to use tape encryption 284
  - verifying an encryption backup 287

## F

- fat client authorization object
  - permissions 221
- fat server authorization object
  - permissions 221
- firewall connect options
  - on a NetBackup server or client 110
  - specifying for a source computer to apply to
    - specific destination computers 113
- firewall connection options
  - on Media Manager 116
- firewall considerations 104
- firewall environment
  - NDMP 118
- firewall problems
  - when using NetBackup with other products 118
- firewalls and deduplication hosts 103

## G

- General tab
  - contains name of user group 201
- granting
  - permissions 208

## H

- HMK and KPK
  - updating 290

- HMK ID
  - display 297
- host master key (HMK)
  - modify 296
- host properties
  - access control 148
  - client
    - accessing 152
  - master server and media server 148
- HostProperties authorization object
  - permissions 218

**I**

- ICMP
  - pinging NDMP 118
- identify
  - KPK and HMK 289
- importing
  - KMS encrypted images 288
- inactive
  - key record state 278
- individual users
  - description 195
- installation
  - on server for push to client 235
  - pushing configuration to clients (legacy) 246
  - pushing pass phrases to clients (legacy) 247
- installation prerequisites
  - for encryption security 235
- installing
  - KMS 267
    - with HA clustering 270
- installing encryption
  - locally on a NetBackup UNIX client 236
  - locally on a NetBackup Windows client 236
  - on a UNIX NetBackup server 235
  - on a Windows NetBackup server 236

**J**

- Java console
  - outgoing ports 102
- job authorization object
  - permissions 216

**K**

- key
  - delete 295
  - recover 296

- key attributes
  - modify 293
- key creation
  - options 298
- key database
  - creating 273
- key file 232–234
  - automatic backup 241
  - backing up (legacy) 250
  - bpkeyutil command 238
  - creating (legacy) 249
  - creating (standard) 240
  - defining (legacy) 246
  - encrypting (legacy) 249
  - encrypting with admin's pass phrase (legacy) 253
  - encrypting with admin's pass phrase (standard) 238
  - explanation (legacy) 247
  - for redirected restore (standard) 242, 251
  - in a cluster (legacy) 249, 253
  - in a cluster (standard) 238
  - legacy 233
  - managing (standard) 238
  - pass phrase (legacy) 254
- key file pass phrase protection
  - manual retention 241
- key file restoration
  - best practices 241
- key files
  - creating
    - on clients notes 239
- key group
  - delete 295
- key group attributes
  - modify 293
- key groups
  - creating 275
  - details 294
- key groups and key records
  - definition 274
- Key Management Service (KMS)
  - about 259
- key protection key (KPK)
  - modify 297
- key record
  - creating 282
- key record state
  - active 278
  - considerations 277

- key record state *(continued)*
  - deprecated 278
  - inactive 278
  - prelive 278
  - terminated 279
- key record states
  - overview 276
- key records
  - creating 275
- keys
  - details 294
  - listing 283
- keystore
  - statistics 297
- KMS
  - configuring 272
  - configuring NetBackup to work with 283
  - considerations 259
  - database constituents 288
  - installing 267
    - with HA clustering 270
  - NetBackup and key records 283
  - principles of operation 263
  - recovering
    - by restoring all data files 280
    - by restoring only KMS data file 280
    - regenerating the data encryption key 280
  - terminology 265
  - troubleshooting 299
  - using for encryption 286
  - with NBAC 270
- KMS Administrator Access Control user group 199
- KMS data files
  - problems backing up 281
  - solutions for backing up 282
- KMS database
  - creating an empty one 289
  - quiesce 298
  - unquiesce 298
- KMS database files
  - backing up 279
- KMS encrypted images
  - importing 288
- Kms group authorization object
  - permissions 223
- KMS keystore and administrator keys
  - backups 290
- KMS service
  - disabling the monitoring 272

- KMS service *(continued)*
  - enabling cluster use 271
  - enabling the monitoring 271
  - removing from monitored list 272
- KPK ID
  - display 297
- KPK ID and HMK ID
  - importance 289

## L

- legacy encrypted backup created on another client
  - restoring 251
- legacy encryption
  - backup process 232
  - configuring 243
  - managing 248
- legacy encryption attribute
  - setting in policies 251
- legacy encryption configuration
  - pushing to clients 246
- legacy encryption configuration options
  - managing 245
- legacy encryption from the server
  - configuring 244
- legacy encryption pass phrases
  - pushing to clients 247
- legacy key file security
  - for UNIX clients 252
- libraries
  - defining for encryption (legacy) 246
- license authorization object
  - permissions 218
- limitations
  - data at rest encryption 226
- list of NetBackup authorization objects
  - Permissions tab 206
- listing
  - keys 283
- logging on
  - as new user 205

## M

- managing
  - clients for encryption
    - from client (standard) 237
  - key file (standard) 238
  - legacy encryption configuration options 245
  - legacy encryption key files 248

- managing *(continued)*
  - NetBackup encryption key file 238
  - standard encryption configuration options 237
- managing key file (legacy) 249
- manually configuring
  - access control host properties 145
- master server
  - outgoing ports 98
- Master server and media server
  - host properties 148
- master server settings
  - verifying 157
- master server verification points
  - for a mixed UNIX master server 175
  - for a mixed Windows master server 181
  - for Windows 186
- master, media server, and GUI security
  - NBAC 33
- media authorization object
  - permissions 211
- Media Manager
  - firewall connection options 116
- media manager configuration
  - random port assignments 109
- media server
  - outgoing ports 99
- media server encryption
  - administration 255
  - option 2 254
- Media Server Encryption Option (MSEO)
  - security 30
  - single datacenter 46
  - with multi-datacenter 66
- media server verification points
  - for a mixed UNIX master server 175
  - for a mixed Windows master server 181
  - for Windows 190
- mixed UNIX master server
  - master server verification points 175
  - media server verification points 175
- mixed Windows master server
  - client verification points 183
  - master server verification points 181
  - media server verification points 181
- modify
  - host master key (HMK) 296
  - key attributes 293
  - key group attributes 293
  - key protection key (KPK) 297

- multi-datacenter 39
  - with all NetBackup security 88
  - with client side encryption 71
  - with Media Server Encryption Option (MSEO) 66
  - with NBAC complete 82
  - with NBAC on master and media servers 76
  - with standard NetBackup 62

## N

- name of user group
  - on the General tab 201
- NBAC
  - configuration 127
  - configuration overview 128
  - configure command 134
  - configuring 127
    - on a clustered master server 130
    - on media servers 131
    - on standalone master servers 129
  - master, media server, and GUI security 33
  - upgrading 139
- NBAC complete
  - multi-datacenter 82
  - security 35
  - single datacenter 55
- NBAC on master and media servers
  - multi-datacenter 76
  - single datacenter 51
- nbac\_cron utility 162
- nbac\_cron.exe 162
- NBU security
  - workgroup 39
- NBU\_Admin Access Control user group 198
- NBU\_Catalog authorization object
  - permissions 213
- NBU\_KMS Admin Access Control user group 199
- NBU\_Operator Access Control user group 198
- NBU\_Security Admin Access Control user group 198
- NBU\_User Access Control user group 198
- NDMP
  - in firewall environment 118
- NetBackup
  - components
    - used in security 20
  - default user groups 197
  - determining access 195
  - ports 95
  - security
    - all 36



- NetBackup *(continued)*
  - security *(continued)*
    - implementation levels 16
    - security implementation types 26
    - security vulnerabilities 28
- NetBackup Access Control (NBAC)
  - components 20
  - individual users 195
  - nbac\_cron utility 162
  - nbac\_cron.exe 162
  - user groups 196
    - Administrator 198
    - configuring 199
    - Default User 198
    - KMS Administrator 199
    - Operator 198
    - renaming user groups 200
    - SAN Administrator 198
    - Security Administrator 198
    - Vault Operator 199
  - using 123
- NetBackup access management
  - administration 126
- NetBackup Administration Console
  - authorization objects 210
  - authorization objects and permissions 206
- NetBackup and key records
  - KMS 283
- NetBackup Authentication and Authorization
  - troubleshooting topics 156
- NetBackup client encryption
  - option 1 230
- NetBackup legacy encryption
  - restore process 234
- NetBackup Management infrastructures
  - unifying with the setuptrust command 146
- NetBackup security
  - standard 29
- NetBackup Service Layer (NBSL) 108
- NetBackup standard encryption
  - restore process 233
- NetBackup UNIX client
  - installing encryption 236
- NetBackup user groups
  - viewing specific user permissions 209
- NetBackup Windows client
  - installing encryption 236
- Network Settings
  - tab 149, 154

- new key
  - create 292
- new key group
  - create 292
- new user
  - logging on 205
- new user group
  - creating 199
    - by copying an existing user group 200

## O

- operating system
  - security 28
- Operator Access Control user group 198
- option 1
  - NetBackup client encryption 230
- option 2
  - media server encryption 254
- options
  - BPCD connect-back 110
  - daemon connection port 110
  - data at rest encryption 229
  - key creation 298
  - ports 110
- outgoing ports
  - client 101
  - EMM server 100
  - Java console 102
  - master server 98
  - media server 99
  - Windows administration console and Java server 101
- overriding or modifying
  - port numbers 95
- overview
  - key record states 276
  - of legacy encryption backup 232
  - of legacy restore 234
  - of standard encryption backup 232
  - of standard restore 233

## P

- pass phrase
  - for encrypting key file (legacy) 249, 253
  - for redirected restore (legacy) 251
  - for redirected restore (standard) 242
  - pushing to clients (legacy) 247
- passphrase\_prompt option 247

- passphrase\_stdin option 247
- permissions
  - BUAndRest authorization object 216
  - DevHost authorization object 220
  - DiskPool authorization object 215
  - Drive authorization object 212
  - fat client authorization object 221
  - fat server authorization object 221
  - granting 208
  - HostProperties authorization object 218
  - job authorization object 216
  - Kms group authorization object 223
  - license authorization object 218
  - media authorization object 211
  - NBU\_Catalog authorization object 213
  - policy authorization object 211
  - report authorization object 213
  - robot authorization object 214
  - security authorization object 220
  - server group authorization object 222
  - service authorization object 217
  - StorageUnit authorization object 214
  - vault authorization object 222
  - volume group authorization object 219
  - VolumePool authorization object 219
- Permissions tab
  - contains list of NetBackup authorization objects 206
- pinging NDMP
  - ICMP 118
- policy authorization object
  - permissions 211
- port numbers
  - about overriding or modifying 95
  - backup and archive products 105
  - default for NetBackup 97
  - HTTP 106
  - HTTPS 106
  - key OpsCenter components 104
- port usage
  - and deduplication 103
- port usage settings in the NetBackup configuration
  - bp.conf 114
- port usage-related Media Manager configuration settings
  - vm.conf 116
- ports
  - about 95
  - authentication 160

- ports *(continued)*
  - authorization 160
  - configuring 109
  - NetBackup 95
  - options 110
- prelive
  - key record state 278
- pushing
  - configuration to clients (legacy) 246
  - legacy encryption pass phrases to clients 247
  - pass phrases to clients (legacy) 247
- pushing the legacy encryption configuration to clients 246

## Q

- quiesce
  - KMS database 298

## R

- random port assignments
  - disable 109
  - in media manager configuration 109
- reading
  - encrypted tape 265
- recover
  - key 296
- recovering
  - KMS
    - by restoring all data files 280
    - by restoring only KMS data file 280
    - regenerating the data encryption key 280
- redirected restore
  - of other client's backup (legacy) 251
  - of other client's backup (standard) 242
  - preventing (legacy) 248
- redirected restores
  - for an encrypted backup file 242
  - of legacy encrypted files 251
- removing from monitored list
  - KMS service 272
- report authorization object
  - permissions 213
- REQUIRED (encryption option) 237, 245
- restore
  - overview (legacy) 234
  - overview (standard) 233
- restore process
  - NetBackup legacy encryption 234

- restore process (*continued*)
  - NetBackup standard encryption 233
- restore with an improper key record state
  - troubleshooting example 304
- restores not decrypting
  - solution 300
- restoring
  - legacy encrypted backup created on another client 251
- robot authorization object
  - permissions 214
- running
  - bpkeyfile command 253
  - encryption backup 231
- running an encrypted tape backup
  - example 287

## S

- security
  - client side encryption 31
  - datacenter-level 20
  - enterprise level 18
  - implementation levels 16
  - Media Server Encryption Option (MSEO) 30
  - NBAC complete 35
  - NetBackup
    - all 36
  - operating system 28
  - world-level 17
- Security Administrator Access Control user group 198
- security authorization object
  - permissions 220
- security implementation types
  - NetBackup 26
- security vulnerabilities
  - NetBackup 28
- server group authorization object
  - permissions 222
- service authorization object
  - permissions 217
- setting encryption attribute
  - in policies 243
- setting up NetBackup to use tape encryption
  - example 284
- setuptrust command
  - unifying NetBackup Management infrastructures 146
  - using 147

- single datacenter
  - with all security implemented 58
  - with client side encryption 49
  - with Media Server Encryption Option (MSEO) 46
  - with NBAC complete 55
  - with NBAC on master and media servers 51
  - with standard NetBackup 43
- SNMP port 108
- solution
  - backups not encrypting 300
  - restores not decrypting 300
- solutions for backing up
  - KMS data files 282
- specifying
  - bpclient command 115
- standard
  - NetBackup security 29
- standard encryption
  - backup process 232
- standard encryption from the server
  - configuring 239
- standard NetBackup
  - with multi-datacenter 62
- statistics
  - keystore 297
- StorageUnit authorization object
  - permissions 214

## T

- tab
  - Authentication Domain 150, 153
  - Authorization Service 151
  - Network Settings 149, 154
- tar header for legacy encryption 233, 235
- tar header for standard encryption 232, 234
- terminated
  - key record state 279
- terminology
  - data at rest encryption 226
- troubleshooting
  - KMS 299
- troubleshooting example
  - backup with no active key record 300
  - restore with an improper key record state 304
- troubleshooting guidelines
  - access management 155
- troubleshooting topics
  - for NetBackup Authentication and Authorization 156

## U

- UNIX
  - verification procedures 165
- UNIX client
  - verification 171
- UNIX clients
  - legacy key file security 252
- UNIX master server
  - verification 166
  - verification points in a mixed environment 173
- UNIX media server
  - verification 169
- UNIX NetBackup server
  - installing encryption 235
- unquiesce
  - KMS database 298
- updating
  - HMK and KPK 290
- Upgrading
  - NBAC 139
- usage help
  - CLI 291
- user group
  - adding a new user 203
  - assigning a user 205
- user group and users
  - defining 203
- user groups
  - Administrator 198
  - Default User 198
  - description 196
  - KMS Administrator 199
  - Operator 198
  - renaming user groups 200
  - SAN Administrator 198
  - Security Administrator 198
  - Vault Operator 199
- Users tab
  - Assigned Users pane 203
  - controls users in user groups 201
  - Defined Users pane 202
- using
  - setuptrust command 147
- utility
  - Access Management 194

## V

- vault authorization object
  - permissions 222

- Vault Operator User Access Control user group 199
- Vault\_Operator Access Control user group 199
- verification
  - UNIX client 171
  - UNIX master server 166
  - UNIX media server 169
- verification points
  - Windows 185
- verification points in a mixed environment
  - with a UNIX master server 173
  - with a Windows master server 178
- verification procedures
  - UNIX 165
- verifying
  - master server settings 157
- verifying an encryption backup
  - example 287
- viewing specific user permissions
  - for NetBackup user groups 209
- vm.conf
  - port usage-related Media Manager configuration settings 116
- volume group authorization object
  - permissions 219
- VolumePool authorization object
  - permissions 219
- VxSS authentication port 160
- VxSS authorization port 160

## W

- Windows
  - client verification points 192
  - master server verification points 186
  - media server verification points 190
  - verification points 185
- Windows administration console and Java server
  - outgoing ports 101
- Windows master server
  - verification points in a mixed environment 178
- Windows NetBackup server
  - installing encryption 236
- workgroup
  - NBU security 39
  - with NetBackup 40
- world-level
  - security 17
- writing
  - encrypted tape 264