

Veritas NetBackup™ Security and Encryption Guide

UNIX, Windows, and Linux

Release 8.0



Veritas NetBackup™ Security and Encryption Guide

Legal Notice

Copyright © 2016 Veritas Technologies LLC. All rights reserved.

Veritas, Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third party software for which Veritas 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. Refer to the third party legal notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

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 Veritas Technologies LLC 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. VERITAS TECHNOLOGIES LLC 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, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. 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.

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

<http://www.veritas.com>

Technical Support

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

<https://www.veritas.com/support>

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

<https://my.veritas.com>

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

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

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

<https://sort.veritas.com/documents>

Documentation feedback

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1	Increasing NetBackup security	12
	About NetBackup security and encryption	13
	NetBackup security implementation levels	13
	World-level security	14
	Enterprise-level security	15
	Datacenter-level security overview	17
	NetBackup Access Control (NBAC)	17
	Combined world, enterprise, and data center levels	22
	NetBackup security implementation types	23
	Operating system security	25
	NetBackup security vulnerabilities	25
	Standard NetBackup security	26
	Media Server Encryption Option (MSEO) security	27
	Client side encryption security	28
	NBAC on master, media server, and graphical user interface security	31
	NBAC complete security	32
	All NetBackup security	33
Chapter 2	Security deployment models	36
	Workgroups	37
	Single datacenters	37
	Multi-datacenters	37
	Workgroup with NetBackup	38
	Single datacenter with standard NetBackup	41
	Single datacenter with Media Server Encryption Option (MSEO)	44
	Single datacenter with client side encryption	47
	Single datacenter with NBAC on master and media servers	49
	Single datacenter with NBAC complete	53
	Single datacenter with all security implemented	56
	Multi-datacenter with standard NetBackup	60
	Multi-datacenter with Media Server Encryption Option (MSEO)	64
	Multi-datacenter with client side encryption	69
	Multi-datacenter with NBAC on master and media servers	74
	Multi-datacenter with NBAC complete	80

	Multi-datacenter with all NetBackup security	86
Chapter 3	Port security	93
	About NetBackup TCP/IP ports	93
	About NetBackup daemons, ports, and communication	95
	Standard NetBackup ports	95
	NetBackup master server outgoing ports	96
	NetBackup media server outgoing ports	97
	NetBackup enterprise media management (EMM) server outgoing ports	98
	Client outgoing ports	99
	Windows administration console and Java server outgoing ports	99
	Java console outgoing ports	100
	About MSDP port usage	101
	About Cloud port usage	101
	Additional port information for products that interoperate with NetBackup	101
	About configuring ports	106
	Enabling or disabling random port assignments	107
	Specifying firewall connection options on a NetBackup server or client	108
	Specifying firewall connection options for destination computers from a source computer	111
	Editing port information in configuration files	113
	Updating client connection options	114
	Updating port settings for the Media Manager in the vm.conf file	114
	Port requirements for NDMP backups	116
	Known firewall problems encountered when using NetBackup with third-party robotic products	116
Chapter 4	Auditing NetBackup operations	118
	About NetBackup auditing	119
	Viewing the current audit settings	121
	Configuring auditing on a NetBackup master server	122
	User identity in the audit report	125
	About Enhanced Auditing	125
	Enabling Enhanced Auditing	126
	Configuring Enhanced Auditing	127
	Connecting to a media server with Enhanced Auditing	127
	Changing a server across NetBackup domains	128

	Configuration requirements if using Change Server with NBAC or Enhanced Auditing	130
	Disabling Enhanced Auditing	131
	Auditing host property changes	131
	Retaining and backing up audit trail records	132
	Viewing the audit report	132
	Using the command line -reason or -r option	137
	nbaudit log behavior	138
	Audit alert notification for audit failures	139
Chapter 5	Access control security	140
	About access control in NetBackup	140
	User management	147
	User authentication	148
	Impact of Access Control via Enhanced Auditing on Java interface authorization	148
Chapter 6	NetBackup Access Control Security (NBAC)	150
	About using NetBackup Access Control (NBAC)	150
	NetBackup access management administration	153
	About NetBackup Access Control (NBAC) configuration	153
	Configuring NetBackup Access Control (NBAC)	154
	NBAC configuration overview	154
	Configuring NetBackup Access Control (NBAC) on standalone master servers	155
	Installing the NetBackup master server highly available on a cluster	156
	Configuring NetBackup Access Control (NBAC) on a clustered master server	157
	Configuring NetBackup Access Control (NBAC) on media servers	158
	Installing and configuring access control on clients	160
	About including authentication and authorization databases in the NetBackup hot catalog backups	160
	NBAC configure commands summary	160
	Unifying NetBackup Management infrastructures with the setuptrust command	165
	Using the setuptrust command	166
	Configuring Access Control host properties for the master and media server	167
	Authentication Domain tab	168
	Authorization Service tab	170

Network Attributes tab	171
Access Control host properties dialog for the client	171
Authentication Domain tab for the client	172
Network Attributes tab for the client	173
Troubleshooting Access Management	174
Troubleshooting NBAC issues	175
Configuration and troubleshooting topics for NetBackup	
Authentication and Authorization	176
Windows verification points	183
UNIX verification points	192
Verification points in a mixed environment with a UNIX master server	199
Verification points in a mixed environment with a Windows master server	205
About the nbac_cron utility	212
Using the nbac_cron utility	212
Using the Access Management utility	214
About determining who can access NetBackup	215
Individual users	216
User groups	216
NetBackup default user groups	218
Configuring user groups	219
About defining a user group and users	221
Viewing specific user permissions for NetBackup user groups	225
Granting permissions	226
Authorization objects	227
Media authorization object permissions	228
Policy authorization object permissions	228
Drive authorization object permissions	229
Report authorization object permissions	230
NBU_Catalog authorization object permissions	230
Robot authorization object permissions	231
Storage unit authorization object permissions	231
DiskPool authorization object permissions	231
BUAndRest authorization object permissions	232
Job authorization object permissions	233
Service authorization object permissions	233
HostProperties authorization object permissions	235
License authorization object permissions	235
Volume group authorization object permissions	235
VolumePool authorization object permissions	236
DevHost authorization object permissions	236
Security authorization object permissions	237

Fat server authorization object permissions	237
Fat client authorization object permissions	238
Vault authorization object permissions	238
Server group authorization object permissions	239
Key management system (kms) group authorization object permissions	239
Upgrading NetBackup Access Control (NBAC)	240
Upgrading NetBackup when an older version of NetBackup is using a root broker installed on a remote machine	240

Chapter 7	Security certificates in NetBackup	246
	Overview of security certificates in NetBackup	246
	Deploying security certificates on NetBackup hosts	247
	About the Security Management utilities	248
	About login activity	250
	Troubleshooting auditing issues related to the Access History tab	251
	About host name-based certificates	251
	Deploying host name-based certificates	251
	About host ID-based certificates	253
	Web login requirements for nbcertcmd command options	254
	Using the Certificate Management utility to issue and deploy host ID-based certificates	255
	About certificate deployment security levels	258
	Automatic host ID-based certificate deployment	260
	Deploying host ID-based certificates	260
	Implication of clock skew on certificate validity	262
	Setting up trust with the master server (Certificate Authority)	263
	Deploying certificates from multiple masters	267
	Forcing or overwriting certificate deployment	267
	Retaining host ID-based certificates when reinstalling NetBackup on non-master hosts	268
	Deploying certificates on a client that has no connectivity with the master server	269
	About host ID-based certificate expiration and renewal	270
	Cleaning host ID-based certificate information from a host before cloning a virtual machine	271
	About reissuing host ID-based certificates	272
	About Token Management for host ID-based certificates	276
	Creating authorization tokens	277
	Deleting authorization tokens	279
	Viewing authorization token details	279

About expired authorization tokens and cleanup	280
About revoking host ID-based certificates	281
Removing trust between a host and a master server	281
Revoking a host ID-based certificate	282
Security certificate deployment in a clustered NetBackup setup	284
About deployment of a host ID-based certificate on a clustered NetBackup host	285
Deploying a host ID-based certificates on inactive master server nodes	287
Deploying a host ID-based certificate on a clustered NetBackup media server (upgrade only)	287
Renewing a host ID-based certificate on a clustered NetBackup host	288
About deploying a new host ID-based certificate	288
Viewing certificate details for a clustered NetBackup setup	290
Removing CA certificates from a clustered NetBackup setup	291

Chapter 8 Data at rest encryption security 292

Data at rest encryption terminology	292
Data at rest encryption considerations	293
Encryption security questions to consider	294
Comparison of encryption options	295
About NetBackup client encryption	296
Installation prerequisites for encryption security	296
About running an encryption backup	297
NetBackup standard encryption restore process	299
NetBackup legacy encryption restore process	300
Configuring standard encryption on clients	301
Managing standard encryption configuration options	301
Managing the NetBackup encryption key file	302
About configuring standard encryption from the server	303
Restoring an encrypted backup file to another client	306
About configuring standard encryption directly on clients	306
Setting standard encryption attribute in policies	307
Changing the client encryption settings from the NetBackup server	307
Configuring legacy encryption on clients	308
About configuring legacy encryption from the client	308
About configuring legacy encryption from the server	312
Restoring a legacy encrypted backup created on another client	315
About setting legacy encryption attribute in policies	315

	Changing client legacy encryption settings from the server	316
	Additional legacy key file security for UNIX clients	316
	Media server encryption	318
Chapter 9	Data at rest key management	320
	Federal Information Processing Standards (FIPS)	320
	About FIPS enabled KMS	321
	About the Key Management Service (KMS)	323
	KMS considerations	324
	KMS principles of operation	328
	About writing an encrypted tape	328
	About reading an encrypted tape	329
	KMS terminology	329
	Installing KMS	331
	Using KMS with NBAC	335
	About installing KMS with HA clustering	335
	Enabling cluster use with the KMS service	336
	Enabling the monitoring of the KMS service	336
	Disabling the monitoring of the KMS service	337
	Removing the KMS service from monitored list	337
	Configuring KMS	337
	Creating the key database	338
	About key groups and key records	339
	Overview of key record states	341
	About backing up the KMS database files	344
	About recovering KMS by restoring all data files	345
	Recovering KMS by restoring only the KMS data file	345
	Recovering KMS by regenerating the data encryption key	345
	Problems backing up the KMS data files	346
	Solutions for backing up the KMS data files	347
	Creating a key record	347
	Listing keys from a key group	347
	Configuring NetBackup to work with KMS	348
	About using KMS for encryption	352
	Example of running an encrypted tape backup	352
	Example of verifying an encryption backup	353
	About importing KMS encrypted images	354
	KMS database constituents	354
	Creating an empty KMS database	354
	Importance of the KPK ID and HMK ID	355
	About periodically updating the HMK and KPK	355
	Backing up the KMS keystore and administrator keys	355

Command line interface (CLI) commands	356
CLI usage help	357
Create a new key group	357
Create a new key	358
Modify key group attributes	358
Modify key attributes	359
Get details of key groups	359
Get details of keys	360
Delete a key group	361
Delete a key	361
Recover a key	361
About exporting and importing keys from the KMS database	362
Modify host master key (HMK)	366
Get host master key (HMK) ID	366
Get key protection key (KPK) ID	366
Modify key protection key (KPK)	366
Get keystore statistics	367
Quiesce KMS database	367
Unquiesce KMS database	367
Key creation options	368
Troubleshooting KMS	368
Solution for backups not encrypting	369
Solution for restores that do not decrypt	369
Troubleshooting example - backup with no active key record	370
Troubleshooting example - restore with an improper key record state	372
Index	374

Increasing NetBackup security

This chapter includes the following topics:

- [About NetBackup security and encryption](#)
- [NetBackup security implementation levels](#)
- [World-level security](#)
- [Enterprise-level security](#)
- [Datacenter-level security overview](#)
- [NetBackup Access Control \(NBAC\)](#)
- [Combined world, enterprise, and data center levels](#)
- [NetBackup security implementation types](#)
- [Operating system security](#)
- [NetBackup security vulnerabilities](#)
- [Standard NetBackup security](#)
- [Media Server Encryption Option \(MSEO\) security](#)
- [Client side encryption security](#)
- [NBAC on master, media server, and graphical user interface 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 13.

See [“NetBackup Access Control \(NBAC\)”](#) on page 17.

See [“Operating system security”](#) on page 25.

See [“Standard NetBackup security”](#) on page 26.

See [“Media Server Encryption Option \(MSEO\) security”](#) on page 27.

See [“Client side encryption security”](#) on page 28.

See [“NBAC on master, media server, and graphical user interface security”](#) on page 31.

See [“NBAC complete security”](#) on page 32.

See [“All NetBackup security”](#) on page 33.

NetBackup security implementation levels

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

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

Table 1-1 NetBackup security implementation levels

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

World-level security

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

Figure 1-1 World-level security scope

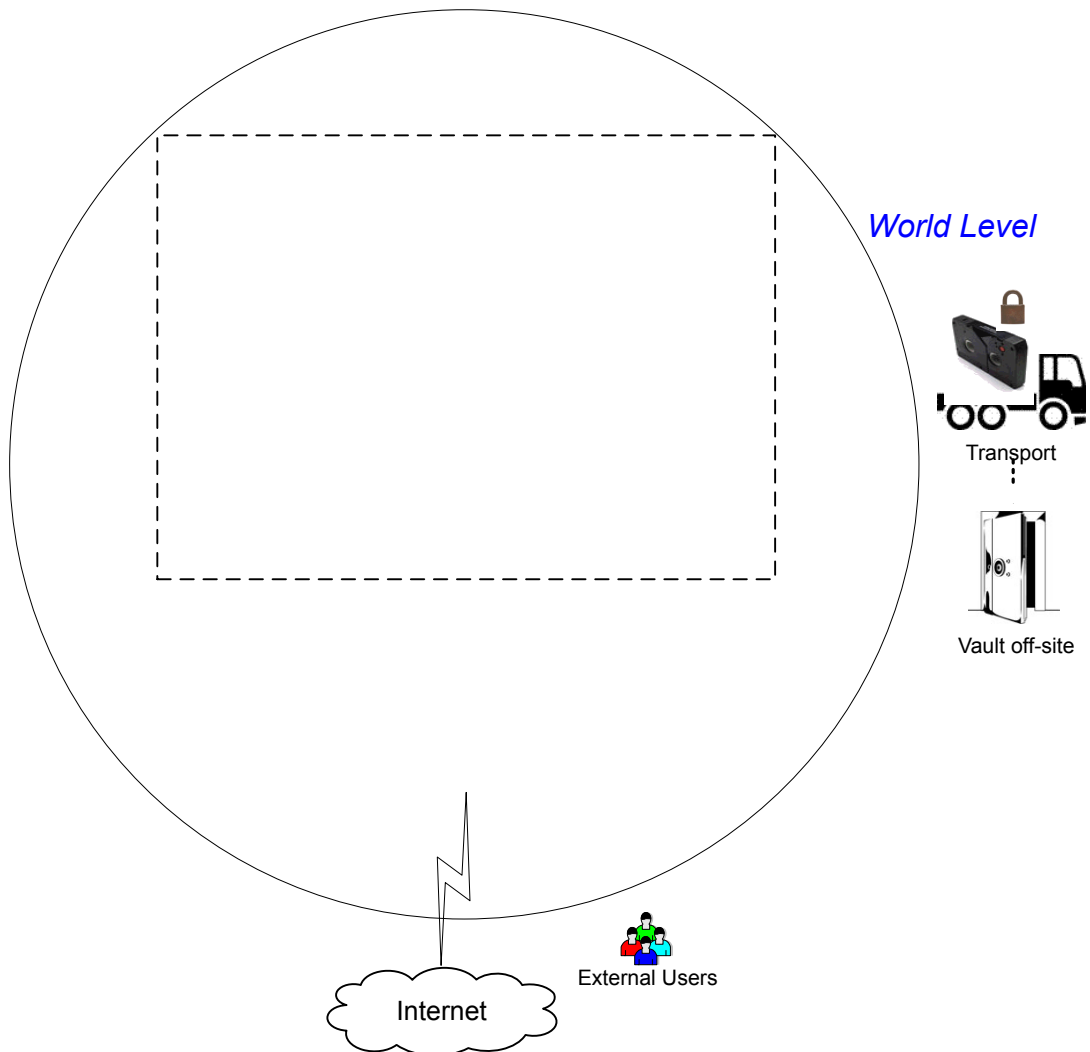


Table 1-2 Types of world-level security

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

Enterprise-level security

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

Figure 1-2 Enterprise-level security scope

Security Overview

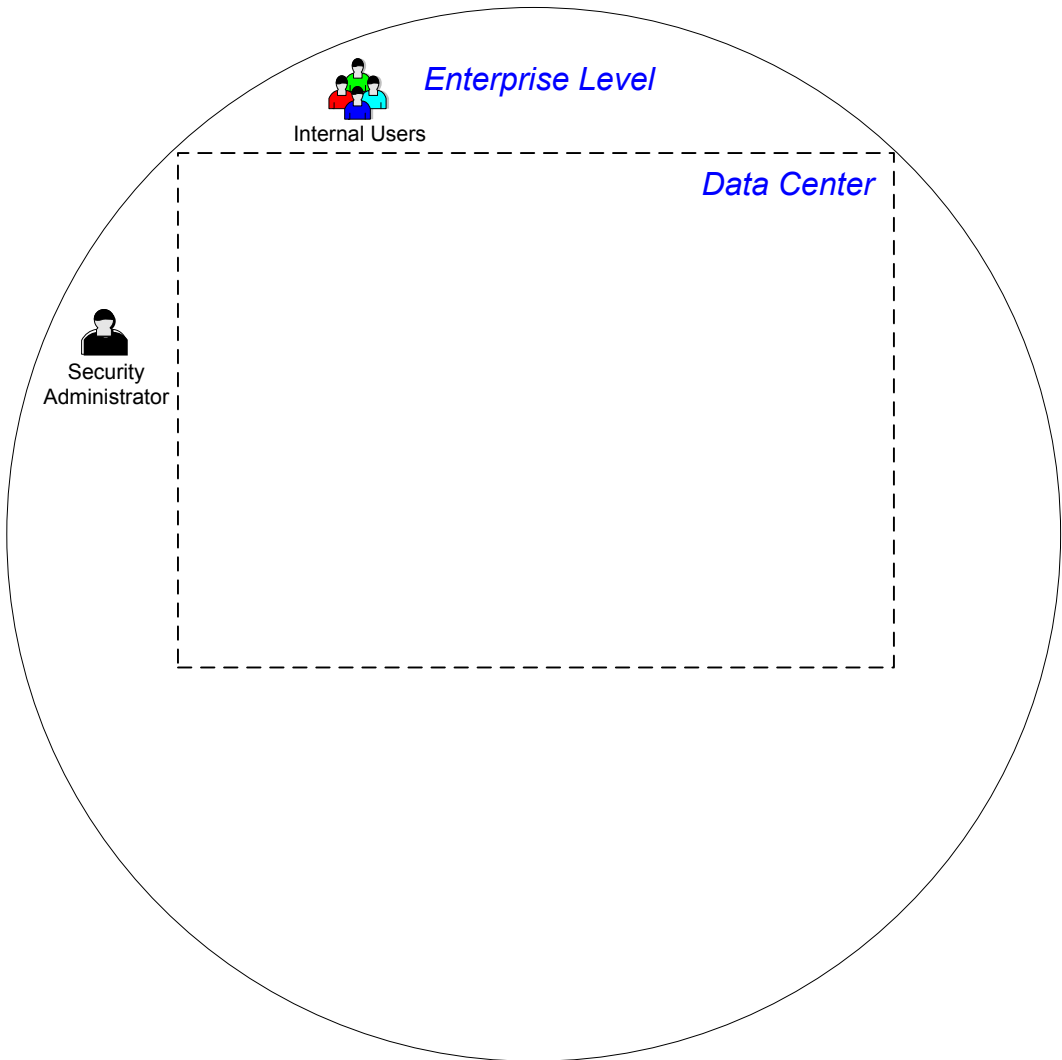


Table 1-3 Types of enterprise-level security

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

Datacenter-level security overview

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

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

Table 1-4 Deployment models for datacenter-level security

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

See [“NetBackup security implementation levels”](#) on page 13.

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 13.

Important points about NBAC include:

- Authentication and Authorization are used together

- NBAC uses authentication identities from a trusted source to reliably identify involved parties. Access decisions can then be made for manipulation of NetBackup based on those identities. Note that NetBackup Security Services are now embedded.
- The NetBackup Product Authentication and Authorization consist of the root broker, authentication broker, authorization engine, and the graphical user interface.
- Oracle, Oracle Archiver, DB2, Informix, Sybase, SQL Server, SAP and EV Migrator are not supported with NBAC.
- NBAC is not supported on Appliances.
- The NetBackup catalog backup is supported with NBAC.

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

Table 1-5 NetBackup components used in security

Component	Description
Root broker	<p>The NetBackup master server is the root broker in a data center installation. There is no provision to use another root broker. The recommendation is to allow trust between root brokers.</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, graphical user interface, and clients by establishing credentials with each one of them. The authentication broker also authenticates a user when operating a command prompt. There can be more than one authentication broker in a data center installation. The authentication broker can be combined with the root broker.</p>
Authorization engine	<p>Communicates with the master server and the media server to determine the permissions of an authenticated user. These permissions determine the functionality available to a given server. The authorization engine also stores user groups and permissions. Only one authorization engine is required in a data center installation. The authorization engine also communicates over the WAN to authorize other media servers in a multi-datacenter environment.</p>
graphical user interface	<p>Specifies a Remote Administration Console that receives credentials from the authentication brokers. The graphical user interface then may use the credentials to gain access to functionality on the clients, media, and master servers.</p>
MSEO	<p>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.</p>

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

Component	Description
Master server	Communicates with the root broker and authentication broker, graphical user interface, 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 data center.
Media server	Communicates with the master server, root broker and authentication broker, authorization engine, MSEO, and clients 1 through 6. The media server writes unencrypted data to tape for client 5 and encrypted data to tape for client 6.
Clients	Specifies that clients 1 through 4 are standard NetBackup types. Client 5 is a web server type located in the DMZ. Client 6 is a client side encrypted type also located in the DMZ. All client types are managed by the master server and have their data backed up to tape through the media server. Clients 5 and 6 communicate to NetBackup using NetBackup only ports through the internal firewall. Client 5 also receives connections from the Internet using HTTP only ports through the external firewall.
Tapes	<p>Specifies that the tape security in NetBackup can be increased by adding the following:</p> <ul style="list-style-type: none"> ■ Client side encryption ■ MSEO (media server Encryption Option) ■ Encryption of data at rest <p>Unencrypted and encrypted data tapes are produced in the data center. The unencrypted tape data is written for clients 1 through 5 and stored on-site at the data center. The encrypted tapes are written for client 6 and are transported off-site to a vault for disaster recovery protection.</p>
Encryption	<p>Specifies that NetBackup encryption can increase security by providing the following:</p> <ul style="list-style-type: none"> ■ Greater data confidentiality ■ The loss of physical tape is not as critical if all the data is effectively encrypted ■ The best risk mitigation strategy <p>For more information about encryption: See “Encryption security questions to consider” on page 294.</p>

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

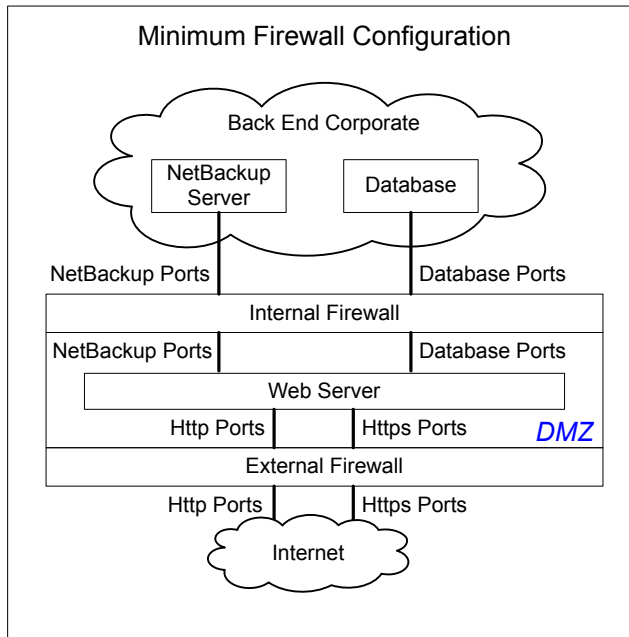
Component	Description
Data over the wire security	<p>Includes the communication between master servers, media servers, clients, and communication using ports through firewalls and over WANs.</p> <p>For more information about ports:</p> <p>See “About NetBackup TCP/IP ports” on page 93.</p> <p>The data over the wire part of NetBackup can help increase security in the following ways:</p> <ul style="list-style-type: none"> ■ NetBackup Access Control (NBAC) ■ Classic NetBackup daemons employ authentication when NBAC is enabled ■ CORBA daemons use the fully encrypted channels that support confidentiality, and provide data integrity ■ Firewalls ■ Disabling the unused ports in NetBackup and in other products: See “Enabling or disabling random port assignments” on page 107. ■ PBX and VNETD dedicated ports provide increased NetBackup security ■ Central set of ports to monitor and open through firewalls
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"> ■ Veritas recommends the use of firewall and intrusion detection protection for NetBackup ■ Firewall protection relates to general network security from a NetBackup standpoint. It focuses on reducing the possible "door locks" for a thief to try and pick. It might make sense to review the possibility of blocking NFS, telnet, FTP, email, etc., ports. They are not strictly needed for NetBackup use and can provide an "open door" for unwanted access. ■ Secure the master server as much as possible ■ Firewalls can include internal firewalls and external firewalls, as follows: <ul style="list-style-type: none"> ■ Internal firewall - allows NetBackup to access web server client 5 and encrypted client 6 in the DMZ. Only selected NetBackup ports and possibly other application ports are enabled for data communication through the internal firewall and into and out of the DMZ. The HTTP ports are open in the External Firewall and are not allowed to pass through the internal firewall. ■ External firewall - allows external users to access the web server client 5 located in the DMZ from the Internet over HTTP ports. NetBackup ports are open for web server client 5 to communicate through the internal firewall to NetBackup. The NetBackup ports are not allowed to pass through the external firewall to the Internet. Only the HTTP ports of web server client 5 can pass through the external firewall to the Internet.

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

Component	Description
Demilitarized zone (DMZ)	<p>Specifies that the demilitarized zone (DMZ) increases security as follows:</p> <ul style="list-style-type: none"> ■ The DMZ is a restricted area in which the number of ports that are allowed for specific hosts is highly controlled ■ The DMZ exists between the external firewall and the internal firewall. The common area in this example is the web server. The external firewall blocks all ports except for the HTTP (standard) and HTTPS (secure) web ports. The internal firewall blocks all ports except for NetBackup and database ports. The DMZ eliminates the possibility of external Internet access to internal NetBackup server and database information. <p>The DMZ provides a "safe" area of operation for the web server client 5 and encrypted client 6 between the internal firewall and external firewall. The web server client 5 in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports. The web server client 5 can also communicate through the external firewall to the Internet using only HTTP ports.</p> <p>Figure 1-3 shows an example internal and external firewall with DMZ.</p>

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

Figure 1-3 Example firewalls and DMZ

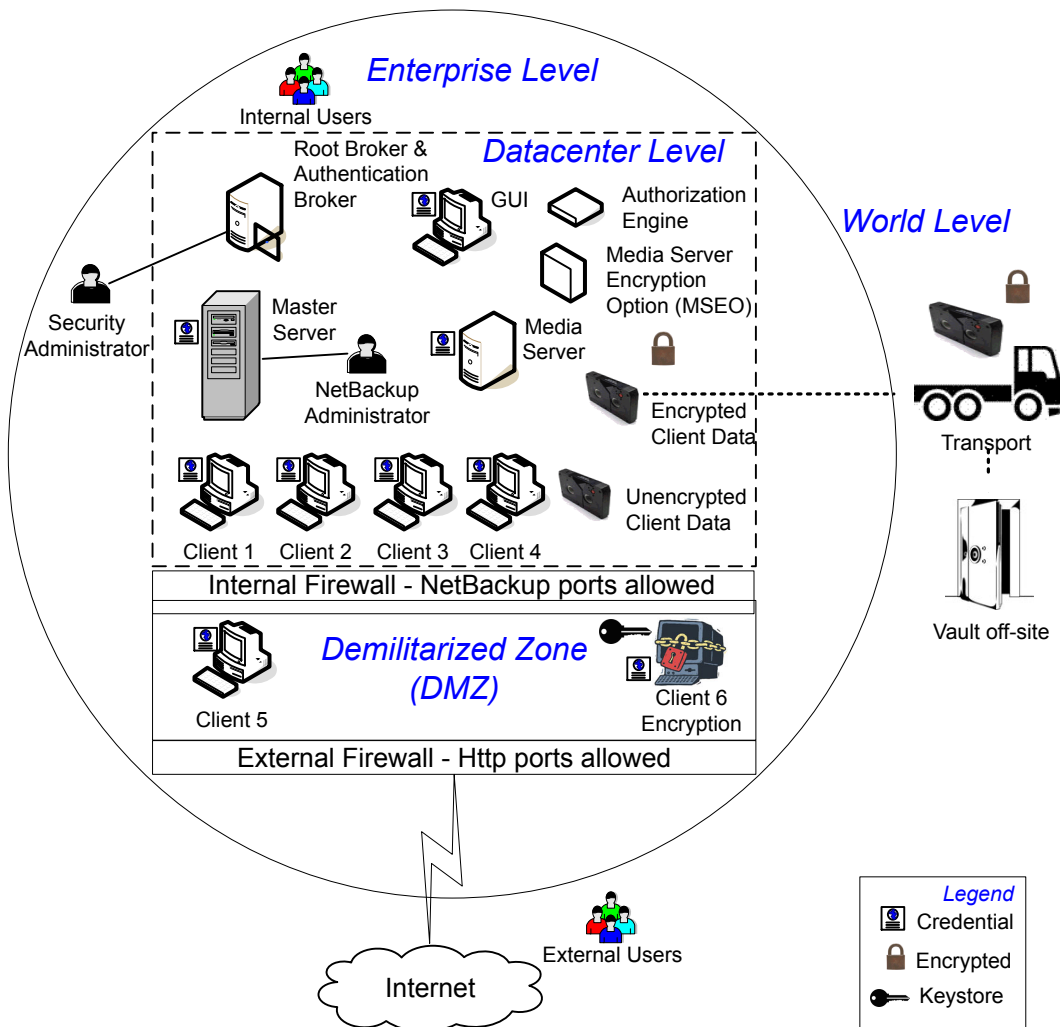


Combined world, enterprise, and data center levels

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

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

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



NetBackup security implementation types

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

Table 1-6 Security implementation types

Security implementation type	Characteristics	Complexity	Security deployment models
See “Operating system security” on page 25.	<ul style="list-style-type: none"> ■ Operating system dependent ■ Varies based on system components 	Variable	Workgroup Single data center Multi-datacenter
See “Standard NetBackup security” on page 26.	<ul style="list-style-type: none"> ■ Manage as root or administrator ■ Data is not encrypted 	Low	Workgroup with NetBackup Single data center with standard NetBackup Multi-datacenter with standard NetBackup
See “Media Server Encryption Option (MSEO) security” on page 27.	<ul style="list-style-type: none"> ■ Media server encryption ■ Client to media server traffic is not encrypted ■ May affect CPU performance on the media server ■ Location of keys 	Low	Single data center with media server Encryption Option (MSEO) Multi-datacenter with media server Encryption Option (MSEO)
See “Client side encryption security” on page 28.	<ul style="list-style-type: none"> ■ Data is encrypted on the client ■ Encrypted data is sent over the wire ■ Can affect CPU performance on the client ■ Location of keys 	Medium	Single data center with client side encryption Multi-datacenter with client side encryption
See “NBAC on master, media server, and graphical user interface security” on page 31.	<ul style="list-style-type: none"> ■ NBAC gives authorization to access master and media servers ■ Authenticates the system and users to access master and media servers 	Medium	Single data center with NBAC on master and media servers Multi-datacenter with NBAC on master and media servers
See “NBAC complete security” on page 32.	<ul style="list-style-type: none"> ■ NBAC gives authorization throughout the system ■ NBAC gives authentication throughout the entire system (servers, clients, and users) 	High	Single data center with NBAC complete Multi-datacenter with NBAC complete

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

Security implementation type	Characteristics	Complexity	Security deployment models
See “All NetBackup security” on page 33.	<ul style="list-style-type: none">■ Incorporates all NetBackup security types■ The example diagrams and documentation employ all security mechanisms together	Very High	Single data center 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 the upgrades applied to the operating system to keep it running at the highest level of system integrity. Upgrades and patches should be kept at the level that is specified by the vendor.
- Following safe firewall procedures
- Employing least privilege administration
- Limiting root users
- Applying the security protocol over IP (IPSEC) hardware
- Turning off unused ports of the outward facing applications
- Providing a secure base on which to run NetBackup
- Adding a first line of intelligence in an investigation to determine if the operating system has been compromised
- Making sure that security implementation is the same for all operating systems
- Adding full interoperability between various systems using NBAC in a heterogenous environment

NetBackup security vulnerabilities

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

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

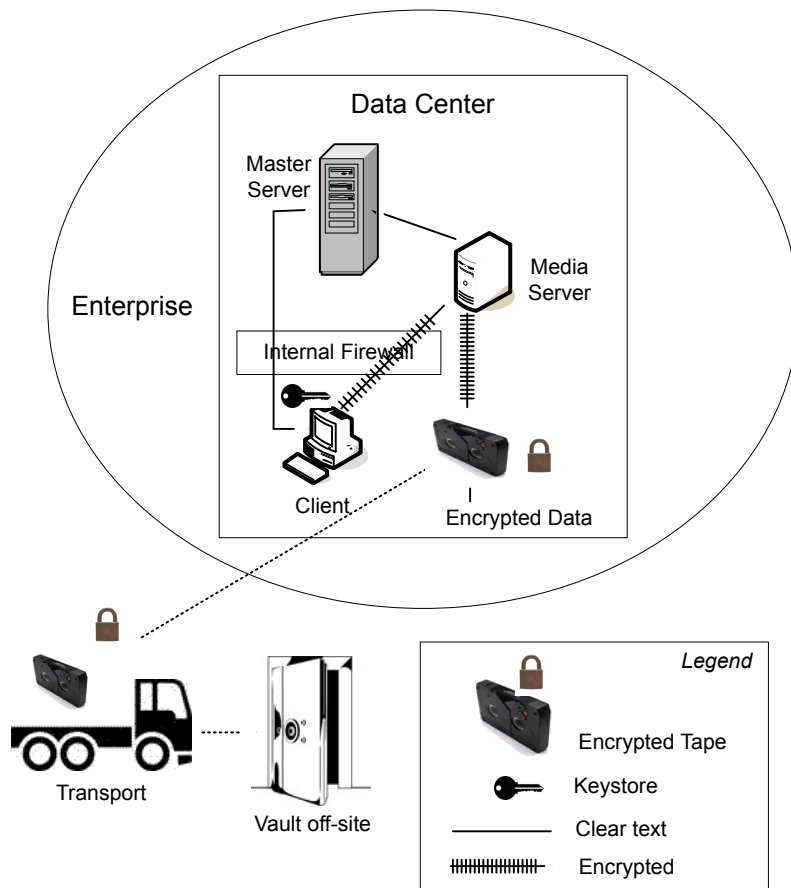
- The importance of accumulative NetBackup updates
- Use the Veritas website for information on possible security vulnerability issues:
https://www.veritas.com/content/support/en_US/security.html, or
<http://www.veritas.com/security>
- Use email contacts for possible security vulnerability issues:
secure@veritas.com

Standard NetBackup security

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

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

Figure 1-5 Standard NetBackup

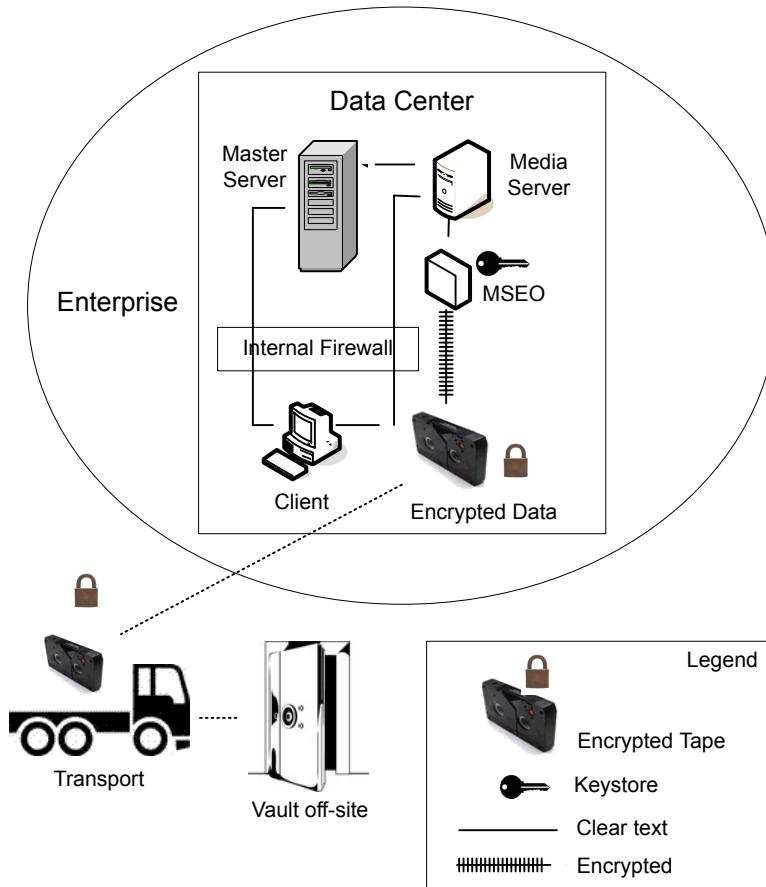


Media Server Encryption Option (MSEO) security

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 data center. 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 accessed in the future.

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. You cannot select the encryption check box in the policy attributes interface for these policy types.

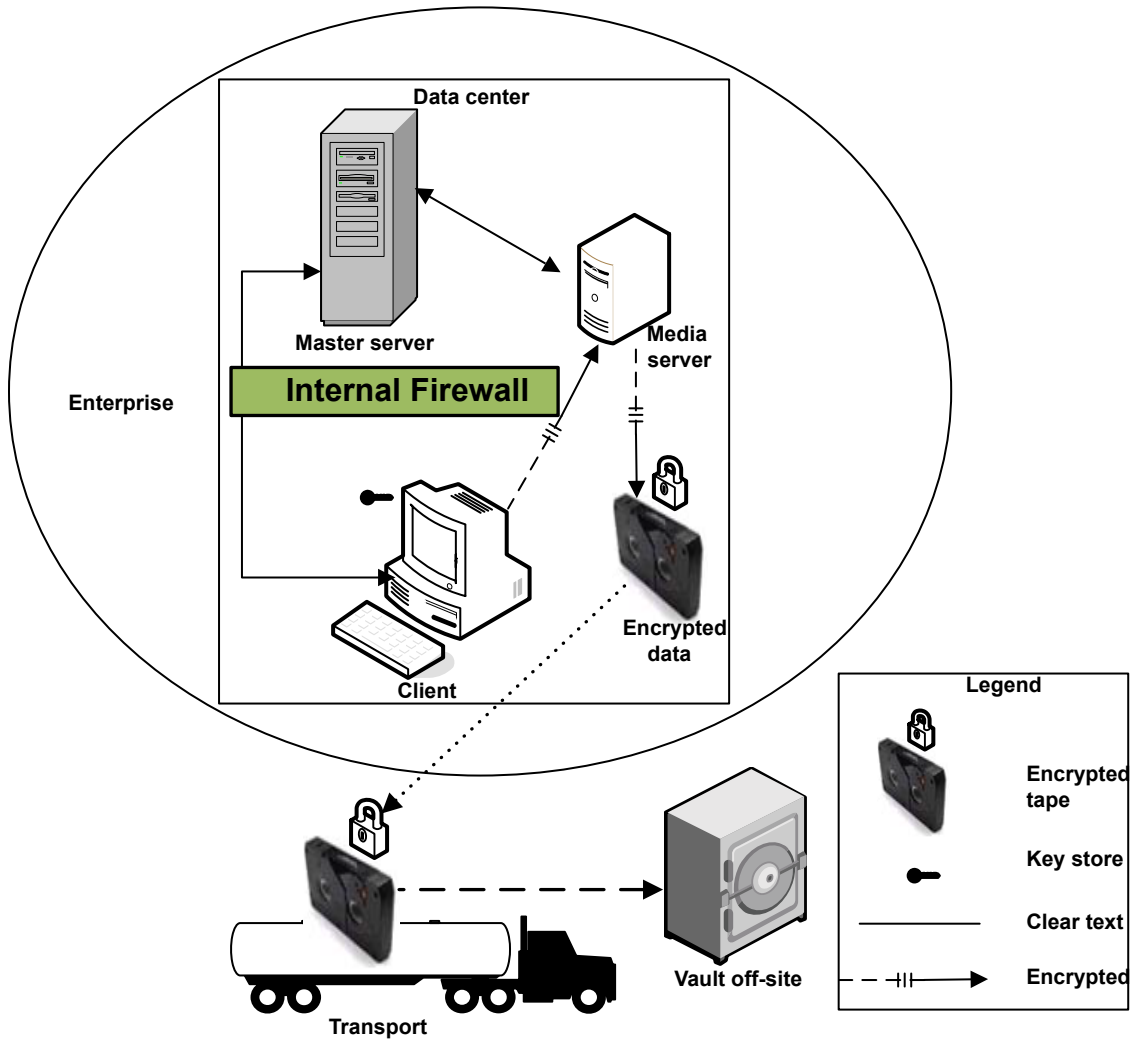
- FlashBackup
- FlashBackup-Windows
- NDMP
- NetWare
- OS/2
- Vault

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

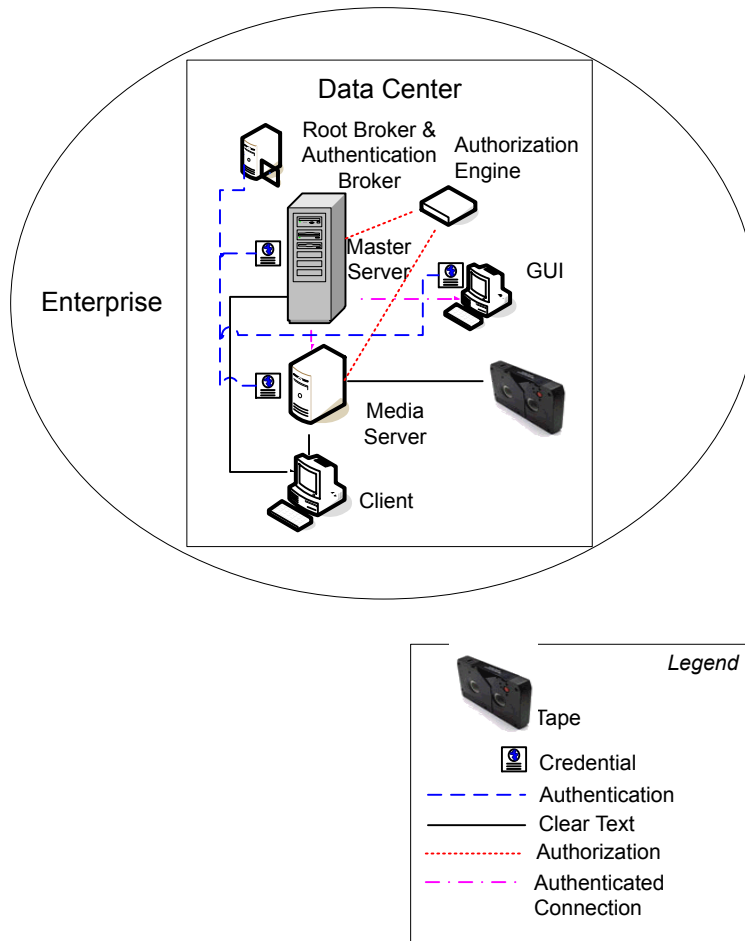


NBAC on master, media server, and graphical user interface security

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

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

Figure 1-8 NBAC on master and media server



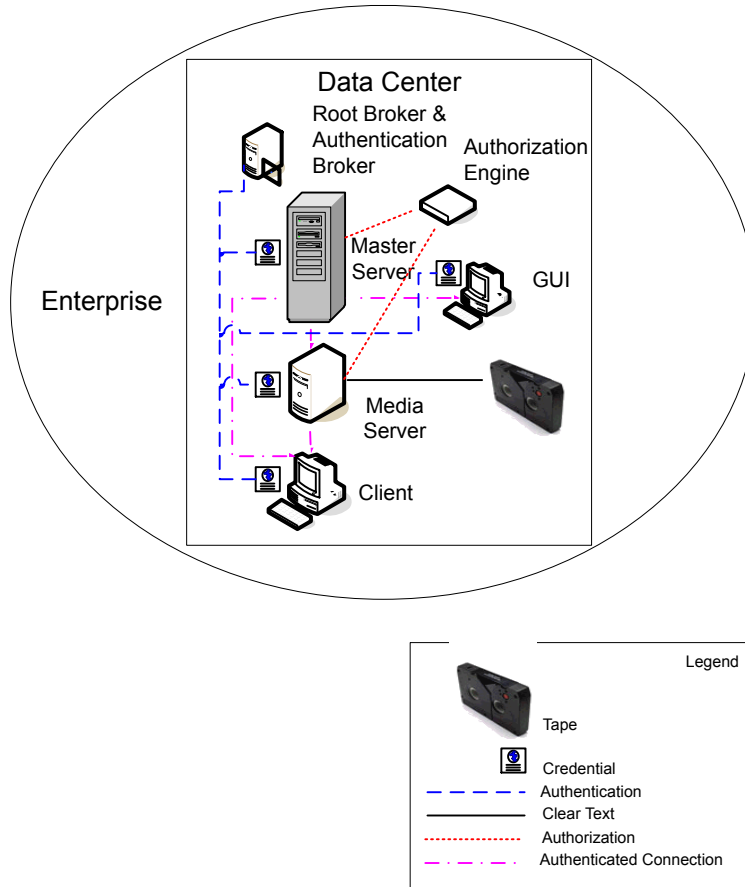
NBAC complete security

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 graphical user interface model. The main differences are that all hosts participating in the NetBackup environment are reliably identified using credentials. And non-root administrators have the ability to manage the NetBackup clients based on configurable levels of access. Note that user identities can exist in global repositories such as Active Directory in Windows

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

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

Figure 1-9 NBAC complete



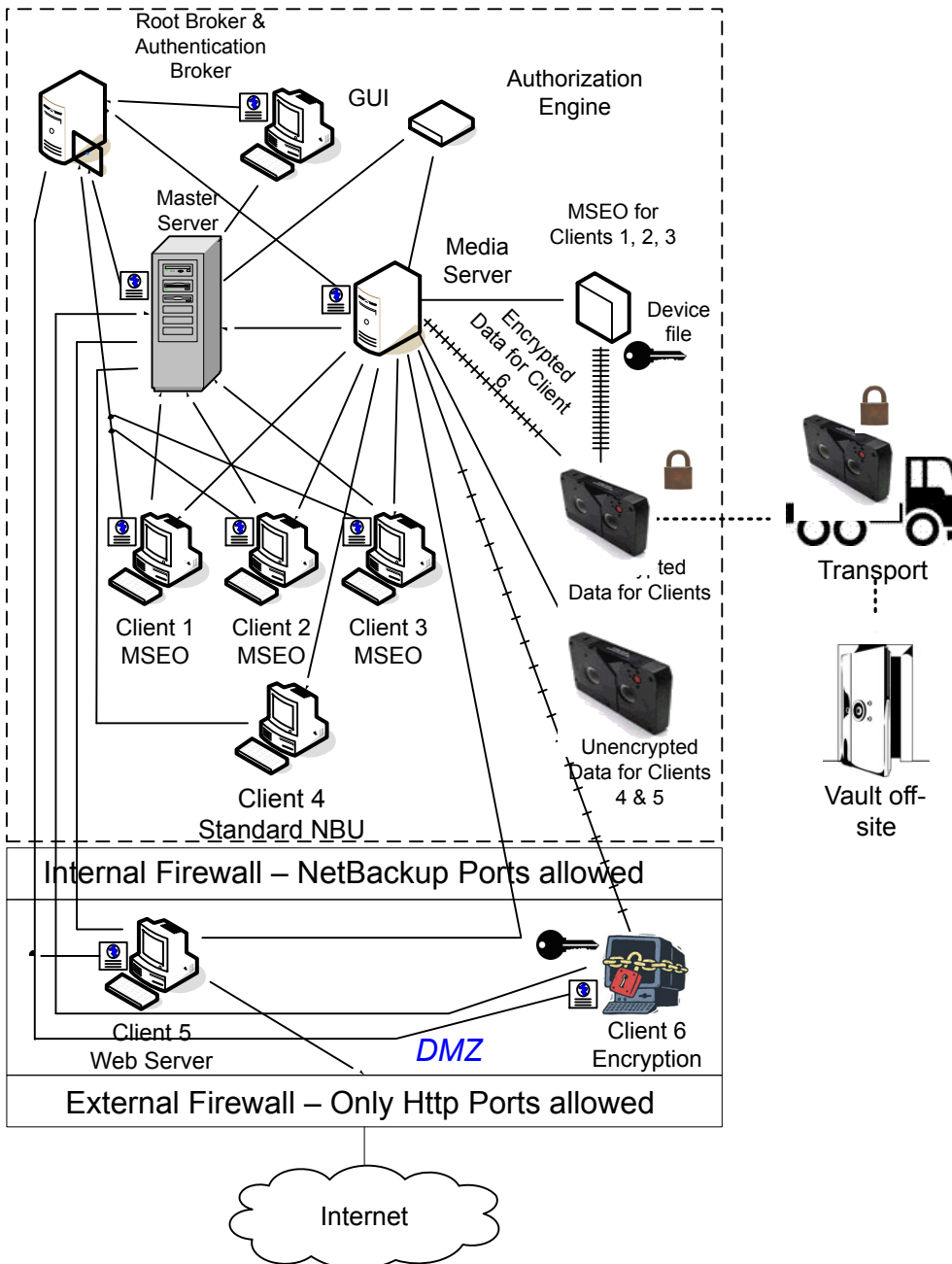
All NetBackup security

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 38.

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 41.
- See [“Single datacenter with Media Server Encryption Option \(MSEO\)”](#) on page 44.
- See [“Single datacenter with client side encryption”](#) on page 47.
- See [“Single datacenter with NBAC on master and media servers”](#) on page 49.
- See [“Single datacenter with NBAC complete”](#) on page 53.
- See [“Single datacenter with all security implemented”](#) on page 56.

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 60.
- See [“Multi-datacenter with Media Server Encryption Option \(MSEO\)”](#) on page 64.
- See [“Multi-datacenter with client side encryption”](#) on page 69.
- See [“Multi-datacenter with NBAC on master and media servers”](#) on page 74.
- See [“Multi-datacenter with NBAC complete”](#) on page 80.
- See [“Multi-datacenter with all NetBackup security”](#) on page 86.

Workgroup with NetBackup

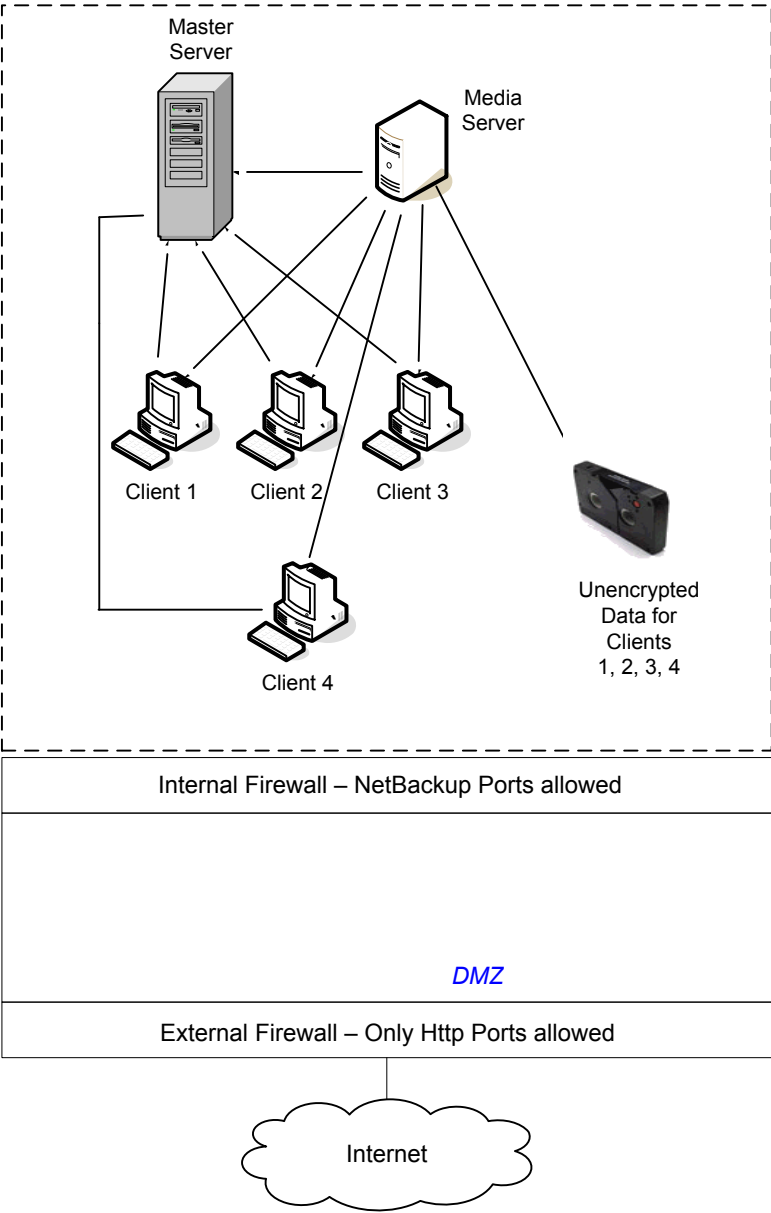
A workgroup with NetBackup is classified as a small group of systems (less than 50). The workgroup is used with NetBackup internally. Typically, this configuration does not have a unified naming service such as NIS or Active Directory. It may not have an authoritative host naming service such as DNS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

The workgroup with NetBackup includes the following highlights:

- Very few NetBackup servers
- Small computer environments
- No externally facing equipment involved

[Figure 2-1](#) shows an example workgroup with NetBackup.

Figure 2-1 Workgroup with NetBackup



The following table describes the NetBackup parts that are used with the workgroup.

Table 2-1 NetBackup parts used with the workgroup

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

Single datacenter with standard NetBackup

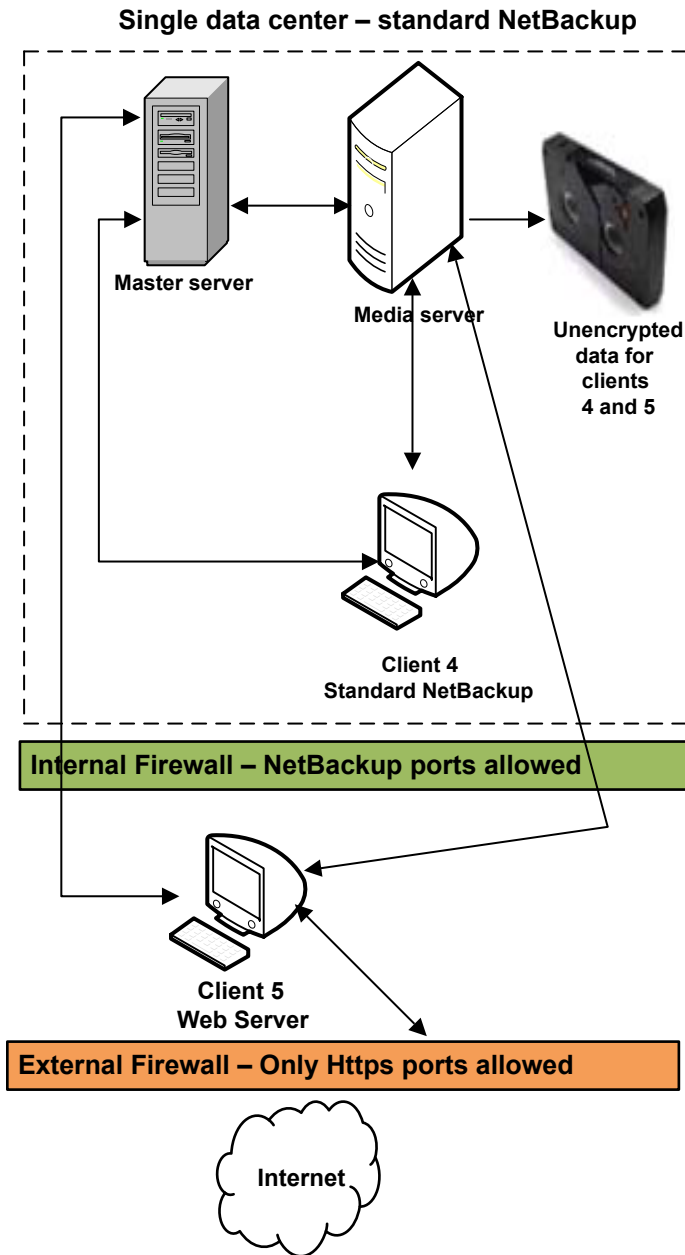
A single datacenter with standard NetBackup is defined as a medium to large group of hosts (greater than 50). It includes the hosts that are both internal only and those that expand through the DMZ to the Internet. This configuration typically has centralized naming service for hosts (such as DNS or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

The single datacenter with standard NetBackup includes the following highlights:

- Externally facing hosts
- Centralized naming services typically exist
- Greater than 50 hosts in size
- Simplest to configure requiring only general NetBackup knowledge
- Typical configuration that is used for NetBackup customers
- Assumes no fear of passive data interception on the wire as the backup runs

[Figure 2-2](#) shows an example single datacenter with standard NetBackup.

Figure 2-2 Single datacenter with standard NetBackup



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

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

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

Single datacenter with Media Server Encryption Option (MSEO)

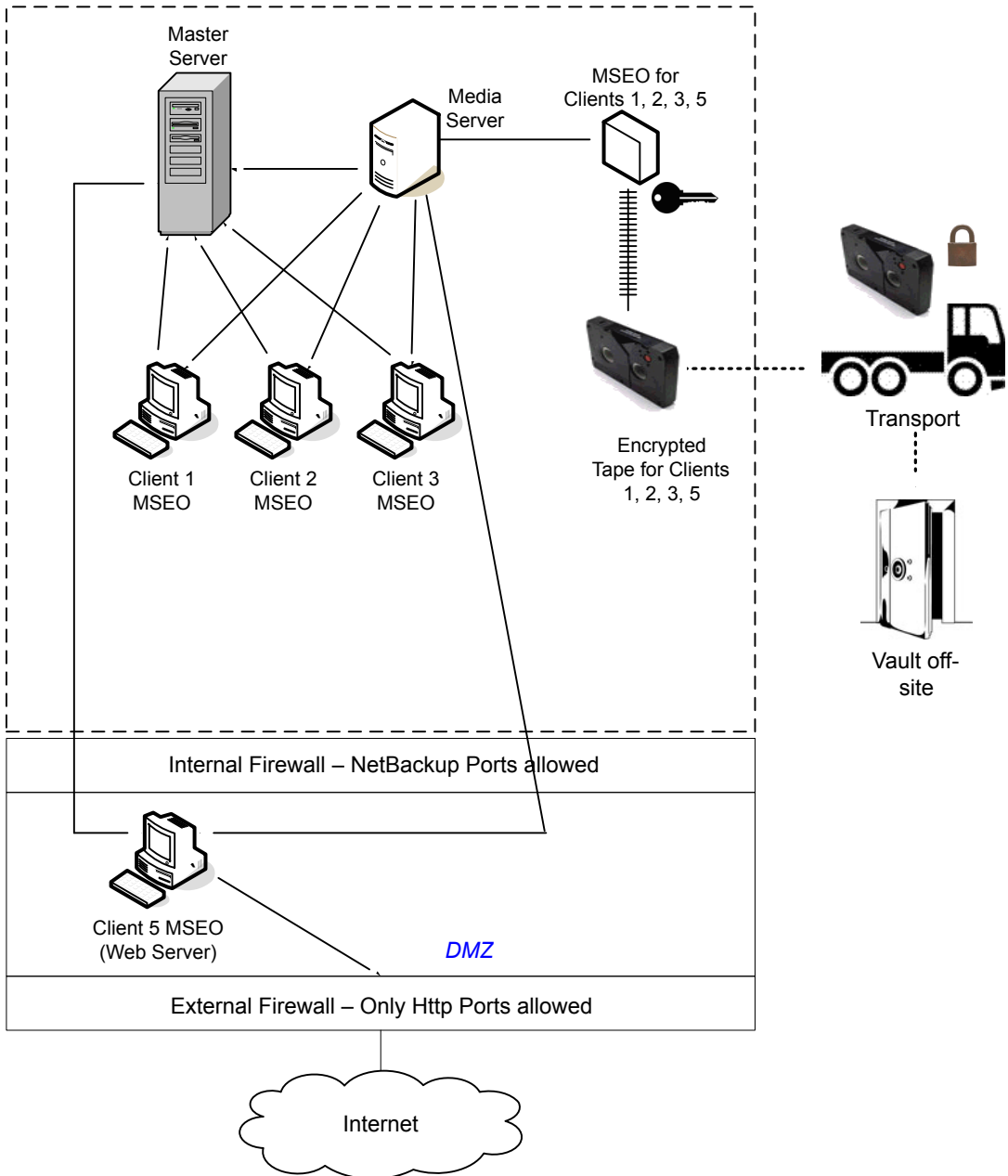
This single datacenter with the Media Server Encryption Option (MSEO) example typically includes more than 50 hosts. All externally facing hosts make use of the Media Server Encryption Option (MSEO). In this example, clients use the MSEO option for all hosts.

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

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

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

Figure 2-3 Single datacenter with MSEO



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

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

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

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

Part	Description
External firewall	Allows external users to access the Web server client 5 located in the DMZ from the Internet over HTTP ports. NetBackup ports are open for Web server client 5 to communicate through the internal firewall to NetBackup. The NetBackup ports are not allowed to pass through the external firewall to the Internet. Only the HTTP ports of Web server client 5 can pass through the external firewall to the Internet.
Internet	Specifies a collection of interconnected computer networks that are linked by copper wires, fiber-optic cables and wireless connections. The Web server client 5 can communicate over the Internet using HTTP ports through the external firewall.

Single datacenter with client side encryption

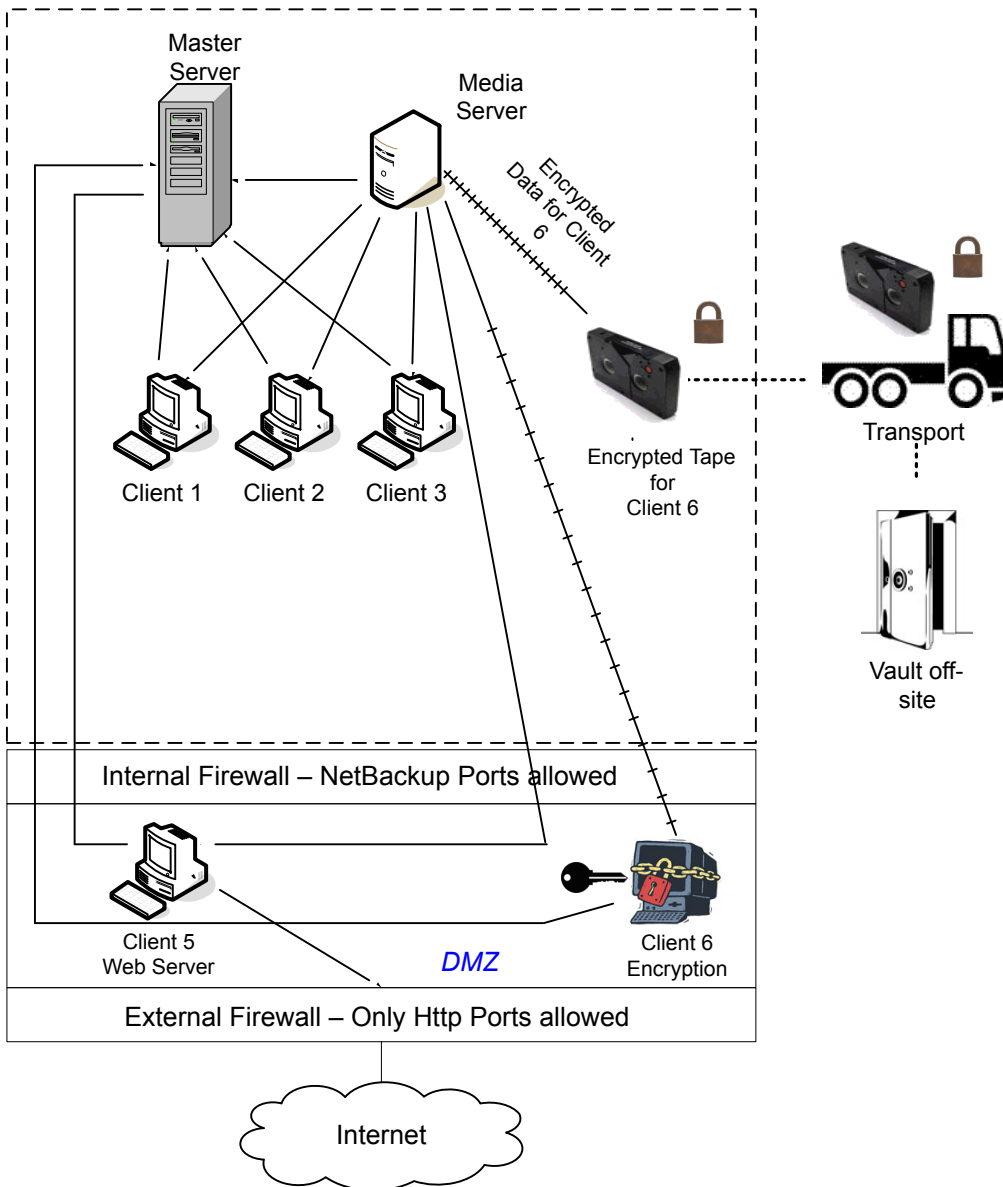
This single datacenter with client side encryption example uses the client side encryption to ensure data confidentiality across the wire as well as on tape. The client side encryption mitigates the risk of passive wire tapping within the organization. The risk of data exposure is reduced as tapes are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

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

- Useful for protecting off-site data
- Data from client is encrypted and eliminates passive interception of the data on the wire
- Key management is de-centralized on to the clients
- The original NetBackup encryption option
- Client CPU is used to perform encryption
- Must have the key to get data back. A lost key means lost data.
- Useful when you need to scan tapes off-site and/or you need confidentiality on the wire

Figure 2-4 shows an example single datacenter with client side encryption.

Figure 2-4 Single datacenter with client side encryption



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

Table 2-4 NetBackup parts for a single datacenter with client side encryption

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

Single datacenter with NBAC on master and media servers

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

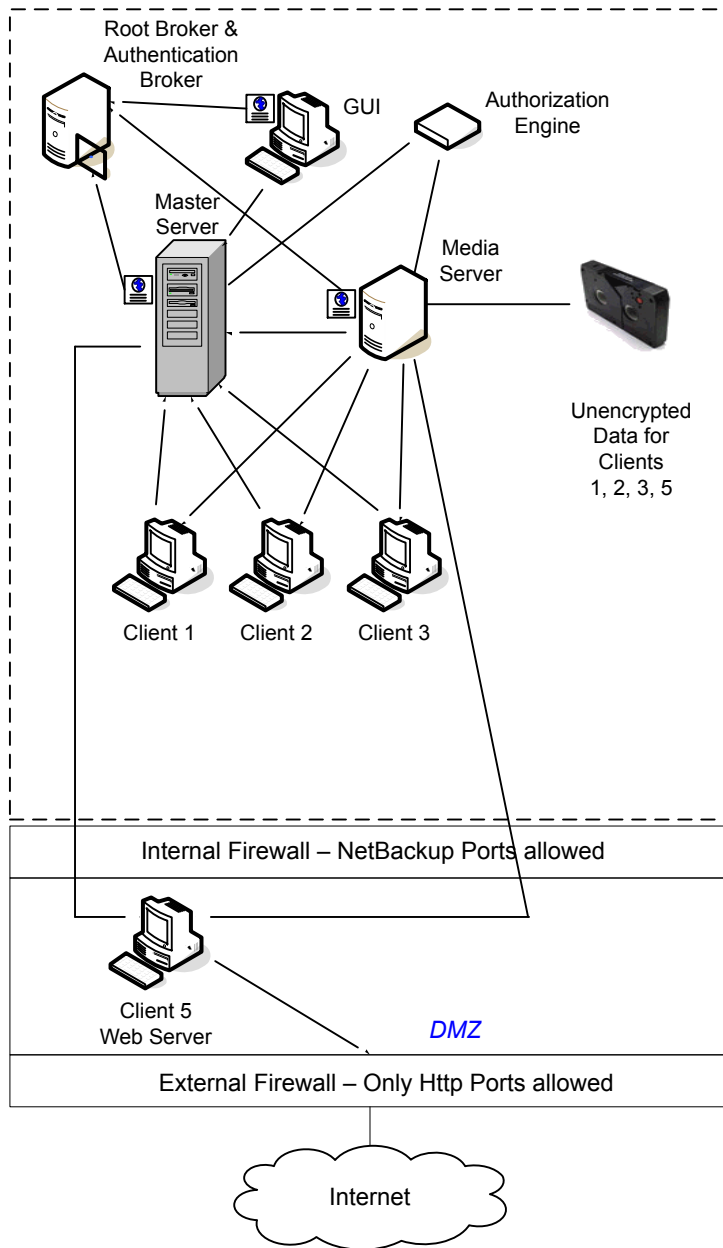
The single datacenter with NBAC on master and media servers includes the following highlights:

- Administer non-root users
- Administer UNIX with a Windows User ID
- Administer Windows with a UNIX account

- Segregate and limit the actions of specific users
- Root or Administrator or client hosts can still do local client backups and restores
- Can be combined with other security-related options
- All servers must be NetBackup version 7.x and higher

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

Figure 2-5 Single datacenter with NBAC on master and media servers



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

Table 2-5 NetBackup parts for a single datacenter with NBAC on the master and media servers

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

Table 2-5 NetBackup parts for a single datacenter with NBAC on the master and media servers (*continued*)

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

Single datacenter with NBAC complete

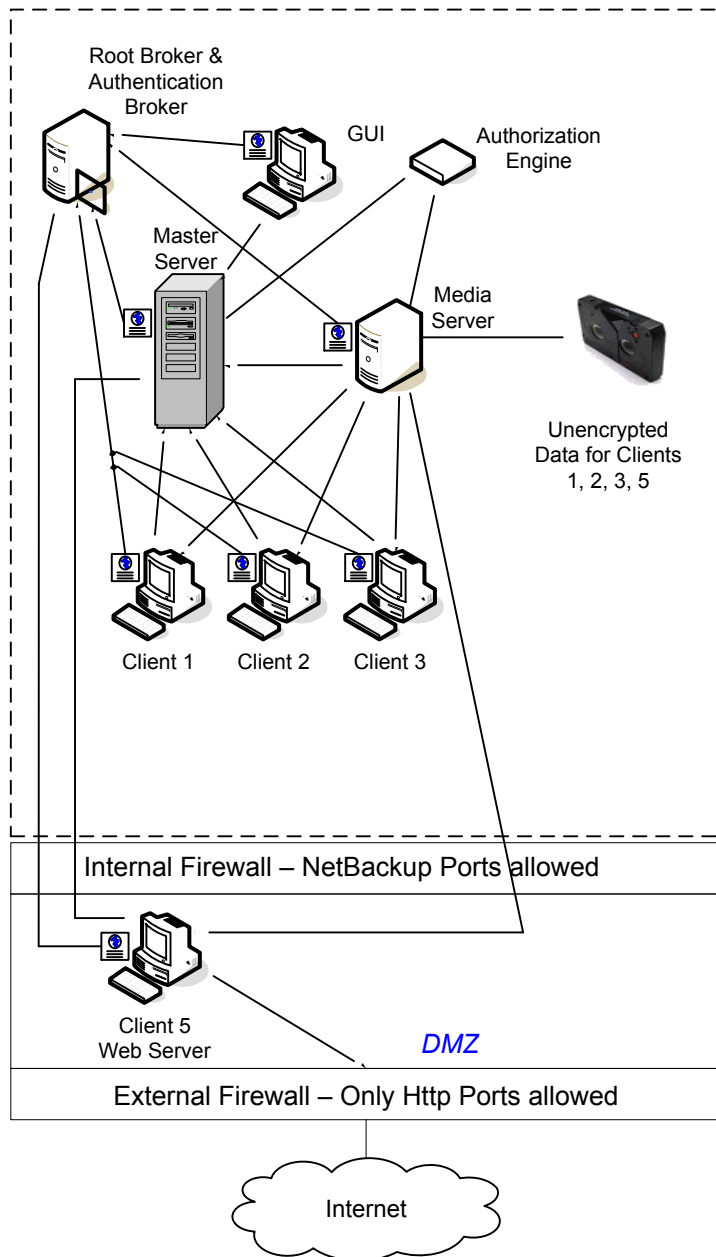
The single datacenter with NBAC complete environment is very similar to the single datacenter with NBAC master and media server. The main differences are that all of the hosts that participate in the NetBackup environment are reliably identified using credentials. And non-root administrators can manage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

The single datacenter with NBAC complete includes the following highlights:

- Similar to highlights for single datacenter with NBAC master and media server, except for root or administrator on client
- On client systems, non-root / administrator users may be configured to do local backup and restores (setup by default)
- The environment facilitates trusted identification of all hosts participating in NetBackup
- Requires all hosts to be at NetBackup version 7.x or later

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

Figure 2-6 Single datacenter with NBAC complete



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

Table 2-6 NetBackup parts for a single datacenter with NBAC complete

Part	Description
Master server	<p>Communicates with the media server, root broker, authentication broker. It also communicates with the authorization engine, clients 1, 2, 3, and client 5, Web server, in the DMZ. The master server further communicates with and receives a credential from the authentication broker.</p> <p>When a CLI or GUI accesses a daemon on a master server, a credential is exchanged to identify the user. The authorization engine is contacted to determine accessibility to the daemons functions.</p>
Media server	<p>Communicates with the master server, clients 1, 2, 3, and client 5, Web server, in the DMZ. The media server also communicates with the authorization engine and receives a credential from the authentication broker. The media server enables the writing of unencrypted data to tape for clients 1, 2, 3, and 5.</p> <p>When a CLI or GUI accesses a daemon on a media server, a credential is exchanged to identify the user. The authorization engine is contacted to determine accessibility to the daemons functions.</p>
GUI	Specifies that the remote administration console, GUI, receives a credential from the authentication broker. The GUI then uses this credential to gain access to functionality on the media servers and master servers.
Root broker	Authenticates the authentication broker but not the clients. Figure 2-6 , shows the root broker and the authentication broker as the same component.
Authentication broker	Authenticates the master server, media server, GUI, clients, and users by establishing credentials with each.
Authorization engine	<p>Communicates with the master server and media server to determine permissions of an authenticated user. It also stores user groups and permissions. Only one authorization engine is needed.</p> <p>Note: The authorization engine resides on the master server as a daemon process. It is shown in the figure as a separate image for the example only.</p>
Tape	Contains unencrypted backup data that is written for clients 1, 2, 3, and 5.

Table 2-6 NetBackup parts for a single datacenter with NBAC complete
(continued)

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

Single datacenter with all security implemented

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

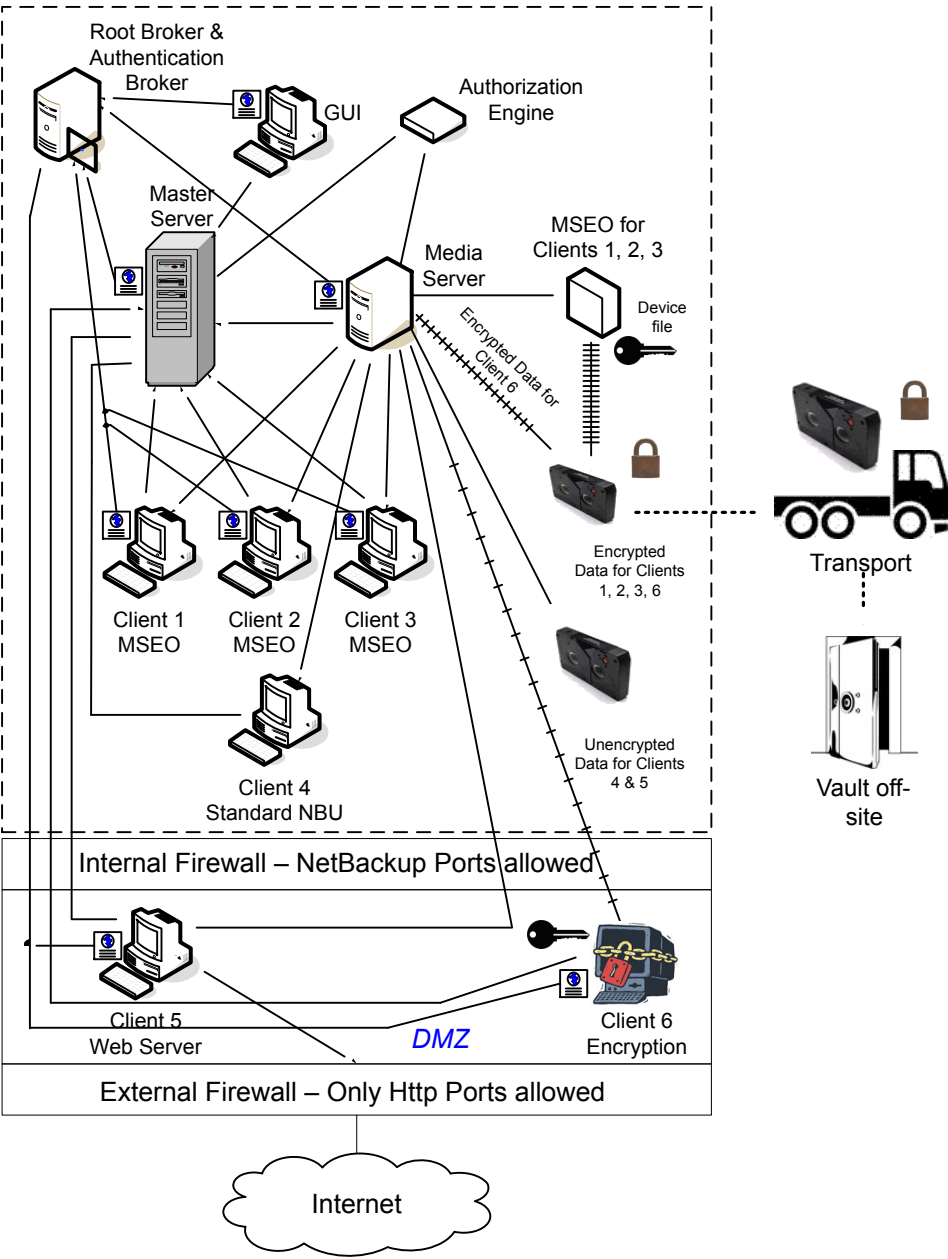
The single datacenter with all security implemented includes the following highlights:

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

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

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

Figure 2-7 Single datacenter with all security implemented



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

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

Part	Description
Master server	<p>Communicates with the media server, root broker, authentication broker, authorization engine, clients 1, 2, 3, and client 5, Web server, in the DMZ. The master server also communicates with and receives a credential from the authentication broker.</p> <p>When a CLI or GUI accesses a daemon on a master server, a credential is exchanged to identify the user. The authorization engine is contacted to determine accessibility to the daemons functions.</p>
Media server	<p>Communicates with the master server, clients 1, 2, 3 and client 5, Web server, in the DMZ. The media server also communicates with the authorization engine and receives a credential from the authentication broker. The media server enables the writing of unencrypted data to tape for clients 1, 2, 3, and 5.</p> <p>When a CLI or GUI accesses a daemon on a media server, a credential is exchanged to identify the user. The authorization engine is contacted to determine accessibility to the daemons functions.</p>
GUI	Specifies that this remote administration console, GUI, receives a credential from the authentication broker. The GUI then uses this credential to gain access to functionality on the media servers and master servers.
Root broker	Authenticates the authentication broker but not clients. In the figure, the root broker and authentication broker are shown as the same component.
Authentication broker	Authenticates the master server, media server, GUI, clients, and users by establishing credentials with each.
Authorization engine	<p>Communicates with the master server and media server to determine permissions of an authenticated user. It also stores user groups and permissions. Only one authorization engine is needed.</p> <p>Note: The authorization engine resides on the master server as a daemon process. It is shown in the figure as a separate image for example only.</p>
Tapes	Specifies that the first tape contains encrypted MSEO backup data written for clients 1, 2, 3, and client encrypted data for client 6. The second tape contains unencrypted backup data that is written for clients 4 and 5.
Transport	Specifies that the transport truck moves encrypted tapes off-site to a secure vault facility. If a tape is lost during transport, the datacenter manager has mitigated the risk. The risk of data exposure has been mitigated through the use of encryption.

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

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

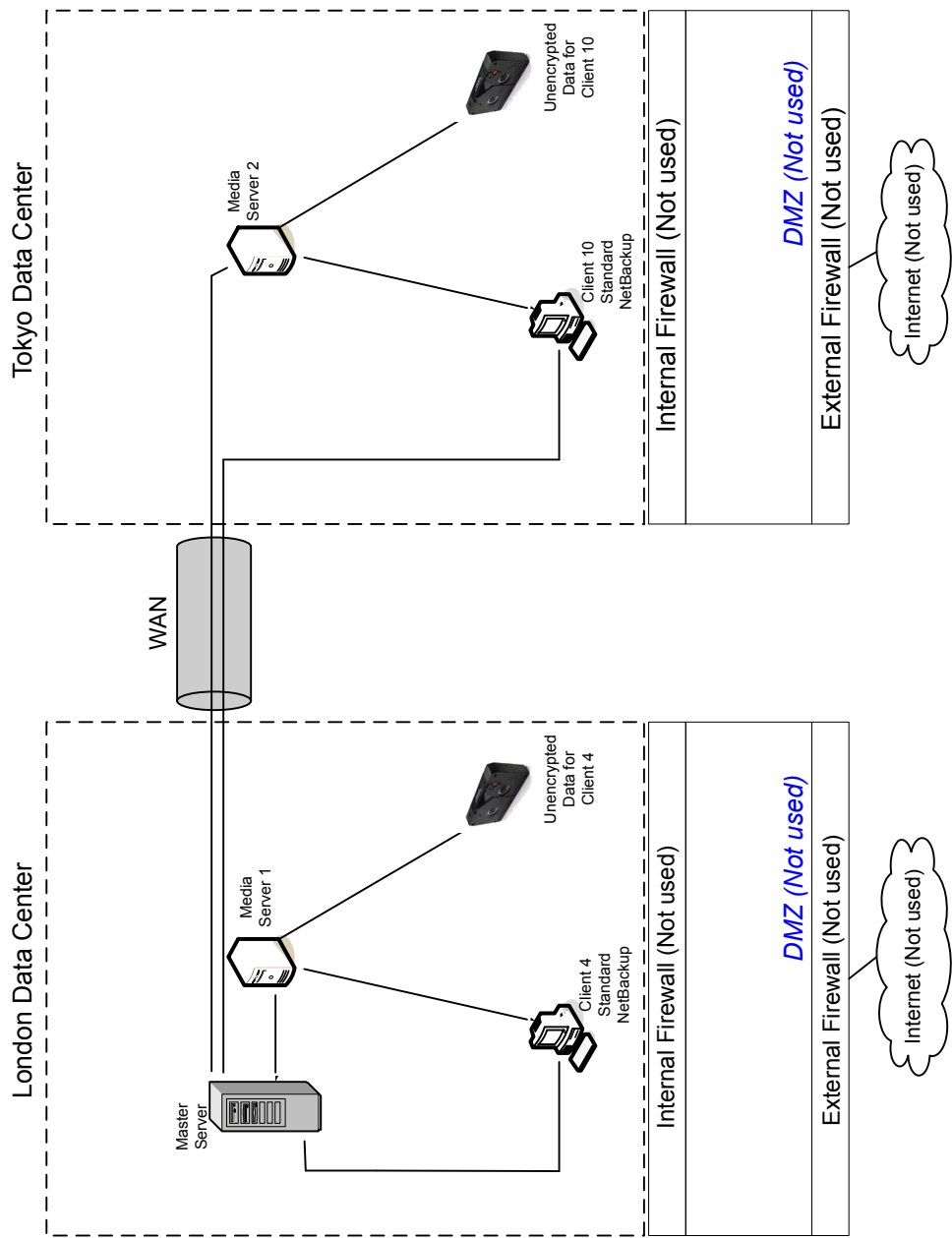
A multi-datacenter includes the hosts that are both internal only and those that expand through the DMZ to the Internet. This configuration typically has centralized naming service for hosts (such as DNS or WINS). It also has a centralized naming service for users (such as NIS or Active Directory).

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

[Figure 2-8](#) shows an example multi-datacenter with standard NetBackup.

Figure 2-8 Multi-datacenter with standard NetBackup



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

Table 2-8 NetBackup parts for a multi-datacenter with standard NetBackup implemented

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

Table 2-8 NetBackup parts for a multi-datacenter with standard NetBackup implemented (*continued*)

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

Multi-datacenter with Media Server Encryption Option (MSEO)

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

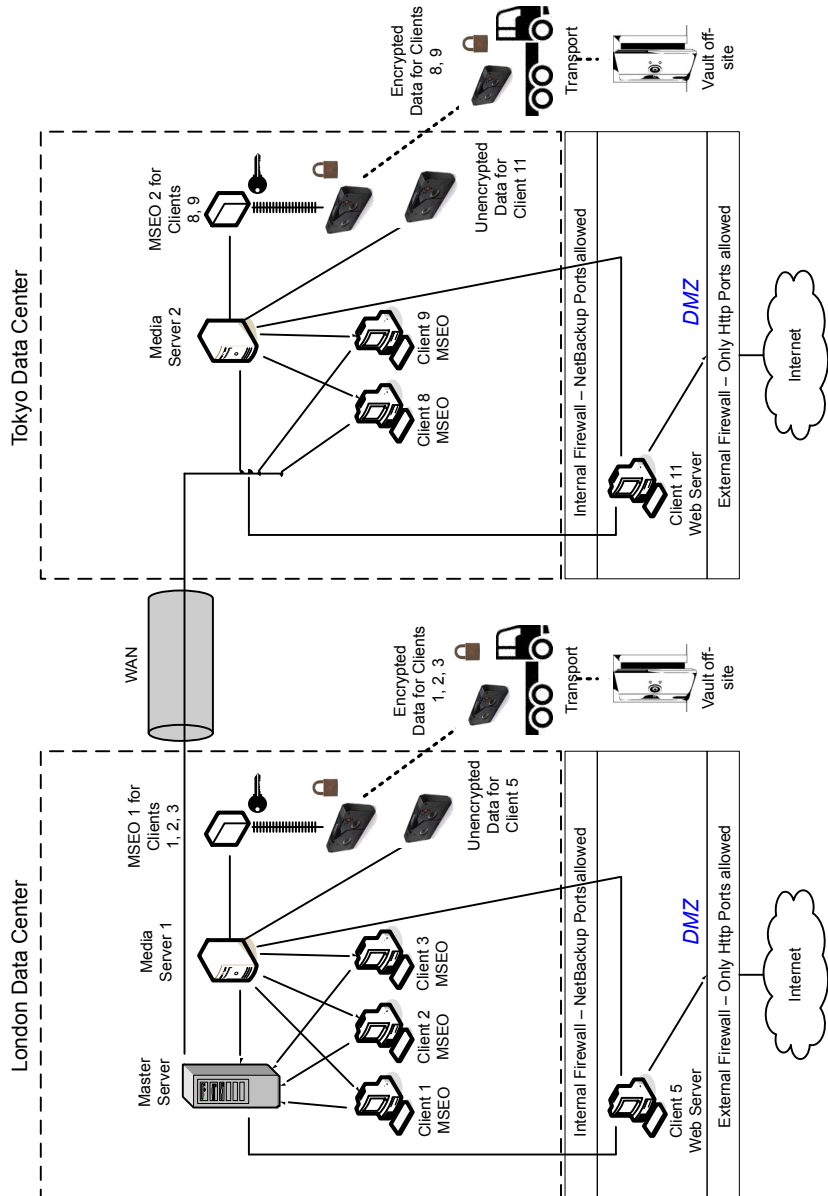
This multi-datacenter example can typically include more than 50 hosts. All externally facing hosts use the Media Server Encryption Option (MSEO). In this example, clients use both encrypted backups for some clients and the MSEO option for other hosts. Data that is too sensitive to be archived off-site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

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

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

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

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



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

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

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

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

Part	Description
Tapes	<p>Specifies that both the unencrypted and encrypted data tapes are produced in the London datacenter and in the Tokyo datacenter. The encrypted tape contains MSEO encrypted backup data. In London, the unencrypted tape is written for client 5 and stored on-site at the London datacenter. The encrypted tape is written for clients 1, 2, and 3. The encrypted tape for clients 1, 2, and 3 is transported off-site to a vault in London for disaster recovery protection.</p> <p>In Tokyo, the unencrypted tape is written for client 11 and stored on-site at the Tokyo datacenter. The encrypted tape is written for clients 8 and 9. The encrypted tape for clients 8 and 9 is transported off-site to a vault in Tokyo for disaster recovery protection.</p> <p>Note: To decrypt the data, the key(s) used to encrypt the data must be made available.</p>
Transports	<p>Specifies that there are two transports. One transport is located in London and the other is located in Tokyo. The transport truck in London moves the encrypted tape for clients 1, 2, and 3 off-site to a secure London vault facility. The transport truck in Tokyo moves the encrypted tape for clients 8 and 9 off-site to a secure Tokyo vault facility.</p> <p>Note: If a tape is lost during transport, the datacenter manager has potentially reduced the risk of a data breach. This breach has been reduced through the use of data encryption.</p>
Vaults off-site	<p>Specifies that there are two vaults that are located off-site. One vault is located in London and the other is located in Tokyo. Both vaults provide safe encrypted tape storage facilities off-site at different locations than the datacenters.</p> <p>Note: Good disaster recovery protection promotes having the encrypted tapes stored at locations separate from the datacenters.</p>
Clients	<p>Specifies that clients are located in both the London and Tokyo datacenters. In London, clients 1, 2, and 3 are of the MSEO type and client 5 is a Web server type (not using MSEO) that is located in the DMZ. Both server types can be managed by the master server. And they can have their encrypted data backed up to tape through media server 1 attached MSEO hardware appliance. Client 5 communicates to NetBackup using NetBackup only ports through the internal firewall. Client 5 receives connections from the Internet using HTTP only ports through the external firewall.</p> <p>Tokyo clients 8 and 9 are of the MSEO type. Client 11 is a Web server type (not using MSEO) located in the DMZ. Both server types can be managed by the master server located in London. And they can have their encrypted data backed up to tape through media server 2 attached MSEO hardware appliance. Client 11 communicates to NetBackup using NetBackup only ports through the internal firewall. Client 5 receives connections from the Internet using HTTP only ports through the external firewall.</p>

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

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

Multi-datacenter with client side encryption

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

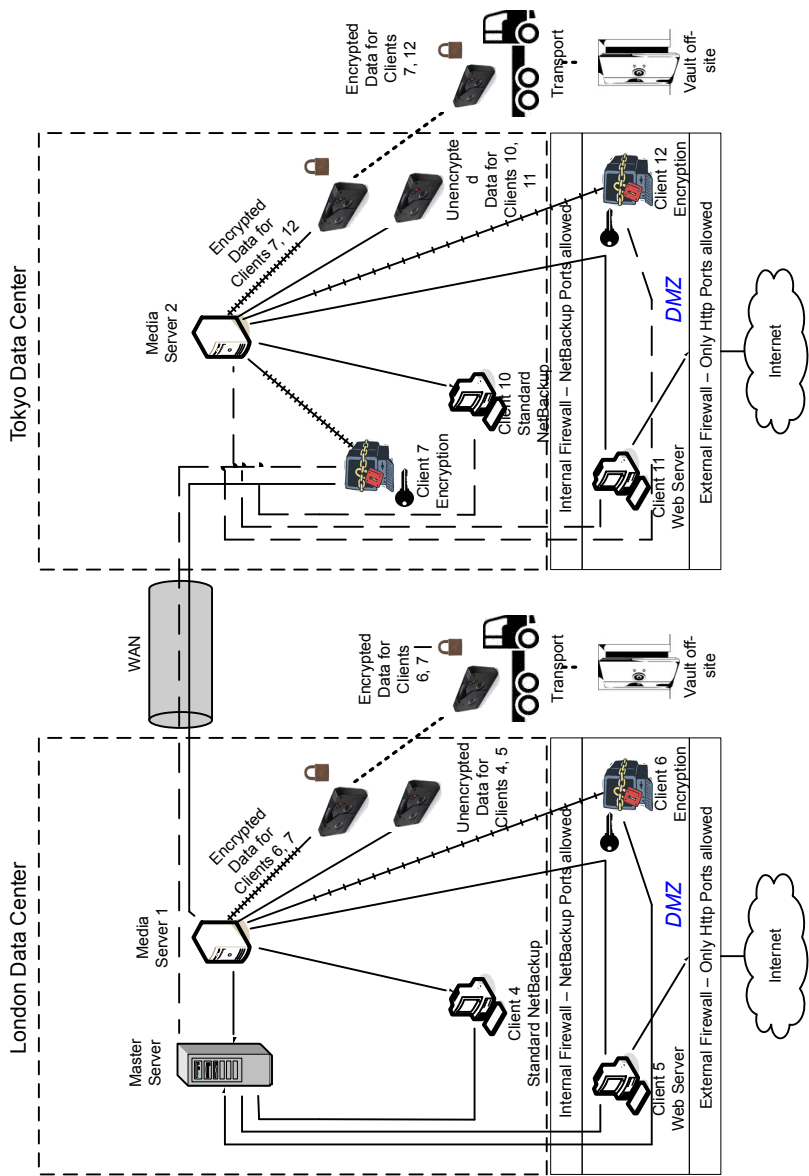
The example multi-datacenter can use client side encryption to ensure data confidentiality across the wire as well as on tape. This encryption helps to mitigate the risk of passive wire tapping within the organization. Risk of data exposure as the tapes are moved off site. This datacenter model assures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

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

- NetBackup spans two or more geographic regions through a WAN
- Useful for protecting off-site data
- Data from client is encrypted and eliminates the passive interception of the data on the wire
- Key management is de-centralized on to the clients
- The original NetBackup encryption option
- Client CPU is used to perform encryption
- Must have the key to get data back. A lost key means lost data.
- Useful when you need to scan tapes off-site or you need confidentiality on the wire

[Figure 2-10](#) shows an example multi-datacenter with client side encryption.

Figure 2-10 Multi-datacenter with client side encryption



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

Table 2-10 NetBackup parts for a multi-datacenter with client side encryption implemented

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

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

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

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

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

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

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

Multi-datacenter with NBAC on master and media servers

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

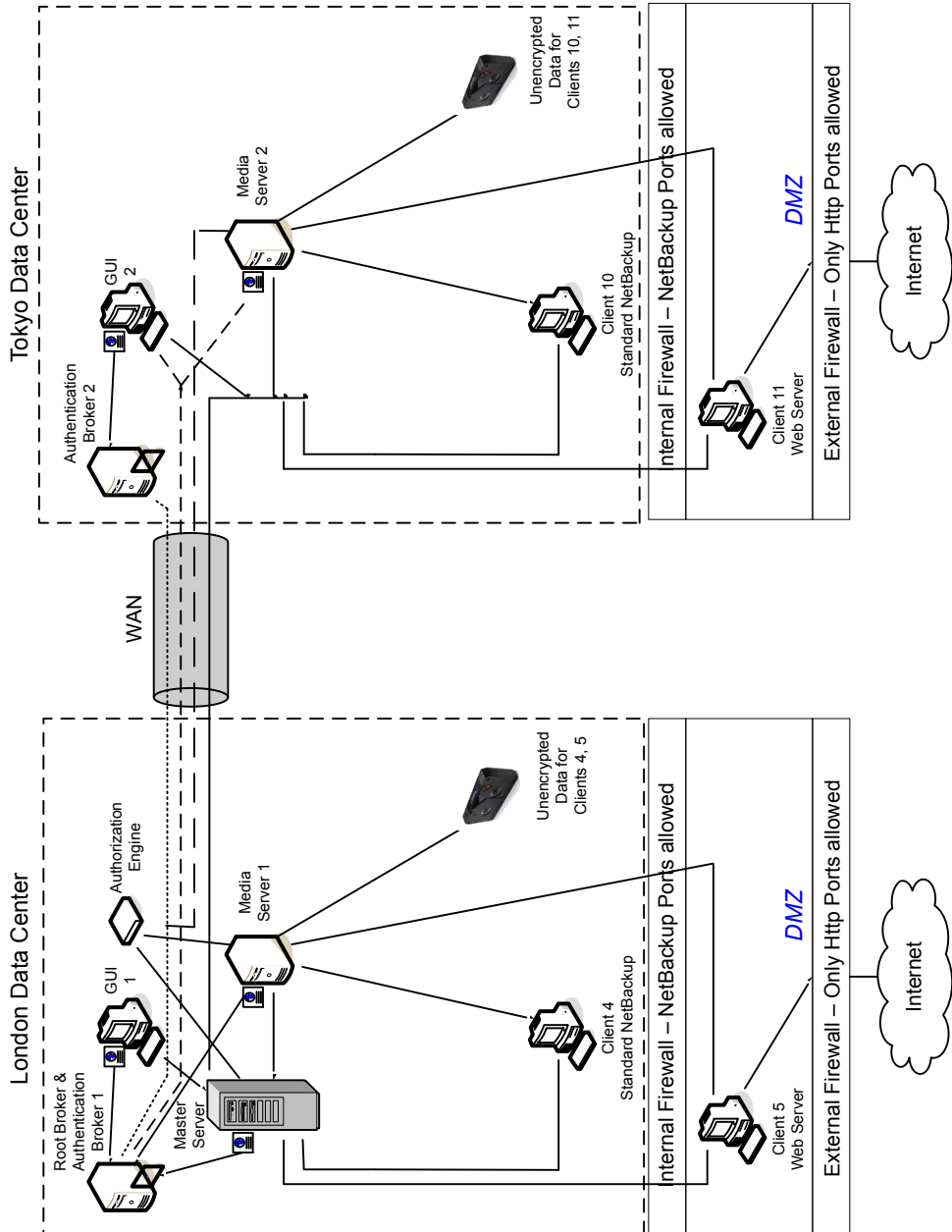
This datacenter example uses NetBackup Access Control on the master servers and media servers. The datacenter limits access to portions of NetBackup and can use non-root administration of NetBackup. Within this environment, NBAC is configured for use between the servers and the GUIs. Non-root users can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

NetBackup. In addition, NBAC can be used to limit the level of access to NetBackup for certain individuals. For example, you can segregate day to day operational control from environmental configuration such as adding new policies, robots, etc. The multi-datacenter with NBAC on master and media servers includes the following highlights:

- NetBackup spans two or more geographic regions through a WAN
- Administer as non-root users
- Administer UNIX with a Windows User ID.
- Administer Windows with a UNIX account.
- Segregate and limit the actions of specific users.
- Root or Administrator or client hosts can still perform local client backups and restores
- Can be combined with other security-related options
- All servers must be NetBackup version 7.x or later.

[Figure 2-11](#) shows an example multi-datacenter with NBAC on the master servers and media servers.

Figure 2-11 Multi-datacenter with NBAC on the master servers and media servers



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

Table 2-11 NetBackup parts used for a multi-datacenter with NBAC on the master and media servers

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

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

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

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

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

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

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

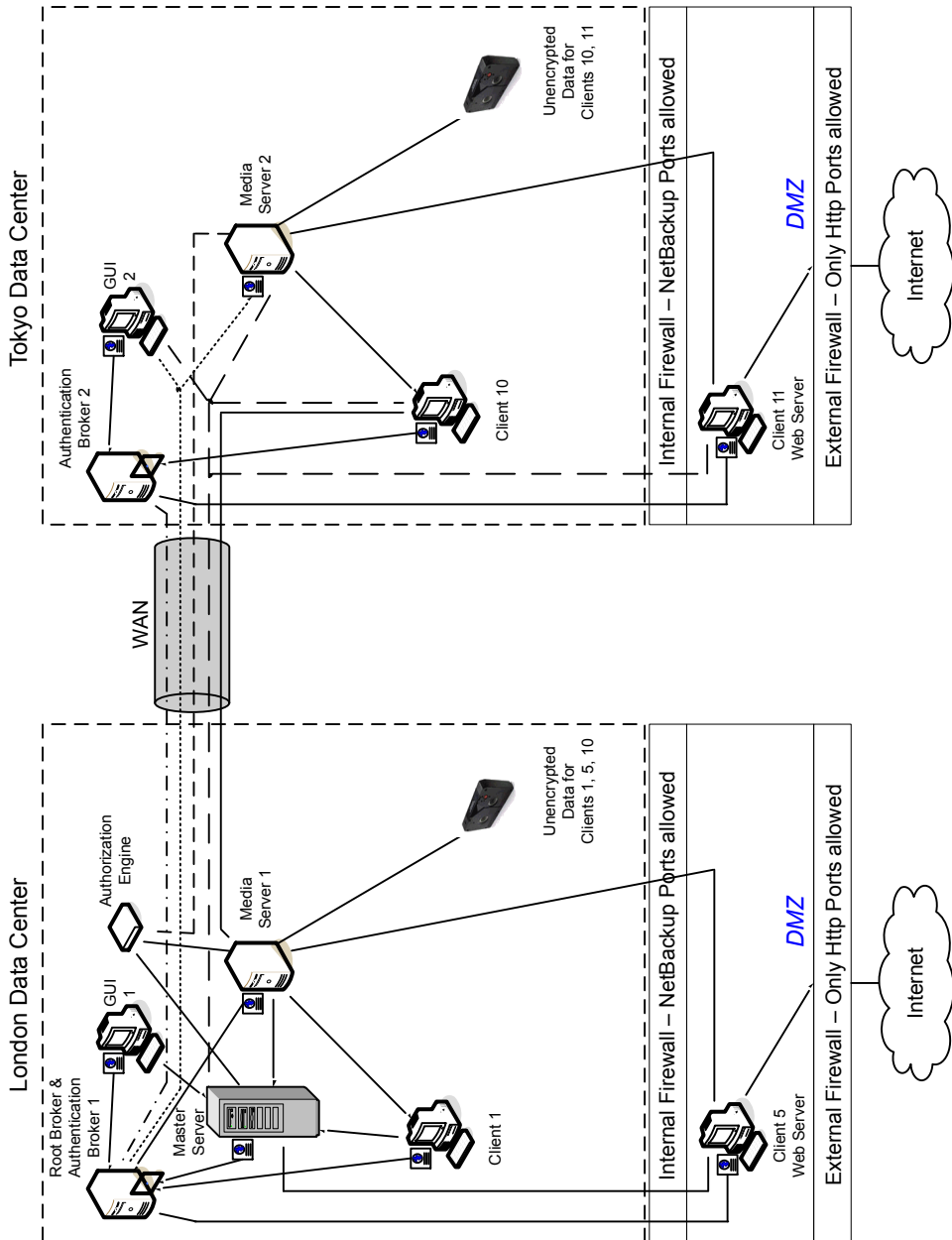
The multi-datacenter with NBAC complete includes the following highlights:

- 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 7.x or later.

[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	Specifies that there is only one authorization engine required in a datacenter installation. The authorization engine communicates with the master server and media server to determine permissions of an authenticated user. These permissions determine the functionality available to the user. The authorization engine also stores user groups and permissions. The authorization engine resides in London and communicates with the master server, and media server 1. The authorization engine also communicates over the WAN to authorize access to media server 2 in Tokyo. Note: The authorization engine resides on the master server as a daemon process. It is shown in the figure as a separate image for example only.
Tapes	Specifies that the unencrypted data tapes are produced in both the London and Tokyo datacenters. In London, the unencrypted tape is written for clients 1, 5 and 10 and stored on-site at the London datacenter. In Tokyo, the unencrypted tape is written for clients 10 and 11 and stored on-site at the Tokyo datacenter. Note that even though client 10 is located in Tokyo and is backed up in Tokyo, client 10 is also backed up in London.

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

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

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

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

Multi-datacenter with all NetBackup security

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

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

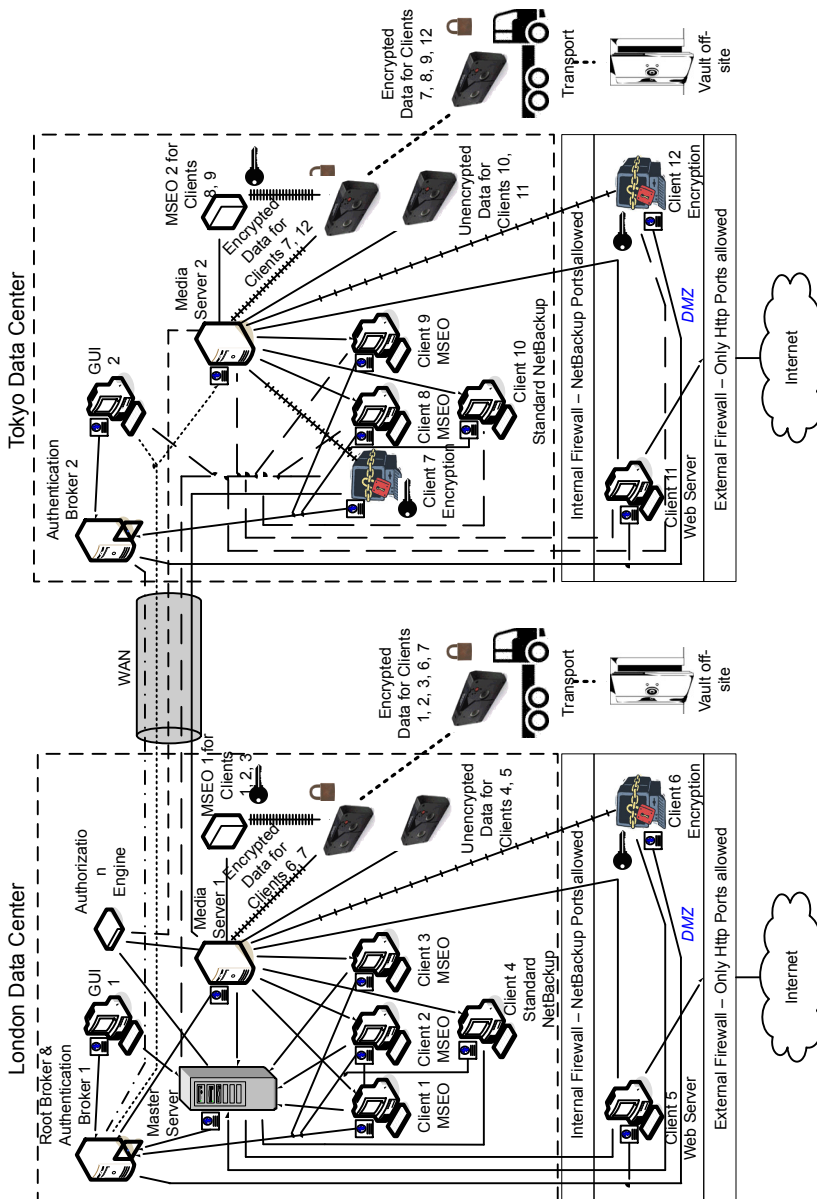
The multi-datacenter with all NetBackup security includes the following highlights:

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

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

[Figure 2-13](#) shows an example multi-datacenter with all NetBackup security.

Figure 2-13 Multi-datacenter with all NetBackup security



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

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

Part	Description
London datacenter	Contains the root broker, authentication broker 1, GUI 1. It also contains the authorization engine, master server, media server 1, MSEO 1, clients 1 through 6, transport and vault off-site. The London datacenter also contains the encrypted data tape for clients 1, 2, 3, 6, and 7 and the unencrypted data tape for clients 4 and 5. The London datacenter connects to the Tokyo datacenter through a dedicated WAN connection.
Tokyo datacenter	Contains the authentication broker 2, GUI 2, media server 2, MSEO 2, clients 7 through 12, transport and vault off-site. The Tokyo datacenter also contains the encrypted data tape for clients 7, 8, 9, and 12 and the unencrypted data tape for clients 10 and 11. The Tokyo datacenter connects to the London datacenter through a dedicated WAN connection.
Wide Area Network (WAN)	Specifies that the dedicated WAN link connects the London datacenter with the Tokyo datacenter. The WAN provides connectivity between the root broker and authentication broker 1 and authentication broker 2. In addition, the WAN provides connectivity between the root broker and authentication broker 1 and GUI 2 along with media server 2. The WAN connects the authorization engine to media server 2. The WAN connects the master server to GUI 2, media server 2, and clients 7 through 12. Finally the WAN connects media server 1 to client 7.
Master server	Specifies that the master server, located in the London datacenter, communicates with the root broker and authentication broker 1, GUI 1, authorization engine, media server 1, and clients 1 through 6. The master server also communicates with GUI 2 and media server 2, and clients 7 through 12 in Tokyo.
Media servers	<p>Specifies that there can be two media servers in this multi-datacenter example. Media server 1 is located in the London datacenter and media server 2 is located in the Tokyo datacenter. In London, media server 1 communicates with the master server, root broker and authentication broker 1. It also communicates with the authorization engine, MSEO 1, and clients 1 through 6, and 7. Media server 1 writes unencrypted data to tape for clients 4 and 5 and encrypted data to tape for clients 1 through 6.</p> <p>In Tokyo, media server 2 communicates with the master server, root broker, and authentication broker 1 and authorization engine in London through the WAN. Media server 2 also communicates with MSEO 2, GUI 2, and clients 7 through 12 in Tokyo. Media server 2 writes unencrypted data to tape for clients 10 and 11 and encrypted data to tape for clients 7, 8, 9, and 12.</p>

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

Part	Description
GUIs	Specifies that there can be two GUIs in this multi-datacenter example. The GUI 1 is in London and GUI 2 is in Tokyo. These remote administration console GUIs receive credentials from the authentication brokers. The GUIs then use the credentials to gain access to functionality on the media servers and master servers. In London, GUI 1 receives a credential from authentication broker 1. GUI 1 has access to functionality on the master server and media servers 1 and 2. In Tokyo, GUI 2 receives a credential from the authentication broker 2. GUI 2 has access to functionality on the master server and media servers 1 and 2.
Root broker	Specifies that one root broker is required in a multi-datacenter installation. Sometimes the root broker is combined with the authentication broker. In this example, the root broker and authentication broker are shown as the same component and are located in the London datacenter. In London, the root broker authenticates the authentication broker 1 also in London and the authentication broker 2 in Tokyo. The root broker does not authenticate clients.
Authentication brokers	Specifies that there can be more than one authentication broker in a datacenter installation. Sometimes the authentication broker can be combined with the root broker. In this datacenter installation, there are two authentication brokers used. The authentication broker authenticates the master server, media server, GUI, and clients by establishing credentials with each. The authentication broker also authenticates a user with a command prompt. In London, authentication broker 1 authenticates a credential with the master server, media server 1, GUI 1, and clients 1 through 6. All NetBackup servers and clients in Tokyo and London authenticate to authentication broker 1 in London. GUI 1 authenticates to authentication broker 1 in London. GUI 2 authenticates to authentication broker 2 in Tokyo.
Authorization engine	<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>Note: The authorization engine resides on the master server as a daemon process. It is shown in the figure as a separate image for example only.</p>

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

Part	Description
Tapes	<p>Specifies that unencrypted and encrypted data tapes are produced in the London datacenter and in the Tokyo datacenter. In London, the unencrypted tape is written for clients 4 and 5 and stored on-site at the London datacenter. The encrypted tape is written for clients 1, 2, 3, 6, and 7, and is transported off-site to a vault in London for disaster recovery. In Tokyo, the unencrypted tape is written for clients 10 and 11 and stored on-site at the Tokyo datacenter. The encrypted tape is written for clients 7, 8, 9, and 12 and is transported off-site to a vault in Tokyo for disaster recovery protection. Even though client 7 is located in Tokyo and is backed up in Tokyo, client 7 is also backed up in London greater security and backup redundancy.</p> <p>Note: To decrypt the data, the key(s) used to encrypt the data must be made available.</p>
Transports	<p>Specifies that there can be two transports. One transport is in London and the other is in Tokyo. The transport truck in London moves the encrypted tape for clients 1, 2, 3, 6, and 7 off-site to a secure London vault facility. The transport truck in Tokyo moves the encrypted tape for clients 7, 8, 9, and 12 off-site to a secure Tokyo vault facility. Note that a backup copy of client 7 is vaulted both in London and in Tokyo.</p> <p>Note: If a tape is lost during transport, the datacenter manager has potentially reduced the risk of a data breach by using client side data encryption.</p>
Vaults off-site	<p>Specifies that there can be two vaults off-site. One vault is in London and the other is in Tokyo. Both vaults provide safe encrypted tape storage facilities off-site at different locations than the datacenters.</p> <p>Note: Storing the encrypted tapes at a separate location from the datacenter promotes good disaster recovery protection.</p>
Clients	<p>Specifies that clients are located in both the London and Tokyo datacenters. In London, clients 1 through 3 are MSEO encrypted types. Client 4 is a standard NetBackup type. Client 5 is a Web server type located in the DMZ. Client 6 is a client side encrypted type also located in the DMZ. All client types can be managed by the master server and have their data backed up to tape through media server 1. Client 5 communicates to NetBackup using NetBackup only ports through the internal firewall. Client 5 also receives connections from the Internet using HTTP only ports through the external firewall.</p> <p>In Tokyo, clients 7 through 9 are MSEO encrypted types. Client 10 is a standard NetBackup type. Client 11 is a Web server type located in the DMZ. Client 12 is a client side encrypted type also located in the DMZ. All client types can be managed by the master server and have their data backed up to tape through media server 2. Note that client 7 can be managed by both media server 1 and 2. Client 11 communicates to NetBackup using NetBackup only ports through the internal firewall. Client 11 also receives connections from the Internet using HTTP only ports through the external firewall</p>

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

Part	Description
Internal firewalls	<p>Specifies that there 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.</p>
Demilitarized Zones (DMZs)	<p>Specifies that there can be two DMZs in this multi-datacenter example. One DMZ is located in London and the other is located in Tokyo. In London, the DMZ provides a "safe" area of operation for the Web server client 5 and encrypted client 6. These clients exist between the internal firewall and external firewall. The Web server client 5 in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports. The Web server client 5 can also communicate through the external firewall to the Internet using only HTTP ports.</p> <p>In Tokyo, the DMZ provides a "safe" area of operation for the Web server client 11 and encrypted client 12. These clients exist between the internal firewall and external firewall. The Web server client 11 in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports. The Web server client 11 can also communicate through the external firewall to the Internet using only HTTP ports.</p>
External firewalls	<p>Specifies that there can be two external firewalls in this multi-datacenter example. One external firewall is located in London and the other is located in Tokyo. In London, the external firewall 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>

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"> On UNIX systems, you can specify ports in the <code>/etc/services</code> file. On Windows systems, you can specify ports in the <code>%systemroot%\System32\drivers\etc\services</code> file.
Dynamically allocated ports	<p>Specifies 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: Veritas recommends that you use the default port number settings for NetBackup services and internet service ports.

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

The following other guides contain information about NetBackup ports:

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

The following topics contain information about NetBackup ports:

- See [“About NetBackup daemons, ports, and communication”](#) on page 95.
- See [“About configuring ports”](#) on page 106.
- See [“Port requirements for NDMP backups”](#) on page 116.
- See [“Known firewall problems encountered when using NetBackup with third-party robotic products”](#) on page 116.

About NetBackup daemons, ports, and communication

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

- See [“Standard NetBackup ports”](#) on page 95.
- See [“NetBackup master server outgoing ports”](#) on page 96.
- See [“NetBackup media server outgoing ports”](#) on page 97.
- See [“NetBackup enterprise media management \(EMM\) server outgoing ports”](#) on page 98.
- See [“Client outgoing ports”](#) on page 99.
- See [“Windows administration console and Java server outgoing ports”](#) on page 99.
- See [“Java console outgoing ports”](#) on page 100.
- See [“Additional port information for products that interoperate with NetBackup”](#) on page 101.

Standard NetBackup ports

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

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

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

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

Source	Port name and/or number	Destination	Notes
Client	veritas_pbx 1556	NetBackup master server	Veritas private branch exchange service, VxPBX.
NetBackup master server, media server, or client	13783	NetBackup master server	<p>NetBackup authentication service, VxAT.</p> <p>In the case of NetBackup versions that are older than 7.1, the <code>nbatd</code> process listens on the port 13783 for back-level media servers and clients.</p> <p>NetBackup hosts of version 7.1 and later connect using the PBX port.</p>
NetBackup master server or media server	13722	NetBackup master server	<p>NetBackup Authorization Service, VxAZ.</p> <p>In the case of NetBackup versions that are older than 7.1, the <code>nbazd</code> process listens on the port 13722 for back-level media servers and clients.</p> <p>NetBackup hosts of version 7.1 and later connect using the PBX port.</p>

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

NetBackup master server outgoing ports

[Table 3-3](#) shows the ports that the master server uses to connect to remote hosts.

Table 3-3 NetBackup master server outbound ports and destinations

Port name and number	Destination	Notes
veritas_pbx 1556	Media server	<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.
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"> NetBackup access control (NBAC) is enabled. Media servers and clients in the NetBackup environment host a NetBackup software release level that is lower than the release level on the master server.
13722	Authorization server	<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 connect to remote hosts. The table shows the port name, port number, destination, and additional information.

Table 3-4 NetBackup media server outbound ports and destinations

Port name and number	Destination	Notes
veritas_pbx 1556	Master server	<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 and is used to backup or restore the client files or data.
13783	Authentication server	<p>Authenticates users and machines.</p> <p>Used only when NetBackup access control (NBAC) is enabled.</p>
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

This information applies to remote EMM servers in the NetBackup setups that are older than 7.6.

[Table 3-5](#) shows the ports that the EMM server uses to connect to remote hosts.

Table 3-5 NetBackup EMM server outbound ports and destinations

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

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

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

Client outgoing ports

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

Table 3-6 NetBackup client outbound ports and destinations

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

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 connect to remote hosts.

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.
13783	Authentication server	Establishes user credentials for administration.

Java console outgoing ports

[Table 3-8](#) shows the ports that the Java console uses to connect to remote hosts.

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

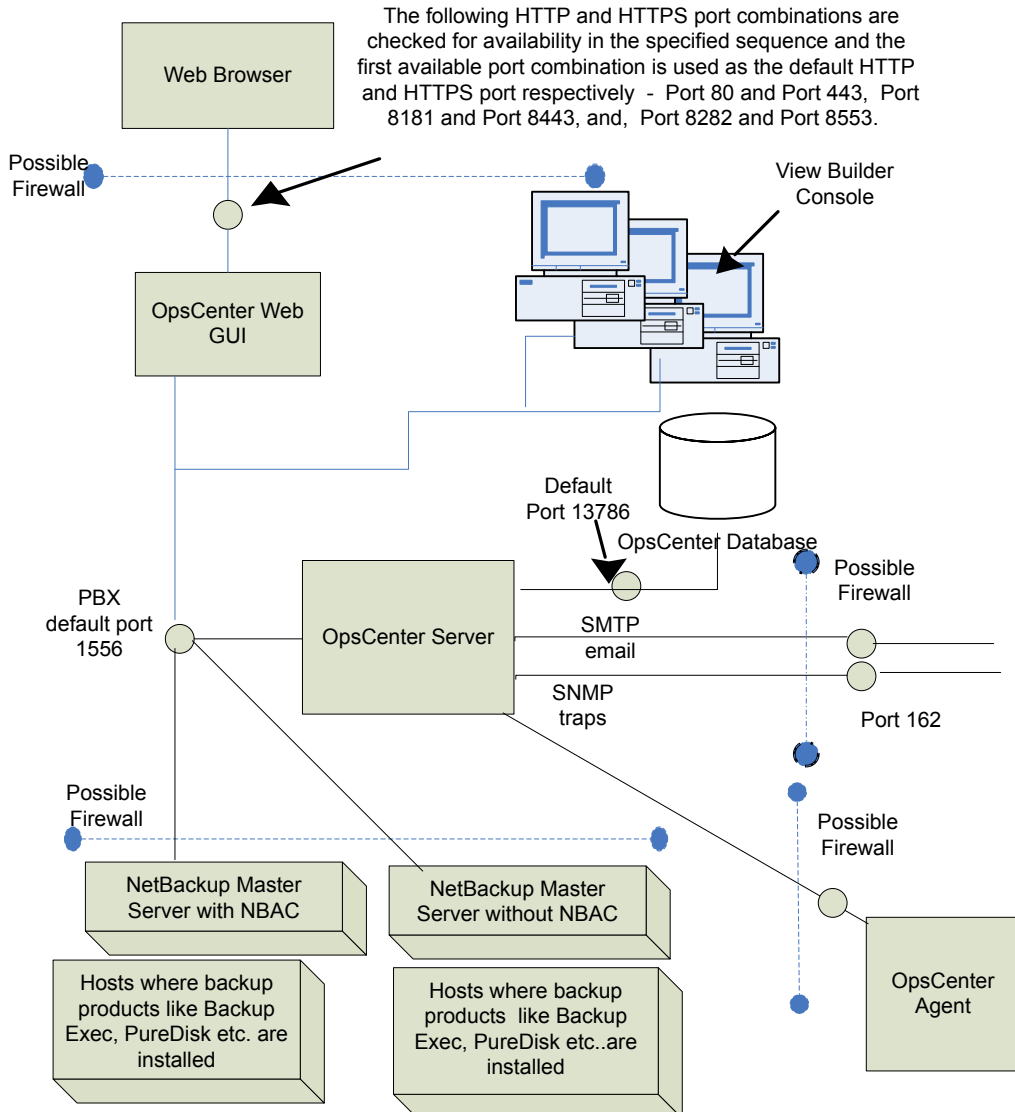
- The following topics describe port information that is important if you use NetBackup with OpsCenter, Backup Exec, and other products that interoperate with NetBackup:
- See [“About communication and firewall considerations”](#) on page 102.
 - See [“Ports required to communicate with backup products”](#) on page 103.
 - See [“Web browser to NetBackup Web GUI connection”](#) on page 104.
 - See [“About NetBackup user interface and NetBackup server software communication”](#) on page 105.
 - See [“About NetBackup server to NetBackup master server \(NBSL\) communication”](#) on page 105.
 - See [“About SNMP traps”](#) on page 106.

- See [“About communication between NetBackup and Sybase database communication”](#) on page 106.
- See [“About email communication in NetBackup”](#) on page 106.

About communication and firewall considerations

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

Figure 3-1 Key NetBackup components and how they communicate



Ports required to communicate with backup products

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

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

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

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

Web browser to NetBackup Web GUI connection

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

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

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

Table 3-11 Default HTTP and HTTPS ports

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

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

Sr. No.	HTTP port number	HTTPS port number	Description
2.	8181	8443	Port 8181 and Port 8443 are checked for availability. <ul style="list-style-type: none"> ■ If port 8181and port 8443 are available, port 8181 is used as the default HTTP port and port 8443 is used as the default HTTPS port. ■ In case another application like VRTSWeb installed with VCS or any other product uses one or both ports, then the next port combination is checked for availability.
3.	8282	8553	Port 8282 and Port 8553 are checked for availability.

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

About NetBackup user interface and NetBackup server software communication

The NetBackup web graphical user interface uses Veritas 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.

Veritas Private Branch Exchange (PBX) is used for communication and requires a port opened on the OpsCenter server and the NetBackup master server for input and output. The default PBX port that is used is 1556. Configuring the PBX port is not supported in OpsCenter 7.5 and later versions.

About SNMP traps

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

About communication between NetBackup and 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 email communication in NetBackup

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 107.
- See [“Specifying firewall connection options on a NetBackup server or client”](#) on page 108.
- See [“Specifying firewall connection options for destination computers from a source computer”](#) on page 111.
- See [“Editing port information in configuration files”](#) on page 113.
- See [“Updating client connection options”](#) on page 114.

- See [“Updating port settings for the Media Manager in the vm.conf file”](#) on page 114.

Enabling or disabling random port assignments

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

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

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

The following procedure explains how to specify port assignments.

To specify port assignments from the NetBackup Administration Console

- 1 In the **NetBackup Administration Console**, expand one of the following:
 - To specify a master server's port assignments, expand **NetBackup Management > Host Properties > Master Servers**
 - To specify a media server's port assignments, expand **NetBackup Management > Host Properties > Media Servers**
- 2 Double click the host you want to configure.
- 3 Click **Port Ranges**.
- 4 Check or clear **Use random port assignments**.

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

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).

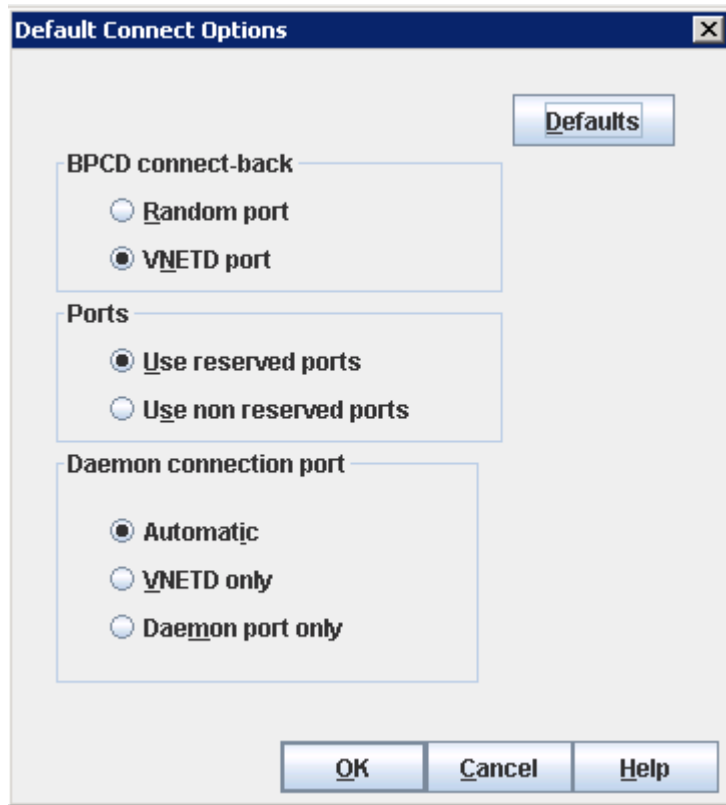
In addition, you can set the default connection options for all of the other destination computers from the source computer. For example, if there is a firewall between the master server and the media servers, you can specify all the connection options from the NetBackup master server.

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** in the left pane.
- 2 In the right pane, select the master server.
- 3 On the **Actions** menu, click **Properties**.
- 4 In the properties dialog box in the left pane, select **Firewall**
- 5 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.

■

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

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

Choose one of the following:

- **Random port.**
Specifies that the host computer use the legacy `bpcd` random port callback method to connect to other computers.
- **VNETD port.**
Specifies that the host computer use the `vnetd` daemon to connect to other computers.

7 (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 non-reserved ports.**
When in effect, the source computer connects to `bpcd` on destination computers using a non-reserved port number.
Make sure to perform step 9 of this procedure, which ensures that other computers in the NetBackup environment also are configured for non-reserved ports.

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

Choose one of the following:

- **Automatic.**
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.**
Specifies that other computers use the legacy port number to connect to this host.
When `bpcd` connections are made using the `vnetd` port number, the **Ports** and **BPCD connect-back** options are ignored. In this case, NetBackup uses non-reserved 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.

- 9 (Conditional) Configure other computers in the NetBackup environment to use non-reserved ports.

Perform this step if you selected **Use non-reserved ports**.

Configure the clients to use non-reserved 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](#).

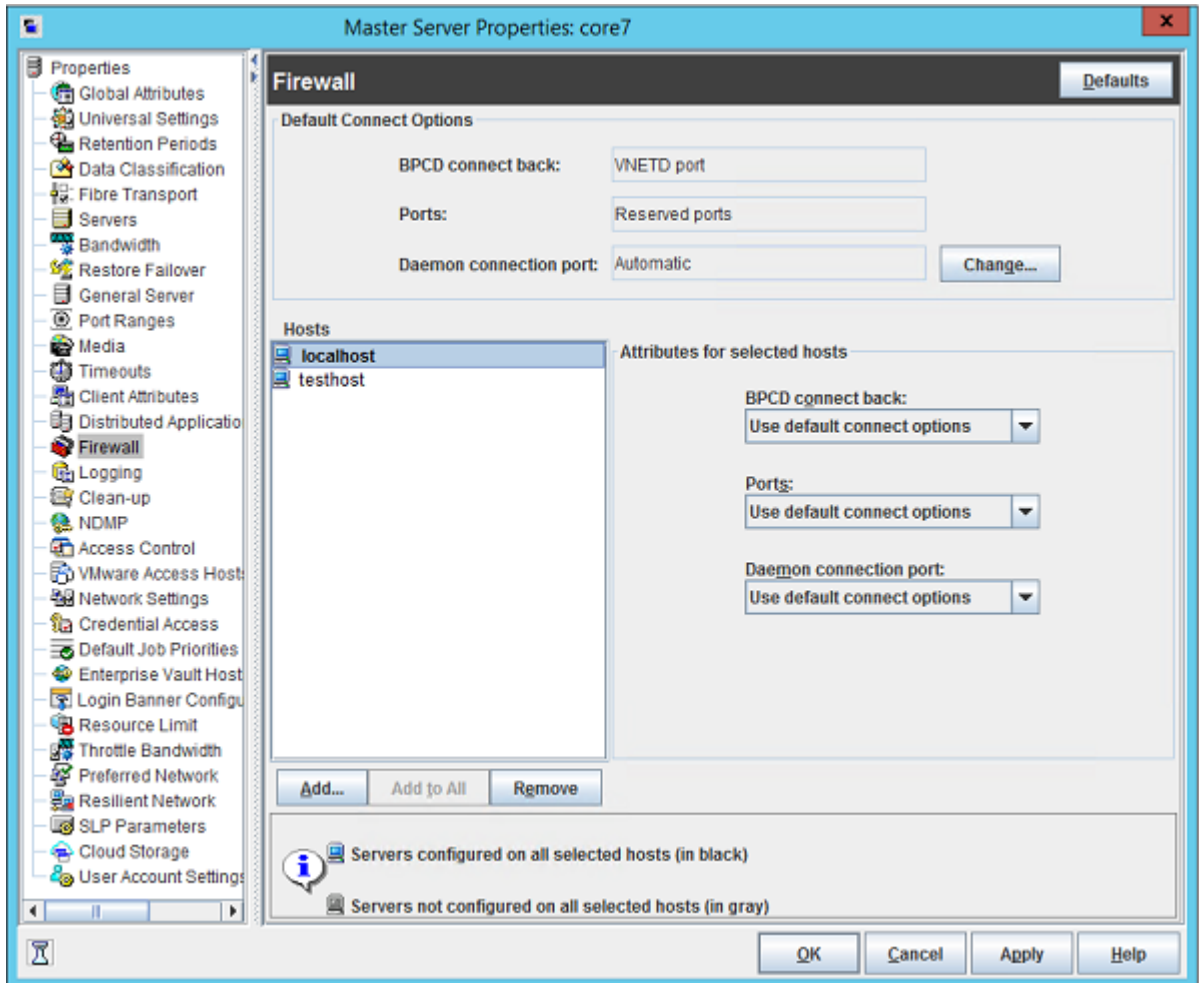
Specifying firewall connection options for destination computers from a source computer

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 108.

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

Editing port information in configuration files

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

- `ALLOW_NON_RESERVED_PORTS`
- `CLIENT_PORT_WINDOW`
- `CLIENT_RESERVED_PORT_WINDOW`
- `CONNECT_OPTIONS`
- `DEFAULT_CONNECT_OPTIONS`
- `RANDOM_PORTS`
- `SERVER_RESERVED_PORT_WINDOW`
- `SERVER_PORT_WINDOW`

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

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

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

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

```
bpgetconfig options > outputfile
```

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

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

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

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

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

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

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

Updating client connection options

NetBackup provides the following ways to specify client connection options:

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

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

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

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

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

- On Linux or UNIX, the path is as follows:
`/usr/openv/volmgr/vm.conf`
- On Windows systems, the path is as follows:
`install_path\volmgr\vm.conf`

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

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

Setting	Description
<code>CLIENT_PORT_WINDOW</code>	<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>Note: The <code>CONNECT_OPTIONS</code> setting affects only connections to hosts that run NetBackup 7.0. 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"> ■ If <code>0</code>, the host uses the <code>vnetd</code> port. If that attempt fails, the hosts uses the legacy port number. ■ If <code>1</code>, the host uses only <code>vnetd</code> to connect to the server. ■ If <code>2</code>, the host uses the legacy Media Manager port. <p>You can specify multiple <code>CONNECT_OPTIONS</code> settings in the <code>vm.conf</code> file.</p> <p>For NetBackup, 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.

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

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

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

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

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

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

Auditing NetBackup operations

This chapter includes the following topics:

- [About NetBackup auditing](#)
- [Viewing the current audit settings](#)
- [Configuring auditing on a NetBackup master server](#)
- [User identity in the audit report](#)
- [About Enhanced Auditing](#)
- [Enabling Enhanced Auditing](#)
- [Configuring Enhanced Auditing](#)
- [Disabling Enhanced Auditing](#)
- [Auditing host property changes](#)
- [Retaining and backing up audit trail records](#)
- [Viewing the audit report](#)
- [Using the command line -reason or -r option](#)
- [nbaudit log behavior](#)
- [Audit alert notification for audit failures](#)

About NetBackup auditing

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

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

About the NetBackup Audit Manager

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

The Audit Manager provides the mechanism to query and report on auditing information. For example, an administrator can search specifically for information based on the following:

- When an action occurred
- The actions that a specific user performed
- The actions that were performed in a specific content area
- Changes to the audit configuration

Actions that NetBackup audits

You can view the actions NetBackup audits with the `nbauditreport` command or in NetBackup OpsCenter.

See [“Viewing the audit report”](#) on page 132.

When auditing is enabled, NetBackup records the following user-initiated actions.

Policies actions	Adding, deleting, or updating policy attributes, clients, schedules, and backup selections lists.
Activity monitor actions	Canceling, suspending, resuming, restarting, or deleting any type of job creates an audit record.
Storage units actions	Adding, deleting, or updating storage units. Note: Actions that are related to Storage Lifecycle Policies are not audited.
Storage servers actions	Adding, deleting, or updating storage servers.
Disk pools and Volume pools actions	Adding, deleting, or updating disk or volume pools.
(Conditional) Host properties actions	Updates to the host properties. You must enable NetBackup Access Control (NBAC) to audit these changes.
Catalog information	<ul style="list-style-type: none">■ Verifying and expiring images.■ Read requests sent for the front-end usage data.
Certificate management	Creating, revoking, renewing, and deploying of certificates and specific certificate failures.
Token management	Creating, deleting, and cleanup of tokens and specific token issuing failures.
User management	Adding and deleting users in the Enhanced Auditing mode.
Hold operations	Creating, modifying, and deleting hold operations.
Host database	NetBackup host database related operations.
Login attempts	Any successful or failed login attempts for NetBackup Administration Console and NetBackup API.
Security configuration	Information related to changes made to the security configuration settings.
Starting a restore job	NetBackup does not audit when other types of jobs begin. For example, NetBackup does not audit when a backup job begins.
Enabling or disabling NetBackup Auditing	
Starting and stopping the NetBackup Audit Manager (<code>nbaudit</code>).	Starting and stopping of the <code>nbaudit</code> manager is always audited, even if auditing is disabled.
User action that fails to create an audit record	If auditing is enabled but a user action fails to create an audit record, the audit failure is captured in the <code>nbaudit</code> log.

Changes to the <code>bp.conf</code> file (UNIX) or the registry (Windows).	To audit changes to the <code>bp.conf</code> file or the registry, you must enable NetBackup Access Control (NBAC). Manual changes to the <code>bp.conf</code> file or the registry are not audited. See “Auditing host property changes” on page 131. See “Configuring NetBackup Access Control (NBAC)” on page 154.
Authorization failure	<ul style="list-style-type: none">■ When you enable Enhanced Auditing, authorization failure is audited. See “About Enhanced Auditing” on page 125.

Actions that NetBackup does not audit

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

Any failed actions.	NetBackup logs failed actions in NetBackup error logs. Failed actions do not display in audit reports because a failed attempt does not bring about a change in the NetBackup system state.
The effect of a configuration change.	The results of a change to the NetBackup configuration are not audited. For example, the creation of a policy is audited, but the jobs that result from its creation are not.
The completion status of a manually initiated restore job.	While the act of initiating a restore job is audited, the completion status of the job is not audited. Nor is the completion status of any other job type, whether initiated manually or not. The completion status is displayed in the Activity Monitor.
Internally initiated actions.	NetBackup-initiated internal actions are not audited. For example, the scheduled deletion of expired images, scheduled backups, or periodic image database cleanup is not audited.
Storage Lifecycle Policy actions	Actions that are related to Storage Lifecycle Policies are not audited.

Viewing the current audit settings

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

For directions about how to use OpsCenter to configure auditing, see the [Veritas NetBackup OpsCenter Administrator's Guide](#).

To view the current audit settings

- 1 From a command prompt, locate the `nbemmcmd` command on the master server in the following directory:
 - On Windows:
`Install_path\Veritas\NetBackup\bin\admincmd`

- On UNIX:

```
/usr/opensv/netbackup/bin/admincmd
```

- 2 Enter the `nbemmcmd` command using the following syntax:

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

Where *masterserver* is the master server in question.

Note: The options are case-sensitive.

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

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

Configuring auditing on a NetBackup master server

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

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

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

See the [Veritas NetBackup OpsCenter Administrator's Guide](#) for more details.

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

To configure NetBackup auditing on a master server

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

- On Windows:

```
Install_path\Veritas\NetBackup\bin\admincmd
```

- On UNIX:

```
/usr/opensv/netbackup/bin/admincmd
```

- 2 Enter the `nbemmcmd` command using the following syntax:

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

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

Note: The options are case-sensitive.

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

For example:

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

3 Configure the audit retention period using the following syntax:

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

Where *number_of_days* indicates (in days) how long audit records are to be retained for the audit report. If no retention period is indicated, the default audit retention period is 90 days.

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

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

See the following topic for more information.

See [“Retaining and backing up audit trail records”](#) on page 132.

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

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

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

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

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

Note: When a back level media server connects to an 8.0 master server, the `nbauditreport` operation fails. Upgrade the media server to 8.0 to successfully run the `nbauditreport` operation.

See [“Viewing the audit report”](#) on page 132.

User identity in the audit report

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

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

- By default, only a root or an administrator user can perform NetBackup operations through a command-line interface as well as through the **NetBackup Administration Console**. The root or the administrator are hence audited with root or administrator user name.
- When either Enhanced Auditing or NBAC is enabled, the actual name of the user who performed NetBackup operations through the command-line interface or through the **NetBackup Administration Console** are recorded in the audit report.
- For certain actions that are performed through web services, the user cannot be identified. For example: `nbcertcmd -getcertificate`. NetBackup attributes these actions to **<anonymous>** user. The audit report shows **<anonymous>** as the user for such actions or commands.
- All tasks are audited as root or administrator when neither Enhanced Auditing nor NBAC is enabled.

See [“About using NetBackup Access Control \(NBAC\)”](#) on page 150.

See [“About Enhanced Auditing”](#) on page 125.

About Enhanced Auditing

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

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

By default, only a root or administrator can perform NetBackup operations through the command-line interface. However, with NetBackup configured for Enhanced Auditing and with the right NetBackup Administrator privileges, users can perform

NetBackup operations through the command-line interface. Enhanced Auditing provides coarse access control where the user is either an administrator or not one. Enhanced Auditing is not supported on the NetBackup Appliances.

Note: NBAC and Enhanced Auditing are mutually exclusive features.

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

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

Table 4-1 Commands and categories supported for Enhanced Auditing

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

Enabling Enhanced Auditing

Use the following procedure to enable Enhanced Auditing.

To configure NetBackup for Enhanced Auditing

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

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

- 2 Restart the NetBackup services.

See [“Disabling Enhanced Auditing”](#) on page 131.

See [“Configuring Enhanced Auditing”](#) on page 127.

Configuring Enhanced Auditing

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

- A security certificate is mandatory when you connect to a media server through the **NetBackup Administration Console**.
See [“Connecting to a media server with Enhanced Auditing”](#) on page 127.
- When you do a change server from a master server to another master server, you have to execute additional steps on the master server.
See [“Changing a server across NetBackup domains”](#) on page 128.

Connecting to a media server with Enhanced Auditing

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

To generate a security certificate for a server

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

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

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

The following is the output:

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

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

```
Certificate deployed successfully
```

```
Operation completed successfully.
```

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

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

Changing a server across NetBackup domains

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

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

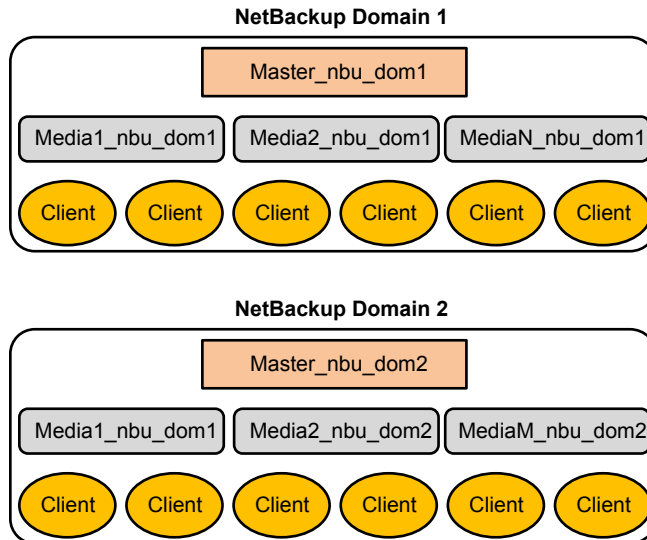
The following steps help you to change the server and set up the trust on both master servers.

To change server from a master to master server

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

Consider two master servers, `Master_nbu_dom1` and `Master_nbu_dom2`.

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



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

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

On UNIX and Linux:

```
/usr/opensv/netbackup/sec/at/bin/vssat setuptrust -b
Master_server_nbu_dom1:1556:nbatd -s high on Host_nbu_dom2.
```

On Windows:

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

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

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

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

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

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

You can also invoke `/usr/openv/java/sec/at/bin/vssat setuptrust -b Master_server_nbu_dom2:1556:nbatd -s high` on the NetBackup Administration Console host.

Configuration requirements if using Change Server with NBAC or Enhanced Auditing

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

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

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

- Add *fromServer* to the host properties Additional Servers list on *toServer*.
- If *fromServer* and *toServer* are from different NetBackup domains (media servers of different master servers):
 - Use the `vssat` command to set up trust between the master servers of *fromServer* and *toServer*. (See [“Changing a server across NetBackup domains”](#) on page 128. Refer to step 2 in the procedure.)
 - Add the master server of *fromServer* to the host properties Additional Servers list on *toServer*.
- If *fromServer* or *toServer* are media servers:
 - Use the `bpnbaz -ProvisionCert` command to deploy the security (Machine) certificate if needed. (See [“Connecting to a media server with Enhanced Auditing”](#) on page 127.)

Additional configuration steps

To use the `auth.conf` file:

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

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

```
USE_AUTH_CONF_NBAC = YES
```

To use the Remote Administration Console:

- Set up trust with each master server by using either the `vssat` command or explicitly log on to each server at least once. (See [“Changing a server across NetBackup domains”](#) on page 128. Refer to step 2 in the procedure.)

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

Disabling Enhanced Auditing

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

To disable Enhanced Auditing

- 1 Run the `bpbaz -DisableExAudit` command.
- 2 Restart the NetBackup services.

Auditing host property changes

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

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

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

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

Retaining and backing up audit trail records

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

See [“Configuring auditing on a NetBackup master server”](#) on page 122.

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

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

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

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

Viewing the audit report

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

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

See the [Veritas NetBackup OpsCenter Administrator's Guide](#) for more details.

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

The **Alert Notification** button in the **NetBackup Administration Console** can notify administrators when an audit failure occurs.

See [“Audit alert notification for audit failures”](#) on page 139.

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

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

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

To view the NetBackup audit report

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

`Install_path\Veritas\NetBackup\bin\admincmd`
- On UNIX:

`/usr/opensv/netbackup/bin/admincmd`
- 2 In its simplest form, enter the `nbauditreport` command using the following syntax:

`nbauditreport`

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

Note: The options are case-sensitive.

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

<code>-ctgy AUDITCFG</code>	Use <code>-ctgy AUDITCFG</code> to display information pertaining to audit configuration changes.
<code>-ctgy AUDITSVC</code>	Use <code>-ctgy AUDITSVC</code> to display information pertaining to the starting and stopping of the NetBackup Audit service (<code>nbaudit</code>).
<code>-ctgy BPCONF</code>	Use <code>-ctgy BPCONF</code> to display information pertaining to changes in the <code>bp.conf</code> file.
<code>-ctgy CERT</code>	Use <code>-ctgy CERT</code> to display information pertaining to changes in certificate deployment.
<code>-ctgy LOGIN</code>	Use <code>-ctgy LOGIN</code> to display information related to NetBackup Administration Console and NetBackup API login attempts.
<code>-ctgy TOKEN</code>	Use <code>-ctgy TOKEN</code> to display information related to authorization tokens.
<code>-ctgy SEC_CONFIG</code>	Use <code>-ctgy SEC_CONFIG</code> to display information related to changes made to the security configuration settings.
<code>-ctgy HOLD</code>	Use <code>-ctgy HOLD</code> to display information related to creating, modifying, and deleting hold operations.
<code>-ctgy AZFAILURE</code>	Use <code>-ctgy AZFAILURE</code> to display information related to authorization failure when Enhanced Auditing is enabled.
<code>-ctgy CATALOG</code>	Use <code>-ctgy CATALOG</code> to display information related to verifying and expiring images; and read requests sent for the front-end usage data.
<code>-ctgy HOST</code>	Use <code>-ctgy HOST</code> to display NetBackup host database related operations.
<code>-ctgy USER</code>	Use the <code>-ctgy USER</code> to display information pertaining to addition and deletion of users in the Enhanced Auditing mode.
<code>-user</code> <code><username[:domainname]></code>	Use to indicate the name of the user for whom you'd like to display audit information.

`-fmt SUMMARY`

If no report output format option (`-fmt`) is specified, the `SUMMARY` option is used by default.

`-fmt DETAIL`

The `-fmt DETAIL` option displays a comprehensive list of audit information. For example, when a policy is changed, this view lists the name of the attribute, the old value, and the new value.

`-fmt PARSABLE`

The `-fmt PARSABLE` option displays the same set of information as the `DETAIL` report but in a parsable format. The report uses the pipe character (`|`) as the parsing token between the audit report data.

`[-nottruncate]`

Use the `-nottruncate` option to display the old and new values of a changed attribute on separate lines in the details section of the report.

Note: `-nottruncate` is valid only with the `-fmt DETAIL` option.

`[-pagewidth <NNN>]`

Use the `-pagewidth` option to set the page width for the details section of the report.

Note: `-pagewidth` is valid only with the `-fmt DETAIL` option.

`[-order`

`<DTU|DUT|TDU|TUD|UDT|UTD>]`

The `-order` option is valid only with `-fmt PARSABLE`. Use it to indicate the order in which the information appears.

Use the following parameters:

- D (Description)
- T (Timestamp)
- U (User)

3 The audit report contains the following details:

DESCRIPTION

The details of the action that was performed. The details include the new values that are given to a modified object and the new values of all attributes for a newly created object. The details also include the identification of any deleted objects.

USER	<p>The identity of the user who performed the action. The identity includes the user name, the domain, and the domain type of the authenticated user.</p> <p>See “User identity in the audit report” on page 125.</p>
TIMESTAMP	<p>The time that the action was performed. The time is given in Coordinated Universal Time (UTC) and indicated in seconds. (For example, 12/06/11 10:32:48.)</p>
CATEGORY	<p>The category of user action that was performed. The CATEGORY displays only with the <code>-fmt DETAIL PARSABLE</code> options.</p> <p>Examples include the following:</p> <ul style="list-style-type: none">■ AUDITSVC START, AUDITSVC STOP■ POLICY CREATE, POLICY MODIFY, POLICY DELETE
ACTION	<p>The action that was performed. The ACTION displays only with the <code>-fmt DETAIL PARSABLE</code> options.</p> <p>Examples include the following:</p> <ul style="list-style-type: none">■ START, STOP■ CREATE, MODIFY, DELETE
REASON	<p>The reason that the action was performed. A reason displays if a reason was specified in the command that created the change. The <code>bpsetconfig</code> and the <code>nbsetconfig</code> commands accept the <code>-r</code> option.</p> <p>See “Using the command line -reason or -r option” on page 137.</p> <p>The reason displays only with the <code>-fmt DETAIL PARSABLE</code> options.</p>
DETAILS	<p>An account of all of the changes, listing the old values and the new values. Displays only with the <code>-fmt DETAIL PARSABLE</code> options.</p>

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

[Figure 4-1](#) shows the default contents of an audit report that was run on `server1`.

Figure 4-1 Summary audit report example

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

Audit records fetched: 3
```

Using the command line **-reason** or **-r** option

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

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

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

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

- `bpdjobs`
- `bpplcatdrinfo`
- `bpplclients`
- `bppldelete`
- `bpplinclude`
- `bpplinfo`
- `bpplsched`
- `bpplschedrep`
- `bpolicynew`
- `bpsetconfig`

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

- `bpstuadd`

- `bpstudel`
- `bpsturep`
- `nbdecommission`
- `nbdevconfig`
- `nbcertcmd`
- `nbsetconfig`
- `vmppool`

For more information on using the commands, see the [NetBackup Commands Reference Guide](#).

nbaudit log behavior

The `nbaudit` log is found in the following location:

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

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

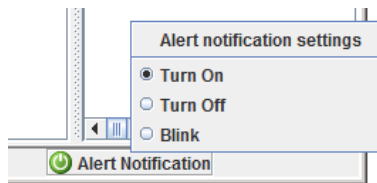
The **Alert Notification** button in the **NetBackup Administration Console** can notify administrators when an audit failure occurs.

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

- The audit record limits the details of an entry to a maximum of 4096 characters. (For example, the Policy name.) The remaining characters are truncated while stored in the audit database.
- The audit record limits the restore image IDs to a maximum of 1024 characters. The remaining characters are truncated while stored in the audit database.
- Rollback operations are not audited.
Some operations are carried out as multiple steps. For example, creating an MSDP-based storage server consists of multiple steps. Every successful step is audited. Failure in any of the steps results in a rollback, or rather, the successful steps may need to be undone. The audit record does not contain details about rollback operations.

Audit alert notification for audit failures

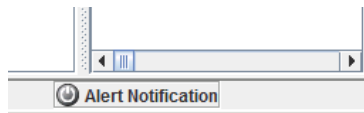
The **Alert Notification** option is located in the status bar at the bottom of the **NetBackup Administration Console**. If it is configured to do so, the option can indicate when an auditable action has failed to create an audit record. For example, if a policy attribute is changed but the NetBackup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



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

Table 4-2 Audit alert notification settings

Turn on	<p>When it is set to Turn on, a pop-up message displays in the following situation:</p> <p>Auditing is enabled, but an auditable action is performed in the NetBackup Administration Console and has failed to create an audit record.</p> <p>A pop-up message appears to alert the administrator about the failure.</p>
Blink	<p>When it is set to Blink, the option blinks in the event of an auditing failure. Click the option to display the failure message.</p>
Turn off	<p>When it is set to Turn off, an auditing failure does not display a notification. The option appears as gray.</p>



Note: **Turn off** does not mean that auditing is disabled. Auditing continues, but audit failure messages in the **NetBackup Administration Console** are disabled.

Access control security

This chapter includes the following topics:

- [About access control in NetBackup](#)
- [User management](#)
- [User authentication](#)
- [Impact of Access Control via Enhanced Auditing on Java interface authorization](#)

About access control in NetBackup

NetBackup provides the following types of access control:

- The NetBackup Admin Console (default).

Access control is limited to the NetBackup Administration Console. (Interfaces like the Backup, Archive, and Restore client and the NetBackup MS SQL Client are not affected.) Any non-root or non-administrator user can access the NetBackup Administration Console. Access control is view-based, not role-based. The `auth.conf` defines the NetBackup applications that users can access. A user must be a root user or administrator to perform NetBackup operations with the CLI.

For detailed information about access control with the NetBackup Administration Console, refer to the [NetBackup Administrator's Guide, Volume I](#).
- Enhanced Auditing.

This feature allows a non-root user or a non-administrator to perform all the NetBackup operations through a command line interface or the NetBackup Administration Console. The user is authorized to either perform all operations or no operations. This feature does not offer role-based access control. See [“About Enhanced Auditing”](#) on page 125.
- NetBackup Access Control (NBAC)

NBAC is the role-based access control provided with NetBackup. It provides access control for master servers, media servers, and clients in situations where you want to:

- Use a set of permissions for different levels of administrators for an application. A backup application can have operators (to monitor jobs) or administrators (with full permission to access, configure, and operate any NetBackup authorization object). You can also have Security administrators who can only configure access control.
- Separate the administrators, so that root or administrator permissions are not required to administer the system. You can have separate administrators for the systems other than administrators for applications.

See [“About using NetBackup Access Control \(NBAC\)”](#) on page 150.

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

Table 5-1

Access and auditing	NetBackup Admin Console and <code>auth.conf</code>	Enhanced Auditing	NBAC
Who can use the NetBackup Admin Console?	Root users and administrators have full access to the Admin Console. Non-root users or non-administrators are limited to the Backup, Archive, and Restore application by default. Otherwise, these users can access the applications defined for them in the <code>auth.conf</code> file.	Root users, administrators, and NetBackup administrators have full access to the Admin Console. Non-root users or non-administrators are limited to the Backup, Archive, and Restore application by default.	Root users and administrators have full access to the Admin Console. A user's NBAC group membership determines which applications they are authorized to use.
Who can use the CLI?	Root users and administrators have full access to the CLI.	Root users, administrators, and NetBackup administrators have full access to the CLI.	Root users or administrators have full access to the CLI. Users authorized by NBAC can use the CLI. Their NBAC group membership determines which commands they are authorized to use.
How is a user audited?	As root or administrator	With the real user name	With the real user name

Table 5-1 (continued)

Access and auditing	NetBackup Admin Console and auth.conf	Enhanced Auditing	NBAC
Compatibility with other features	Enhanced Auditing	NBAC works independently.	NetBackup Admin Console and auth.conf Enhanced Auditing is not compatible with NBAC.

Refer to the following flowcharts for details about the different access control methods.

Figure 5-1 Access control for CLI users with Enhanced Auditing

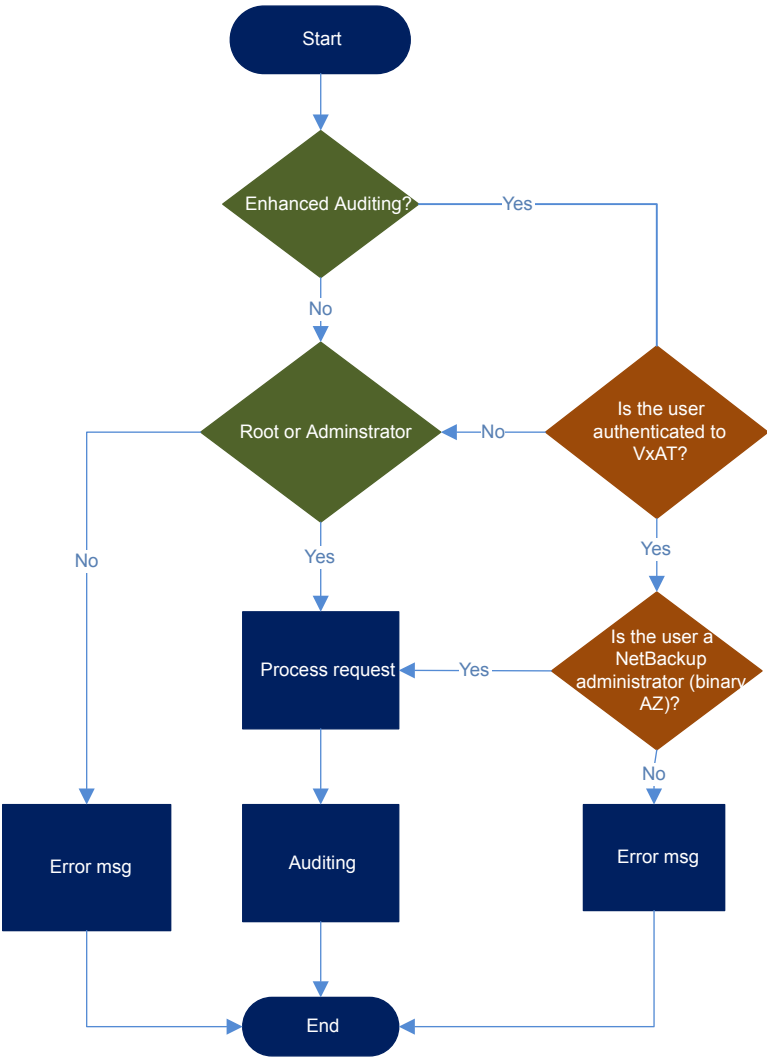


Figure 5-2 Access control for NetBackup-Java based users with Enhanced Auditing enabled

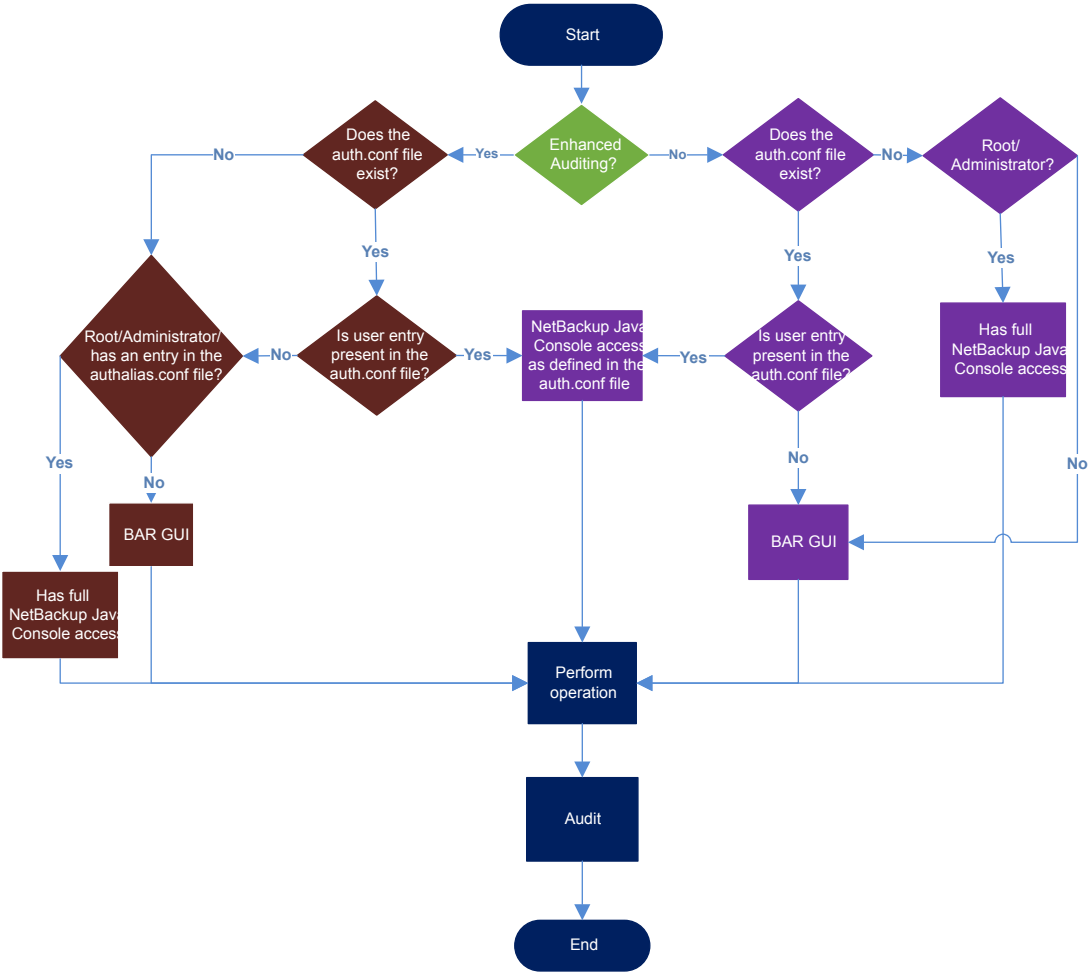


Figure 5-3 Access control for CLI users with NBAC

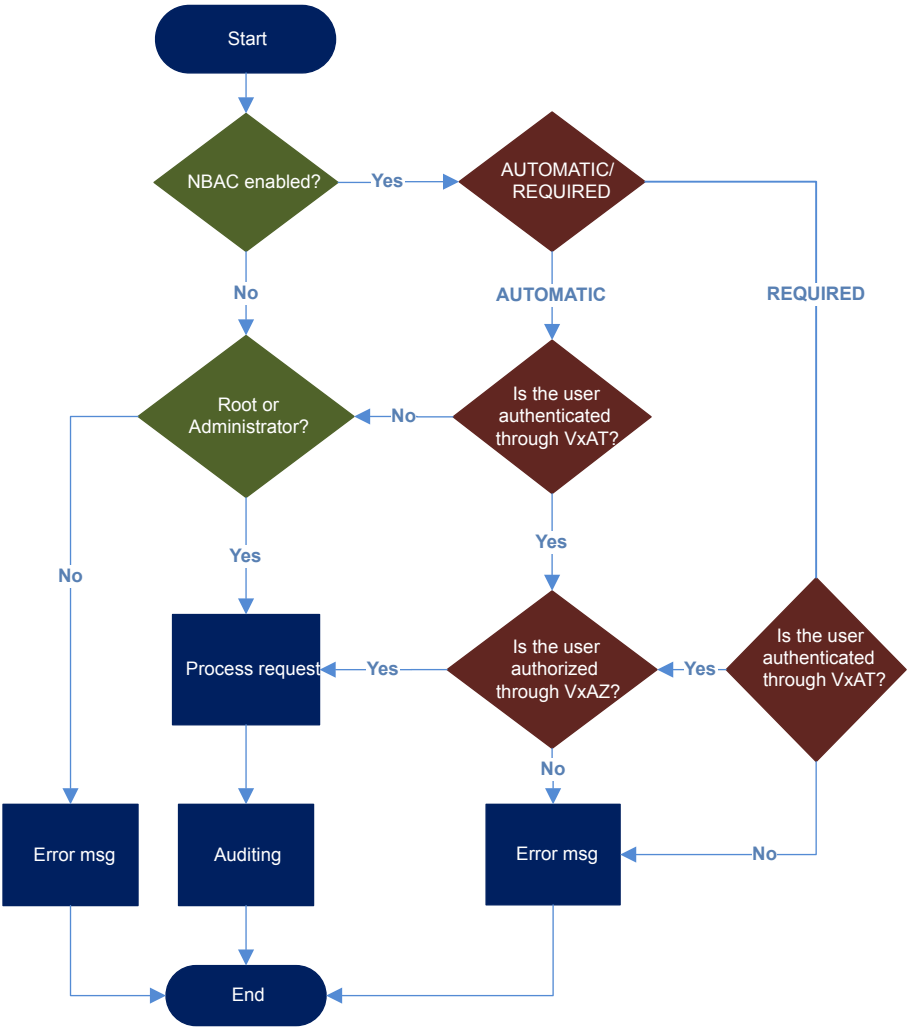
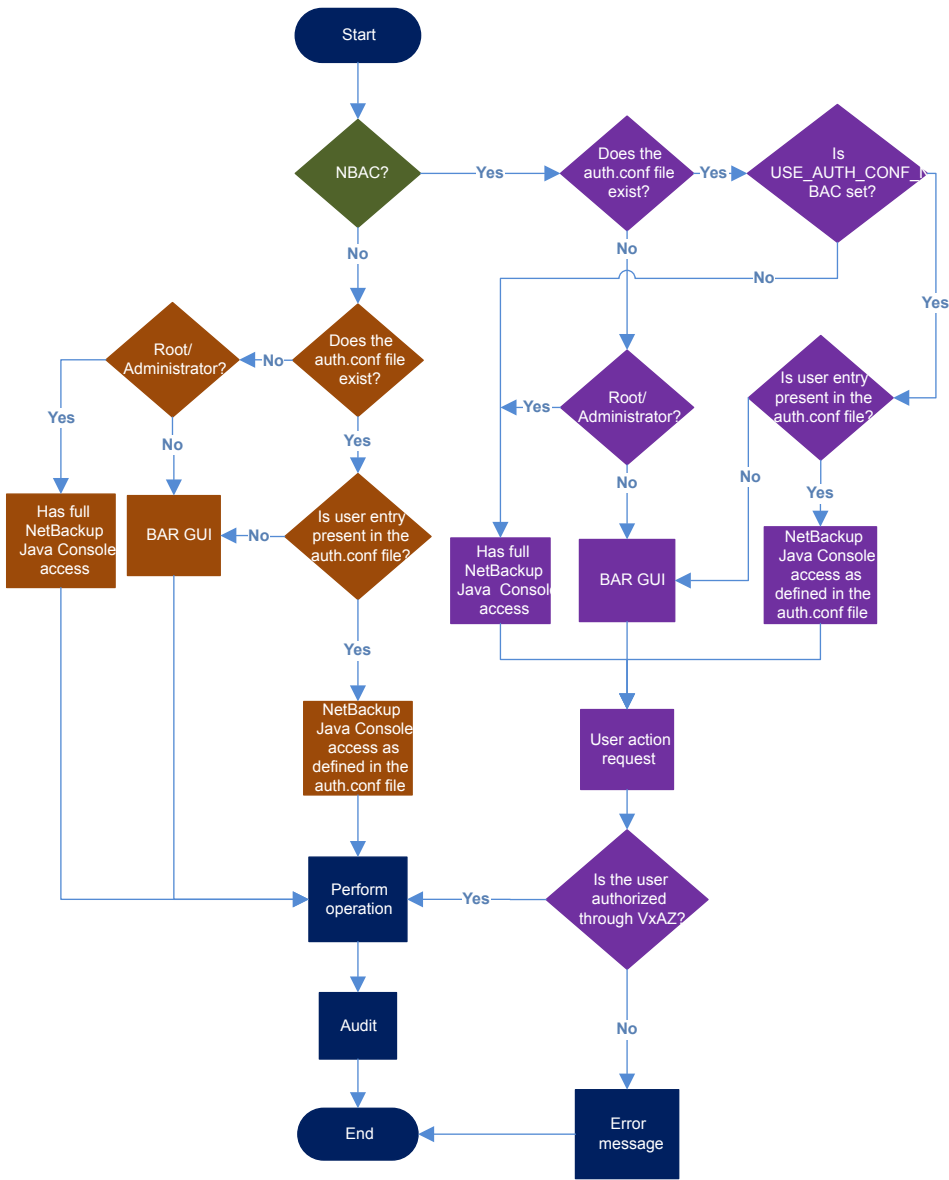


Figure 5-4 Access control for NetBackup-Java based users with NBAC



User management

With NetBackup configured for Enhanced Auditing, the administrator can:

- Grant and revoke NetBackup administrator privileges to users.
- Look up a user who has NetBackup administrator privileges.
- List users with NetBackup administrator privileges.

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

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

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

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

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

The following table lists information about each command:

Table 5-2

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

For more information about the `bpnbaz` command, see the [NetBackup Commands Reference Guide](#).

User authentication

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

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

The log in process for UNIX and Windows users varies.

UNIX

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

Windows

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

Impact of Access Control via Enhanced Auditing on Java interface authorization

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

See “[User management](#)” on page 147.

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

Table 5-3 User access

auth.conf entry	CLI access	Java interface access
Debbie has an entry in the <code>auth.conf</code> file.	No access	Access as specified in the <code>auth.conf</code> file

Table 5-3 User access (*continued*)

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

NetBackup Access Control Security (NBAC)

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 \(NBAC\)](#)
- [Configuring Access Control host properties for the master and media server](#)
- [Access Control host properties dialog for the client](#)
- [Troubleshooting Access Management](#)
- [Using the Access Management utility](#)
- [About determining who can access NetBackup](#)
- [Viewing specific user permissions for NetBackup user groups](#)
- [Upgrading NetBackup Access Control \(NBAC\)](#)
- [Upgrading NetBackup when an older version of NetBackup is using a root broker installed on a remote machine](#)

About using NetBackup Access Control (NBAC)

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

- Use a set of permissions for different levels of administrators for an application. A backup application can have operators (perhaps load and unload tapes). It can have local administrators (manage the application within one facility). It can also have overall administrators who may have responsibility for multiple sites and determine backup policy. Note that this feature is very useful in preventing user errors. If junior level administrators are restricted from certain operations, they are prevented from making inadvertent mistakes.
- Separate administrators so that root permission to the system is not required to administer the system. You can then separate the administrators for the systems themselves from the ones who administer the applications.

The following table lists the NBAC considerations.

Table 6-1 NBAC considerations

Consideration or issue	Description or resolution
Prerequisites before you configure NBAC	<p>This prerequisites list can help you before you start to configure NBAC. These items ensure an easier installation. The following list contains the information for this installation:</p> <ul style="list-style-type: none"> ■ User name or password for master server (root or administrator permission). ■ Name of master server ■ Name of all media servers that are connected to the master server ■ Name of all clients to be backed up ■ Host name or IP address <p>Note: Host names should be resolvable to a valid IP address.</p> <ul style="list-style-type: none"> ■ Use the <code>ping</code> or <code>tracert</code> command as one of the tools to ensure that you can see the hosts. Using these commands ensures that you have not configured a firewall or other obstruction to block access.
Determine if the master server, media server, or client is to be upgraded	<p>Determine if the master server, media server, or client is to be upgraded as follows:</p> <ul style="list-style-type: none"> ■ Some features are provided by upgrading master servers, some by media servers, and some from upgrading clients. ■ NetBackup works with a higher revision master server and lower revision clients and media servers. ■ Feature content determines what is deployed. ■ Deployment can be step wise if required.

Table 6-1 NBAC considerations (*continued*)

Consideration or issue	Description or resolution
Information about roles	<p>Determine the roles in the configuration as follows:</p> <ul style="list-style-type: none"> ■ Who administers the hosts (root permission on master server equals head administrator). ■ Determine roles to start and then add on the roles as required.
NBAC license 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. The solution is to grant the root and the administrator users <code>NBU_Admin</code> and <code>KMS_Admin</code> permissions manually.</p>
Windows Server Failover Clustering (WSFC) error messages while unhooking shared security services from PBX	<p>In WSFC environments running the <code>bpnbaz -UnhookSharedSecSvcsWithPBX <virtualhostname></code> command can trigger error messages. However the shared Authentication and Authorization services are successfully unhooked from PBX and the errors can be ignored.</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 REQUIRED mode	<p>If NBAC is running in REQUIRED mode and a catalog recovery was performed, NBAC needs to be reset back from PROHIBITED mode to REQUIRED mode.</p>
Policy validation fails in NBAC mode (USE_VXSS = REQUIRED)	<p>Back up, restore, and verification of policy for snapshot can fail in NBAC enabled mode if one of the following has been done.</p> <ul style="list-style-type: none"> ■ Authenticated Principle is removed from the NBAC group: <code>NBU_Users</code> group ■ Back up and restore permissions of <code>NBU_User</code> group have been removed

Table 6-1 NBAC considerations (*continued*)

Consideration or issue	Description or resolution
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 information about the <code>bpnbaz</code> command, see the NetBackup Commands Reference Guide.</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 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 154.

Configuring NetBackup Access Control (NBAC)

Note: The manual authentication and authorization client installs need to be done for older media servers and client hosts (less than NetBackup version 7.5). NetBackup version 7.5 has the authentication clients and authorization clients that are embedded in them. No authentication servers and authorization servers are needed on media servers and clients.

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

Configuring NetBackup Access Control (NBAC)

- 1 Configure the master server for NetBackup Access Control (NBAC).
See [“Configuring NetBackup Access Control \(NBAC\) on standalone master servers”](#) on page 155.

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

- 2 Configure media servers for NBAC.
See [“Configuring NetBackup Access Control \(NBAC\) on media servers”](#) on page 158.
- 3 Configure clients for NBAC.
See [“Installing and configuring access control on clients”](#) on page 160.

NBAC configuration overview

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

The `bpnbaz` utility is required to configure NBAC on the master servers, media servers, and clients. This tool also configures NBAC for all the back revision media's and client's hosts. See the following topic for a summary of the `bpnbaz` command: See [“NBAC configure commands summary”](#) on page 160. This topic provides an example of how to use these commands with specific details on recommended usage. Note that the services should be restarted on each of the servers and clients after configuration.

Since the configuration is done from the master server, ensure that operational communications links exist between the master server, the media servers, and the clients. To review the prerequisites list: See [“About using NetBackup Access Control \(NBAC\)”](#) on page 150. Review the list to ensure that you have noted all the associated media servers, clients, and the addresses to communicate with them.

See the following topic for troubleshooting information: See [“Configuration and troubleshooting topics for NetBackup Authentication and Authorization”](#) on page 176. 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 6-2 Example host names

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

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

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

Configuring NBAC on standalone master servers

- 1 Complete all of the NetBackup master server installations or upgrades.
- 2 Run the `bpnbaz -setupmaster` command.

Enter `y`. The system begins to gather configuration information. Then, the system begins to set up the authorization information.
- 3 Restart the NetBackup services on this computer after the `bpnbaz -setupmaster` command completes successfully.
- 4 Proceed to set up the media servers. See [“Configuring NetBackup Access Control \(NBAC\) on media servers”](#) on page 158.

Installing the NetBackup master server highly available on a cluster

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

Installing NetBackup with clustering

- 1 Configure the cluster system on which the NetBackup master server is to be installed.
- 2 Install the NetBackup master server on all nodes of the cluster.
- 3 Cluster the NetBackup master server.

HA information for replication and disaster recovery is described in the [NetBackup in Highly Available Environments Administrator's Guide](#)

Clustering information is described in the [NetBackup Clustered Master Server Administrator's Guide](#).
- 4 Do a test backup to ensure that it works within the NetBackup domain without having NBAC enabled.

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

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

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

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

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

- 1 Log on to the primary cluster node.
- 2 If you use Windows, open a command console.
- 3 For UNIX, change the directory to `/usr/opensv/netbackup/bin/admincmd`.
For Windows, change the directory to `C:\Program Files\Veritas\NetBackup\bin\admincmd`.
- 4 Run `bpbaz -setupmaster` on the active node.

- 5 Log on to the master server console GUI.
- 6 Restart the NetBackup services to ensure that the NBAC settings take place.

Configuring NetBackup Access Control (NBAC) on media servers

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

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

Configuring access control on media servers

- 1 Log on to the master server computer.
- 2 Run the `bpnbat -login` command.

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

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

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

See [“NBAC configure commands summary”](#) on page 160.

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

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

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

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

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

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

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

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

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

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

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

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

See [“Installing and configuring access control on clients”](#) on page 160.

Installing and configuring access control on clients

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

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

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

```
bpnbaz -setupClient
```

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

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

NBAC configure commands summary

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

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

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

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

Table 6-3 NBAC configure commands summary

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

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

Command	Description
<pre>bpbaz -SetupMaster [-fsa [<domain type>:<domain name>:]<user name>]</pre>	<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. The syntax is:</p> <ul style="list-style-type: none"> ■ <code>-fsa</code> option is used for provisioning a specific OS user as NBU Administrator. When using this option you are asked for the password for your current OS user identity. ■ <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. ■ <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. ■ <code>user name</code> is the particular OS user name you are designating as an NBU Administrator. <p>Note: The user is verified for the existence in the specified domain. Existing behavior of provisioning the logged-on Administrator or root as NBU Admin is preserved.</p>

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

Command	Description
<pre>bpbaz -SetupMedia [media.server.com [-out file] -all [-out file] -file progress.file] [-dryrun] [-disable]</pre>	<p>The <code>bpbaz -SetupMedia</code> command is run by an NBU_Administrator group member on the master server. It should not be run until a <code>bpbaz -SetupMaster</code> has been completed successfully. It expects connectivity between the master server and target media server systems. Either the <code>-all</code> or <code>target.server.com</code> options are required for this command.</p> <p>The syntax is:</p> <ul style="list-style-type: none"> ■ <code>media.server.com</code> is the name of a single target host. Use this option to add a single additional host for use with NBAC. ■ <code>-out</code> option is used to specify a custom output file name. By default, the output is written to the <code>SetupMedia.nbac</code> file. This option can be used with <code>-all</code> and the single host configuration options. ■ <code>-all</code> goes through all the storage units and collect all unique host names that are found in the storage unites. These can be tried in a sorted order. The results are written to the progress file. ■ <code>-file progress_file</code> option is used to specify an input file with a specific set of media server host names. After the run, status for each media server is updated in the progress file. Successfully completed ones are commented out for the subsequent runs. This command can be repeated until all the media servers in the input file are successfully configured. ■ <code>-dryrun</code> can generate the list of media server names and write them to the log. This option can work with <code>media.server.com</code> but it is intended to be used with the <code>-all</code> option. ■ <code>-disable</code> option can disable NBAC (USE_VXSS = PROHIBITED) on targeted hosts.

Table 6-3 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"> ■ <code>client.server.com</code> is the name of a single target host. If for example you wished to add a single additional host for use with NBAC, then this name is the option for you. ■ <code>-out</code> is an option that is used to specify a custom output file name. By default, the output is written to the <code>SetupClient.nbac</code> file. This option can be used with <code>-all</code> and the single host configuration options. The <code>-out</code> option is used to specify a custom output file name. By default, the output is written to the <code>SetupClient.nbac</code> file. This option can be used with <code>-all</code> and the single host configuration options. ■ <code>-all</code> is an option that goes through all the policies and collects all unique host names that are found within the policies. The policies are tried in a sorted order. The results are written to the progress file. ■ <code>-images</code> is an option that searches all images for unique host names. This option cannot be recommended for customers with large catalogs unless they add the <code>-dryrun</code> option. This option yields all unique clients that are contained in the image catalog. Older catalogs can contain a larger number of decommissioned hosts, hosts that are moved to new masters, or are renamed. Run time of the command can increase as attempts are made to contact unreachable hosts. ■ <code>-dryrun</code> is an option that generates the list of client names and writes them to the log. It does not result in actual configuration of the target systems. ■ <code>-disable</code> is an option that disables NBAC (USE_VXSS = PROHIBITED) on targeted hosts. ■ <code>-file progress.file</code> is an option used to specify a different file name for the progress log. The CLI reads the host names from the <code>progress_file</code>. The status is appended next to each host name with a [# 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.

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

- The OPS sets up trust with master server A.
- The OPS sets up trust with master server B.
- The OPS sets up trust with master server C.

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

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

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

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

Details on the `setuptrust` command are described in the [NetBackup Commands Reference Guide](#). See “Using the `setuptrust` command” on page 166.

Using the `setuptrust` command

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

- High security (2): If a previously untrusted root is acquired from the peer (that is, if no certificate with the same signature exists in our trust store), the user is prompted to verify the hash.
- Medium security (1): The first authentication broker is trusted without prompting. Any attempts to trust subsequent authentication brokers causes the user to be prompted for a hash verification before the certificate is added to the trusted store.
- Low security (0): The authentication broker certificate is always trusted without any prompting. The `vssat` CLI is located in the authentication service 'bin' directory.

The `setuptrust` command uses the following syntax:

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

The `setuptrust` command uses the following arguments:

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

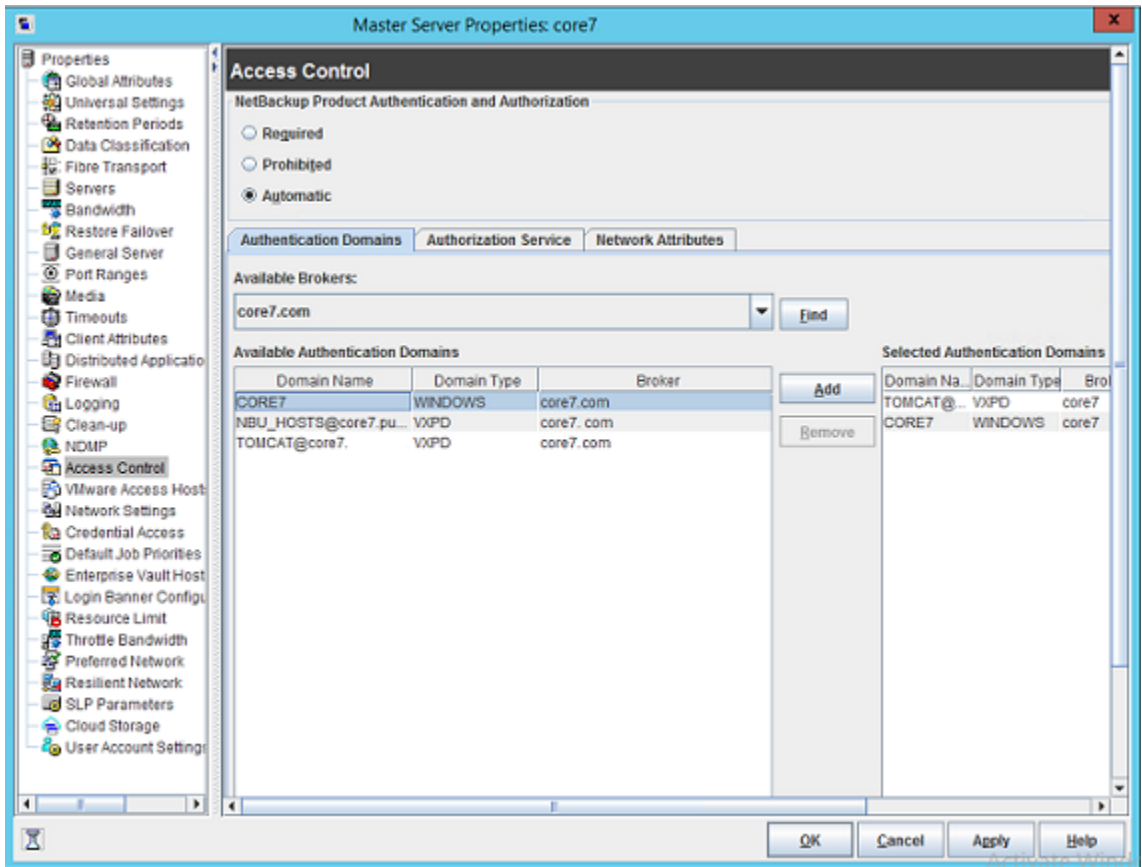
Configuring Access Control host properties for the master and media server

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

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

[Figure 6-1](#) shows the **Access Control** host properties dialog box.

Figure 6-1 Access control host properties dialog box



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

Authentication Domain tab

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

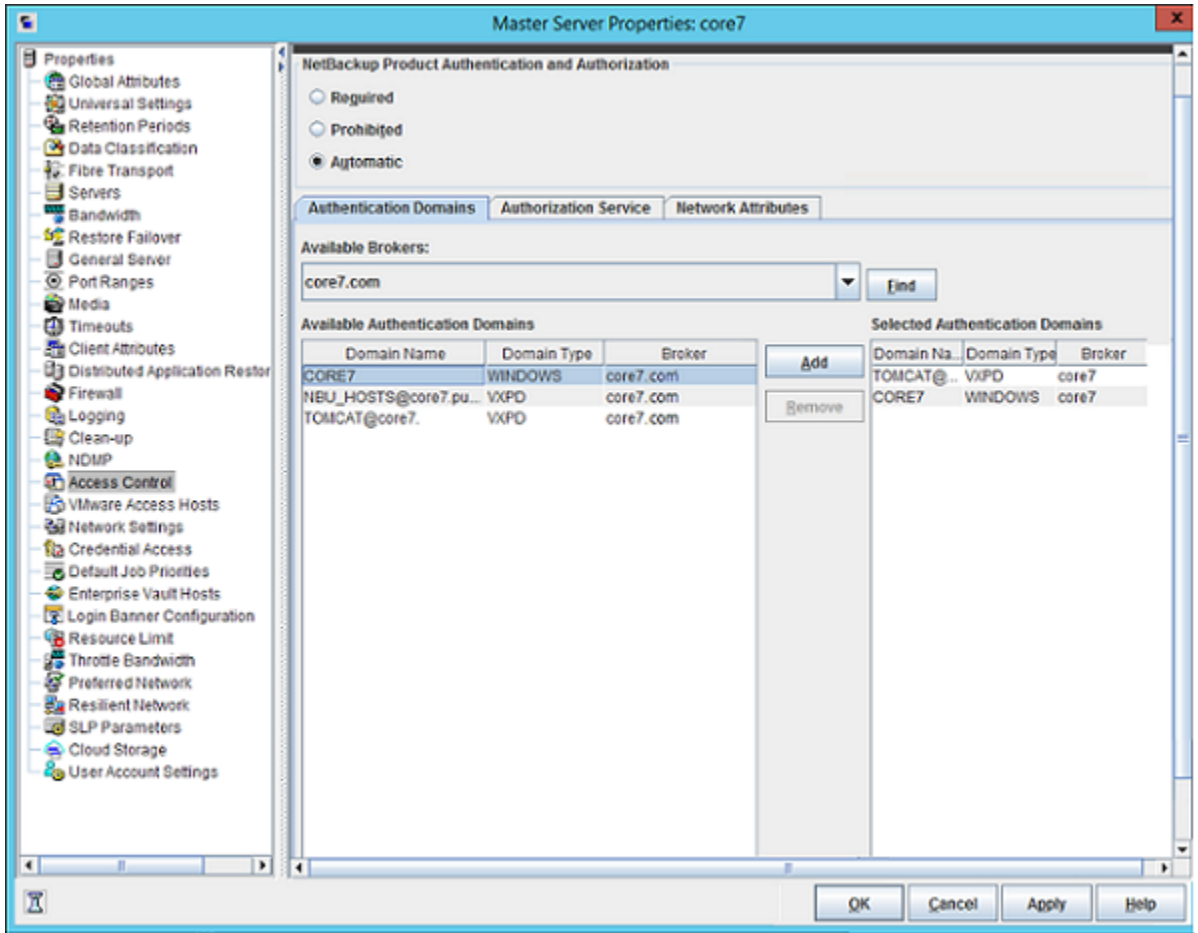
- Which authentication servers support which authentication mechanisms
- What each domain supports.

Add the domain that you want users to authenticate against.

The following examples contain six authentication domains.

Figure 6-2 shows the **Authentication Domain** tab.

Figure 6-2 Authentication Domain tab



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

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

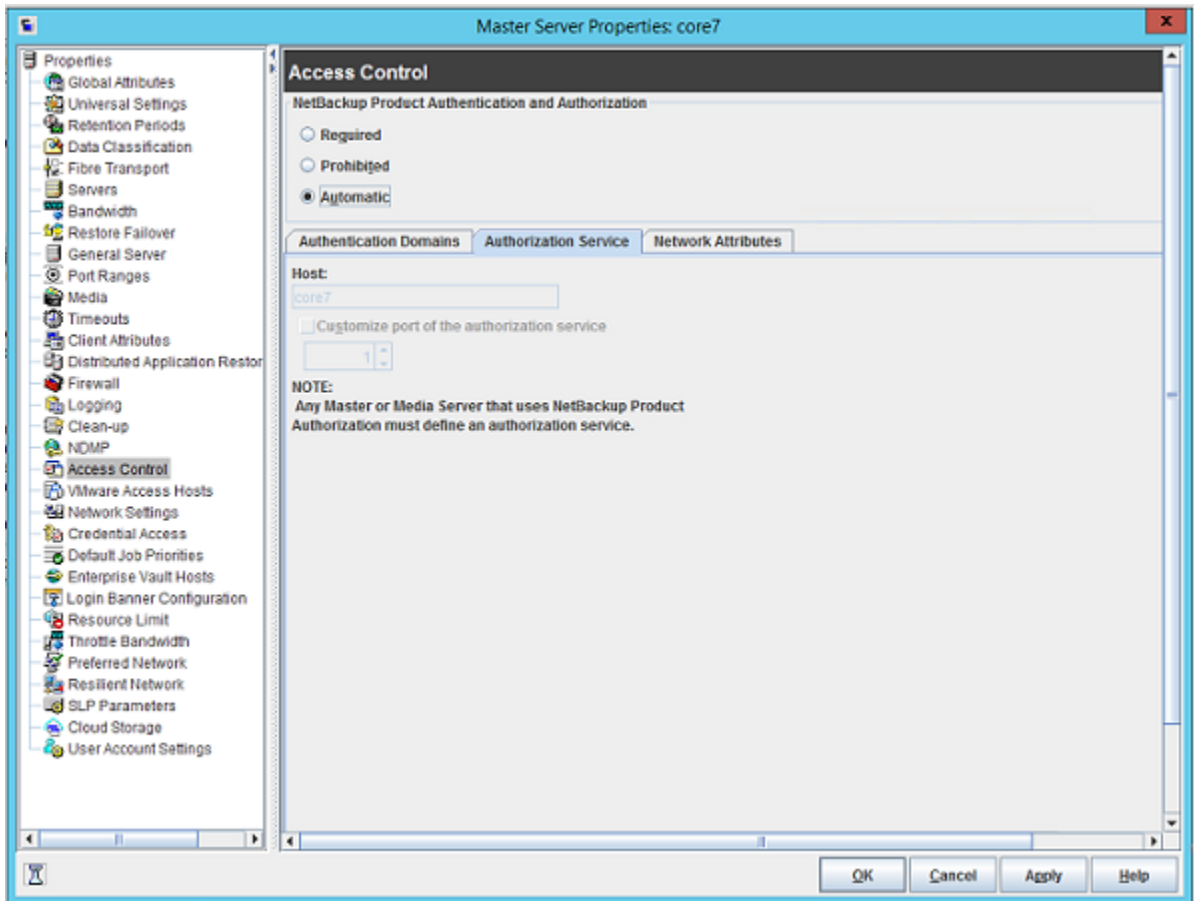
Authorization Service tab

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

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

Figure 6-3 shows the authorization service tab.

Figure 6-3 Authorization Service tab



Network Attributes tab

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

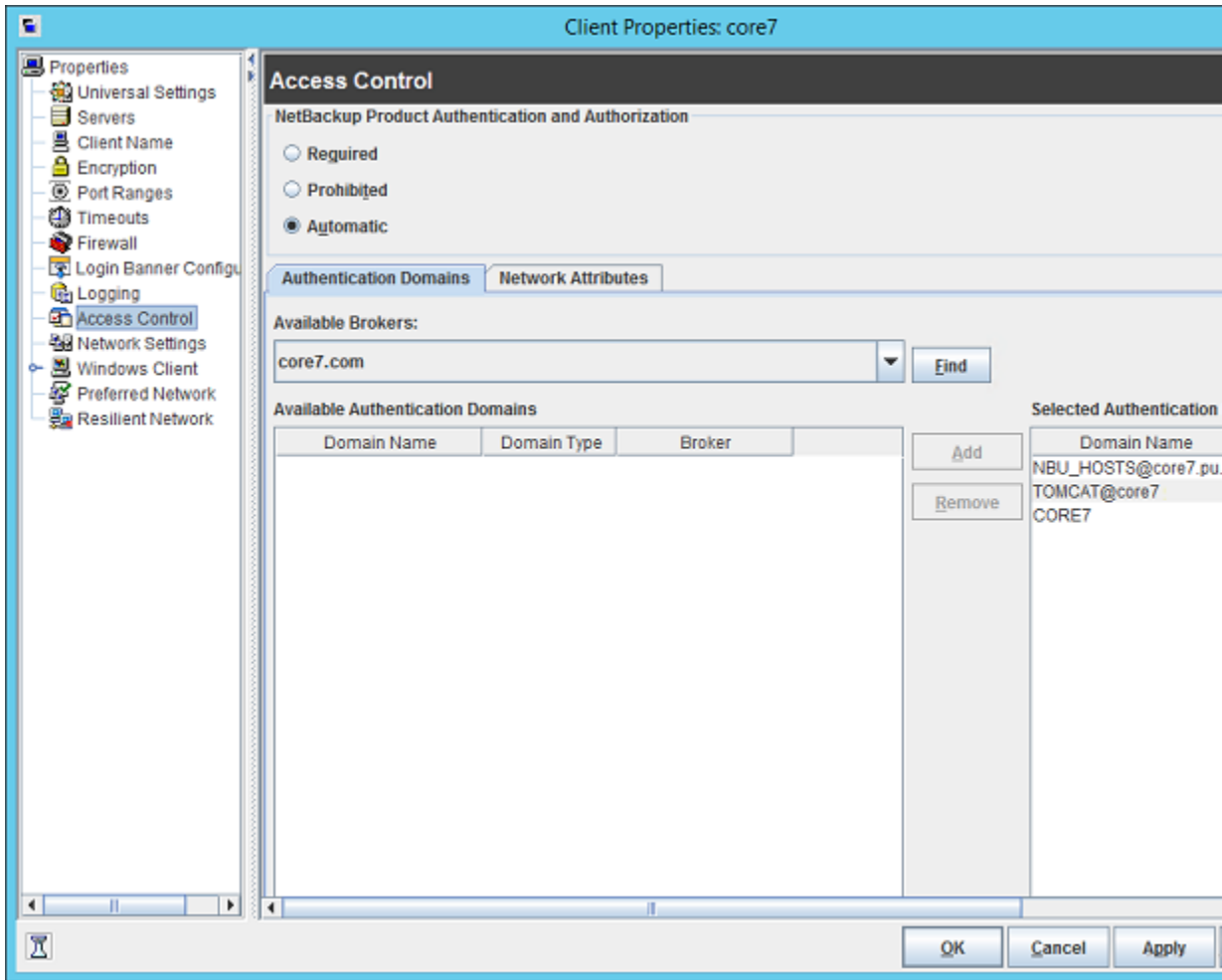
Each new NetBackup client or media server that is added to the NetBackup master needs to have the **Access Control** properties configured. These properties are configured on both itself and the master. This configuration can be done through the host properties on the master server.

Access Control host properties dialog for the client

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

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

Figure 6-4 Access control host properties for the client



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

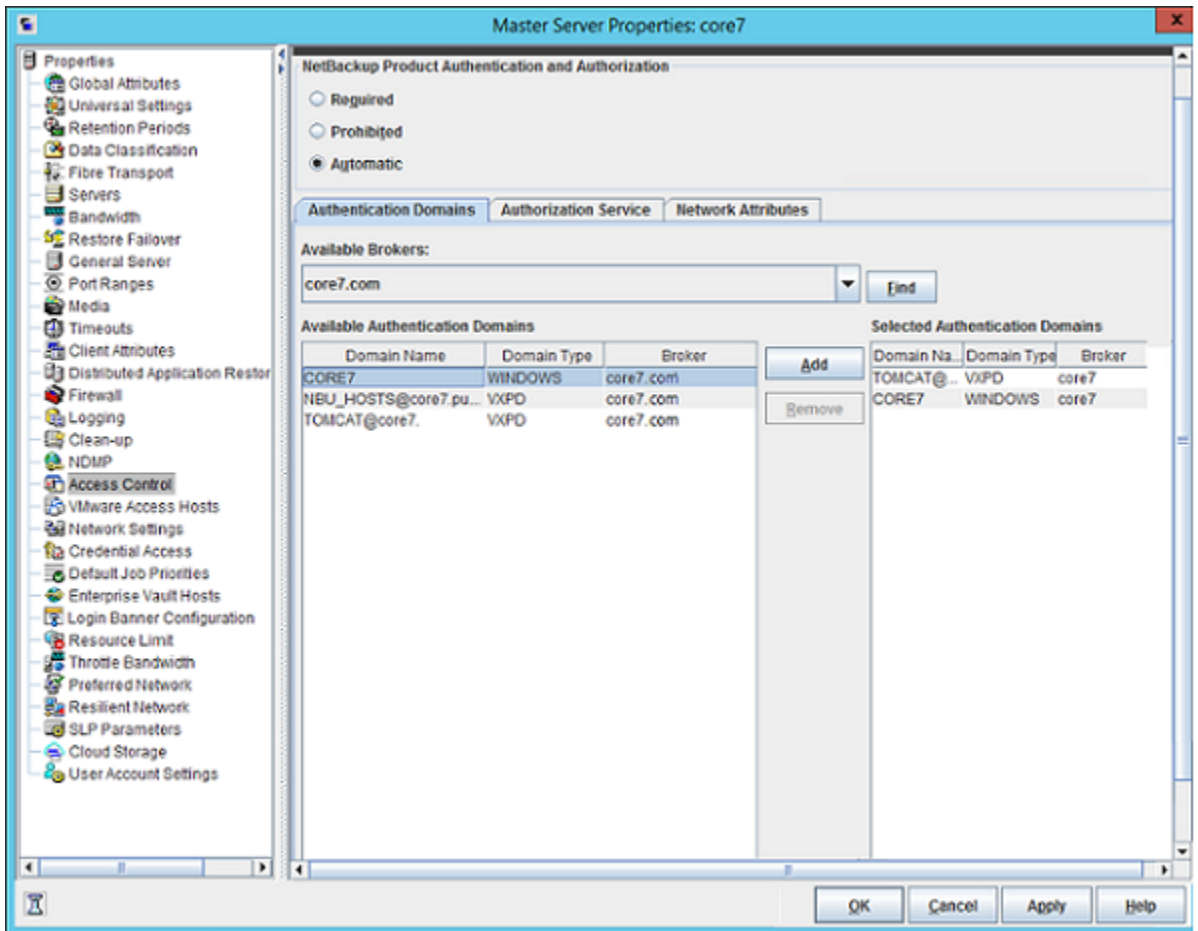
Authentication Domain tab for the client

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

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

Figure 6-5 shows the **Authentication Domain** tab and the selected authentication domains.

Figure 6-5 Authentication Domain tab for client

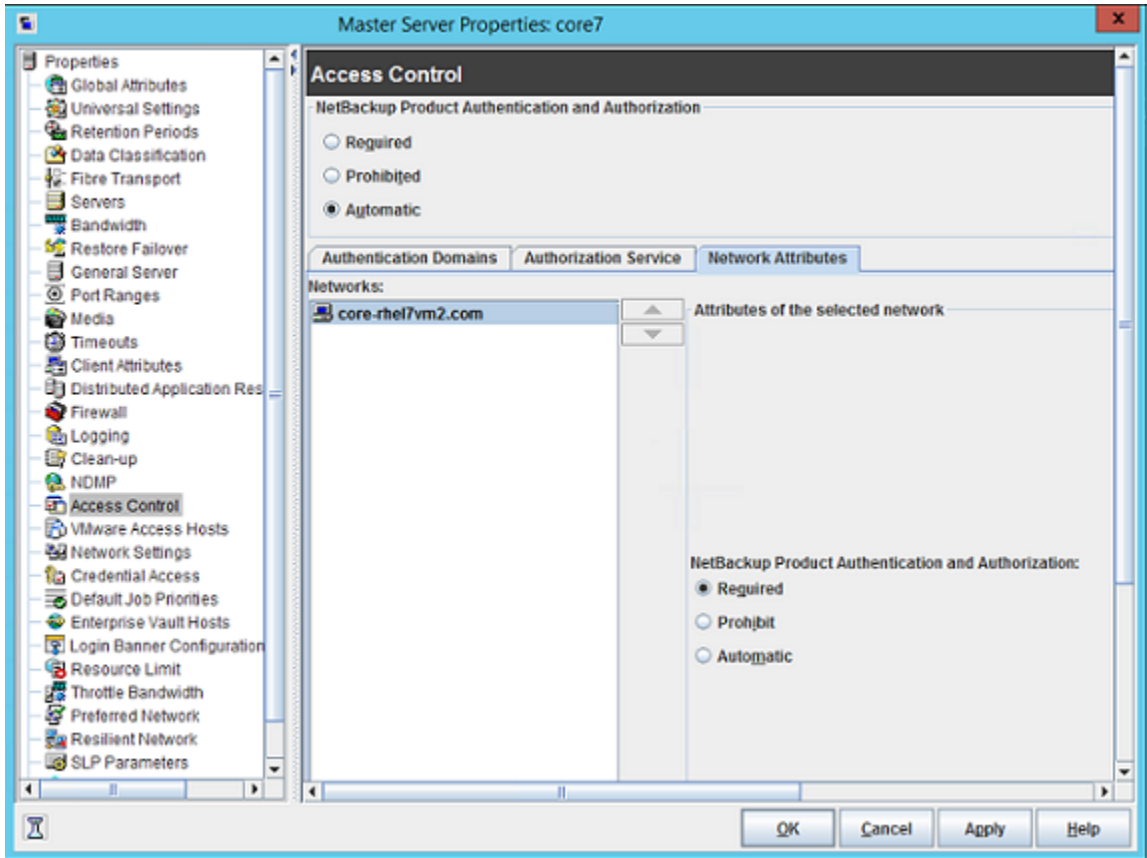


Network Attributes tab for the client

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

Figure 6-6 shows the **Network Attributes** tab for the client.

Figure 6-6 Network Attributes tab for the client



Troubleshooting Access Management

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

See [“Configuration and troubleshooting topics for NetBackup Authentication and Authorization”](#) on page 176.

These verification points include:

- Windows verification points
See [“Windows verification points”](#) on page 183.

- UNIX verification points
See [“UNIX verification points”](#) on page 192.
- Verification points in a mixed environment with a UNIX master server
See [“Verification points in a mixed environment with a UNIX master server”](#) on page 199.
- Verification points in a mixed environment with a Windows master server
See [“Verification points in a mixed environment with a Windows master server”](#) on page 205.

Troubleshooting NBAC issues

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

Table 6-4 NBAC issues

Issue and Cause	Solution
<p>A user directed backup or restore fails</p> <p>A user-directed backup or restore fails with NBAC in the automated mode. The Backup, Archive, and Restore interface shows some errors in the Windows interface when NBAC is configured.</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 interface without first configuring the interface for such a setup. Another reason may be that there is an expired certificate in the home directory.</p>	<p>Configure the Windows interface 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 TECH199281 for steps to configure the Windows interface to make use of existing users from Active Directory to manage or operate or use a NetBackup environment that is primarily on UNIX/Linux platforms.</p> <p>After you correctly configure the setup run the <code>bpbmat -logout</code> command to log out from the setup before you restart the interface.</p>
<p>Authentication failure with error 116</p> <p>The authentication fails with 'error 116-VxSS authentication' when you try to set up NBAC on a target host.</p>	<p>Check whether NBAC authentication is configured correctly and also if you have a valid usable credential for the target host.</p>
<p>Error when a non-admin user from the NBU_Operator group tries to use Access Management</p> <p>A non-admin user is added to the NBU_Operator group. Read, Browse, and Configure permissions are assigned along with the permission to configure the Host Properties. However, when the user tries to open the Access Management utility, an error displays.</p>	<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 “NetBackup default user groups” on page 218.</p>

Table 6-4 NBAC issues (*continued*)

Issue and Cause	Solution
The authorization file (auth.conf) functionality does not work in an NBAC-enabled environment. By default, the auth.conf file is supported by the Java interface in non-NBAC environments only.	<p>For the auth.conf file to work in an NBAC-enabled environment, use the <code>nbgetconfig</code> and <code>nbsetconfig</code> commands to add the <code>USE_AUTH_CONF_NBAC</code> entry to the Windows registry or the <code>bp.conf</code> file on UNIX. The entry must be set to <code>YES</code>, as follows:</p> <pre>USE_AUTH_CONF_NBAC = YES</pre> <p>For more details about the auth.conf file, refer to the NetBackup Administrators Guide, Volume I.</p>

Configuration and troubleshooting topics for NetBackup Authentication and Authorization

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

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

Topic	Configuration tips
Verifying master server settings	<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: Veritas 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 6-5 Configuration and troubleshooting topics and tips for NetBackup Authentication and Authorization (*continued*)

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

Table 6-5 Configuration and troubleshooting topics and 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 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><user_home_dir>\Application Data\VERITAS\VSS</code></p>
How system time affects access control	<p>Credentials have a birth time and death time. Computers with large discrepancies in system clock time view credentials as being created in the future or prematurely expired. Consider synchronizing system time if you have trouble communicating between systems.</p>

Table 6-5

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

Topic	Configuration tips
Stopping NetBackup Authentication and Authorization daemons for Shared Services	<p>When the NetBackup Authentication and Authorization services are stopped, stop authorization first, then stop authentication.</p> <p>UNIX -Use the following commands.</p> <p>To stop authorization use the term signal as shown in the example:</p> <pre># ps -fed grep nbazd root 17018 1 4 08:47:35 ? 0:01 ./nbazd root 17019 16011 0 08:47:39 pts/2 0:00 grep nbazd # kill 17018</pre> <p>To stop authentication use the term signal as shown in the example:</p> <pre># ps -fed grep nbatd root 16018 1 4 08:47:35 ? 0:01 ./nbatd root 16019 16011 0 08:47:39 pts/2 0:00 grep nbatd # kill 16018</pre> <p>Windows</p> <p>Use the Services utility that Windows provides, since these services do not appear in the NetBackup Activity Monitor.</p>
If you lock yourself out of NetBackup	<p>You can lock yourself out of the NetBackup Administration Console if access control is incorrectly configured.</p> <p>If this lockout occurs, use <code>vi</code> to read the <code>bp.conf</code> entries (UNIX) or <code>regedit</code> (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: <code>AUTHORIZATION_SERVICE</code>, <code>AUTHENTICATION_DOMAIN</code>, and <code>USE_VXSS</code>.</p> <p>The administrator may not want to use NetBackup Access Control or does not have the authorization libraries installed. Make certain that the <code>USE_VXSS</code> entry is set to <code>Prohibited</code>, 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 <code>bp.conf</code> file should be the same.</p>

Table 6-5 Configuration and troubleshooting topics and 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>For more information about the <code>nbac_cron</code> utility:</p> <p>See “About the nbac_cron utility” on page 212.</p> <p><code>nbac_cron.exe</code> is found in the following location:</p> <p>UNIX <code>-/opt/openv/netbackup/bin/goodies/nbac_cron</code></p> <p>Windows <code>-Install_path\Veritas\netbackup\bin\goodies\nbac_cron.exe</code></p> <p>For detailed information about using the <code>nbac_cron</code> utility:</p> <p>See “Using the nbac_cron utility” on page 212.</p>
Enabling NBAC after a recovery on Windows	<p>Use the following procedure to manually enable NBAC after a recovery on Windows.</p> <ul style="list-style-type: none"> ■ Add <code>AUTHENTICATION_DOMAIN</code>, <code>AUTHORIZATION_SERVICE</code>, and <code>USE_VXSS</code> entries in Registry. ■ Change the service type of NetBackup Authentication and Authorization services to <code>AUTOMATIC</code>. ■ Restart the NetBackup services. ■ Verify that the <code>nbatd</code> and <code>nbazd</code> services are running. <p>Note: On a cluster run the <code>bpclusterutil -enableSvc nbatd</code> and <code>bpclusterutil -enable nbazd</code> commands.</p>
In cluster installations the <code>setupmaster</code> might fail	<p>A known issue exists 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>A known issue exists 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 6-5 Configuration and troubleshooting topics and tips for NetBackup Authentication and Authorization (*continued*)

Topic	Configuration tips
Known issue in a clustered master server upgrade with NBAC, that all the <code>AUTHENTICATION_DOMAIN</code> entries in the <code>bp.conf</code> file are updated with the master server virtual name as the authentication broker	A known issue exists where in a clustered master server upgrade with NBAC, all the <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>A known issue exists in which <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 __1cH__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	A known issue exists on Windows 2003 dual stack computers. You need Microsoft patch kb/928646 from http://support.microsoft.com/ .
Known issue relating to access control failures and short and long host names	A known issue exists that includes failures with respect to access control. Determine if the short and long host names are properly resolvable and are resolving to the same IP address.
Known issue in a cluster upgrade with NBAC when the broker profile has <code>ClusterName</code> set to the virtual name of AT	A known issue exists 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> set to 1 in its profile. When a request is sent for broker domain maps, it uses the virtual name of the shared AT as the broker name. The <code>bpbaz -GetDomainInfosFromAuthBroker</code> returns none. In upgrades, the <code>bp.conf</code> file is updated to have the NetBackup virtual name.
Known issue of multiple instances of <code>bpcd</code> causing a possible error	A known issue exists where 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 6-5 Configuration and troubleshooting topics and tips for NetBackup Authentication and Authorization (*continued*)

Topic	Configuration tips
Known issue with clusters using shared AT with configuration files on the shared drive	A known issue exists with clusters that use a shared AT with configuration files on the shared drive. Unhooking shared services only works on the node where this shared drive is accessible. Unhook fails on the remaining nodes. The implication of this is that while doing a <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>A known issue exists in which 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>

Windows verification points

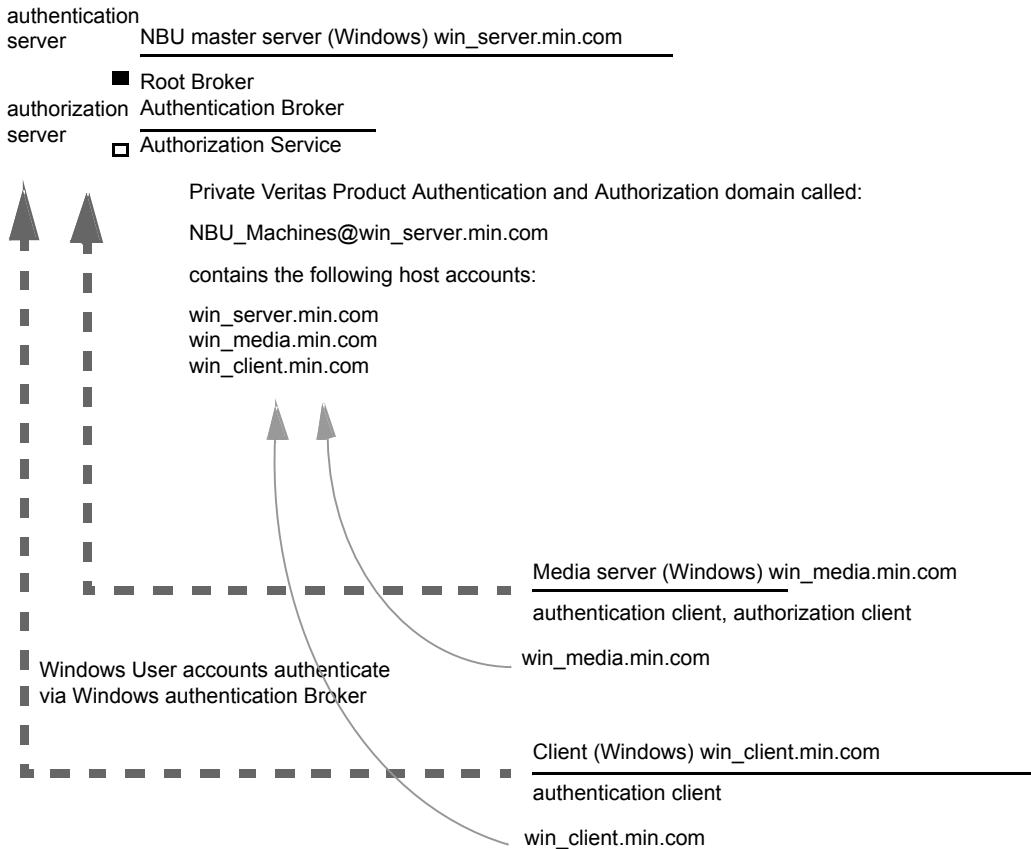
The following configuration procedures can help you verify that the master server, media server, and client are configured correctly for access control.

These Windows verification points include:

- See [“Master server verification points for Windows”](#) on page 184.
- See [“Media server verification points for Windows”](#) on page 188.
- See [“Client verification points for Windows”](#) on page 190.

[Figure 6-7](#) shows an example configuration containing Windows systems only.

Figure 6-7 Example configuration containing Windows systems only



Note:

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

Master server verification points for Windows

The following topics describe procedures to:

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

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

Table 6-6 Master server verification procedures for Windows

Procedure	Description
Verify Windows master server settings	<p>You can determine the domain in which a host is registered (where the primary authentication broker resides). Or you can determine the name of the computer the certificate represents. Run <code>bpnbat</code> with <code>-whoami</code> and specify the host credential file. The server credentials are located in the <code>c:\Program Files\Veritas\Netbackup\var\vxss\credentials\...</code> directory.</p> <p>For example:</p> <pre> bpnbat -whoami -cf "c:\Program Files\Veritas\Netbackup\var\vxss\credentials\ win_master" Name: win_master.company.com Domain: NBU_Machines@win_master.company.com Issued by: /CN=broker/OU=root@win_master.company.com/ O=vx Expiry Date: Oct 31 20:17:51 2007 GMT Authentication method: Veritas Private Security Operation completed successfully. </pre> <p>If the domain listed is not <code>NBU_Machines@win_master.company.com</code>, consider running <code>bpnbat -addmachine</code> for the name in question (<code>win_master</code>). This command is run on the computer with the authentication broker that serves the <code>NBU_Machines</code> domain (<code>win_master</code>).</p> <p>Then, on the computer where we want to place the certificate (<code>win_master</code>), run:</p> <pre>bpnbat -loginmachine</pre> <p>Note: As you determine when a user's credentials expire, keep in mind that the output displays the expiration time in GMT, not local time.</p> <p>Note: For the remaining procedures in this verification section, assume that the commands are performed from a console window. And that the user identity in question has run <code>bpnbat -login</code> from that window. The user is an identity that is a member of <code>NBU_Security Admin</code>. This identity is usually the first identity with which the security was set up.</p>

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

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

Table 6-6 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>Figure 6-8 shows an example of the host properties settings on the Authentication domain tab.</p> <p>In the Access Control host properties, verify that the listed authentication domains are spelled correctly and point to the proper servers (valid authentication brokers). If all of the domains are Windows-based, they should point to a Windows computer that runs the authentication broker.</p>

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

Figure 6-8 Host properties settings

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

Media server verification points for Windows

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

- Verify the media server.
- Verify that the server has access to the authorization database.
- Unable to load library message

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

Table 6-7 Media server verification procedures for Windows

Procedure	Description
Verify the media server	<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 6-7 Media server verification procedures for Windows (*continued*)

Procedure	Description
Verify that the server has access to the authorization database	<p>To make sure that the media server is able to access the authorization database as it needs, run <code>bpnbaz -ListGroup -CredFile "machine_credential_file"</code></p> <p>For example:</p> <pre>bpnbaz -ListGroup -CredFile "C:\Program Files\Veritas\NetBackup\var\vxss\credentials\ win_media.company.com" NBU_Operator NBU_Admin NBU_SAN Admin NBU_User NBU_Security Admin Vault_Operator Operation completed successfully.</pre> <p>If this command fails, run <code>bpnbaz -AllowAuthorization</code> on the master server that is the authorization server (<code>win_master.company.com</code>).</p>
Unable to load library message	<p>Verify the media server and that it has access to the proper database. This verification indirectly informs you that the NetBackup Authentication and Authorization client libraries for both authentication and authorization are properly installed. If either of these procedures fail with a message "unable to load libraries": Check to make certain the authentication client libraries and authorization client libraries are installed.</p> <p>You may also verify that the authentication domains are correct by viewing the access control host properties for this media server.</p>

Client verification points for Windows

The following topics describe the client verification procedures for Windows:

- Verify the credential for the client.
- Verify that the authentication client libraries are installed.
- Verify correct authentication domains.

The following table describes the client verification procedures for Windows.

Table 6-8 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>Note:</p> <p>Run <code>bpnbat -login</code> on the client to verify that the authentication client libraries are installed.</p> <pre> bpnbat -login Authentication Broker: win_master Authentication port [Enter = default]: Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd) : WINDOWS Domain: ENTERPRISE Name: Smith Password: Operation completed successfully. </pre> <p>If the libraries are not installed, a message displays: The NetBackup Authentication and Authorization libraries are not installed. This verification can also be done by looking at the Windows Add/Remove Programs.</p>

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

Procedure	Description
Verify correct authentication domains	Check that any defined authentication domains for the client are correct either in the Access Control host properties or by using <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.

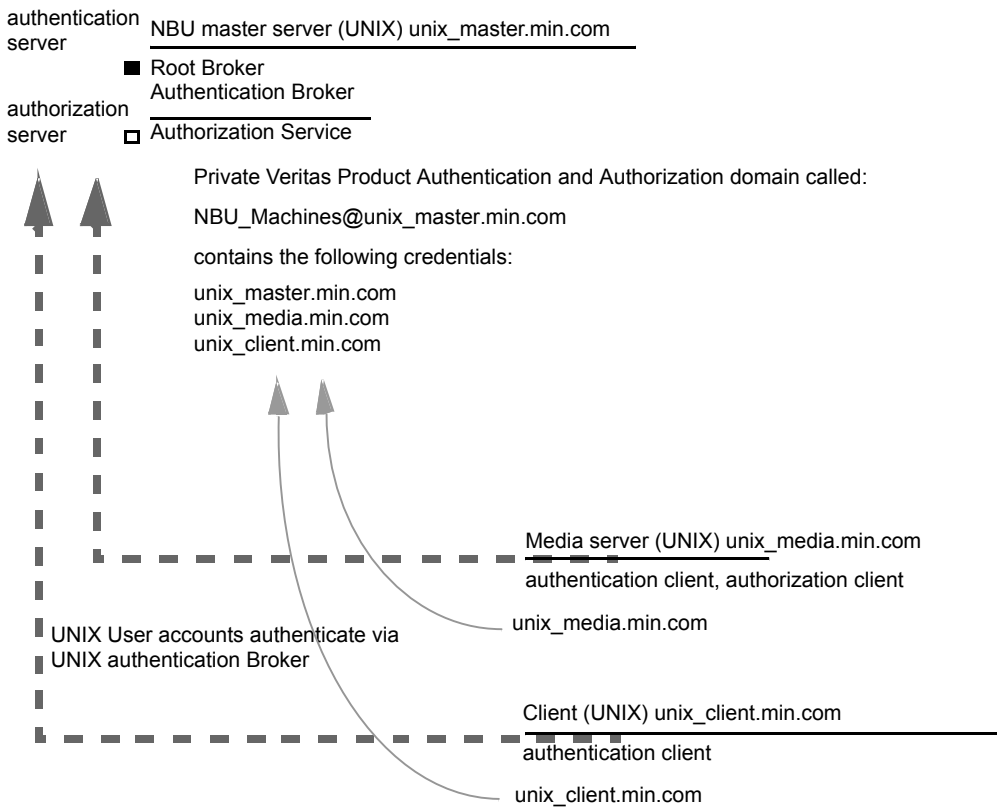
UNIX verification points

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

- UNIX master server verification
See [“UNIX master server verification”](#) on page 193.
- UNIX media server verification
See [“UNIX media server verification”](#) on page 196.
- UNIX client verification
See [“UNIX client verification”](#) on page 198.

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

Figure 6-9 Example configuration containing UNIX systems only



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

UNIX master server verification

Use the following procedures to verify the UNIX master server:

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

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

Table 6-9 Verification process for the UNIX master server

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

Table 6-9 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> bpbaz -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>bpbaz -allowauthorization <server_name></code> to add the missing computer.</p>
Verify that the database is configured correctly	<p>To make sure that the database is configured correctly, run <code>bpbaz -listgroups</code>:</p> <pre> bpbaz -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>bpbaz -listmainobjects</code> does not return data, run <code>bpbaz -SetupSecurity</code>.</p>

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

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

UNIX media server verification

Perform the following to verify the UNIX media server:

- Verify the media server.
- Verify that the server has access to the authorization database.
- Understand the unable to load library message.

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

Table 6-10 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 6-10 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 6-11 Verification procedures for the UNIX client

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

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

Procedures	Description
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_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 correct authentication domains	<p>Check that any defined authentication domains for the client are correct in the Access Control host properties or by using <code>cat (1)</code>. Ensure that the domains are spelled correctly. Also ensure that the authentication brokers on the list for each of the domains are valid for that domain type.</p> <p>This process can also be verified in <code>bp.conf</code> using <code>cat (1)</code>.</p> <pre> cat bp.conf SERVER = unix_master SERVER = unix_media CLIENT_NAME = unix_master AUTHENTICATION_DOMAIN = min.com "default company NIS namespace" NIS unix_master 0 AUTHENTICATION_DOMAIN = unix_master.company.com "unix_master password file" PASSWD unix_master 0 AUTHORIZATION_SERVICE = unix_master.company.com 0 USE_VXSS = AUTOMATIC </pre>

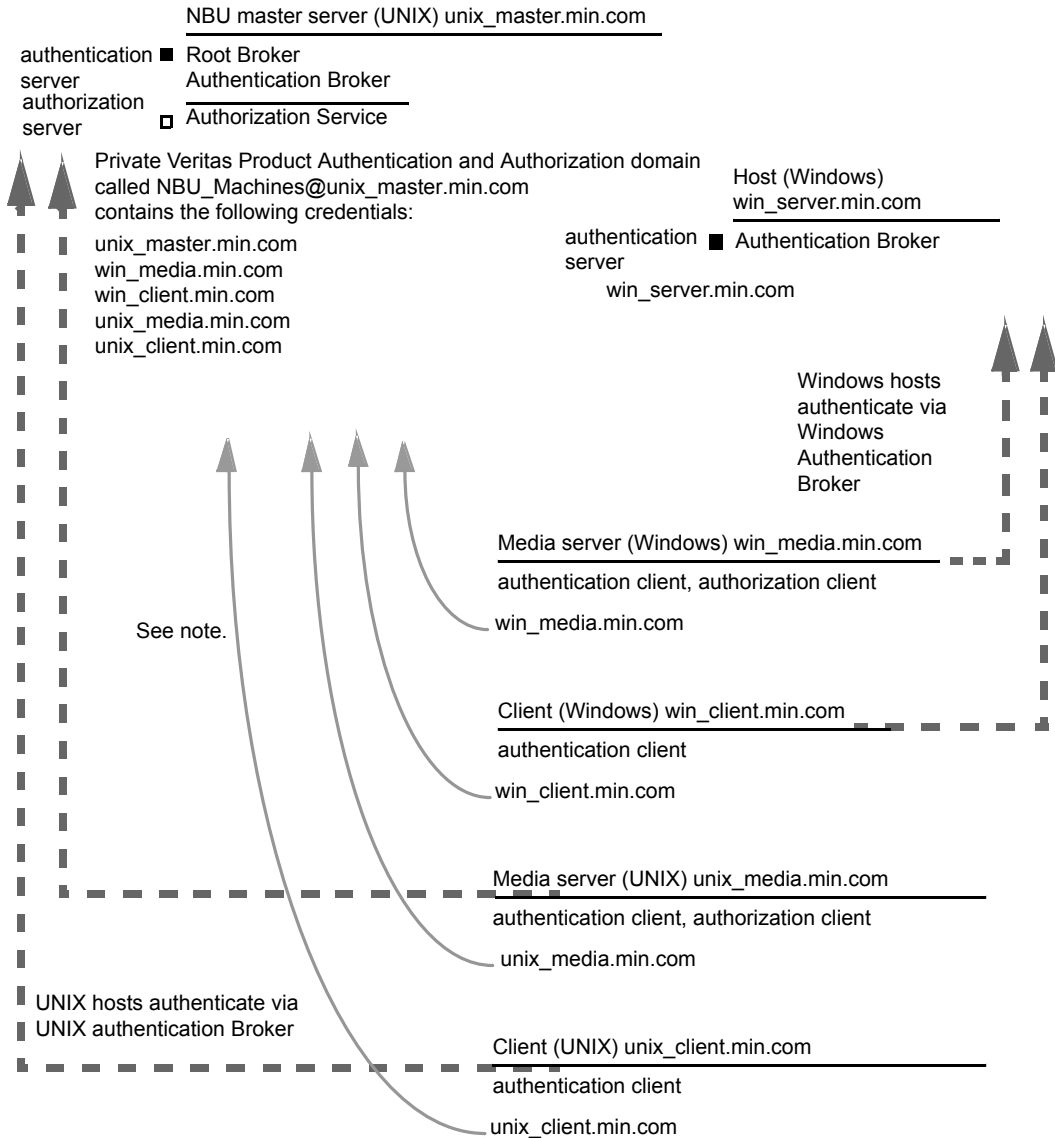
Verification points in a mixed environment with a UNIX master server

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

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

Figure 6-10 is an example of a mixed configuration that contains a UNIX master server.

Figure 6-10 Example mixed configuration containing a UNIX master server



Master server verification points for a mixed UNIX master server

See the following topic for the verification procedure for a UNIX master server:
See [“UNIX master server verification”](#) on page 193.

Media server verification points for a mixed UNIX master server

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

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

Procedure	Description
Verify the UNIX media server	See the following topic for the verification procedure for a UNIX media server: See “UNIX media server verification” on page 196.
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">■ <code>bpnbat -addmachine</code> on the root authentication broker (in this example, <code>unix_master</code>)■ <code>bpnbat -loginmachine</code> (in this example, <code>win_media</code>) <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 6-12 Verification procedures for a mixed UNIX master server
(continued)

Procedure	Description
Verify that a media server is permitted to perform authorization lookups	<p>Ensure that the media server is allowed to perform authorization checks by running <code>bpnbaz -listgroups -CredFile</code>.</p> <p>For example:</p> <pre>bpnbaz -listgroups -CredFile "C:\Program Files\Veritas\Netbackup\var\vxss\credentials\ win_media.company.com" NBU_User NBU_Operator NBU_Admin NBU_Security Admin Vault_Operator Operation completed successfully.</pre> <p>If the media server is not allowed to perform authorization checks, run <code>bpnbaz -allowauthorization</code> on the master server for the media server name in question.</p>
Unable to load library message	<p>Verify the Windows media server and that it can perform authorization checks indirectly. This verification informs us that the NetBackup Authentication and Authorization client libraries for both authentication and authorization are properly installed. If either of these procedures fail with a message "unable to load libraries," make certain the authentication client libraries and authorization client libraries are installed.</p>
Verify authentication domains	<p>Verify that the authentication domains are correct by viewing the access control host properties for this media server.</p> <p>You can also use <code>regedit</code> (or <code>regedit32</code>) directly on the media server in the following location:</p> <pre>HKEY_LOCAL_MACHINE\Software\Veritas\NetBackup\ CurrentVersion\config\AUTHENTICATION_DOMAIN</pre>

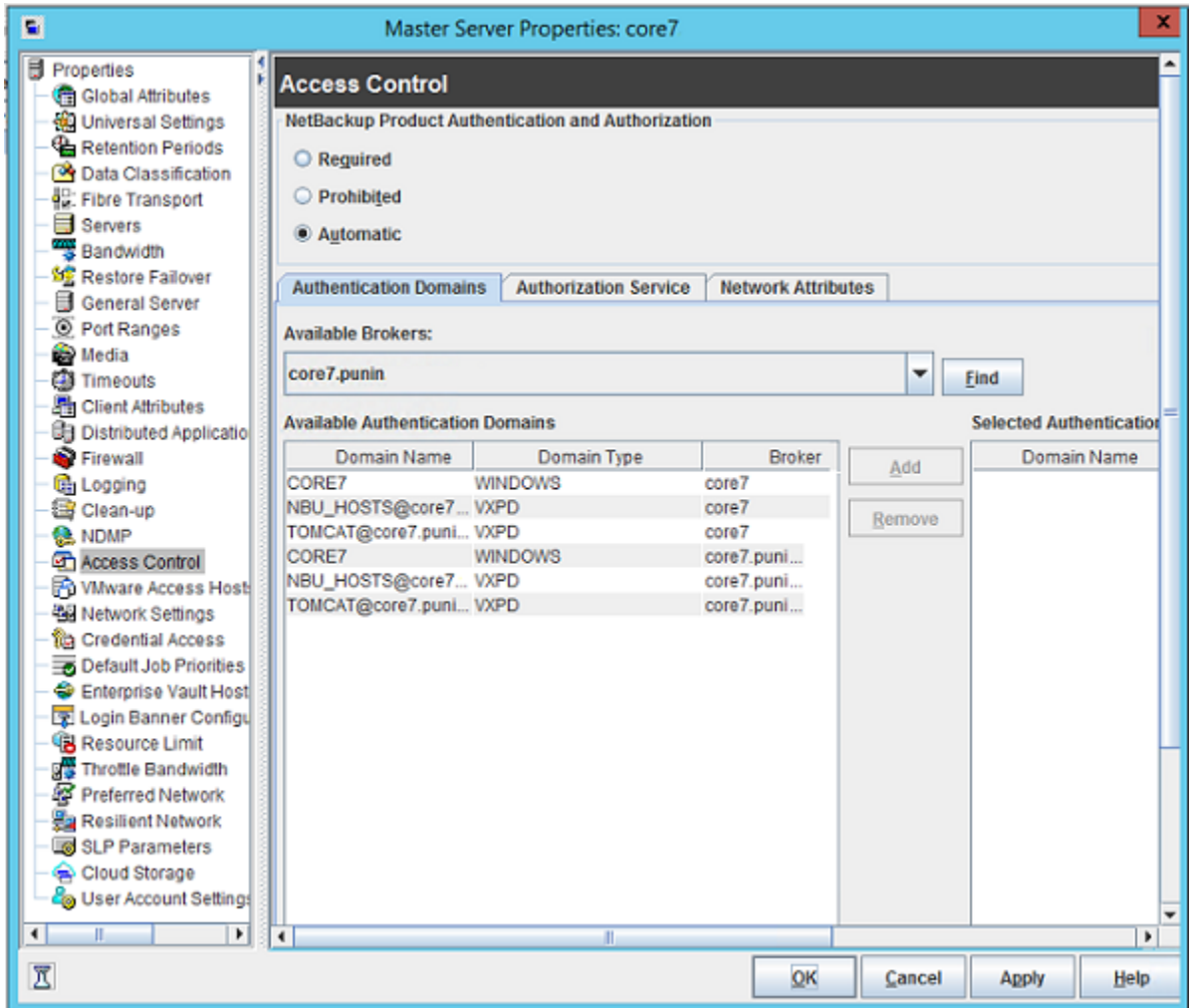
Table 6-12

Verification procedures for a mixed UNIX master server

(continued)

Procedure	Description
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>Figure 6-11 for a display on how to match the platform to the most useful authentication domains.</p>

Figure 6-11 Cross platform authentication domains



Client verification points for a mixed UNIX master server

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

See [“UNIX client verification”](#) on page 198.

The following table describes the procedures to verify Windows clients.

Table 6-13 Procedures to verify Windows clients

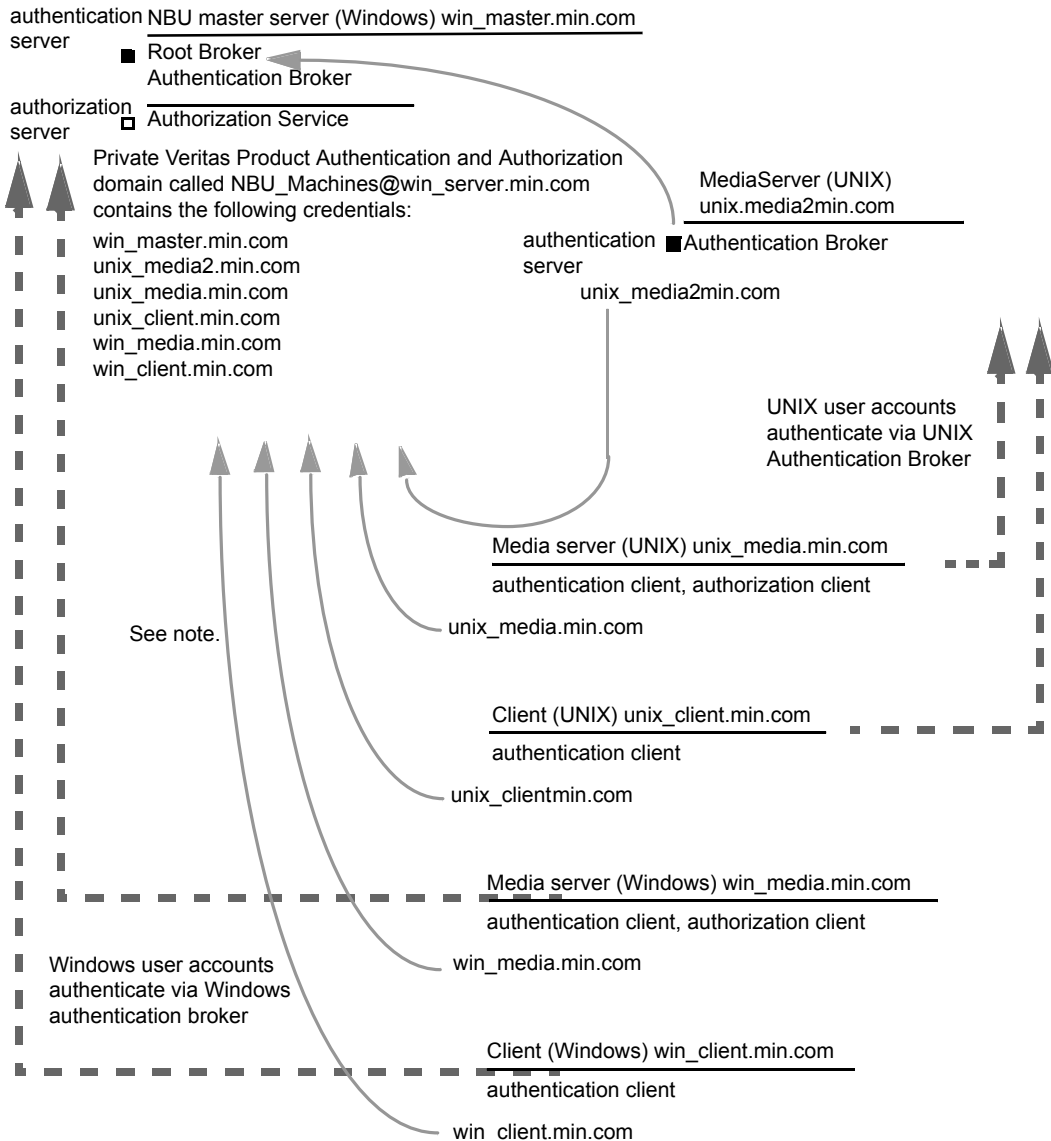
Procedures	Description
Verify the credential for the Windows client	<p>Check that the credential for the client is indeed for the correct client and comes from the correct domain. Run <code>bpnbat -whoami</code> with <code>-cf</code> for the client's credential file.</p> <p>For example:</p> <pre> bpnbat -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 208.
 - Media server verification points for mixed Windows master
See [“Media server verification points for a mixed Windows master server”](#) on page 208.
 - Client verification points for mixed Windows master
See [“Client verification points for a mixed Windows master server”](#) on page 210.
- [Figure 6-12](#) is an example configuration that contains a Windows master server.

Figure 6-12 Example mixed configuration containing a Windows master server



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

Master server verification points for a mixed Windows master server

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

See [“Master server verification points for Windows”](#) on page 184.

Media server verification points for a mixed Windows master server

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

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

Procedure	Description
Verify the Windows media server for a mixed Windows master server	See the following topic for the verification procedures for a Windows media server: See “Media server verification points for Windows” on page 188.
Verify the UNIX media server	Check that the computer certificate is issued from the root authentication broker, found on the Windows master server (win_master). To determine which authentication broker the media server is authenticated against, run <code>bpnbat -whoami</code> with <code>-cf</code> for the media server's credential file. For example: <pre>bpnbat -whoami -cf /usr/opensw/ssl/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 6-14 Media server verification procedures for a mixed Windows master server (*continued*)

Procedure	Description
Verify that the server has access to the authorization database	<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/<hostname>"</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 6-14 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 6-15 Verification procedures for a mixed Windows master server

Procedure	Description
Verify the credential for the Windows client	<p>See the following topic for the verification procedures for Windows clients:</p> <p>See “Client verification points for Windows” on page 190.</p>

Table 6-15 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>bpbnet -whoami</code> with <code>-cf</code> for the client's credential file.</p> <p>For example:</p> <pre> bpbnet -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>bpbnet -login</code> on the client to verify that the authentication client libraries are installed.</p> <pre> bpbnet -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>

About the nbac_cron utility

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

The utility is found in the following location:

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

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

See [“Using the nbac_cron utility”](#) on page 212.

Using the nbac_cron utility

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

Using the nbac_cron utility to run cron jobs

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

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

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

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

Password:*****

Password:*****

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

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

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

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

Operation completed successfully.

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

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

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

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

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

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

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

Name: Dan

Password:*****

You do not currently trust the server:

`amp.sec.punin.sen.veritas.com`, do you wish to trust it? (Y/N): Y

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

Operation completed successfully.

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

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

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

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

```
Name: CronAt_dan
Domain: CronAtUsers@amp.sec.punin.sen.veritas.com
Issued by: /CN=broker/OU=amp.sec.punin.sen.veritas.com
Expiry Date: Feb 4 13:36:08 2016 GMT
Authentication method: Veritas Private Domain
Operation completed successfully.
```

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

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

Using the Access Management utility

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

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

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

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

UNIX

`bnpbaz` is located in directory `/usr/opensv/netbackup/bin/admincmd`

Windows

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

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

```
bnpbaz -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 216.
- The creation of user groups.
See [“User groups”](#) on page 216.

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

See [“Viewing specific user permissions for NetBackup user groups”](#) on page 225.

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

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

- Functional units in your organization (UNIX administration, for example)
- NetBackup resources (drives, policies, for example)
- Location (East Coast or West coast, for example)
- Individual responsibilities (tape operator, for example)

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

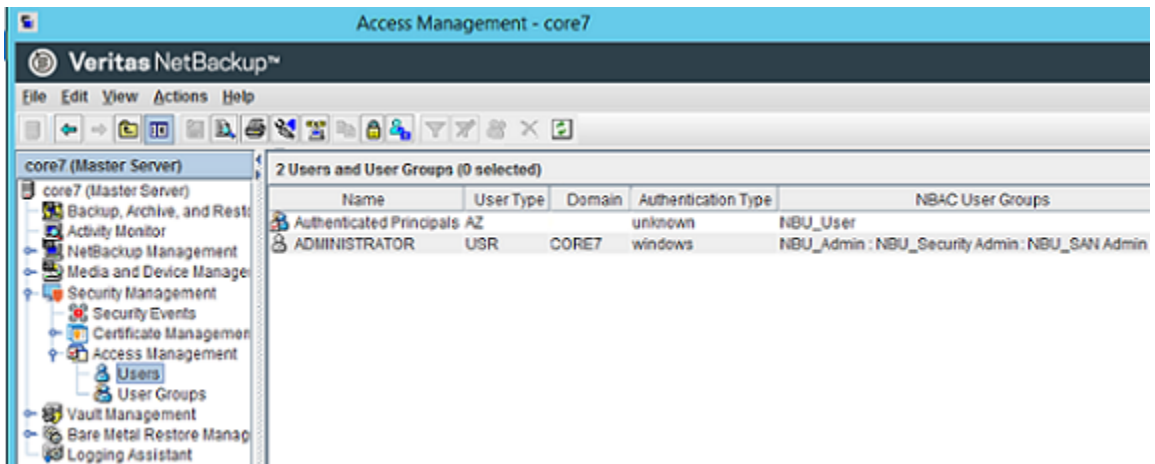
Individual users

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

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

Figure 6-13 shows individual authenticated users.

Figure 6-13 Individual users



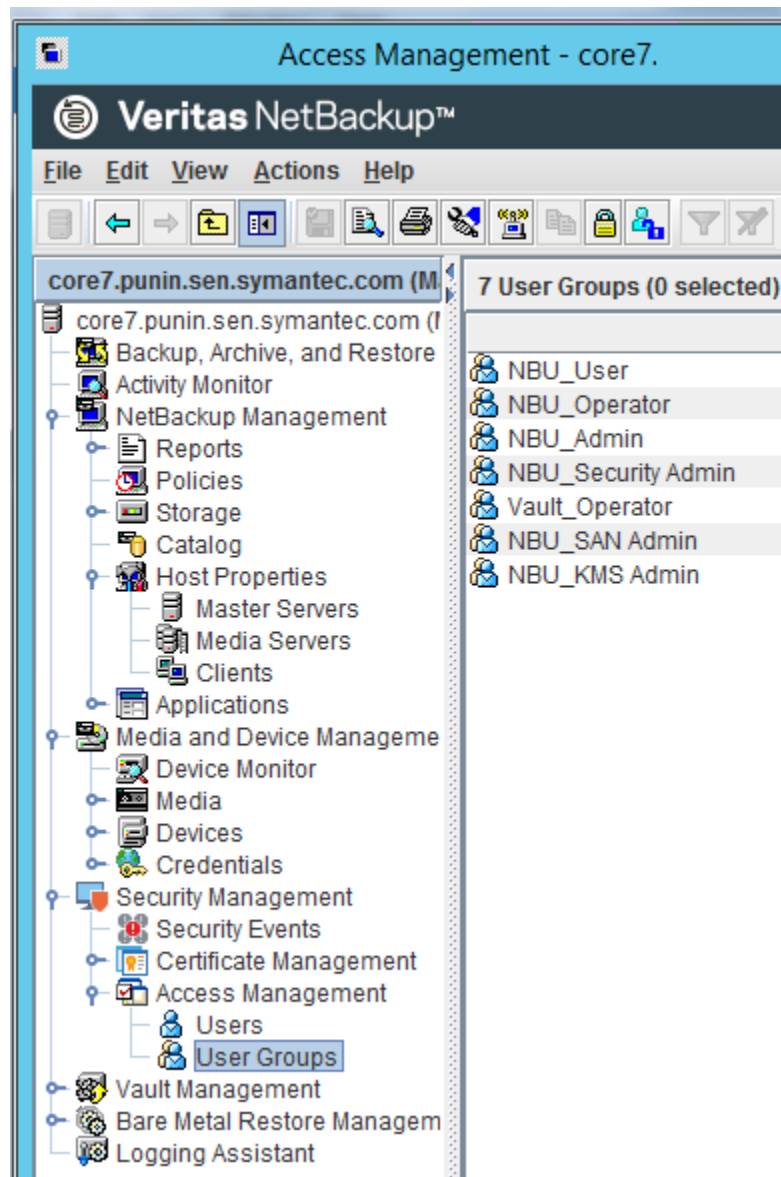
All authenticated users are implicit members of the NBU_Users user group. All other groups must have members defined explicitly. The NetBackup Security Administrator can delete a manually added member to other groups. However, the Security Administrator may not delete the predefined implicit members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

User groups

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

Figure 6-14 show a list of user groups.

Figure 6-14 User groups



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

of **Access Management** are only visible to members of the NBU_Security Admin group.

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

NetBackup default user groups

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

The following table describes each NetBackup default user group.

Table 6-16 NetBackup default user groups

Default user group	Description
Operator (NBU_Operator)	<p>The main task of the NBU_Operator user group is to monitor jobs. For example, members of the NBU_Operator user group might monitor jobs and notify a NetBackup administrator if there is a problem. Then, the administrator can address the problem. Using the default permissions, a member of the NBU_Operator user group would probably not have enough access to address larger problems.</p> <p>Members of the NBU_Operator user group have the permissions that allow them to perform tasks such as moving tapes, operating drives, and inventorying robots.</p>
Administrator (NBU_Admin)	<p>Members of the NBU_Admin user group have full permission to access, configure, and operate any NetBackup authorization object. Some exceptions exist for SAN Administrators. In other words, members have all of the capabilities that are currently available to administrators without Access Management in place. However, as members of this group, you do not necessary log on as root or administrator in the OS.</p> <p>Note: Members of the NBU_Admin user group cannot see the contents of Access Management, and therefore, cannot ascribe permissions to other user groups.</p>
SAN Administrator (NBU_SAN Admin)	<p>By default, members of the NBU_SAN Admin user group have full permissions to browse, read, operate, and configure disk pools and host properties. These permissions let you configure the SAN environment and NetBackup's interaction with it.</p>

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

Default user group	Description
User (NBU_User)	The NBU_User user group is the default NetBackup user group with the fewest permissions. Members of the NBU_User user group can only back up, restore, and archive files on their local host. NBU_User user group members have access to the functionality of the NetBackup client interface (BAR).
Security administrator (NBU_Security Admin)	<p>Usually very few members exist in the NBU_Security Admin user group. The only permission that the Security Administrator has, by default, is to configure access control within Access Management. Configuring access control includes the following abilities:</p> <ul style="list-style-type: none"> ■ To see the contents of Access Management in the NetBackup Administration Console ■ To create, modify, and delete users and user groups ■ To assign users to user groups ■ To assign permissions to user groups
Vault operator (Vault_Operator)	The Vault_Operator user group is the default user group that contains permissions to perform the operator actions necessary for the Vault process.
KMS Administrator (NBU_KMS Admin)	By default, members of the NBU_KMS Admin user group have full permissions to browse, read, operate and configure encryption key management properties. These permissions make sure that you can configure the KMS environment and NetBackup's interaction with it.
Additional user groups	The Security Administrator (member of NBU_Security Admin or equivalent) can create user groups as needed. The default user groups can be selected, changed, and saved. Veritas recommends that the groups be copied, renamed, and then saved to retain the default settings for future reference.

Configuring user groups

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

Creating a new user group

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

To create a new user group

- 1 As a member of the NBU_Security Admin user group (or equivalent), expand **Access Management > NBU User Groups**.
- 2 Select **Actions > New User Group**. The Add New user group dialog displays, opened to the **General** tab.
- 3 Type the name of the new group in the **Name** field, then click the **Users** tab.
- 4 Select the defined users that you want to assign to this new user group. Then click **Assign**. Or, to include all the defined users in the group, click **Assign All**. To remove users from the assigned users list, select the user name, then click **Remove**.
- 5 Click the **Permissions** tab.
- 6 Select a resource from the Resources list and an Authorization Object. Then select the permissions for the object.
- 7 Click **OK** to save the user group and the group permissions.

Creating a new user group by copying an existing user group

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

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

- 1 As a member of the NBU_Security Admin user group (or equivalent), expand **Access Management > NBU User Groups**.
- 2 Select an existing user group in the **Details** pane. (The pane on the left side of the **NetBackup Administration Console**.)
- 3 Select **Actions > Copy to New User Group**. A dialog that is based on the selected user group displays, opened to the **General** tab.
- 4 Type the name of the new group in the **Name** field, then click the **Users** tab.
- 5 Select the defined users that you want to assign to this new user group. Then click **Assign**. Or, to include all the defined users in the group, click **Assign All**. To remove users from the assigned users list, select the user name, then click **Remove**.
- 6 Click the **Permissions** tab.
- 7 Select a resource from the Resources list and Authorization Object, then select the permissions for the object.
- 8 Click **OK** to save the user group and the group permissions. The new name for the user group appears in the **Details** pane.

Renaming a user group

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

Adding a new user to the user group

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

See [“Assigning a user to a user group”](#) on page 222.

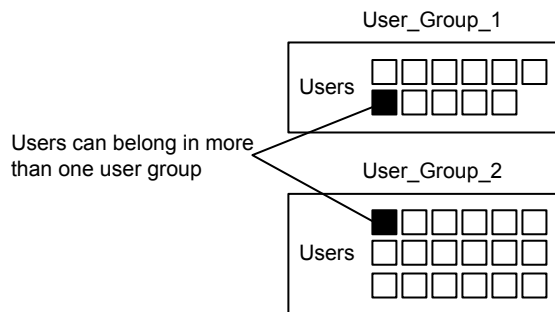
About defining a user group and users

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

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

[Figure 6-15](#) shows defining a user group.

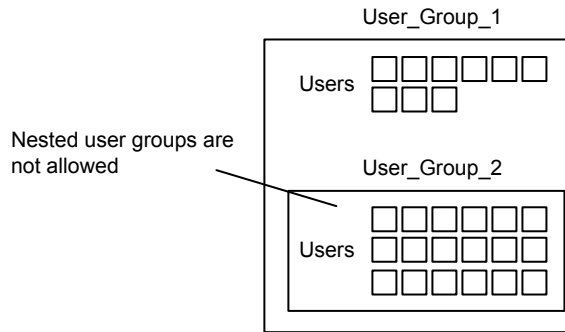
Figure 6-15 Defining a user group



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

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

Figure 6-16 Nested user groups are not allowed



Logging on as a new user

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

To log on as a new user

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

Assigning a user to a user group

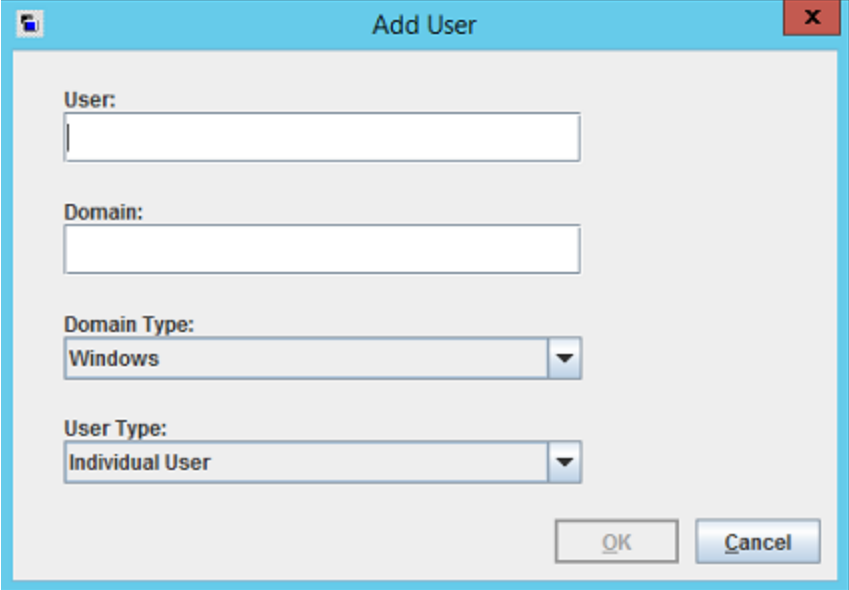
You can use the following procedure to assign a user to a user group. A user is assigned from a pre-existing name space (NIS, Windows, etc.) to an NBU user group. No new user accounts are created in this procedure.

To add a user to a user group

- 1 As a member of the NBU_Security Admin user group (or equivalent), expand **Access Management > NBU User Groups**.
- 2 Double-click on the user group to which you want to add a user.

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

A display similar to the following appears:



The screenshot shows a window titled "Add User". Inside the window, there are four labeled input fields arranged vertically: "User:" with a text box, "Domain:" with a text box, "Domain Type:" with a dropdown menu currently showing "Windows", and "User Type:" with a dropdown menu currently showing "Individual User". At the bottom right of the window are two buttons: "OK" and "Cancel".

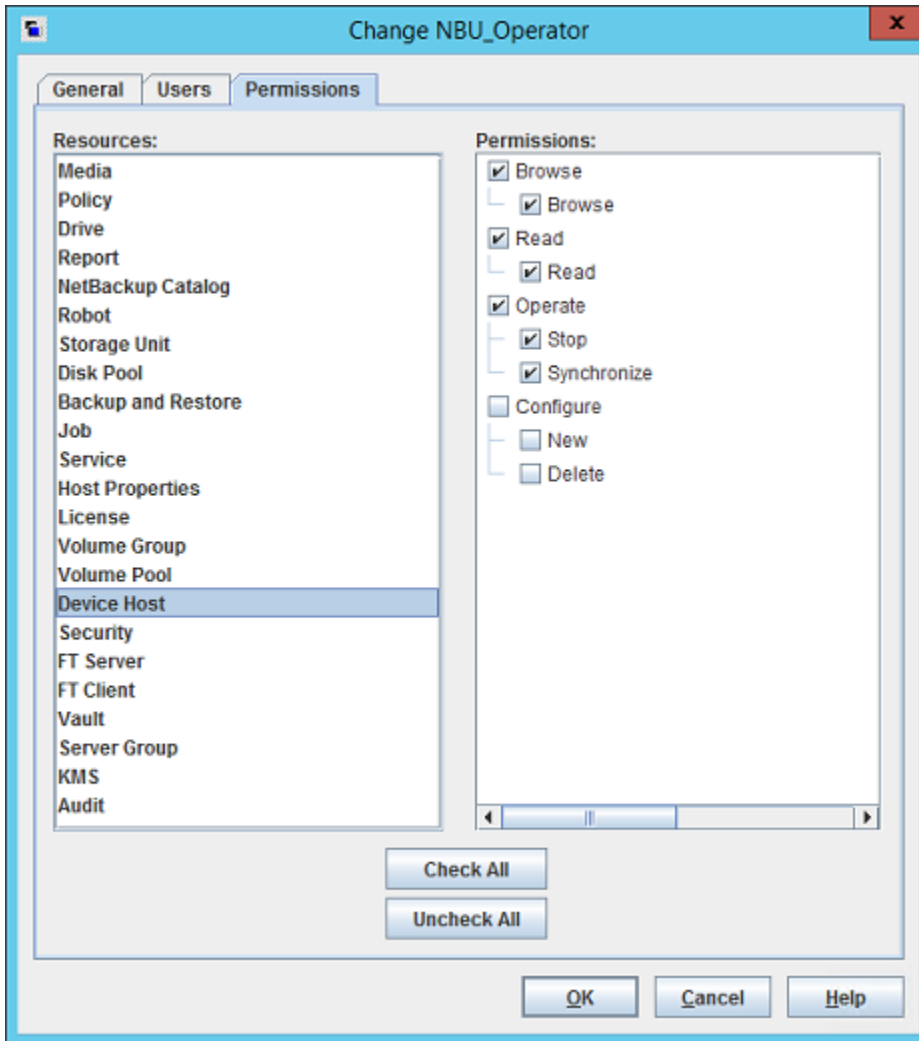
- 4 Enter the user name and the authentication domain. Select the domain type of the user: NIS, NIS+, PASSWD, Windows, or Vx.
- 5 Select the **Domain Type** of the user:
 - NIS
Network Information Services
 - NIS+
Network Information Services Plus
 - PASSWD
UNIX password file on the authentication server
 - Windows
Primary domain controller or Active Directory
 - Vx
Veritas private database
- 6 For the **User Type**, select whether the user is an individual user or an OS domain.
- 7 Click **OK**. The name is added to the **Assigned Users** list.

About authorization objects and permissions

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

The following figure shows the authorization objects.

Figure 6-17 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.

Viewing specific user permissions for NetBackup user groups

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

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

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

Note: More information on this subject can be found by referring to the [Veritas](#) technical support site.

To View specific user permissions

- 1** In the **NetBackup Administration Console**, expand **Access Management > NBU User Groups**.
- 2** Double click on the appropriate NBU_Operator, NBU_Admin, NBU_SAN Admin, NBU_User, NBU_Security Admin, or Vault_Operator in the **Security** window.
- 3** In the **NBU_Operator** window, select the **Permissions** tab.
- 4** In the **Authorization Objects** pane, select the desired authorization object.
 The **Permissions** pane displays the permissions for that authorization object.

Granting permissions

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

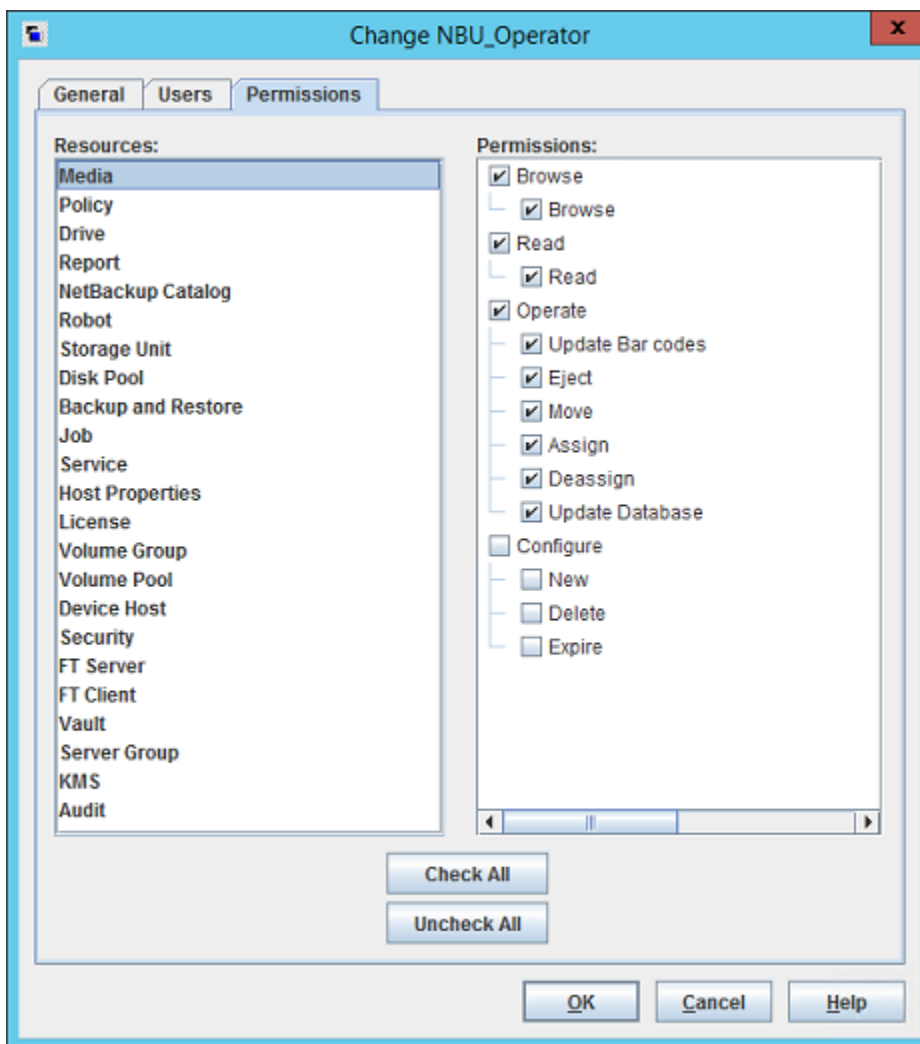
To grant a permission to the members of a user group

- 1** Select an authorization object.
- 2** Then place a check in front of a permission that you want to grant the members of the user group currently selected.

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

The following figure shows an example of a permissions list.

Figure 6-18 Permissions list



Authorization objects

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

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

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

Media authorization object permissions

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

Table 6-17 Media authorization object permissions

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

Policy authorization object permissions

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

Table 6-18 Policy authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	---	---
Read	Read	X	X	---	---	---	---	---
Operate	Back up	X	X	---	---	---	---	---
Configure	Activate	---	X	---	---	---	---	---
	Deactivate	---	X	---	---	---	---	---
	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---

Drive authorization object permissions

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

Table 6-19 Drive authorization object permissions

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

Report authorization object permissions

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

Table 6-20 Report authorization object permissions

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

NBU_Catalog authorization object permissions

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

Table 6-21 NBU_Catalog authorization object permissions

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

Robot authorization object permissions

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

Table 6-22 Robot authorization object permissions

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

Storage unit authorization object permissions

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

Table 6-23 Storage unit authorization object permissions

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

DiskPool authorization object permissions

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

Table 6-24 DiskPool authorization object permissions

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

BUAndRest authorization object permissions

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

Table 6-25 BUAndRest authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	X	X	---	---	X
Read	Read	X	X	X	X	---	---	X

Table 6-25 BUAndRest authorization object permissions (*continued*)

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

Job authorization object permissions

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

Table 6-26 Job authorization object permissions

Set	Activity	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	X	---
Read	Read	X	X	---	---	---	X	---
Operate	Suspend	X	X	---	---	---	X	---
	Resume	X	X	---	---	---	X	---
	Cancel	X	X	---	---	---	X	---
	Delete	X	X	---	---	---	X	---
	Restart	X	X	---	---	---	X	---
	New	X	X	---	---	---	X	---

Service authorization object permissions

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

Table 6-27 Service authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	X	---
Read	Read	X	X	---	---	---	X	---
Operate	Stop	X	X	---	---	---	---	---

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

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

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

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

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

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

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

(For example, `bprdreq -terminate`, `bpdbrm -terminate`, or `stopltid`.)

If a user is a member of the NBU_Admin user group, but is not logged on as an OS administrator (root). That user is not able to restart a daemon from the **NetBackup Administration Console** or from the command line.

HostProperties authorization object permissions

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

Table 6-28 HostProperties authorization object permissions

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

License authorization object permissions

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

Table 6-29 License authorization object permissions

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

Volume group authorization object permissions

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

Table 6-30 Volume group authorization object permissions

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

VolumePool authorization object permissions

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

Table 6-31 VolumePool authorization object permissions

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

DevHost authorization object permissions

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

Note: The DevHost object controls access to the **Media and Device Management > Credentials** node.

Table 6-32 DevHost authorization object permissions

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

Security authorization object permissions

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

Table 6-33 Security authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	---	---	---	---	X	---	---
Read	Read	---	---	---	---	X	---	---
Configure	Security	---	---	---	---	X	---	---

Fat server authorization object permissions

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

Table 6-34 Fat server authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	X	---	---	---	---
Read	Read	X	X	X	---	---	---	---

Table 6-34 Fat server authorization object permissions (*continued*)

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Configure	Modify	---	X	X	---	---	---	---
	Modify SAN Configuration	---	---	X	---	---	---	---

Fat client authorization object permissions

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

Table 6-35 Fat client authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	X	---	---	---	---
Read	Read	X	X	X	---	---	---	--
Operate	Discover	---	X	X	---	---	---	---
Configure	Modify	---	X	X	---	---	---	---

Vault authorization object permissions

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

Table 6-36 Vault authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	---	X	---	---	---	X	---
Read	Read	---	X	---	---	---	X	---
Operate	Manage Containers	---	X	---	---	---	X	---
	Run Reports	---	X	---	---	---	X	---

Table 6-36 Vault authorization object permissions (*continued*)

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Configure	Modify	---	X	---	---	---	---	---
	Run Sessions	---	X	---	---	---	---	---

Server group authorization object permissions

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

Table 6-37 Server group authorization object permissions

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

Key management system (kms) group authorization object permissions

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

Table 6-38 Key management system group authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	---	X	---	---	---	---	X
Read	Read	---	X	---	---	---	---	X

Table 6-38

Key management system group authorization object permissions

(continued)

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Configure	New	---	---	---	---	---	---	X
	Delete	---	---	---	---	---	---	X
	Modify	---	---	---	---	---	---	X

Upgrading NetBackup Access Control (NBAC)

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

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

Upgrading NetBackup Access Control (NBAC)

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

On the media servers and client computers, first stop NetBackup and then upgrade NetBackup. Note that the shared authentication and authorization packages are no longer used on media servers and client computers. These products can be removed if no other Veritas product uses them.

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

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

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

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

On UNIX platforms, use

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

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

On UNIX Platforms, copy the `/usr/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 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 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 authorization service by executing the following commands.

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

On Windows, run `net start nbzd`.

13 Log on to the shared AZ service.

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

On Windows x86 platforms, run `C:\Program`

`Files\VERITAS\Security\Authorization\bin\ vssaz login --domain localhost.`

On Windows X64 platforms, run `C:\Program Files`

`(x86)\VERITAS\Security\Authorization\bin\ vssaz login --domain localhost.`

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

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

On Windows x86 platforms, run `C:\Program`

`Files\VERITAS\Security\Authorization\bin\ vssaz listaps.`

On Windows X64 platforms, run `C:\Program Files`

`(x86)\VERITAS\Security\Authorization\bin\ vssaz listaps.`

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

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

On Windows x86 platforms, run `C:\Program`

`Files\VERITAS\Security\Authorization\bin\vssaz rcexport --toplevelrcname <NBU APS name>.`

On Windows x64 platforms, run `C:\Program Files`

`(x86)\VERITAS\Security\Authorization\bin\vssaz rcexport --toplevelrcname <NBU APS name>.`

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

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

On Windows x86 platforms, run `C:\Program`

`Files\VERITAS\Security\Authorization\bin\ vssaz logout.`

On Windows x64 platforms, run `C:\Program Files`

`(x86)\VERITAS\Security\Authorization\bin\ vssaz logout.`

17 Log on to NetBackup AZ using the following command.

On UNIX platforms, run `/usr/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 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.

Security certificates in NetBackup

This chapter includes the following topics:

- [Overview of security certificates in NetBackup](#)
- [About the Security Management utilities](#)
- [About host name-based certificates](#)
- [About host ID-based certificates](#)
- [About Token Management for host ID-based certificates](#)
- [About revoking host ID-based certificates](#)
- [Security certificate deployment in a clustered NetBackup setup](#)

Overview of security certificates in NetBackup

NetBackup uses security certificates to authenticate NetBackup hosts. The security certificates conform to the X.509 Public Key Infrastructure (PKI) standard. A master server acts as the Certificate Authority (CA) and issues digital certificates to hosts.

Any security certificates that were generated before NetBackup 8.0 are now referred to as host name-based certificates. NetBackup is in the process of replacing these older certificates with newer host ID-based certificates. The transition will be completed in future releases and the use of host name-based certificates will be eliminated.

However, the transition is ongoing and NetBackup 8.0 continues to require the older host name-based certificates for some operations. The following table lists which type of certificate is required for various operations.

Table 7-1 Security certificate requirements

Operation or situation	Type of certificate required
NetBackup master server cluster installation	For a NetBackup master server in a cluster solution other than WSFC and VCS on Windows, you must deploy a host name-based certificate to all of the nodes in the cluster. See “Deploying host name-based certificates” on page 251.
To use the NetBackup Java consoles to connect to media servers and clients	To connect to a media server with the NetBackup Administration Console , the media server must have host name-based and host ID-based certificates installed. To connect to a Windows or UNIX client with the Backup, Archive, and Restore user interface, the client must have a host ID-based certificate installed. See “Deploying host name-based certificates” on page 251. See “About host ID-based certificates” on page 253.
NetBackup Access Control (NBAC)	If NBAC is enabled on a NetBackup host, the hosts require host name-based certificates. These are automatically deployed when NBAC is enabled.
Enhanced Auditing operations	Enhanced Auditing operations require that the hosts have host name-based certificates. See “Deploying host name-based certificates” on page 251.
Targeted Auto Image Replication operations	Targeted Auto Image Replication operations require that the hosts have host name-based certificates. See “Deploying host name-based certificates” on page 251.
Cloud storage	The NetBackup CloudStore Service Container requires that the host name-based certificate be installed on the media server. If one is not installed, the Service Container cannot start. For more information, see the NetBackup Cloud Administrator’s Guide .

Deploying security certificates on NetBackup hosts

Two types of security certificates are required on NetBackup hosts in this release:

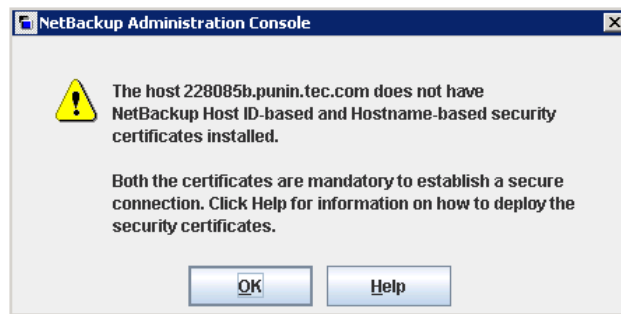
- Host name-based certificates
Any security certificates that were generated before NetBackup 8.0 are now referred to as host name-based certificates. The deployment and management of these certificates has not changed in NetBackup 8.0.
By default, NetBackup master servers are provisioned with a host name-based certificate during installation. To provision a host name-based certificate on a media server or client, the NetBackup administrator runs the `bpbaz` command on the master server to push the certificate to other hosts.

Note: Deploying a host name-based certificate is a one-time activity for a host. If a host name-based certificate was deployed for an earlier release or for a hotfix, it does not need to be done again.

See [“About host name-based certificates”](#) on page 251.

- Host ID-based certificates
NetBackup 8.0 introduces host ID-based certificates that are based on Universally Unique Identifiers (UUIDs) that are assigned by the NetBackup master server. By default, NetBackup master servers are provisioned with a host ID-based certificate during installation. Depending on the security settings for certificate deployment, host ID-based certificates may require authorization tokens when a host ID-based certificate needs to be deployed on a host other than the master server. Use the **NetBackup Administration Console** or the command line to view certificate details and to generate the authorization tokens.
See [“About host ID-based certificates”](#) on page 253.
See [“About certificate deployment security levels”](#) on page 258.

If an administrator uses the **NetBackup Administration Console** to login to a host that does not have both certificates installed, the following message appears:



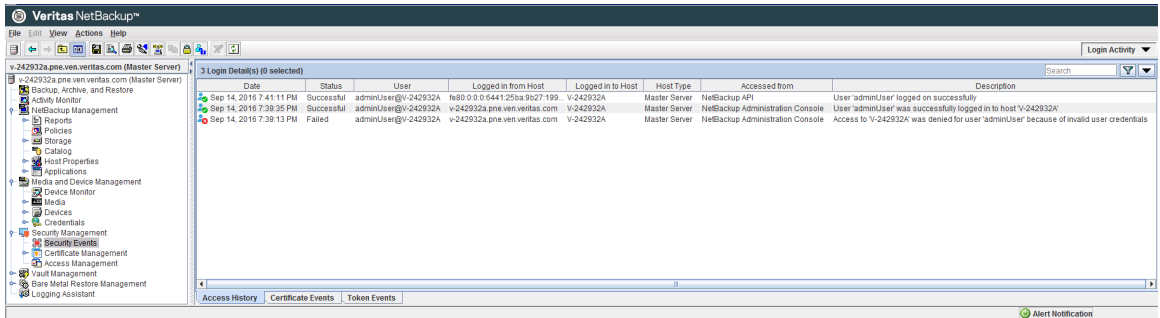
See the following topics for deployment information on each type of certificate:

See [“About host name-based certificates”](#) on page 251.

See [“About host ID-based certificates”](#) on page 253.

About the Security Management utilities

The **NetBackup Administration Console > Security Management** node is visible only to administrators on the NetBackup master server. (An exception to this is NetBackup Access Control administrators. They do not see the **Security Management** node.)



Security Management contains the following utilities to view login activity and to manage host ID-based certificates:

- Use **Security Events** to view the login details about the current administrator and the user-initiated changes that are made to certificates and tokens.

The **Security Events** utility contains three tabs:

- The **Access History** tab displays details about the login activities that the current user has performed. The details include successful and unsuccessful login attempts and information about the hosts that the user has tried to access.

See [“About login activity”](#) on page 250.

The **Accessed from** field displays the component that the user has used to login: **NetBackup Administration Console** or **NetBackup API**.

Note: NetBackup requires the `bprd` service to be running to display the audit details of the users who are logged in using the **NetBackup Administration Console**.

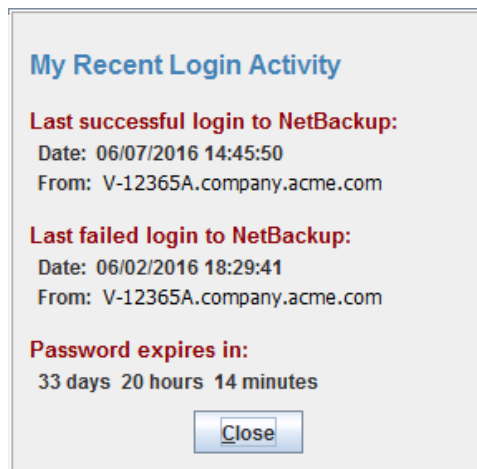
- The **Certificate Events** tab displays the certificate-related activities in the current NetBackup domain. Activities include creating, deleting, and revoking certificates.
- The **Token Events** tab displays the token-related activities in the current NetBackup domain. Activities include creating, deleting, or generating reissue tokens.
- Use the **Certificate Management** node to set the security level for certificate deployment, to view all certificates in the system, to revoke certificates, and to generate reissue tokens.

See [“Using the Certificate Management utility to issue and deploy host ID-based certificates”](#) on page 255.

- **Certificate Management** contains the **Token Management** node. Use the **Token Management** utility to create, delete, and view the tokens.
See “[About Token Management for host ID-based certificates](#)” on page 276.
- Use **Access Management** if NetBackup Access Control (NBAC) is configured. **Access Management** contains options to define who can access NetBackup and the functions that they can perform.
See “[About using NetBackup Access Control \(NBAC\)](#)” on page 150.

About login activity

NetBackup captures information about the access history of users and keeps a track of when a user's password will expire. The information is displayed in the **My Recent Login Activity** window at the top right corner of the **NetBackup Administration Console**.



The **My Recent Login Activity** window closes after you begin to use the **NetBackup Administration Console**.

The password expiration information is not available in the following scenarios:

- If you have remotely logged in to the master server using the Single Sign-on (SSO) feature of the **NetBackup Administration Console**
- If you have logged in to the UNIX or Linux master server using the **NetBackup Administration Console**

Note: The login and the password expiration details are displayed only after the first successful login and logout from the **NetBackup Administration Console**.

The login details are not automatically refreshed. You must log off from the **NetBackup Administration Console** and log in again to view the latest information about the last login details.

This information is also displayed in **Security Events** on the **Access History** tab.

Troubleshooting auditing issues related to the Access History tab

The **NetBackup Administration Console > Security Management > Security Events > Access History** tab displays details about the login activities that the current user has performed.

The **Accessed from** field on the **Access History** tab displays the component that the user has used to login: **NetBackup Administration Console** or **NetBackup API**.

NetBackup requires the `bprd` service to be running to display the audit details of the users who are logged in using the **NetBackup Administration Console**.

If you observe that the required audit records are not being displayed on the **Access History** tab, ensure that the `bprd` service is running.

About host name-based certificates

By default, individual NetBackup master servers are provisioned with a host name-based certificate during installation. Also, during a NetBackup push installation to a Windows Server Failover Cluster (WSFC) and VCS on Windows, a host name-based certificate is deployed to all of the nodes in the failover cluster.

The following topic provides a table that lists the operations that require a host name-based certificate.

See [“Overview of security certificates in NetBackup”](#) on page 246.

Deploying host name-based certificates

Choose one of the following procedures to deploy a host name-based security certificate on NetBackup hosts. Only a NetBackup administrator can deploy certificates.

Table 7-2 Deploying host name-based certificates

Procedure	Description and link to procedure
Deploying a host name-based security certificate for a master server in a cluster	<p>Use this procedure to deploy the host name-based security certificates to all of the nodes in a NetBackup master server cluster.</p> <p>Note the following exception: This procedure is not required for a Microsoft Windows Server Failover Cluster or a Veritas Cluster Server on Windows after a NetBackup push installation to the cluster.</p> <p>See Deploying a host name-based security certificate for a master server in a cluster.</p>
Deploying a host name-based security certificate for media servers or clients	<p>This procedure uses IP address verification to identify the target NetBackup host and then deploy the certificate.</p> <p>With this procedure, you can deploy a host name-based security certificate for an individual host, for all media servers, or for all clients.</p> <p>See Deploying a host name-based security certificate on media servers or clients.</p>

Note: Deploying a host name-based certificate is a one-time activity for a host. If a host name-based certificate was deployed for an earlier release or for a hotfix, it does not need to be done again.

Deploying a host name-based security certificate for a master server in a cluster

Perform this procedure when the master server is part of a cluster.

To deploy a host name-based security certificate for a NetBackup master server in a cluster

- 1 Run the following command on the active node of the master server cluster:

On Windows: `Install_path\NetBackup\bin\admincmd\bpnbaz -setupat`

On UNIX: `/usr/opensv/netbackup/bin/admincmd/bpnbaz -setupat`
- 2 Restart the NetBackup Service Layer (`nbsl`) service and the NetBackup Vault Manager (`nbvault`) service on the active node of the master server.

Deploying a host name-based security certificate on media servers or clients

This procedure works well when you deploy host name-based security certificates to many hosts at one time. As with NetBackup deployment in general, this method assumes that the network is secure.

To deploy a host name-based security certificate for media servers or clients

- 1 Run the following command on the master server, depending on your environment. Either specify a host name, or deploy to all media servers or clients.

On Windows: `Install_path\NetBackup\bin\admincmd\bpnbaz
-ProvisionCert host_name|-AllMediaServers|-AllClients`

On UNIX: `/usr/openv/netbackup/bin/admincmd/bpnbaz -ProvisionCert
host_name|-AllMediaServers|-AllClients`

- 2 Restart the NetBackup Service Layer (nbsl) service on the media server.
No services need to be restarted if the target host is a NetBackup client.

Note: In you use dynamic IPs on the hosts (DHCP), ensure that the host name and the IP address are correctly listed on the master server. To do so, run the following NetBackup `bpclient` command on the master server:

On Windows: `Install_path\NetBackup\bin\admincmd\bpclient -L -All`

On UNIX: `/usr/openv/netbackup/bin/admincmd/bpclient -L -All`

About host ID-based certificates

Each host in a NetBackup domain is assigned a unique identity, which is referred to as the host ID. The master server is the Certificate Authority (CA), and stores the host information in the `nbdb` database. The CA maintains a list of all of the host IDs that have been issued certificates or have had their certificates revoked. The host ID is used in many certificate management operations to identify the host.

For the troubleshooting issues that are related to host-ID based certificates and their resolutions, refer to the Troubleshooting technical article at the following location:

<http://www.veritas.com/docs/DOC5332>

The following topic provides a table that lists the operations that require a host ID-based certificate.

See “[Overview of security certificates in NetBackup](#)” on page 246.

Only a NetBackup administrator can control the settings that are related to certificate deployment and revocation.

If the host certificate is lost due to a communication error during the initial deployment phase, through data loss at a later stage, or even if NetBackup is uninstalled on the host—the master server continues to consider the certificate as a valid certificate.

The host ID remains the same, even when the host name changes. When NetBackup is reinstalled, the host can either retain the same identity or get a new host ID from the master server.

If a host obtains certificates from multiple NetBackup domains, it has multiple host IDs that correspond to each NetBackup domain.

When the master server is configured as part of a cluster, each node in the cluster receives a unique host ID. An additional host ID is assigned for the cluster name. For example, if the master server cluster is comprised of N nodes, the number of host IDs that are allocated for the master server cluster is $N + 1$.

Web login requirements for `nbcertcmd` command options

The `nbcertcmd` command can be used to perform all of the operations that are associated with host-ID based certificates. However, some of the `nbcertcmd` options require that the user first logs in to the NetBackup Web Management Service (`nbwmc`).

- To log in to the NetBackup Web Management Service, run the following command on the master server. (`nbwmc` runs only on the master server.):

```
bpnbat -login -logintype WEB
```

The account must have NetBackup administrator privileges.

The following shows an example `WEB` login:

```
bpnbat -login -LoginType WEB
Authentication Broker: server.domain.com
Authentication port [0 is default]: 0
Authentication type (NIS, NISPLUS, WINDOWS, vx, unixpwd, ldap): unixpwd
Domain: server.domain.com
Login Name: root
Password: *****
Operation completed successfully.
```

- The `bpnbat -login -logintype AT` command creates a session with the NetBackup Authentication Broker (`nbatd`). (The NetBackup Authentication Broker may not always be the master server.)

Note: An `nbatd` session is not necessary to run the `nbcertcmd` commands.

- If neither `WEB` nor `AT` is indicated, `bpnbat -login` creates a login session for both `nbatd` and `nbwmc`. (This is true if the Authentication Broker is located on the master server.)

The procedures in the following topics note whether or not a web login is required.

The [NetBackup Commands Reference Guide](#) lists the privilege details that each `nbcertcmd` option requires. This guide also contains detailed information about running the `bpnbat` command.

Using the Certificate Management utility to issue and deploy host ID-based certificates

The process for host ID-based certificate deployment varies based on the certificate deployment security level configured on the master server. The levels are **Medium**, **High**, and **Very High**. By default, the security level is **High**. A host ID-based certificate is deployed on the master server automatically upon upgrade or new installation.

These levels determine the nature of the Certificate Authority (CA) checks that are performed when the CA receives a certificate request from a NetBackup host. The levels determine which checks are performed before a certificate is issued. Select the certificate deployment level according to the security requirements of your NetBackup environment.

See [“About certificate deployment security levels”](#) on page 258.

In some scenarios, certificate deployment requires the use of authorization tokens that are managed by a NetBackup administrator. The NetBackup administrator creates and shares these tokens with the administrators of individual hosts for certificate deployment on their local hosts. Certificate deployment can happen easily, allowing for scalable deployment across multiple NetBackup hosts without requiring NetBackup administrator intervention.

Table 7-3 Deployment requirements at each certificate deployment level or scenario

Certificate deployment level or scenario	Is an authorization token required?	Deploy host ID-based certificate?
Certificate deployment level setting at Very High	<p>Yes. All certificate requests require an authorization token. The master server administrator creates a token to be used on the non-master host:</p> <p>See “Creating authorization tokens” on page 277.</p>	<p>After receiving the token, the non-master administrator uses it to deploy a host ID-based certificate:</p> <p>See “Deploying host ID-based certificates” on page 260.</p>

Table 7-3 Deployment requirements at each certificate deployment level or scenario (*continued*)

Certificate deployment level or scenario	Is an authorization token required?	Deploy host ID-based certificate?
Certificate deployment level setting at High (default)	<p>Maybe. Certificates are automatically deployed to hosts that are known to the master server.</p> <p>The following topic explains what it means to be known to the master server:</p> <p>See “About certificate deployment security levels” on page 258.</p> <p>If the host is unknown to the master server, the certificate must be deployed using an authorization token. The master server administrator creates a token to be used on the non-master host:</p> <p>See “Creating authorization tokens” on page 277.</p>	<p>After receiving the token, the non-master administrator uses it to deploy a host ID-based certificate:</p> <p>See “Deploying host ID-based certificates” on page 260.</p>
Certificate deployment level setting at Medium	<p>No. Certificates may be automatically deployed to all hosts that request one.</p> <p>See “Automatic host ID-based certificate deployment” on page 260.</p> <p>Note: A certificate may not be automatically deployed if the master server cannot verify that the requested host name matches the IP from which the certificate request originated.</p>	<p>If a host ID-based certificate was deployed automatically, no further action is required.</p> <p>If the master server could not verify the host name, a host ID-based certificate must be deployed:</p> <p>See “Deploying host ID-based certificates” on page 260.</p>
Certificate reissue	Yes, a certificate reissue always requires a token.	See “Creating a reissue token” on page 272.
Hosts that cannot communicate with the master server directly	<p>If a host has no connectivity with the master server, another NetBackup host that can communicate with the master server is used as a proxy for the client.</p> <p>The proxy host requires a token to get a signed certificate from the master server on behalf of the host.</p>	See “Deploying certificates on a client that has no connectivity with the master server” on page 269.

Viewing host ID-based certificate details

Details for each host ID-based certificate can be viewed in the **NetBackup Administration Console** or by using the `nbcertcmd` command.

To view certificate details in the NetBackup Administration Console

- 1 In the **NetBackup Administration Console**, expand **Security Management > Certificate Management**.

The certificate details are displayed in the right pane.

1 Host Certificate(s) (1 selected)								Search	Filter
Certificate State	Host	Host Type	Issued On	Valid From	Valid Until	Days Remaini...	NetBackup Host ID		
Active	caycevm3...	Server	Sep 12, ...	Sep 12, 201...	Sep 12, 2017 8:5...	363	b9e5a819-547e-4150-91c9-fc48		

- 2 By default, the host IDs are not displayed. (See [Table 7-4](#).)

To display or hide columns, right-click on the pane and select **Columns > Layout**. Select the columns to show or hide in the **Column Layout** dialog box.

Table 7-4 Hidden and displayed certificate details

Column head	Description	Displayed by default
Certificate State	The certificate state (Active , Revoked , or Expired).	Yes
Host	The name of the host to which the certificate is issued.	Yes
Host Type	The type of host (server or client).	Yes
Issued On	The date and time on which the certificate was issued.	Yes
Valid From	The date upon which the certificate becomes valid.	Yes
Valid Until	The date until after which the certificate is invalid.	Yes
Days Remaining Until Expiry	The number of days until the certificate expires and cannot be used.	Yes
NetBackup Host ID	The unique ID assigned to the host.	No
Serial Number	The serial number of the certificate.	No
Reason For Revocation	The reason for a certification revocation, if the administrator entered a reason at the time of revocation.	No
Last Updated On	The date when the certificate details were last updated.	No

To view certificate details using the nbcertcmd command

- ◆ To view all of the host IDs that are assigned to a host from different master servers, run the following command on a NetBackup host:

```
nbcertcmd -listCertDetails
```

About certificate deployment security levels

NetBackup offers several levels that determine the nature of the CA checks that are performed when the CA receives a certificate request. The level determines the checks that are performed before the CA issues a certificate to a NetBackup host. Choose a certificate deployment level that corresponds with the security constraints and requirements of your NetBackup environment.

[Table 7-5](#) lists and describes the three deployment levels.

Table 7-5 Description of certificate deployment security levels

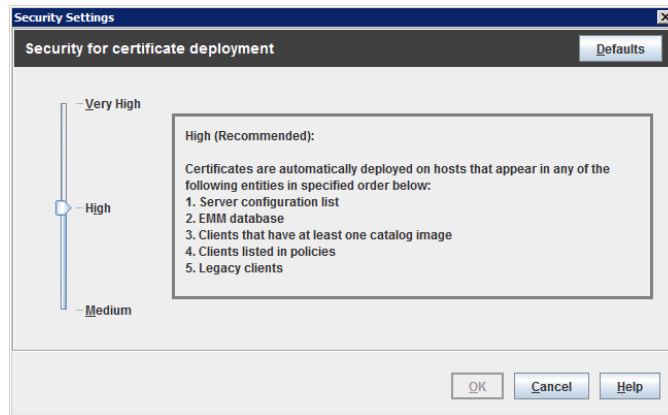
Security Level	Description
Very High	<p>Automatic certificate deployment is disabled. An authorization token must accompany every new certificate request.</p> <p>See “Creating authorization tokens” on page 277.</p>
High (default)	<p>Certificates are automatically issued and deployed. No authorization token is required on any host that is known to the master server.</p> <p>A host is considered to be known to the master server if any of the following are true, in the order listed:</p> <ol style="list-style-type: none">1 If the host is listed as a server in the Server host properties (the server configuration list).2 If the host appears in the EMM database of the master server.3 If at least one catalog image of the client exists. The image must not be older than 6 months.4 If the client is listed in at least one backup policy.5 If the client is a legacy client. That is, a client that the master server added by using the Client Attributes host properties. <p>See “Creating authorization tokens” on page 277.</p>
Medium	<p>Certificates are automatically deployed on all hosts that request one from the master server. The certificates are issued without an authorization token if the master server can resolve the host name to the IP address from which the request originated.</p> <p>See “Automatic host ID-based certificate deployment” on page 260.</p>

Configuring the certificate deployment security levels

Use the **NetBackup Administration Console** or the `nbcertcmd` command to configure the certificate deployment security level in the NetBackup domain.

To configure the certificate deployment level using the NetBackup Administration Console

- 1 In the **NetBackup Administration Console**, expand **Security Management** > **Certificate Management**.
- 2 From the **Actions** menu, select **Configure Security Settings**.
- 3 Slide the indicator to one of three levels: **Very High**, **High** (default), or **Medium**.
See the following topic for a description of each level:
See [“About certificate deployment security levels”](#) on page 258.
- 4 Click **OK**.



To configure the certificate deployment level using the command line

- 1 The master server administrator must be logged in to the NetBackup Web Management Service to perform this task. Use the following command to log in:

```
bpnbat -login -logintype WEB
```

See [“Web login requirements for nbcertcmd command options”](#) on page 254.

- 2 Run the following command to view the current security level:

```
nbcertcmd -getSecConfig -certDeployLevel -server  
master_server_name
```

- 3 Run the following command to change the security level:

```
nbcertcmd -setSecConfig -certDeployLevel 0-2 -server  
master_server_name
```

Where 0 is Very High, 1 is High (default), and 2 is Medium.

Automatic host ID-based certificate deployment

A host ID-based certificate is automatically deployed on the NetBackup master server as part of NetBackup installation.

These certificates are automatically deployed on other NetBackup hosts depending on the certificate deployment level. The NetBackup Client daemon (`bpcd`) periodically checks if the host has all the required certificates. In absence of the required certificates, the daemon tries to establish a trust with the respective master server to request for a host ID-based certificate.

The CA on the NetBackup master server can accept or reject the certificate request depending on the certificate deployment level and the ability of the master server to verify the host information.

You can check the list of the deployed certificates at any time using the following command:

```
nbcertcmd -listCertDetails
```

When a certificate request is rejected, the host administrator must request the NetBackup administrator to generate and share an authorization token to deploy the certificate manually.

See [“Creating authorization tokens”](#) on page 277.

See [“About certificate deployment security levels”](#) on page 258.

Deploying host ID-based certificates

Depending on the certificate deployment security level, a non-master host may require an authorization token before it can obtain a host ID-based certificate from the Certificate Authority (master server). When certificates are not deployed automatically, they must be deployed manually by the administrator on a NetBackup host using the `nbcertcmd` command.

The following topic describes the deployment levels and whether the level requires an authorization token.

See [“About certificate deployment security levels”](#) on page 258.

Deploying when no token is needed

Use the following procedure when the security level is such that a host administrator can deploy a certificate on a non-master host without requiring an authorization token.

To generate and deploy a host ID-based certificate when no token is needed

- 1 The host administrator runs the following command on the non-master host to establish that the master server can be trusted:

```
nbcertcmd -getCACertificate
```

See [“Setting up trust with the master server \(Certificate Authority\)”](#) on page 263.

- 2 Run the following command on the non-master host:

```
nbcertcmd -getCertificate
```

Note: To communicate with multiple NetBackup domains, the administrator of the host must request a certificate from each master server using the `-server` option.

Run the following command to get a certificate from a specific master server:

```
nbcertcmd -getCertificate -server master_server_name
```

- 3 To verify that the certificate is deployed on the host, run the following command:

```
nbcertcmd -listCertDetails
```

Deploying when a token is needed

Use the following procedure when the security level is such that a host requires an authorization token before it can deploy a host ID-based certificate from the CA.

To generate and deploy a host ID-based certificate when a token is required

- 1 The host administrator must have obtained the authorization token value from the CA before proceeding. The token may be conveyed to the administrator by email, by file, or verbally, depending on the various security guidelines of the environment.
- 2 Run the following command on the non-master host to establish that the master server can be trusted:

```
nbcertcmd -getCACertificate
```

See [“Setting up trust with the master server \(Certificate Authority\)”](#) on page 263.

- 3 Run the following command on the non-master host and enter the token when prompted:

```
nbcertcmd -getCertificate -token
```

Note: To communicate with multiple NetBackup domains, the administrator of the host must request a certificate from each master server using the `-server` option.

If the administrator obtained the token in a file, enter the following:

```
nbcertcmd -getCertificate -file authorization_token_file
```

- 4 To verify that the certificate is deployed on the host, run the following command:

```
nbcertcmd -listCertDetails
```

Use the `-cluster` option to display cluster certificates.

Implication of clock skew on certificate validity

When a master server issues a certificate, it determines for how long the certificate will be valid for the host to use. The master server sets the validity of the certificate based on its own time, recording two timestamps: **Not before** and **Not after**. The certificate is valid only between these two timestamps.

The clock on the master server and the clock on the host that will receive the certificate should be in sync so that the certificate is valid for as long as is expected, given the timestamps.

The hosts can reside in different time zones, as long as the clock on each host is set to the correct time for that host's timezone. As a general practice, NetBackup recommends using a service such as Network Time Protocol (NTP) to automatically keep all clocks on all hosts in the NetBackup domain synchronized.

If the clocks are not in sync, the difference can result in the following consequences:

- If the host clock is ahead of the master server, the validity period of the certificate will be less than expected on that particular host. If the difference is extreme and the clocks vary by more than the certificate's validity period, it is possible that if the master server issued a fresh certificate, it could be treated as expired.
- If the host clock is behind the master server, a fresh certificate issued by the master server could be considered as unusable by the host because the host considers the certificate as not yet valid.

To determine whether the master server clock and the host clock are in sync

- 1 Run the following command on the host to determine whether the host clock is in sync with the master server clock:

```
nbcertcmd -checkClockSkew -server master_server_name
```

- 2 The command returns one of the following results:

- If both clocks are in sync, the following displays:

```
The current host clock is in sync with the master server.
```

- If the current host is behind the master server, the command reports the difference in seconds:

```
The current host clock is behind the master server by 36  
seconds(s) .
```

- If the current host is ahead of the master server, the command reports the difference in seconds:

```
The current host clock is ahead of the master server by 86363  
second(s) .
```

- If the command is run on the master server, the command skips the check and displays the following:

```
Specified server is same as the current host. Clock skew check  
is skipped.
```

If the clock skew on the host is causing a problem with the certificate validity, take corrective actions as necessary.

Setting up trust with the master server (Certificate Authority)

Each NetBackup host must first trust the NetBackup master server, which acts as the Certificate Authority (CA). Trust is essential so that the host can request a host ID-based certificate. The CA certificate can be used to authenticate other hosts in the domain, and is stored in the trust store of each host. Setting up trust involves requesting a certificate from the master server.

For security deployment levels of **Medium** or **High**, the NetBackup client daemon (bpcl) automatically performs these steps for each host. If the automatic trust setup fails, the host administrator may need to manually establish the trust.

See [“Automatic host ID-based certificate deployment”](#) on page 260.

Adding a CA certificate to a host's trust store

Run the `nbcertcmd -listCACertDetails` command to see the list of CA certificates that are in the host's trust store. The output displays all of the master servers that the host already trusts.

To establish trust with the master server (CA)

- 1 The host administrator must have the Root Certificate Fingerprint that was communicated to them through an authentic source. The source was most likely the master server administrator, who communicated the fingerprint by email, by file, or on an internal website. The following topic describes that process:

See [“Finding and communicating the fingerprint of a CA certificate”](#) on page 265.

- 2 From the NetBackup host, run the following command:

```
nbcertcmd -getCACertificate -server master_server_name
```

- 3 In the confirmation output, enter **y** to proceed.

For example:

```
nbcertcmd -getCACertificate -server master1
Authenticity of root certificate cannot be established.
The SHA1 fingerprint of root certificate is B8:2B:91:E1:4E:78:D2:
25:86:4C:29:C5:92:16:00:8D:E8:2F:33:DD.
```

Note: The fingerprint that is displayed must match the Root Certificate Fingerprint that the host administrator has received from the master server administrator. Enter **y** to give consent to add the CA certificate to the trust store of the host.

```
Are you sure you want to continue using this certificate ? (y/n): y
The validation of root certificate fingerprint is successful.
CA certificate stored successfully.
```

- 4 Next, the administrator performs the following task:

See [“Deploying host ID-based certificates”](#) on page 260.

Adding a CA certificate via message in the NetBackup Administration Console

The **NetBackup Administration Console** and the **Backup, Archive, and Restore** user interfaces communicate with NetBackup hosts (master server, media server, or client) over a secure channel. NetBackup secures this channel using a NetBackup host ID-based or a host name-based security certificate that the NetBackup Certificate Authority (CA) issues.

[Figure 7-1](#) displays in the **NetBackup Administration Console** in the following situation: A user is running the **NetBackup Administration Console** on a NetBackup host. The user tries to connect to another NetBackup host (a target

host) using the **NetBackup Administration Console**. However, the CA that issued the security certificate to the target host is not in the trust store of the host where the user launched the console.

Figure 7-1 Message inquiring whether to add a Certificate Authority (CA) to the trust store



To verify the CA fingerprint that the dialog displays, see the following topic:

See [“Finding and communicating the fingerprint of a CA certificate”](#) on page 265.

If the user selects **Yes** in this message, the CA is added to the trust store of the host where the console is running. This host will then trust all hosts that have a certificate signed by the CA that is listed in the message.

Finding and communicating the fingerprint of a CA certificate

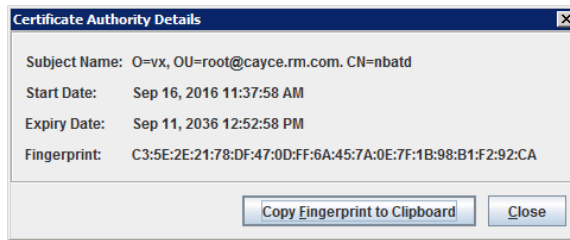
The master server administrator must find the fingerprint of the CA certificate and communicate it to the administrator of the individual host so that the host can add the CA certificate to its trust store.

To find the fingerprint of the CA certificate

- 1 The master server administrator can find the fingerprint using the **NetBackup Administration Console** or the command line:

Using the **NetBackup Administration Console**:

- Expand **Security Management > Certificate Management**.
- On the **Actions** menu, select **View Certificate Authority**. The **Certificate Authority Details** dialog appears.



The **Copy Fingerprint to Clipboard** option is available to help the administrator communicate the fingerprint to the host administrator.

Using the command line:

- Run the following command on the master server to view the Root Certificate Fingerprint:

```
nbcertcmd -listCACertDetails
```

```
Subject Name : /CN=nbatd/OU=root@cayce.rm.com/O=vx
Start Date   : Sep 16 10:37:58 2016 GMT
Expiry Date  : Sep 11 11:52:58 2036 GMT
SHA1 Fingerprint : C3:5E:2E:21:78:DF:47:0D:FF:6A:45:7A:0E:
                  7F:1B:98:B1:F2:92:CA
```

If the master server has multiple CA certificates, run the command on the host to determine whether the host already has a CA certificate from this master server. The **Subject Name** identifies the master server.

- 2 The master server administrator communicates the fingerprint to the host administrator by email, by file, or on an internal web site.

The host administrator uses this fingerprint to verify the fingerprint that displays when the host runs `nbcertcmd -getCACertificate`.

Using the `vssat` command to view the CA certificate fingerprint

The `vssat` command can also be used to view the CA certificate fingerprint. Use `vssat` with the following options:

```
vssat showcred -p nbatd
```

However, note the following differences between using `nbcertcmd -listCACertDetails` and `vssat`:

- `vssat` displays the fingerprint as a hash and does not include colon separators.

- If the host trusts multiple Certificate Authorities, the `nbcertcmd` command displays all CA certificates. The **Subject Name** displays the identity of the CA.

Deploying certificates from multiple masters

A client may have multiple master servers listed in its **Servers** list. (The **Servers** list is displayed in the **Host Properties > Clients > Servers** properties.)

During startup, the host attempts to automatically fetch a host ID-based certificate from the first master server that is listed in the **Servers** list. Follow this procedure to make a client automatically retrieve a certificate from all the master servers that are listed in its **Servers** list. Use this procedure, regardless of the security level setting.

To deploy certificates from multiple masters

- ◆ The host administrator uses the `nbsetconfig` command to enable the `GET_CERT_ALL_MASTERS` option in the configuration file of the non-master host. (The configuration file is the Windows registry or the `bp.conf` file on UNIX.)

Use the following format:

```
GET_CERT_ALL_MASTERS = YES
```

Forcing or overwriting certificate deployment

In some situations it may be necessary to use the `-force` option with the `nbcertcmd -getCertificate` command. For example, to force certificate deployment to a host or to overwrite the existing host ID-based certificate information and fetch a new certificate.

Forcing certificate deployment

A host may already have a host ID-based certificate, but needs to overwrite the old certificate with a new one. This is required, for example, when a master server is replaced with a new server. Since the clients have the old certificate to the old server, when the `nbcertcmd -getCertificate` command is run on the clients, it fails with the following error:

```
Certificate already exists for the server.
```

Use the following procedure to overwrite the existing host ID-based certificate information and fetch a new certificate.

To force certificate deployment on a host

- ◆ The host administrator runs the following command on the non-master host:

```
nbcertcmd -getCertificate -server master_server_name -force
```

- Depending on the security setting on the master server, a token may also need to be specified.
See [“Creating authorization tokens”](#) on page 277.
- Use the `-cluster` option to deploy a cluster certificate.

Overwrite the existing host ID-based certificate information and fetch a new certificate

A host may have been issued a certificate, but over time the certificate has become corrupted or the certificate file has been deleted.

The administrator of the non-master host can run the following command to confirm the condition of the certificate:

```
nbcertcmd -listCertDetails
```

- If the certificate is corrupt, the command fails with the following error:
`Certificate could not be read from the local certificate store.`
- If no certificate details display, the certificate is not available.

Use the following procedure to overwrite the existing host ID-based certificate information and to fetch a new certificate.

To fetch a new host ID-based certificate

- ◆ The host administrator runs the following command on the non-master host:

```
nbcertcmd -getCertificate -force
```

- Depending on the security setting on the master server, a token may also need to be specified.
See [“Creating authorization tokens”](#) on page 277.
- Use the `-cluster` option to deploy a cluster certificate.

Retaining host ID-based certificates when reinstalling NetBackup on non-master hosts

Administrators may want to uninstall NetBackup from a host, and then perform a clean installation on the same host. See the following procedure for instructions on how to retain the identity of a host through the uninstall/reinstall process.

To retain host ID-based certificates when reinstalling NetBackup

- 1** Stop all NetBackup services on the host.
- 2** Back up the following directories:
On Windows:

```
Install_path\NetBackup\var\VxSS
```

```
Install_path\NetBackup\var\webtruststore
```


On UNIX:

```
/usr/opensv/var/vxss
```

```
/usr/opensv/var/webtruststore
```
- 3** Where NetBackup Cluster Server is used, also back up the following directories:

```
Shared_disk\var\global\vxss
```

```
Shared_disk\var\global\webtruststore
```
- 4** Reinstall NetBackup on the host.
- 5** Restore the data that was backed up in step 2 and step 3.

Deploying certificates on a client that has no connectivity with the master server

The `-getCertificate` command that retrieves a host-ID based certificate must communicate directly with the master server. If a client has no connectivity with the master server, another NetBackup host that can communicate with the master server is used as a proxy for the client.

To deploy a certificate via a proxy host

- 1** The host administrator of the non-master host runs the following command on the host where the certificate needs to be deployed:

```
nbcertcmd -createCertRequest -requestFile request_file_name
```

```
-server master_server_name
```


The command generates a certificate signing request.
- 2** Copy the Certificate Signing Request (CSR) file to a proxy NetBackup host that has connectivity with the master server.

- 3 On the proxy host, get a signed certificate from the master server on behalf of the client.

A token is mandatory for the following operation. If the host had already been issued a certificate, then a reissue token is required. Run the following command on the proxy NetBackup host. Any user can run this command on the proxy host:

```
nbcertcmd -signCertificate -requestFile request_file_name  
-certificateFile certificate_file_name -token
```

- 4 Copy the signed certificate that was generated in step 3 and convey it to the administrator of the client.
- 5 To deploy the signed certificate on the client, the host administrator runs the following command on the client:

```
nbcertcmd -deployCertificate -certificateFile  
certificate_file_name
```

About host ID-based certificate expiration and renewal

NetBackup host ID-based certificates expire one year after their issue date. They are automatically renewed 180 days before the expiration date. A certificate renewal request is sent periodically until a certificate is successfully renewed. Automatic renewal ensures that the renew process is transparent to the user.

The renewal request is always authenticated using the existing certificate. Hence, the renewal process does not require the use of an authorization token, regardless of the certificate deployment security level.

If the existing certificate has not expired, the host administrator can initiate a manual renewal request, as described in the following procedure.

To renew a host ID-based certificate manually

- ◆ The host administrator runs the following command on the non-master host:

```
nbcertcmd -renewCertificate
```

- Certificates corresponding to NetBackup domains other than the primary domain can be manually renewed by specifying the `-server` option.
- Use the `-cluster` option to renew the cluster certificate of NetBackup clustered server.

Certificate renewal of a client that does not have direct connectivity to master is not supported. Instead, perform the procedure that is described in the following topic:

See [“Deploying certificates on a client that has no connectivity with the master server”](#) on page 269.

In a scenario where the certificate has expired, the administrator of the host must manually reissue the certificate.

See [“About reissuing host ID-based certificates”](#) on page 272.

Cleaning host ID-based certificate information from a host before cloning a virtual machine

Cloning a virtual machine can present the opportunity for identify theft. Multiple hosts should not have the same key pair. This procedure ensures that each copy of the host gets a unique key pair and identity.

Perform the following procedure before cloning a virtual machine (or before creating a gold image of a machine for cloning) if it is a one-time operation.

To clean the host ID-based certificate information from a host before cloning

- 1 Stop all NetBackup services on the host.
- 2 Delete all files and directories from the following locations:

On Windows:

```
Install_path\NetBackup\var\VxSS\at\*
```

```
Install_path\NetBackup\var\VxSS\credentials\*
```

```
Install_path\NetBackup\var\webtruststore\*
```

On UNIX:

```
/usr/opensv/var/vxss/at/*
```

```
/usr/opensv/var/vxss/credentials/*
```

```
/usr/opensv/var/webtruststore/*
```

- 3 Delete the following file:

On Windows: *Install_path*\NetBackup\var\VxSS\certmapinfo.json

On UNIX: /usr/opensv/var/vxss/certmapinfo.json

- 4 Where NetBackup Cluster Server is used, perform the following steps in addition:

- 5 Delete all files and directories from the following locations:

```
Shared_disk\var\global\vxss\at\*
```

```
Shared_disk\var\global\vxss\credentials\*
```

```
Shared_disk\var\global\webtruststore\*
```

6 Delete the following file:

```
Shared_disk\var\global\vxss\certmapinfo.json
```

7 Proceed to clone the virtual machine.

About reissuing host ID-based certificates

A certificate must be reissued in any of the following cases:

- The certificate was revoked.
- The certificate expired.
- NetBackup was reinstalled on the host where a certificate was already issued.
- The name of the host was changed.
- The key pair for the host was changed.

Reissuing a certificate is one way to prevent malicious users from assuming the identity of an existing NetBackup host that is already registered with the NetBackup master server. A reissue token is always required for certificate reissue, regardless of the security level.

- Reissuing a host ID-based certificate for a NetBackup host is different from deploying the certificate for the first time. Use the following procedure to reissue a certificate.

See [“Creating a reissue token”](#) on page 272.

- Once a reissue token is obtained, the certificate reissue process is similar to manual certificate deployment with an authorization token.

See [“Deploying host ID-based certificates”](#) on page 260.

When the master server receives a certificate reissue request, it first revokes all the previously valid certificates for that host and then generates a new certificate when required.

Creating a reissue token

A host ID-based certificate can be reissued if the non-master host is already registered with the master server but its host ID-based certificate is no longer valid. For example, a certificate is not valid when it has expired, is revoked, or is lost.

A reissue token is a type of token that can be used to reissue a certificate. It is a special type of token because it retains the same host ID as the original certificate. Since a reissue token is bound to a specific host, the token cannot be used to request certificates for additional hosts.

To create a reissue a token using the NetBackup Administration Console

- 1** In the **NetBackup Administration Console**, expand **Security Management > Certificate Management**.
- 2** In the right pane, select the host that requires a reissue token.
- 3** From the **Actions** menu, select **Generate Reissue Token**.
- 4** In the **Create Reissue Token** dialog, enter a name for the token.
- 5** Select a date for token validity from the **Valid until** option.

Note: The **Maximum Uses Allowed** setting is not available as it is when a new token is created. A reissued token must be used one time for a specific host.

- 6** In the **Reason** field, enter a reason for the reissue token. The reason appears in the log as an audit event.
- 7** Click **Create**.
- 8** The reissue token appears in a dialog. Select **Copy** to save the token value to the clipboard.
- 9** Convey the token value to the administrator of the non-master host. How the token is conveyed depends on various security factors in the environment. The token may be transmitted by email, by file, or verbally.

The administrator of the non-master host deploys the token to obtain another host ID-based certificate. See the following topic for instructions:

See [“Deploying host ID-based certificates”](#) on page 260.

To create a reissue a token using the `nbcertcmd` command

- 1 The master server administrator must be logged in to the NetBackup Web Management Service to perform this task. Use the following command to login:

```
bpnbat -login -logintype WEB
```

See [“Web login requirements for nbcertcmd command options”](#) on page 254.

- 2 Run one of the following commands on the master server.

Use the host name for which the certificate needs to be reissued:

```
nbcertcmd -createToken -name token_name -reissue -host host_name
```

Use the host ID for which the certificate needs to be reissued:

```
nbcertcmd -createToken -name token_name -reissue -hostId host_id
```

Additional parameters can be used to indicate validity duration and the reason for creation.

Additional steps to request a certificate for a renamed NetBackup host

In addition to reissuing a token, the following steps are required to request a certificate for a renamed NetBackup host.

To request a certificate for a host after a host name change

- 1 The NetBackup administrator of the master server generates a reissued token for the renamed NetBackup host.
- 2 The NetBackup administrator must revoke the host ID-based certificate for the renamed host.

See [“Revoking a host ID-based certificate”](#) on page 282.

Note: After the certificate is revoked, the host is unable to communicate with the NetBackup Web Management Console service (`nbwmc`). When the host obtains a new certificate using the reissued token, the host can communicate with `nbwmc` again.

- 3 After the certificate is revoked, the administrator of the non-master host must use the reissued token to get a certificate for the renamed host.

See [“Deploying host ID-based certificates”](#) on page 260.

Changing the key pair for a host

Consider changing a key pair only if a key is compromised or leaked. Changing a key pair results in both a new host ID-based certificate and a new host name-based certificate.

The following procedure describes changing a key pair for a host, and then getting a new certificate using the new key pair. Do not perform the procedure for a master server, only a non-master host.

To change a key pair for a non-cluster host

- 1 The NetBackup host administrator backs up the following directories:

On Windows: `Install_path\NetBackup\var\VxSS\at\systemprofile`

On UNIX: `/usr/opensv/var/vxss/at/root`

- 2 The NetBackup host administrator removes the directory from the host.

- 3 Restart the NetBackup services on the host.

- 4 The master server administrator performs the following steps:

- Log in to the NetBackup Web Management Service:

`bpnbat -login -logintype WEB`

See [“Web login requirements for nbcertcmd command options”](#) on page 254.

- Revoke the host ID-based certificate:

`nbcertcmd -revokeCertificate -host host_name`

- Generate a reissue token for the NetBackup host where the key pair is to be changed.

See [“Creating a reissue token”](#) on page 272.

- Deploy a new host name-based certificate:

`bpnbaz -ProvisionCert host_name`

- 5 The NetBackup host administrator uses the reissue token to deploy a new host ID-based certificate with an updated key pair.

Use the following command to enter the token directly:

`nbcertcmd -getCertificate -force -token token`

Use the following command if the token is in a file:

`nbcertcmd -getCertificate -force -file /directory/token_file`

- 6 If the host has more than one master server, repeat the process beginning at step 4 for each master server.

- 7 Restart the NetBackup services on the NetBackup host where the key was changed.

To change a key pair for a host in a cluster

- 1 The NetBackup resource is typically clustered on the master or the media server.

The NetBackup host administrator backs up the following directories:

On Windows:

`Cluster_shared_disk\Veritas\NetBackup\var\VxSS\at\systemprofile`

On UNIX: `/usr/openv/var/vxss/at/root`

- 2 The NetBackup host administrator removes the directory from the host.
- 3 Restart the NetBackup services on the host.
- 4 The master server administrator performs the following steps:
 - Log in to the NetBackup Web Management Service:
`bpnbat -login -logintype WEB`
 - Revoke the host ID-based certificate:
`nbcertcmd -revokeCertificate -host host_name`
 - Generate a reissue token for the NetBackup host where the key pair is to be changed.
 - Deploy a new host name-based certificate:
 - `bpnbaz -ProvisionCert cluster_name`
- 5 The NetBackup host administrator uses the reissue token to deploy a new host ID-based certificate with an updated key pair. Use the following command:

`nbcertcmd -getCertificate -force -file /directory/token_file
-cluster`
- 6 If the host has more than one master server, repeat the process at step 4 for each master server.
- 7 Restart the NetBackup services on the active node where the key was changed.

About Token Management for host ID-based certificates

Master server administrators use the **Token Management** utility to perform the following tasks:

- Create new authorization tokens
Depending on the security level, an authorization token may be required for a non-master NetBackup host to obtain a host ID-based certificate. The NetBackup

administrator of the master server generates the token and shares it with the administrator of the non-master host. That administrator can then deploy the certificate without the presence of the master server administrator.

See [“Creating authorization tokens”](#) on page 277.

- Delete authorization tokens
See [“Deleting authorization tokens”](#) on page 279.
- View authorization token details
See [“Viewing authorization token details”](#) on page 279.
- Clean up invalid or expired authorization tokens
See [“About expired authorization tokens and cleanup”](#) on page 280.

Creating authorization tokens

Depending on the certificate deployment security setting, NetBackup hosts may require an authorization token to obtain a host ID-based certificate from the Certificate Authority (master server).

- If the security setting is **Very High**, all certificate requests require a token. Perform the procedure that is described in this topic.
- If the security setting is **High**, certificates are automatically deployed to hosts that are known to the master server. If the host is not known to the master server, the certificate must be deployed using an authorization token. In that case, perform the procedure that is described in this topic.
To understand what it means to be known to the master server, see the following topic:
See [“About certificate deployment security levels”](#) on page 258.
- If the security setting is **Medium**, this procedure may be less likely because certificates are automatically deployed to all hosts that request one. However, the master server must be able to cross verify the IP and host name of the host that is requesting a certificate.

Note: A token is required to request a certificate on behalf of a host that has no connectivity with the master server.

See [“Deploying certificates on a client that has no connectivity with the master server”](#) on page 269.

Note: Do not use this procedure to create an authorization token for a NetBackup host whose current certificate is not in a valid state because it is lost, corrupt, or expired. In these cases, the token must be reissued.

See [“About reissuing host ID-based certificates”](#) on page 272.

The NetBackup administrator of the master server can use the **NetBackup Administration Console** or the command line to create the token.

To create a token using the NetBackup Administration Console

- 1** In the **NetBackup Administration Console**, expand **Security Management > Certificate Management > Token Management**.
- 2** On the **Actions** menu, select **New Token**.
 The **Create Token** dialog box is displayed.
- 3** Enter a unique and meaningful name for the token. The field cannot be left blank.
 For example, to create a token to request certificates for multiple hosts that belong to master_server_1, name the token Token1_MS1. A good practice is to write a useful description in the **Reason** field for the token.
- 4** Enter a number for the **Maximum Uses Allowed** option for the number of times the token can be used. The default is 1, which indicates that one host can use the token one time.
 To use the same token for multiple hosts, enter any value between 1 and 99999. For example, to use the token for 8 hosts, enter 8. The ninth host that attempts to use the token will not succeed.
- 5** Use the **Valid for** option to indicate how long the token can be used before it is invalid and cannot be used. After the **Valid for** date, the master server must generate another token.
 Select a period between 1 and 999 hours or days.
- 6** Optionally, enter the reason for creating the token. The reason appears in the audit logs, along with the other entries in the dialog.
- 7** Select **Create**.
- 8** The new token appears in a dialog. Select **Copy** to save the token value to the clipboard.

- 9 Convey the token value to the administrator of the non-master host. How the token is conveyed depends on various security factors in the environment. The token may be transmitted by email, by file, or verbally.
- 10 The administrator of the non-master host uses the token to obtain a host ID-based certificate from the Certificate Authority. See the following procedure for instructions:

See [“Deploying host ID-based certificates”](#) on page 260.

To create a token using the `nbcertcmd` command

- ◆ Run the following command on the host:

```
nbcertcmd -createToken -name token_name
```

For example:

```
nbcertcmd -createToken -name testtoken
```

```
Token FCBVYUTDUIELUDOE created successfully.
```

Additional parameters can be used to indicate maximum uses, validity duration, and the reason for creation.

For information about the `nbcertcmd` command, see the [NetBackup Commands Reference Guide](#).

Deleting authorization tokens

Use the **NetBackup Administration Console** or the command line to delete specific authorization tokens. A token can be deleted even though it has not expired and the **Maximum Uses Allowed** count has not yet been exhausted.

To delete a token using the NetBackup Administration Console

- 1 In the **NetBackup Administration Console**, expand **Security Management > Certificate Management > Token Management**.
- 2 In the right pane, select the token to be deleted.
- 3 Select **Edit > Delete**.
- 4 Click **Yes** in the confirmation dialog box to delete the token.

To delete a token using the command line

- ◆ Run the `nbcertcmd -deleteToken` command (with additional parameters).

Viewing authorization token details

Details for each authorization token can be viewed in the **NetBackup Administration Console** or from the command line.

To view token details using the NetBackup Administration Console

- 1 In the **NetBackup Administration Console**, expand **Security Management > Certificate Management > Token Management**.
- 2 The token details are displayed in the right pane.

2 Token Records (0 selected)						Search	
Token State	Name	Maximum Uses Allowed	Uses Remaining	Valid From	NetBackup Host ID	Time Remaining Until Expiry	
Not Valid	MasterServerInstallationToken_1473830907937	2		1 Sep 14, 2016 10:58:29 AM			
Valid	azaaaa	1		1 Sep 14, 2016 1:30:06 PM		17 hour(s) 46 minute(s)	

To view token details using the nbcertcmd command

- ◆ On the master server, run the `nbcertcmd -listToken` command (with additional parameters) to view the token details.

The token details are displayed.

About expired authorization tokens and cleanup

An authorization token expires in either of the following situations (whichever happens first):

- When the current date-time combination is later than the token's **Valid for** amount.
- When the **Maximum Uses Allowed** count reaches the maximum uses.

An expired authorization token remains in the token database, but cannot be used to authorize certificate deployment requests.

Expired tokens can be deleted one by one, or they can be cleaned up all at once by using the **Cleanup** operation. The **Cleanup** operation deletes all expired tokens from the token database.

To clean up expired authorization tokens using the NetBackup Administration Console

- 1 In the **NetBackup Administration Console**, expand **Security Management > Certificate Management > Token Management**.
- 2 On the **Actions** menu, select **Cleanup**.
- 3 Click **Yes** in the confirmation dialog box to clean up all expired tokens and delete them from the token database.

To clean up tokens using the command line

- ◆ Use the `nbcertcmd -cleanupToken` command to delete all the expired tokens.

See [“Deleting authorization tokens”](#) on page 279.

About revoking host ID-based certificates

This topic describes the impact of revoked certificates in a NetBackup environment.

The NetBackup Web Management Console service (`nbwebsvc`) is the only service that verifies the status of the host ID-based certificate before it allows secure communication. That is, `nbwebsvc` checks to see whether the certificate is active or whether it has been revoked. If the certificate has been revoked, for example, `nbwebsvc` does not allow communication to continue.

In NetBackup 8.0, the only service that uses host ID-based certificates but does not check the certificate status is the NetBackup Java Application Server Authentication service (`bpjava`). This means that when the **NetBackup Administration Console** is used to connect to a target NetBackup host, the console only verifies whether the host ID-based certificate is present, but does not verify the certificate status. Both Java interfaces (including **Backup, Archive, and Restore**) allow secure communication, even if the certificate has been revoked.

No other NetBackup component or service, where host ID-based certificates are used, verifies the status of the host ID-based certificate before it allows secure communication. Although secure communication is allowed to proceed even if a certificate has been revoked, the host ID-based certificate must be present on the host.

Removing trust between a host and a master server

A NetBackup host can trust multiple Certificate Authorities (master servers) at any time. For various reasons, it may be necessary for a NetBackup host to remove trust from a master server that previously had been trusted.

For example, if a NetBackup client is moved from one master server to another, it is advisable to remove trust from the first master server. Security best practices suggest trusting the fewest entities required to function correctly. Also, if a NetBackup host no longer needs to communicate with hosts from a specific NetBackup domain, remove the CA certificate for that master from the trust store of the host.

Note: Removing a CA certificate does not remove the host ID-based or host name-based certificates that the host may have obtained from that CA. The `nbcertcmd -listcertdetails` continues to show the host ID-based certificate.

When the CA certificate is removed from a host, the host ID-based certificate issued by that CA will not automatically renew because the host no longer trusts the CA. The host ID-based certificate eventually expires.

Removing trust between a host and a master server

- 1 The administrator of the non-master host runs the following command on the host to determine the CA certificate fingerprint of the master server:

```
nbcertcmd -listCACertDetails
```

In this example output, the host has certificates from two master servers:

```
nbcertcmd -listCACertDetails
      Subject Name : /CN=nbatd/OU=root@master1.abc.com/O=vx
      Start Date  : Aug 23 14:16:44 2016 GMT
      Expiry Date : Aug 18 15:31:44 2036 GMT
      SHA1 Fingerprint : 7B:0C:00:32:96:20:36:52:92:E8:62:F3:56:
74:8B:E3:2E:4F:22:4C

      Subject Name : /CN=nbatd/OU=root@master2.xyz.com/O=vx
      Start Date  : Aug 25 12:09:55 2016 GMT
      Expiry Date : Aug 20 13:24:55 2036 GMT
      SHA1 Fingerprint : 7A:C7:6E:68:71:6B:82:FD:7E:80:FC:47:F6:
8D:B2:E1:40:69:9C:8C
```

- 2 The administrator wants to remove trust to the second master server and runs the following command on the host:

```
nbcertcmd -removeCACertificate -fingerprint 7A:C7:6E:68:71:
6B:82:FD:7E:80:FC:47:F6:8D:B2:E1:40:69:9C:8C
```

Include the entire fingerprint, including the colons.

Warning: This command removes the CA certificate from the trust store. The trust store is referred to by NetBackup services and by the NetBackup Web Management Console service (`nbwebsvc`).

- 3 The **NetBackup Administration Console** on the master server displays the certificate state as **Active**. However, that certificate does not automatically renew and eventually expires. The NetBackup administrator should revoke the certificate of the host if the host is no longer going to be part of the NetBackup domain.

Revoking a host ID-based certificate

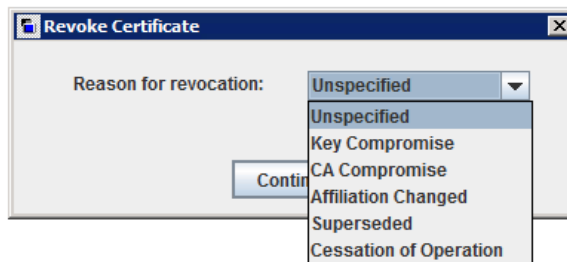
NetBackup administrators may consider revoking a host ID-based certificate under various conditions. For example, if the administrator detects that client security has been compromised, if a client is decommissioned, or if NetBackup is uninstalled

from the host. A revoked certificate cannot be used to communicate with master server web services.

Security best practices suggest that the administrator explicitly revoke the certificates for any host that is no longer active, regardless of whether the certificate is still deployed on the host, or whether it has been successfully removed from the host.

To revoke a host ID-based certificate using the NetBackup Administration Console

- 1 In the **NetBackup Administration Console**, expand **Security Management** > **Certificate Management**.
- 2 Select the certificate to be revoked.
- 3 On the **Actions** menu, select **Revoke Certificate**.
- 4 Select a reason from the drop-down menu and click **Continue**.



The certificate is revoked.

To revoke a host ID-based certificate using the command line

- 1 The master server administrator must be logged in to the NetBackup Web Management Service to perform this task. Use the following command to log in:

```
bpnbat -login -logintype WEB
```

See [“Web login requirements for nbcertcmd command options”](#) on page 254.

- 2 Run one of the following commands to revoke the certificate using the host name or the host ID.

Revoke by the host name:

```
nbcertcmd -revokeCertificate -host host_name
```

Revoke by the host ID:

```
nbcertcmd -revokeCertificate -hostID host_id
```

Additional parameters can be used to indicate a revocation reason code and the master server.

Note: Revoking a certificate does not delete the certificate from the local store of the non-master host.

Security certificate deployment in a clustered NetBackup setup

This section provides information on deployment of host name-based and host ID-based certificates in a NetBackup clustered setup.

For more information on NetBackup clusters, see the *NetBackup Clustered Master Server Administrator's Guide*.

<http://www.veritas.com/docs/DOC5332>

About host ID-based certificate deployment on a NetBackup cluster

In a clustered NetBackup master server setup, the host ID-based certificates are deployed as follows:

- One certificate for each cluster node: A certificate resides on the local disk of each node.
- One certificate for the virtual name: A certificate resides on the shared disk of the cluster.

Consider the following example:

If a cluster setup consists of 4 nodes, 5 host ID-based certificates are deployed. One certificate is deployed on each of the 4 nodes and one on the shared disk, which is used for the virtual name of the master server.

Note: NetBackup does not support clustering of clients.

About host name-based certificate deployment on a NetBackup cluster

In a clustered NetBackup master server setup, the host name-based certificates are deployed as follows:

- One certificate for each cluster node: A certificate resides on the local disk of each node.

- One certificate for the virtual name on each node: A certificate resides on the local disk of each node.

See [“Deploying host name-based certificates”](#) on page 251.

About deployment of a host ID-based certificate on a clustered NetBackup host

Host ID-based certificates are deployed automatically or manually. The following sections describe various deployment scenarios:

See [“Host ID-based certificate deployment on the active master server node”](#) on page 285.

See [“Host ID-based certificate deployment on inactive master server nodes”](#) on page 285.

See [“Host ID-based certificate deployment on active or inactive media server nodes \(upgrade only\)”](#) on page 286.

Host ID-based certificate deployment on the active master server node

During NetBackup installation, host ID-based certificates are deployed for the active master server node and the virtual name. The certificate for the active node is deployed on a local disk. The certificate for the virtual name is deployed on the shared disk.

Host ID-based certificate deployment on inactive master server nodes

On inactive master server nodes, host ID-based certificates are deployed based on the certificate deployment security level on the master server.

See [“About certificate deployment security levels”](#) on page 258.

See [“Configuring the certificate deployment security levels”](#) on page 258.

In the following scenario, the certificates are automatically deployed on inactive master server nodes:

- The security level is **Medium**.
- The security level is **High** and the node is available in the list of hosts that are known to the master server.

For more details on how to determine whether the host is known to the master server or not, refer to the following section:

See [“About certificate deployment security levels”](#) on page 258.

In the following scenarios, you need to manually deploy the certificates on inactive master server nodes:

- The security level is **Very High**.
- The security level is **High**, but the node is not available in the list of hosts that are known to the master server.
 For more details on how to determine whether the host is known to the master server or not, refer to the following section:
 See [“About certificate deployment security levels”](#) on page 258.
- An inactive node is upgraded earlier than the active node.
 As the active node is yet to be upgraded, the security services on the node are not running. This causes automatic certificate deployment on the inactive node to fail.
- Push installation where the installation on inactive nodes completes earlier than the active node.
 Push installation is available only on Windows platform.
 See [“Deploying a host ID-based certificates on inactive master server nodes”](#) on page 287.

Host ID-based certificate deployment on active or inactive media server nodes (upgrade only)

In a clustered media server setup, host ID-based certificates are deployed based on the certificate deployment security level on the master server.

See [“About certificate deployment security levels”](#) on page 258.

See [“Configuring the certificate deployment security levels”](#) on page 258.

In the following scenarios, certificates are automatically deployed on the media server nodes:

- The security level is **Medium**.
- The security level is **High** and the media server is available in the list of hosts that are known to the master server.
 For more details on how to determine whether the host is known to the master server or not, refer to the following section:
 See [“About certificate deployment security levels”](#) on page 258.

In the following scenarios, you need to manually deploy the certificates on the media server nodes:

- The security level is **Very High**.
- The security level is **High**, but the media server is not available in the list of hosts that are known to the master server.

For more details on how to determine whether the host is known to the master server or not, refer to the following section:

See “[About certificate deployment security levels](#)” on page 258.

See “[Deploying a host ID-based certificate on a clustered NetBackup media server \(upgrade only\)](#)” on page 287.

Deploying a host ID-based certificates on inactive master server nodes

In certain scenarios, you need to manually deploy host ID-based certificates on inactive master server nodes.

See “[Host ID-based certificate deployment on inactive master server nodes](#)” on page 285.

To manually deploy a host ID-based certificate on an inactive master server node

- ◆ Run the following commands on the inactive master server node:

- `nbcertcmd -getCACertificate`
- `nbcertcmd -getCertificate [-file authorization_token_file]`

See “[About Token Management for host ID-based certificates](#)” on page 276.

Deploying a host ID-based certificate on a clustered NetBackup media server (upgrade only)

Starting from 7.0 version, NetBackup does not support clustering of media servers. However, if you have a clustered media server of an older version, you can upgrade it to the latest version.

<https://www.veritas.com/docs/TECH147444>

In certain scenarios, you need to manually deploy host ID-based certificates on active or inactive media server nodes.

See “[Host ID-based certificate deployment on active or inactive media server nodes \(upgrade only\)](#)” on page 286.

To manually deploy host ID-based certificates on a clustered media server setup

- 1 Run the following commands on the media server node where you want to deploy the certificate:

- `nbcertcmd -getCACertificate`
- `nbcertcmd -getCertificate [-file authorization_token_file]`

See [“About Token Management for host ID-based certificates”](#) on page 276.

- 2 Run the following commands on the active media server node to deploy the certificate for the virtual name:

- `nbcertcmd -getCACertificate -cluster`
- `nbcertcmd -getCertificate [-file authorization_token_file_virtual] -cluster`

Renewing a host ID-based certificate on a clustered NetBackup host

Host ID-based certificates for the cluster nodes and the virtual name are automatically renewed. The certificates are automatically renewed 180 days before the expiration date.

You can also renew the certificates manually, if required.

See [“About host ID-based certificate expiration and renewal”](#) on page 270.

To manually renew certificate for a cluster node

- ◆ Run the following command from a cluster node to renew the certificate for the node:

```
nbcertcmd -renewCertificate
```

To manually renew certificate for the virtual name

- ◆ Run the following command on the active node to manually renew the certificate for the virtual name:

```
nbcertcmd -renewCertificate -cluster
```

About deploying a new host ID-based certificate

In certain scenarios, NetBackup administrators may revoke a host ID-based certificate.

See [“Revoking a host ID-based certificate from a clustered NetBackup host”](#) on page 289.

After the certificate is revoked, you may need to deploy a new host ID-based certificate. Carry out the following steps to deploy a new certificate:

- Create a reissue token on a clustered setup.
 See [“Creating a reissue token for a clustered NetBackup setup”](#) on page 289.

- Deploy a new certificate on a clustered setup using the reissue token.
 See [“Deploying a new host ID-based certificate on a clustered NetBackup setup”](#) on page 290.

Revoking a host ID-based certificate from a clustered NetBackup host

NetBackup administrators may consider revoking a host ID-based certificate under various conditions. For example, if the administrator detects that client security has been compromised, if a client is decommissioned, or if NetBackup is uninstalled from the host. A revoked certificate cannot be used to communicate with master server web services.

The NetBackup administrator can revoke certificates for a cluster node or the virtual name from any host in a NetBackup domain.

Ensure that you revoke the appropriate certificate.

To revoke a certificate from a cluster node

- 1 Log in to the NetBackup Web Management Service:

```
bpnbat -login -logintype WEB
```

See [“Web login requirements for nbcertcmd command options”](#) on page 254.

- 2 Run the following command to revoke a certificate for a cluster node:

```
nbcertcmd -revokeCertificate -host host_name
```

See [“Revoking a host ID-based certificate”](#) on page 282.

To revoke a certificate for the virtual name

- 1 Log in to the NetBackup Web Management Service:

```
bpnbat -login -logintype WEB
```

- 2 Run the following command to revoke a host ID-based certificate for the virtual name:

```
nbcertcmd -revokeCertificate -host virtual_name
```

See [“Revoking a host ID-based certificate”](#) on page 282.

Creating a reissue token for a clustered NetBackup setup

This topic provides procedures to create reissue tokens for a clustered setup. You can use the reissue tokens to deploy new host ID-based certificates on the clustered setup.

See [“About Token Management for host ID-based certificates”](#) on page 276.

To create a reissue token on a cluster node

- ◆ Run the following command to create a reissue token for the required cluster node:

```
nbcertcmd -createToken -name token_name -reissue -host host_name
```

See [“Creating a reissue token”](#) on page 272.

To create a reissue token for the virtual name

- ◆ Run the following command to create a reissue token token for the virtual name.

```
nbcertcmd -createToken -name token_name_virtual -reissue -host  
virtual_name
```

See [“Creating a reissue token”](#) on page 272.

Deploying a new host ID-based certificate on a clustered NetBackup setup

After a host ID-based certificate is revoked, you can deploy new certificates on a clustered NetBackup setup using reissue tokens.

See [“About deploying a new host ID-based certificate”](#) on page 288.

To deploy a new host ID-based certificate on a cluster node

- ◆ Run the following command to deploy a new certificate on the cluster node using the reissue token:

```
nbcertcmd -getCertificate -file reissue_token_file -force
```

To deploy a new host ID-based certificate for the virtual name

- ◆ Run the following command to deploy a new certificate for the virtual name using the reissue token:

```
nbcertcmd -getCertificate -file reissue_token_file_virtual -force  
-cluster
```

Viewing certificate details for a clustered NetBackup setup

Run the following commands to view the certificate details of a cluster node or the virtual name.

To view certificate details of a cluster node

- ◆ Run the following command on a cluster node:

```
nbcertcmd -listCertDetails
```

See [“Viewing host ID-based certificate details”](#) on page 256.

To view certificate details for the virtual name

- ◆ Run the following command on the active node to view certificate details for the virtual name:

```
nbcertcmd -listCertDetails -cluster
```

```
C:\Program Files\Veritas\NetBackup\bin>nbcertcmd -listCertDetails -cluster
Master Server : ha-w12-vc-c2-nb
Host ID       : caaf54b9-f47d-4a68-9462-72a2a5d34e9a
Issued By     : /CN=broker/OU=root@ha-w12-vc-c2-nb/O=vx
Serial Number : 0x5e1c576b0000000f
Expiry Date   : Sep 13 12:38:30 2017 GMT
SHA1 Fingerprint : 44:A6:0D:56:30:E2:25:A1:FB:32:47:73:D3:6E:F8:00:C3:1C:DB:25
Operation completed successfully.
```

See [“Viewing host ID-based certificate details”](#) on page 256.

Removing CA certificates from a clustered NetBackup setup

Run the following commands to remove the CA (Certificate Authority) certificates from a clustered setup.

Caution: Removing the CA certificate from a master server node or a media server node can adversely impact the NetBackup functionality.

To remove the CA certificates from a cluster node

- 1 Run the following command on a cluster node to view the fingerprints of the CA certificates:

```
nbcertcmd -listCACertDetails
```

- 2 Run the following command to remove the CA certificate by providing the appropriate fingerprint:

```
nbcertcmd -removeCACertificate -fingerprint fingerprint
```

To remove the CA certificates for the virtual name

- 1 Run the following command on the active node to view the fingerprints of the CA certificates for the virtual name:

```
nbcertcmd -listCACertDetails -cluster
```

- 2 Run the following command on the active node to remove the CA certificate for the virtual name by providing the appropriate fingerprint:

```
nbcertcmd -removeCACertificate -fingerprint fingerprint_virtual -cluster
```

Data at rest encryption security

This chapter includes the following topics:

- [Data at rest encryption terminology](#)
- [Data at rest encryption considerations](#)
- [Encryption security questions to consider](#)
- [Comparison of encryption options](#)
- [About NetBackup client encryption](#)
- [Configuring standard encryption on clients](#)
- [Configuring legacy encryption on clients](#)
- [Media server encryption](#)

Data at rest encryption terminology

The following table describes the data at rest encryption terminology.

Table 8-1 Data at rest encryption terminology

Term	Description
Advanced Encryption Standard (AES)	Specifies the synchronous encryption algorithm that replaced DES.
Asynchronous encryption	Includes the encryption algorithms that use both a public key and private key.

Table 8-1 Data at rest encryption terminology (*continued*)

Term	Description
Data Encryption Standard (DES)	Specifies the accepted synchronous data encryption standard from the 1970s until 1998.
Initialization vector	Specifies a seed value that is used to prime an encryption algorithm. Priming is done to obscure any patterns that would exist when using the same key to encrypt a number of data files. These files begin with the same pattern.
Public Key Encryption	Uses asynchronous encryption.
Synchronous encryption	Includes the encryption algorithms that use the same key for both encryption and decryption. For the same key size, synchronous algorithms are faster and more secure than their asynchronous counterparts.

Data at rest encryption considerations

The following table describes the data at rest encryption limitations.

Table 8-2 Data at rest encryption limitations

Limitation	Description
Computer performance effect of data encryption	Encryption algorithms are like data compressions algorithms in that they are very CPU intensive. Compressing data without the addition of computer hardware (either dedicated or shared), can affect computer and NetBackup performance.
Data compression must be performed before data encryption	Data compression algorithms look for data patterns to compress the data. Encryption algorithms scramble the data and remove any patterns. Therefore if data compression is desired, it must be done before the data encryption step.
Choice of an encryption algorithm	There are many encryption algorithms and associated key sizes. What should a user choose for data encryption? AES (Advanced Encryption Standard) is the standard for data encryption and supports 128, 192, or 256 -bit encryption keys.
Suggested key size	Generally, the larger key the more secure, and the longer into the future the data will stay secure. AES is one of the best choices because it is deemed secure with all three supported (128, 192, 256 bit) key sizes.

Table 8-2 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, it should not be the only criteria that is used to evaluate an encryption solution.</p> <p>Other considerations should be part of any decision-making process as follows:</p> <ul style="list-style-type: none"> ■ FIPS certificates only apply to the named version of a product. And then only when the product is used in conformance with the "FIPS security policy" the document that is submitted when the product was validated. Future product versions and non-standard uses would be subject to questioned validation. ■ The security of algorithms like AES is not in the obscurity of how they work. Rather the security is in the difficulty to deduce an unknown encryption key. The years of scrutiny and peer review for AES, have lead to mature implementations. In fact, tests exist for AES where specific keys and data sets are input, and verified against the expected output. ■ Data encryption is much like automobile security. Most problems are related to lost or misplaced keys and not related to malfunctioning locks. ■ Since misuse is more likely to lead to problems, the usability of an encryption product should be part of the consideration. <p>Usability considerations include the following:</p> <ul style="list-style-type: none"> ■ Encryption integration with the product ■ Encryption integration with business processes. ■ Appropriate encryption key granularity ■ Recoverability
Appropriate encryption key granularity	<p>The appropriate encryption key granularity is best explained with the example of home security. A single house key is convenient. You can enter the garage, front door, or backdoor all using the same key. This security is good until the key is compromised (for example, if the key is stolen). Then you need to change all the locks that used the key. An extreme example is to have a key for every drawer and cupboard in a house. Then, a lost key would require the changing of on a single lock.</p> <p>The correct solution is somewhere in between. You must understand your tolerance for a compromised or lost key from your business process perspective. A lost key implies all the data that is encrypted with that key is destroyed. A compromised key implies all the data that is encrypted with that key must be decrypted and reencrypted to become secure.</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?

Comparison of encryption options

The following NetBackup options exist for data at rest encryption:

- NetBackup client encryption, with standard encryption
- NetBackup client encryption, with legacy encryption
- Media server encryption
- Third-party encryption appliances and hardware devices

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

Table 8-3 Encryption options comparison

Encryption option	Potential advantages	Potential disadvantages
Client encryption, standard encryption See “Configuring standard encryption on clients” on page 301.	<ul style="list-style-type: none">■ The encryption key is on the client computer and not controlled by the NetBackup administrator■ Can be deployed without affecting the NetBackup master and media servers■ Can be deployed on a per client basis	<ul style="list-style-type: none">■ The encryption key on the client does not scale well to environments where each client must have a unique encryption key and individual encryption key■ Encryption and compression taking place on the client can affect client performance
Client encryption, legacy encryption See “Configuring legacy encryption on clients” on page 308.	Same advantages as client encryption with standard encryption.	Same disadvantages as client encryption with standard encryption.

Table 8-3 Encryption options comparison (*continued*)

Encryption option	Potential advantages	Potential disadvantages
See "Media server encryption" on page 318.	<ul style="list-style-type: none">■ Does not affect client computer performance■ Master/Media server centralized keys	<ul style="list-style-type: none">■ Master / Media server centralized keys■ Limited options for detailed Key Granularity■ Not tightly integrated with NetBackup configuration and operation■ Encryption and compression taking place on the media server can affect media server performance
Third-party encryption appliances and hardware devices	<ul style="list-style-type: none">■ Little or no performance effect due to added hardware.■ Generally NIST FIPS 140 certified.	<ul style="list-style-type: none">■ The NetBackup Compatibility lab tests some of these solutions. This testing is neither an endorsement or rejection or a particular solution. This effort verifies that basic functionality was verified when used with a specific version of NetBackup.■ No integration with NetBackup configuration, operation, or diagnostics.■ The Disaster recovery scenario is provided by the appliance or device.

About NetBackup client encryption

The NetBackup client encryption option is best for the following:

- Clients that can handle the CPU burden for compression / encryption
- Clients that want to retain control of the data encryption keys
- Situations where the tightest integration of NetBackup and encryption is desired
- Situations where encryption is needed in terms of a per client basis

Installation prerequisites for encryption security

Encrypted backups require the NetBackup encryption software, which is included in NetBackup server and client installations. To use encryption, you must have a valid license. Refer to the [NetBackup Administrator's Guide, Volume I](#) for details on how to administer NetBackup licenses.

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

For a list of the platforms on which you can configure NetBackup Encryption, see the [NetBackup Release Notes](#).

About running an encryption backup

You can run an encryption backup as follows:

- Choosing encryption for a backup
See [“About choosing encryption for a backup”](#) on page 297.
- Standard encryption backup process
See [“Standard encryption backup process”](#) on page 298.
- Legacy encryption backup process
See [“Legacy encryption backup process”](#) on page 298.

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 8-4 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 298.

See [“NetBackup standard encryption restore process”](#) on page 299.

See [“Legacy encryption backup process”](#) on page 298.

See [“NetBackup legacy encryption restore process”](#) on page 300.

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.

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 8-5 Three encryption-related configuration options

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

Table 8-5 Three encryption-related configuration options (*continued*)

Option	Value	Description
	<code>required</code> <code>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 kind on NetBackup clients. The <i>kind</i> option can be set to any of the following option values.
	<code>NONE</code>	Neither standard encryption nor legacy encryption is configured on the client.
	<code>STANDARD</code>	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.
	<code>LEGACY</code>	Specifies that you want to use the legacy-based encryption, with 40-bit DES or 56-bit DES.
<code>CRYPT_CIPHER = cipher</code>		Defines the cipher type to use. It can be set to any of the following option values.
	<code>AES-128-CFB</code>	128-bit Advanced Encryption Standard. This is the default value.
	<code>BF-CFB</code>	128-bit Blowfish
	<code>DES-EDE-CFB</code>	Two Key Triple DES
	<code>AES-256-CFB</code>	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 7.0 or later versions.

About creating encryption key files on the clients

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

- If the server is in a cluster and is also an encryption client, all nodes in the cluster must have the same key file.
- The `bpkeyutil` command sets the cipher-based encryption key file and pass phrase on each NetBackup Encryption client.
 - For a Windows server, the full path to the command is as follows:

```
install_path\NetBackup\bin\bpkeyutil
```

- For a UNIX server, the full path to the command is as follows:

```
/usr/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 I](#) for details on redirected restores.
- 2 Obtain the pass phrase that was used on the other client when the encrypted backup was made. Without that pass phrase, you cannot restore the files.

Note if the pass phrase is the same on both clients, skip to step 5.
- 3 To preserve your own (current) key file, move or rename it.
- 4 Use the `bpkeyutil` command to create a key file that matches the other client's. When the `bpkeyutil` process prompts you for the pass phrase, specify the other client's pass phrase.
- 5 Restore the files to the other client.

After you restore the encrypted files from the client, rename or delete the key file that you created in step 4.

Next, you move or rename the original key file to its original location or name. If you do not re-establish your key file to its original location and name, you may not be able to restore your own encrypted backups.

About configuring standard encryption directly on clients

You can also configure NetBackup encryption directly on clients as explained in the following topics:

- Setting standard encryption attribute in policies
See [“Setting standard encryption attribute in policies”](#) on page 307.
- Changing client encryption settings from the server
See [“Changing the client encryption settings from the NetBackup server”](#) on page 307.

Setting standard encryption attribute in policies

You must set the **Encryption** attribute on your NetBackup policy as follows:

- If the attribute is set, the NetBackup server requests that NetBackup clients in that policy perform encrypted backups.
- If the attribute is not set, the NetBackup server does not request that NetBackup clients in that policy perform encrypted backups.

You can use the **Attributes** tab of the policy in the **NetBackup Administration Console** to set or clear the **Encryption** attribute for a policy.

Refer to the [NetBackup Administrator's Guide, Volume I](#) for more information on how to configure policies.

Changing the client encryption settings from the NetBackup server

You can change the encryption settings for a NetBackup client from the **Client Properties** dialog on the NetBackup server.

To change the client encryption settings from the NetBackup server

- 1 Open the **NetBackup Administration Console** on the server.
- 2 Expand **Host Properties > Clients**.
- 3 In the **Clients** list, double click the name of the client that you want to change. The **Client Properties** window displays.
- 4 Expand **Properties > Encryption** to display the encryption settings for that client.

See the following topic for information about the configuration options that correspond to the settings in the **Encryption** pane:

See [“Managing standard encryption configuration options”](#) on page 301.

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

Configuring legacy encryption on clients

This topic discusses configuring legacy NetBackup encryption.

The configuration options are in the `bp.conf` file on UNIX clients and in the registry on Windows clients.

The options are as follows:

- CRYPT_OPTION
- CRYPT_STRENGTH
- CRYPT_LIBPATH
- CRYPT_KEYFILE

You can also use the **NetBackup Administration Console** to configure the options from the server. They are on the **Encryption** tab in the **Client Properties** dialog box.

Refer to the [NetBackup Administrator's Guide, Volume I](#) for details.

You can set the CRYPT_OPTION and CRYPT_STRENGTH options on the `bpinst -LEGACY_CRYPT` command. The equivalent option settings are `-crypt_option`, `-crypt_strength`, respectively.

About configuring legacy encryption from the client

The following table contains the legacy encryption-related configuration options that are on a NetBackup client. Ensure that these options are set to the appropriate values for your client. These are set if you run the `bpinst -LEGACY_CRYPT` command from the server to the client name.

Table 8-6 Legacy encryption configuration options

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

Table 8-6 Legacy encryption configuration options (*continued*)

Option	Value	Description
	<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:
	<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.

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 316.

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.

If you want to enter a new NetBackup pass phrase on a Windows client, enter a command similar to the following example:

```
bpkeyfile.exe -cnpp install_path\NetBackup\bin\keyfile.dat
Enter old keyfile pass phrase: (standard keyfile pass phrase)
Enter new NetBackup pass phrase: *****
Re-enter new NetBackup pass phrase: *****
```

Caution: You must ensure that pass phrases, whether they are new or were in use previously, are secure and retrievable. If a client's key file is damaged or lost, you need all of the previous pass phrases to recreate the key file. Without the key file, you cannot restore the files that were encrypted with the pass phrases.

The key file must only be accessible to the administrator of the client machine.

For a UNIX client, you must ensure the following:

- The owner is root.
- The mode bits are 600.
- The file is not on a file system that can be NFS mounted.

You must consider whether to back up your key file. For encrypted backups, such a backup has little value, because the key file can only be restored if the key file is already on the client. Instead, you can set up a NetBackup policy that does non-encrypted backups of the key files of the clients. This policy is useful you require an emergency restore of the key file. However, this method also means that a client's key file can be restored on a different client.

If you want to prevent the key file from being backed up, add the key file's path name to the client's exclude list.

About configuring legacy encryption from the server

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

Prerequisites for this method include the following:

- The NetBackup client software must be running on a platform that supports NetBackup encryption.
Refer to the *NetBackup Release Notes* for details on supported platforms.
- The NetBackup clients must be running NetBackup 7.0 or later versions.
- 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 about the options that are available with the `bpinst` command.

For examples about how to use `bpinst`:

See [“About pushing the legacy encryption configuration to clients”](#) on page 312.

See [“About pushing the legacy encryption pass phrases to clients”](#) on page 313.

Normally, you specify client names in the `bpinst` command. However, if you include the `-policy_names` option, you specify policy names instead. The option affects all clients in the specified policies.

About pushing the legacy encryption configuration to clients

You can use the `-crypt_option` and `-crypt_strength` options on the `bpinst` command to set encryption-related configuration on NetBackup clients as follows:

- The `-crypt_option` option specifies whether the client should deny encrypted backups (denied), allow encrypted backups (allowed), or require encrypted backups (required).

- The `-crypt_strength` option specifies the DES key length (40 or 56) that the client should use for encrypted backups.

To install the encryption client software and require encrypted backups with a 56-bit DES key, use the following command from the server:

```
bpinst -LEGACY_CRYPT -crypt_option required -crypt_strength des_56 \  
-policy_names policy1 policy2
```

The example uses a UNIX continuation character (`\`) because it is long. To allow either encrypted or non-encrypted backups with a 40-bit DES key, use the following command:

```
bpinst -LEGACY_CRYPT -crypt_option allowed -crypt_strength des_40 \  
client1 client2
```

In clustered environments you can do the following:

- Push the configuration to the client only from the active node.
- Specify the host names of the individual nodes (not the virtual names) in the list of clients.

Note: The master server `USE_VXSS` setting in `bp.conf` should be set to `AUTOMATIC`. Use this setting when pushing from an NBAC enabled master to a host that does not have NetBackup previously installed. Also use this setting when NBAC has not enabled the master server's `USE_VXSS` setting in `bp.conf`.

About pushing the legacy encryption pass phrases to clients

To send a pass phrase to a NetBackup client, you can use the `bpinst` options `-passphrase_prompt` or `-passphrase_stdin`. The NetBackup client uses the pass phrase to create or update data in its key file.

The key file contains the data that the client uses to generate DES keys to encrypt backups as follows:

- If you use the `-passphrase_prompt` option, you are prompted at your terminal for a zero to 62 character pass phrase. The characters are hidden while you type the pass phrase. You are prompted again to retype the pass phrase to make sure that is the one you intended to enter.
- If you use the `-passphrase_stdin` option, you must enter the zero to 62 character pass phrase twice through standard input. Generally, the `-passphrase_prompt` option is more secure than the `-passphrase_stdin` option, but `-passphrase_stdin` is more convenient if you use `bpinst` in a shell script.

To enter a pass phrase for the client named client1 from a NetBackup server through standard input, you would enter commands like the following:

```
bpinst -LEGACY_CRYPT -passphrase_stdin client1 <<EOF
This pass phrase is not very secure
This pass phrase 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`.

Restoring a legacy encrypted backup created on another client

If a server allows redirected restores, you (the user) must be authorized to perform such restores.

Refer to the [NetBackup Administrator's Guide, Volume I](#) for details on redirected restores.

To restore an encrypted backup that was created on another client:

- 1 Obtain the pass phrase that was used on the other client when the encrypted backup was made. Without that pass phrase, you cannot restore the files.

Note if the pass phrase is the same on both clients, skip to step 4.

- 2 To preserve your own (current) key file, move or rename it.
- 3 Use the `bpkeyfile` command to create a key file that matches the other client's. When the `bpkeyutil` process prompts you for the pass phrase, specify the other client's pass phrase.

```
bpkeyfile -change_key_file_pass_phrase key_file_path
```

The *key_file_path* is the path for a new key file on your client. This key file matches the other client's.

After you enter the command, `bpkeyfile` prompts you for the client's pass phrase (obtained in step 1).

For more information on the `bpkeyfile` command, refer to the [NetBackup Commands Reference Guide](#).

- 4 Restore the files to the other client.

After you restore the encrypted files from the client, rename or delete the key file that you created in step 3.

Next, you move or rename the original key file to its original location or name. If you do not re-establish your key file to its original location and name, you may not be able to restore your own encrypted backups.

About setting legacy encryption attribute in policies

You must set the **Encryption** attribute in your NetBackup policy according to the following:

- If the attribute is set, the NetBackup server requests that NetBackup clients in that policy perform encrypted backups.
- If the attribute is not set, the NetBackup server does not request that NetBackup clients in that policy perform encrypted backups.

You can use the **Attributes** tab of the policy in the **NetBackup Administration Console** to set or clear the **Encryption** attribute for a policy.

Refer to the [NetBackup Administrator's Guide, Volume I](#) for more information on how to configure policies.

You can also use the `bpinst` command to set or clear the **Encryption** attribute for NetBackup policies. This method is convenient if you want to set or clear the attribute for several policies.

For example, to set the **Encryption** attribute for policy1 and policy2 from a NetBackup server, enter a command like the following:

```
bpinst -LEGACY_CRYPT -policy_encrypt 1 -policy_names policy1 policy2
```

The 1 parameter sets the encryption attribute (0 would clear it).

Changing client legacy encryption settings from the server

You can change the encryption settings for a NetBackup client from the **Client Properties** dialog on the NetBackup server.

To change the client encryption settings from the NetBackup server

- 1 In the **NetBackup Administration Console** on the server, expand **Host Properties > Clients**.
- 2 In the **Clients** list, double click the name of the client you want to change. The **Client Properties** dialog displays.
- 3 In the **Properties** pane, click **Encryption** to display the encryption settings for that client.

For additional explanation of the settings, click the Help option on the dialog, or refer to the [NetBackup Administrator's Guide, Volume I](#).

Additional legacy key file security for UNIX clients

This topic applies only to UNIX NetBackup clients. The additional security is not available for Windows clients.

Note: Veritas does not recommend using the additional key file security feature in a cluster.

The key file for an encryption client is encrypted using a DES key that is generated from a key file pass phrase. By default, the key file is encrypted using a DES key that is generated from the standard pass phrase that is hard-coded into NetBackup.

Using the standard key file pass phrase lets you perform automated encrypted backups and restores the same way you perform non-encrypted backups and restores.

This method has potential problems, however, if an unauthorized person gains access to your client's key file. That person may be able to figure out what encryption keys you use for backups or use the key file to restore your client's encrypted backups. For this reason, you must ensure that only the administrator of the client has access to the key file.

For extra protection, you can use your own key file pass phrase to generate the DES key to encrypt the key file. An unauthorized person may still gain access to this key file, but the restore is more difficult.

If you use your own key file pass phrase, backup, and restore are no longer as automated as before. Following is a description of what happens on a UNIX NetBackup client if you have used your own key file pass phrase.

To start a backup or restore on a client, the NetBackup server connects to the `bpcd` daemon on the client and makes a request.

To perform an encrypted backup or restore, `bpcd` needs to decrypt and read the key file.

If the standard key file pass phrase is used, `bpcd` can decrypt the key file automatically.

If you use your own key file pass phrase, `bpcd` can no longer decrypt the key file automatically, and the default `bpcd` cannot be used. You must initiate `bpcd` with a special parameter. See [“Running the `bpcd -keyfile` command”](#) on page 317.

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.

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

Information about administering the media server encryption option is located in the following documents on the [Veritas](#) Support site.

NetBackup Media Server Encryption Option Administrator's Guide

NetBackup Media Server Encryption Option Release Notes

Data at rest key management

This chapter includes the following topics:

- [Federal Information Processing Standards \(FIPS\)](#)
- [About FIPS enabled KMS](#)
- [About the Key Management Service \(KMS\)](#)
- [Installing KMS](#)
- [Configuring KMS](#)
- [About using KMS for encryption](#)
- [KMS database constituents](#)
- [Command line interface \(CLI\) commands](#)
- [Troubleshooting KMS](#)

Federal Information Processing Standards (FIPS)

The Federal Information Processing Standards (FIPS) define U.S. and Canadian Government security and interoperability requirements for computer systems. The FIPS 140-2 standard specifies the security requirements for cryptographic modules. It describes the approved security functions for symmetric and asymmetric key encryption, message authentication, and hashing.

For more information about the FIPS 140-2 standard and its validation program, see the National Institute of Standards and Technology (NIST) and the

Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program website at <http://csrc.nist.gov/groups/STM/cmvp>.

The NetBackup Cryptographic Module is now FIPS validated. NetBackup KMS uses the NetBackup Cryptographic Module and can now be operated in FIPS mode.

See “[About FIPS enabled KMS](#)” on page 321.

About FIPS enabled KMS

NetBackup KMS can now be operated in the FIPS mode, wherein the encryption keys that you create are always FIPS approved. FIPS configuration is enabled by default.

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

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

When you create a new key using 7.7 or later version, a salt is always generated with the new key. Providing the salt value is mandatory when you want to recover a key.

Consider the following example; `hrs09tol2hrs` is a key created using an older version of NetBackup:

```
Key Group Name : ENCR_Monday
Supported Cipher : AES_256
Number of Keys : 8
Has Active Key : Yes
Creation Time : Wed Feb 25 22:46:32 2015
Last Modification Time: Wed Feb 25 22:46:32 2015
Description : -
Key Tag :
5e16a6ea988fc8ec7cc9bdbbc230811b65583cdc0437748db4521278f9c1bbdf9
Key Name : hrs09tol2hrs
Current State : ACTIVE
Creation Time : Wed Feb 25 22:50:01 2015
```

Last Modification Time: Wed Feb 25 23:14:18 2015

Description : active

Post upgrade to NetBackup 7.7, the key hrs09to12hrs is moved from key group ENCR_Monday to a new key group ENCR_77.

```
C:\Program Files\Veritas\NetBackup\bin\admincmd>nbkmsutil -modifykey  
-keyname hrs09to12hrs -kname ENCR_Monday -move_to_kname ENCR_77
```

Key details are updated successfully

Now list all the keys of the ENCR_77 key group. Note that the new key Fips77 would be FIPS approved, but not hrs09to12hrs that was created using an older version of NetBackup.

```
C:\Program Files\Veritas\NetBackup\bin\admincmd>nbkmsutil -listkeys  
-kname NCR_77
```

Key Group Name : ENCR_77 Supported

Cipher : AES_256

Number of Keys : 2

Has Active Key : Yes

Creation Time : Thu Feb 26 04:44:12 2015

Last Modification Time: Thu Feb 26 04:44:12 2015

Description : -

Key Tag :

5e16a6ea988fc8ec7cc9bdbc230811b65583cdc0437748db4521278f9c1bbdf9

Key Name : hrs09to12hrs

Current State : ACTIVE

Creation Time : Wed Feb 25 22:50:01 2015

Last Modification Time: Thu Feb 26 04:48:17 2015

Description : active

FIPS Approved Key : No

Key Tag :

4590e304aa53da036a961cd198de97f24be43b212b2a1091f896e2ce3f4269a6

Key Name : Fips77

Current State : INACTIVE

Creation Time : Thu Feb 26 04:44:58 2015

Last Modification Time: Thu Feb 26 04:48:17 2015

Description : active

FIPS Approved Key : Yes

Salt : 53025d5710ab36ac1099194fb97bad318da596e27fdfe1f2

Number of Keys: 2

The new key `Fips77` is FIPS approved and also has a Salt value.

KMS with FIPS compliance is supported on the following platforms:

- MS Windows Server 2012
- Linux.2.6.16 x86-64 Suse-10
- Linux.2.6.18 x86-64 RHEL-5
- HP-UX IA64 11.31
- AIX 5.3 TL12 SP2
- AIX 5.3 TL12 SP2

About the Key Management Service (KMS)

The NetBackup Key Management Service (KMS) feature is included as part of the NetBackup Enterprise Server and NetBackup Server software. An additional license is not required to use this functionality. KMS runs on NetBackup and is a master server-based symmetric Key Management Service. The KMS manages symmetric cryptography keys for the tape drives that conform to the T10 standard. KMS has been designed to use volume pool-based tape encryption. KMS is used with the tape hardware that has a built-in hardware encryption capability. An example of a tape drive that has built-in encryption is the IBM ULTRIUM TD4 cartridge drive. KMS is also used with disk volumes associated with NetBackup AdvancedDisk storage solutions. KMS runs with Cloud storage providers. KMS runs on Windows and UNIX. KMS generates keys from your passcodes or it auto-generates keys. The KMS operations are done through the KMS command line interface (CLI) or the Cloud Storage Server Configuration Wizard (when KMS is used with Cloud storage providers). The CLI options are available for use with both `nbms` and `nbnbmkmsutil`.

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 9-1 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.
NetBackup wide changes	<p>Changes were necessary throughout NetBackup for the following:</p> <ul style="list-style-type: none">■ To allow for the <code>ENCR_</code> prefix on the volume pool names.■ To communicate with the key Management Service.■ To provide support for the T10 / SCSI standard tape drives with embedded encryption.■ NetBackup GUI and CLI changes to report the encryption key tag addition to the NetBackup image information The <code>bpimmedia</code> and <code>bpimagelist</code> were modified.■ An emphasis on recoverability and ease of use for this NetBackup release The recommended option is that all encryption keys are generated with pass phrases. You type in a pass phrase and the key management system creates a reproducible encryption key from that pass phrase.
KMS installation and deployment decisions	<p>Following are decisions you must make for KMS deployment:</p> <ul style="list-style-type: none">■ Whether to choose KMS random generated keys or pass phrase generated keys■ Whether to include NBAC deployment
KMS security	No burden is placed on existing NetBackup services with additional security concerns.
Cipher types	<p>The following cipher types are supported in KMS:</p> <ul style="list-style-type: none">■ AES_128■ AES_192■ AES_256 (default cipher)
KMS recoverability	You can use KMS in such a way where all of the encryption keys are generated from pass phrases. You can record these pass phrases and then use them at a later time to recreate the entire KMS for NetBackup.

Table 9-1

Considerations that relate to the functionality and use of KMS
(continued)

Consideration	Description
KMS files	<p>KMS files associated with it where information on the keys is kept, as follows:</p> <ul style="list-style-type: none">■ Key file or key database Contains the data encryption keys. The key file is located at /opt/opensv/kms/db/KMS_DATA.dat.■ Host master key Contains the encryption key that encrypts and protects the KMS_DATA.dat key file using AES 256. The host master key is located at /opt/opensv/kms/key/KMS_HMKF.dat■ Key protection key Encryption key that encrypts and protects individual records in the KMS_DATA.dat key file using AES 256. The key protection key is located at /opt/opensv/kms/key/KMS_KPKF.dat. Currently the same key protection key is used to encrypt all of the records.■ Back up KMS files If you want to back up the KMS files, the best practices should be followed. Put the KMS database file on one tape and the HMK files and KPK files on another tape. To gain access to encrypted tapes, someone would then need to obtain both tapes. Another alternative is to back up the KMS data files outside of the normal NetBackup process. You can copy these files to a separate CD, DVD, or USB drive. You can also rely on pass phrase generated encryption keys to manually rebuild KMS. All of the keys can be generated by pass phrases. If you have recorded all of the encryption key pass phrases you can manually recreate KMS from information you have written down. If you only have a few encryption keys you generate this process could be short.

Table 9-1 Considerations that relate to the functionality and use of KMS
(continued)

Consideration	Description
Key records	<p>Key records contain many fields but the primary records are the encryption key, the encryption key tag, and the record state. Key records also contain some metadata.</p> <p>These key records are defined as follows:</p> <ul style="list-style-type: none">■ Encryption key This key is given to the tape drive.■ Encryption key Tag This tag is the identifier for the encryption key.■ Record state Each of the key records has a state. The states are prelive, active, inactive, deprecated, and terminated.■ Metadata Metadata includes logical name, creation date, modification date, and description.
Key groups	<p>Key groups are a logical name and grouping of key records. All key records that are created must belong to a group. A key group can only have one active state key record at any time. NetBackup supports 100 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 T10 standard. Some well-known tape drives we support (that adhere to the T10 standard) are LT0-4, LT0-5, LT0-6, IBM TS1120/30/40, Oracle T10000B/C, and so on.</p> <p>You can still run earlier LTO versions for reading and writing but you cannot encrypt the data. For example, if you use LT02 media, that data can be read in LT04 drives but they cannot be written in either unencrypted or encrypted format.</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>Refer to Table 9-2 for brief information about interoperability between media and tape drives. Veritas recommends that you refer to vendor-specific user guides for detailed information.</p> <p>Refer to the article HOWTO56305 for more details.</p>
KMS with NBAC	<p>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.</p>

Table 9-1 Considerations that relate to the functionality and use of KMS
(continued)

Consideration	Description
KMS with HA clustering	Information on using KMS with HA clustering is included where applicable in various sections of this document. For further information, refer to the NetBackup HA documentation
KMS logging	The service uses the new unified logging and has been assigned OID 286. The <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 NetBackup Cloud Administrator's Guide .
KMS with AdvancedDisk	Information on using KMS with AdvancedDisk storage is included where applicable in various sections of this document. For further information, refer to the NetBackup AdvancedDisk Storage Solutions Guide .
NBAC and KMS permissions	Typically when using NBAC and the <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. The solution is to grant the root and administrator users <code>NBU_Admin</code> and <code>KMS_Admin</code> permissions manually.

Table 9-2 Media support for encryption

Media	LTO4 tape drives	LTO5 tape drives	LTO6 tape drives
LTO-2 media	Read only no encryption support	Not supported	Not supported
LTO-3 media	Read and Write no encryption support	Read only no encryption support	Not supported
LTO-4 media	Read and Write encryption enabled	Read and Write encryption enabled	read-only encryption enabled
LTO-5 media	Not supported	Read and Write encryption enabled	Read and Write encryption enabled
LTO-6 media	Not supported	Not supported	Read and Write encryption enabled

KMS principles of operation

KMS works with encryption capable tape drives. KMS is integrated into NetBackup in such a way so as to eliminate difficulties in using NetBackup from a system management perspective. KMS provides encryption key management for tape drives with built-in encryption capabilities. These tape drives adhere to the SCSI standard. A SCSI command enables encryption on the tape drive. NetBackup accesses this capability through the volume pool name.

About writing an encrypted tape

BPTM receives a request to write to a tape and to use a tape from a volume pool with the `ENCR_` name prefix. The `ENCR_` prefix is a signal to BPTM that the information to be written to tape is to be encrypted.

BPTM contacts KMS and requests an encryption key from the key group with a name that matches the name of the volume pool.

KMS hands back to BPTM an encryption key and a key identifier (known as the encryption key tag).

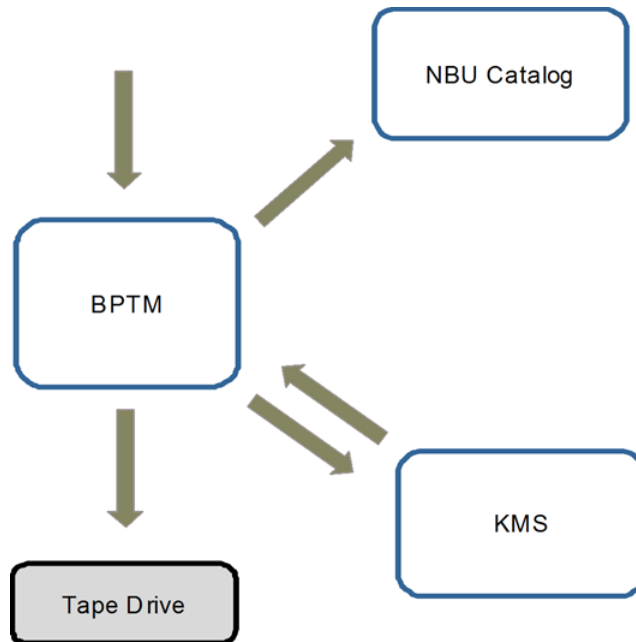
BPTM places the drive in encryption mode and registers the key tag and identifier tag with the drive. This process is all done with the SCSI security protocol in or out command that has been added to the SCSI specification.

The backup then proceeds as normal.

When the backup is complete, BPTM unregisters the key and tag with the drive and sets the drive back into regular mode.

BPTM then records the tag in the NetBackup image record catalog.

[Figure 9-1](#) shows how the process flows.

Figure 9-1 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 9-3](#) defines the terms that are associated with KMS.

Table 9-3 Definitions for common KMS terms

Term	Definition
Command line interface (CLI)	From the CLI, you can operate the KMS feature from the provided command line using the <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.
Key Protection Key (KPK)	A key protection key is an encryption key that encrypts and protects individual records in the <code>KMS_DATA.dat</code> key file using AES 256. The key protection key is <code>kms/key/KMS_KPKF.dat</code> . Currently the same key protection key is used to encrypt all of the records.
Key file (key database)	A key file or key database contains the data encryption keys. The key file <code>/opt/opensv/kms/db/KMS_DATA.dat</code> .
Key group	The key group is a logical name and grouping of key records. A key group can only have one active state key record at any time. One hundred key groups are supported.
Key record	Key records include the encryption key, encryption key tag, and the record state. Other useful metadata such as logical name, creation date, modification date, and description are also included.

Table 9-3 Definitions for common KMS terms (continued)

Term	Definition
Key record states	<p>Key record states are as follows:</p> <ul style="list-style-type: none">■ Prelive, which means that the key record has been created, but has never been used.■ Active, which means that the key record can be used for encryption and decryption in both backup and restore.■ Inactive, which means that the key record cannot be used for encryption, but can be used for decryption only during restore.■ Deprecated, which means that the key record cannot be used for encryption or decryption.■ Terminated, which means that the key record is not available for use but it can be deleted.■ Keystore, which means that the keystore is the file that keeps the data encryption keys.■ Pass phrase, which means that the pass phrase is a user-specified random string. Seed to create encryption keys. You have a choice of creating the HMK, the KPK, and the encryption key with or without a pass phrase. <p>Note: Keep track of all pass phrases by recording them and storing them in a safe place for future use.</p> <p>Using a pass phrase has definite benefits. It results in keys with better security strength. And if keys are lost, you can regenerate them by providing the pass phrase that was used to create the original key.</p>
Quiesce	<p>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.</p>
Tag	<p>A tag is a unique identifier (UUID) used to identify an individual key or key group in a keystore.</p>

Installing KMS

The following procedure describes how to install KMS.

Note: For more information on configuring KMS in a Cloud storage environment refer to the [NetBackup Cloud Administrator's Guide](#).

The KMS service is called `nbkms`.

The service does not run until the data file has been set up, which minimizes the effect on environments not using KMS.

To install KMS

- 1 Run the `nbkms -createemptydb` command.
- 2 Enter a pass phrase for the host master key (HMK). You can also press **Enter** to create a randomly generated key.
- 3 Enter an ID for the HMK. This ID can be anything descriptive that you want to use to identify the HMK.
- 4 Enter a pass phrase for the key protection key (KPK).
- 5 Enter an ID for the KPK. The ID can be anything descriptive that you want to use to identify the KPK.

The KMS service starts when after you enter the ID and press Enter.

- 6 Start the service by running the following command:

```
nbkms
```

- 7 Use the `grep` command to ensure that the service has started, as follows:

```
ps -ef | grep nbkms
```

- 8 Create the key group. The key group name must be an identical match to the volume pool name. All key group names must have a prefix `ENCR_`.

Note: When using key management with Cloud storage, the `ENCR_` prefix is not required for the key group name.

To create a (non-Cloud storage) key group use the following command syntax.

```
nbkmsutil -creatkg -kgname ENCR_volumepoolname
```

The `ENCR_` prefix is essential. When BPTM receives a volume pool request that includes the `ENCR_` prefix, it provides that volume pool name to KMS. KMS identifies it as an exact match of the volume pool and then picks the active key record for backups out of that group.

To create a Cloud storage key group use the following command syntax.

```
nbkmsutil -creatkg -kgname cloud_provider_URL:volume_name
```

9 Create a key record by using the `-createkey` option.

```
nbkmsutil -createkey -kgname ENCR_volumepool -keyname keyname -activate -desc "message"
```

The key name and message are optional; they can help you identify this key when you display the key.

The `-activate` option skips the prelive state and creates this key as active.

10 Provide the pass phrase again when the script prompts you.

In the following example the key group is called `ENCR_pool1` and the key name is `Q1_2008_key`. The description explains that this key is for the months January, February, and March.

```
nbkmsutil -createkey -kgname ENCR_pool1 -keyname Q1_2008_key -activate -desc "key for  
Jan, Feb, & Mar"
```

- 11** You can create another key record using the same command; a different key name and description help you distinguish 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: Veritas recommends that you keep a record of the output of the `nbkmsutil -listkeys` command. The key tag that is listed in the output is necessary if you need to recover keys.

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

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

Key Tag            : f63af53ead99920e98f3e0f4a586afccf32e79e75240e65499d1cd0cbd7c7fdd
Key Name           : Q1_2013_key
Current State       : INACTIVE
Creation Time       : Thu Aug  8 16:25:03 2013
Last Modification Time: Thu Aug  8 16:25:19 2013
Description         : key for Jan, Feb, & March
FIPS Approved Key   : No

Number of Keys: 2
```

See [“About installing KMS with HA clustering”](#) on page 335.

See “Using KMS with NBAC” on page 335.

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 9-4](#) shows the default KMS permissions for each of the NetBackup user groups.

Table 9-4 Default KMS permissions for NetBackup user groups

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

Besides the KMS permissions listed above, the `NBU_KMS` admin group also has the following permissions on other authorization objects:

- `BUAndRest` has Browse, Read, Backup, Restore, List
- `HostProperties` has Browse, Read
- `License` has Browse, Read

About installing KMS with HA clustering

In a typical NetBackup environment, it is possible that not all the optional packages are installed, licensed or configured. In such scenarios, any services that pertain to these optional products may not be active all the time. These services are hence not monitored by default and do not cause a NetBackup to failover if they fail. If at a future time an optional product is installed, licensed and configured, its services

can be manually configured then NetBackup can failover. If the fail. In this section, we document the manual steps that set up KMS to get cluster monitored.

Enabling cluster use with the KMS service

You can make the KMS service cluster-enabled by adding it to the list of services that can be monitored.

To enable cluster use with KMS

- 1 Open the command prompt on the active node of the cluster.
- 2 Change the directory, as follows:
On Windows: `<NetBackup_install_path>\NetBackup\bin`
On UNIX: `/usr/openv/netbackup/bin`
- 3 Run the following command:
On Windows: `bpclusterutil -addSvc "NetBackup Key Management Service"`
On UNIX: `bpclusterutil -addSvc nbkms`
- 4 Follow the optional product-specific steps to enable the product. For NetBackup Key Management Service run the command to create the database, and start the service.

Enabling the monitoring of the KMS service

You can enable the monitoring of the KMS service and failover NetBackup when the service fails.

To enable monitoring of the KMS service and failover NetBackup if it fails

- 1 Open a command prompt on the active node of the cluster.
- 2 Change the directory, as follows:
On Windows: `<NetBackup_install_path>\NetBackup\bin`
On UNIX: `/usr/openv/netbackup/bin`
- 3 Run the following command.
On Windows: `bpclusterutil -enableSvc "NetBackup Key Management Service"`
On UNIX: `bpclusterutil -enableSvc nbkms`

Disabling the monitoring of the KMS service

You can disable monitoring of the KMS service.

To disable monitoring of the KMS service

- 1 Open a command prompt on the active node of the cluster.
- 2 Change the directory, as follows:
On Windows: `<NetBackup_install_path>\NetBackup\bin`
On UNIX: `/usr/opensv/netbackup/bin`
- 3 Run the following command:
On Windows: `bpclusterutil -disableSvc "NetBackup Key Management Service"`
On UNIX: `bpclusterutil -disableSvc nbkms`

Removing the KMS service from monitored list

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

To remove the KMS service from the list of monitored services

- 1 Disable monitoring of the optional product service using the previous procedure
- 2 Follow the optional product-specific steps to remove the product
- 3 Open the command prompt on the active node of the cluster
- 4 Change the directory, as follows:
On Windows: `<NetBackup_install_path>\NetBackup\bin`
On UNIX: `/usr/opensv/netbackup/bin`
- 5 Run the following command:
On Windows: `bpclusterutil -deleteSvc "NetBackup Key Management Service"`
On UNIX: `bpclusterutil -deleteSvc nbkms`

Configuring KMS

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

To configure and initialize KMS

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

Creating the key database

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

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

- Keys are generated by pass phrases
- Randomly generated pass phrases

You are prompted to provide a logical ID to be associated with each key. At the end of this operation, the key database and protection keys are established.

On a Windows system they can be found in the following files:

```
\Program Files\Veritas\kms\db\KMS_DATA.dat  
\Program Files\Veritas\kms\key\KMS_HMKF.dat  
\Program Files\Veritas\kms\key\KMS_HKPKF.dat
```

On a UNIX system, they can be found in the following files:

```
/opt/openssl/kms/db/KMS_DATA.dat  
/opt/openssl/kms/key/KMS_HMKF.dat  
/opt/openssl/kms/key/KMS_HKPKF.dat
```

Note: On Windows the following `nbkms` command is run from the `C:\Program Files\Veritas\NetBackup\bin` directory.

To create the key database

- 1 Run the following command:

```
nbkms -createemptydb.
```

- 2 Enter a pass phrase for the Host Master Key, or press Enter to use a randomly generated key. Re-enter the pass phrase at the following prompt.
- 3 Enter an HMK ID. This ID is associated with the HMK; you can use it to find this particular key in the future.
- 4 Enter a pass phrase for the Key Protection Key, or press Enter to use a randomly generated key. Re-enter the pass phrase at the following prompt.
- 5 Enter a KPK ID. This ID is associated with the KPK; you can use it to find this particular key in the future.
- 6 Enter KPK ID: 10.

About key groups and key records

A key group is a logical collection of key records where no more than one record is in the active state.

A key group definition consists of the following:

- Name
Given to a key group. Should be unique within the keystore. Renaming of the key group is supported if the new name is unique within the keystore.
- Tag
Unique key group identifier (not mutable).
- Cipher
Supported cipher. All keys belonging to this key group are created with this cipher in mind (not mutable).
- Description
Any description (mutable).
- Creation Time
Time of creation of this key group (not mutable).
- Last Modification Time
Time of last modification to any of the mutable attributes (not mutable).

About creating key groups

The first step for setting up encryption is to create a key group.

In the following example, the key group `ENCR_mygroup` is created:

```
nbkmsutil -createkg -kgname ENCR_mygroup
```

Note: For this version of KMS, it is important that the group name you create (i.e., `mygroup`), is prefixed with `ENCR_`.

About creating key records

The next step is to create an active key record. The key record can either be created in the prelive state and then transferred to the active state. Or the key record can be created directly in the active state.

A key record consists of the following critical pieces of information:

- **Name**
Name that is given to a Key, should be unique within a KG. The renaming of a Key is supported if the new name is unique within the KG.
- **Key Tag**
Unique Key identifier (not mutable).
- **Key Group Tag**
Unique KG identifier, to which this Key belongs (not mutable).
- **State**
Key's current state (mutable).
- **Encryption key**
Key, used to encrypt or decrypt the backup or restore data (not mutable).
- **Description**
Any description (mutable).
- **Creation Time**
Time of Key creation (not mutable).
- **Last Modification Time**
Time of last modification to any of the mutable attributes (not mutable).

The following key record states are available:

- **Prelive**, which indicates that the record has been created, but has not been used
- **Active**, which indicates that the record and key are used for encryption and decryption
- **Inactive**, which indicates that the record and key cannot be used for encryption. But they can be used for decryption

- Deprecated, which indicates that the record cannot be used for encryption or decryption
- Terminated, which indicates that the record can be deleted

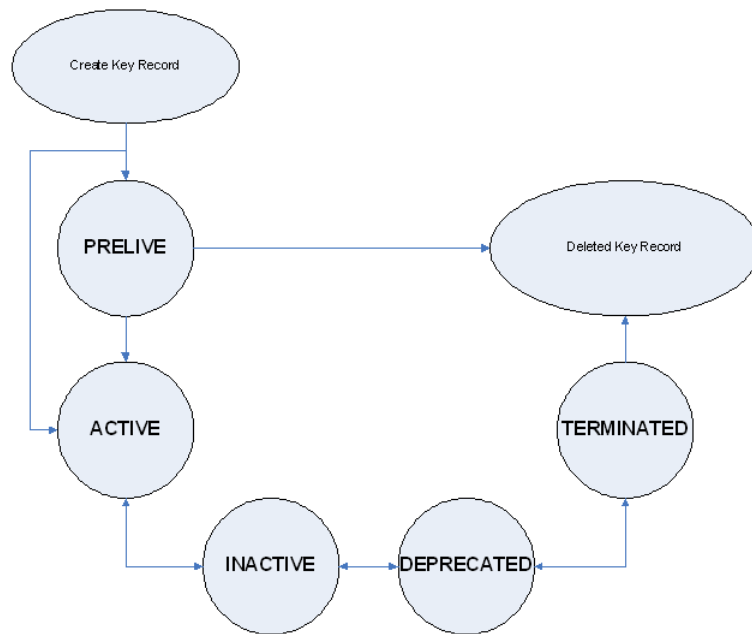
Overview of key record states

The key record states include the prelive, active, inactive, deprecated, and terminated. Key record states adhere to a key record life cycle. Once a key has entered the active state (that is set up for encryption), the key must progress in proper order through the 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 pass phrase), and active keys cannot be moved back to prelive state.

Note: Keys can be created in either the prelive state or the active state. Active key records are available for both backup and restore operations. An inactive key is only available for restore operations. Deprecated keys are not available for use. If your key record is in the deprecated state and you attempt to do a backup or restore with that key record, it can fail. A key record that is in the terminated state can be removed from the system.

The following figure shows the process flow for creating keys in a prelive state or an active state.

Figure 9-2 States possible for key creation

Key record state considerations

The following considerations can be followed for key record states.

- Key record state transitions are well-defined and you must go through the whole path of states to delete a key record.
- Setting a key record to active bumps active key record to the inactive state for that group. There can only be one active record in a group.
- The deprecated state is useful for saving a key and restricting its use. If as an administrator you think that a key has been compromised you can manually put a hold on anyone using that key without that key being deleted from the system. You can set the key record to the deprecated state and someone attempting to do a backup or restore with this deprecated key would get an error.
- The key record deletion involves two steps helping to reduce the possibility of accidentally deleting a key. You must first set deprecated keys to terminated and then you can delete the key record. Only terminated key records can be deleted (other than the keys which are in the prelive state).
- You can use the prelive state to create a key record before use.

Prelive key record state

A key record that is created in the prelive state can be made active or deleted.

The prelive state can be used in the following way:

- The KMS administrator wants to test the creation of a key record without affecting the system. If the record is created correctly it can then be activated. If not created correctly the record can be deleted.
- The KMS administrator wants to create a key record, but then only activate it at some time in the future. The reasons for this issue may include delay setting the record active until the KMS keystore has been backed up (or the pass phrase has been recorded). Or delay setting the record active until some future time. Key records in the prelive state can be made active or deleted from the system.

Active key record state

Active key records can be used to encrypt and decrypt data. If necessary, the active key record could be made inactive. The active state is one of the three most important data management states. The inactive state and deprecated state are the other two important data management states.

Key records can be created directly in the active state bypassing the prelive state. Key records in the active state can either stay active or be made inactive. Active records cannot go back to the prelive state.

Inactive key record state

Inactive key records can be used to decrypt data. If necessary, the inactive key record could be made active again or moved to the deprecated state. The inactive state is one of the three most important data management states. The active state and deprecated state are the other two important data management states.

Key records in the inactive state can either stay inactive, be made active, or be made deprecated.

Deprecated key record state

Deprecated key records cannot be used to encrypt or decrypt data. If necessary, key records in the deprecated state could be made inactive or terminated. The deprecated state is one of the three most important data management states. The active state and inactive state are the other two important data management states.

The deprecated state can be used in the following ways:

- The use of a key needs to be tracked or regulated. Any attempt to use a deprecated key can fail, until its state is changed to the appropriate state.

- A key should not be needed any longer, but to be safe is not set to the terminated state.
Key records in the deprecated state can either stay deprecated, be made inactive, or terminated.

Terminated key record state

The terminated state adds a second step or safety step for deleting a deprecated state key record. A terminated key record can be moved to the deprecated state and ultimately made active again as needed. A terminated key record can also be deleted from the KMS.

Caution: Before deleting a key, make sure that no valid image exists which was encrypted with this key

Key records in the terminated state can either stay terminated, be made deprecated, or physically deleted.

About backing up the KMS database files

Backing up the KMS database involves backing up the KMS files.

The KMS utility has an option for quiescing the database files or temporarily preventing anyone from modifying the data files. It is important to run the quiesce option if you plan to copy the `KMS_DATA.dat`, `KMS_HMKF.dat`, and `KMS_KPKF.dat` files to another location for backing up purposes.

During quiesce, NetBackup removes write access from these files; only read access is allowed.

When you run `nbkmsutil -quiescedb`, it returns with a quiesce successful statement and an indication of the number of outstanding calls. The outstanding calls number is more of a count. A count is placed on the file for the number of outstanding requests on this file.

After quiesce, you can then back up the files by copying them to another directory location.

After you have copied the files, you can unquiesce the KMS database files by using `nbkmsutil -unquiescedb`.

After the outstanding quiesce calls count goes to zero, the KMS can run the commands that can modify the `KMS_DATA.dat`, `KMS_HMKF.dat`, and `KMS_KPKF.dat` files. Write access is once again returned to these files.

About recovering KMS by restoring all data files

If you have made backup copies of the `KMS_DATA.dat`, `KMS_HMKF.dat`, and `KMS_KPKF.dat` files, it is just a matter of restoring these three files. Then startup the `nbkms` service and the KMS system will be up and running again.

Recovering KMS by restoring only the KMS data file

You can restore the backed-up copy of the KMS data file `kms/db/KMS_DATA.dat` by regenerating the `KMS_HMKF.dat` and `KMS_KPKF.dat` files with pass phrases. So, if you have written down pass phrases for the host master key and key protection key, you can run a command to regenerate those files. The system prompts you for the pass phrase and if the pass phrase you now enter matches the pass phrase originally entered, you will be able to reset the files.

To recover KMS by restoring only the KMS data file

- 1 Run the `nbkms -resetkpk` command.
- 2 Run the `nbkms -resethmk` command.
- 3 Startup the `nbkms` service.

Recovering KMS by regenerating the data encryption key

You can regenerate the complete KMS database by regenerating the data encryption keys. The goal is to create a brand new empty KMS database and then repopulate it with all your individual key records.

To recover KMS by regenerating the data encryption key

- 1 Create an empty KMS database by running the following command

```
nbkms -createemptydb
```

You do not have to use the same host master key and key protection key. You can choose new keys.

- 2 Run the `nbkmsutil -recoverkey` command and specify the key group, key name, and tag.

```
nbkmsutil -recoverkey -kgname ENCR_pool1 -keyname Q1_2008_key  
-tag  
d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
```

If you did not keep an electronic copy of the output of the `nbkmsutil -listkey` command when you created the key, you must enter all 64 characters manually.

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

Note: If the tag you enter already exists in the KMS database, you cannot recreate the key.

- 4 If the recovered key is the key that you want to use for backups, run the following command to make the key active:

```
nbkmsutil -modifykey -kgname ENCR_pool1 -keyname Q1_2008_key  
-state active
```

The `-recoverkey` option places the key record in the inactive state, and it is brought into the KMS database in the inactive state.

- 5 If this is a key record that is to be deprecated, run the following command:

```
nbkmsutil -modifykey -kgname ENCR_pool1 -keyname Q1_2008_key  
-state deprecated
```

Problems backing up the KMS data files

There can be problems backing up the KMS data files with the normal NetBackup tapes or with the catalog backup.

Caution: The KMS data files are not included in the NetBackup catalog backups.

If the KPK, HMK, and key files were included in a catalog backup, and the catalog backup tape is lost, the keystore is compromised because the tape contains everything needed to gain access to the keys.

Significant problems can exist if both the catalog backup and data tapes are lost together on the same transport truck, for example. If both tapes are lost together then that situation is not be any better than not ever encrypting the tape in the first place.

Encrypting the catalog is not a good solution either. If the KPK, HMK, and key file were included in a catalog backup, and the catalog backup itself is encrypted, you have done the equivalent of locking the keys in the car. To protect from this problem is why KMS has been established as a separate service for NetBackup and why the KMS files are in a separate directory from the NetBackup directories. However, there are solutions for backing up the KMS data files.

Solutions for backing up the KMS data files

The best solution for backing up KMS data files is to do so outside of the normal NetBackup process, or rely on pass phrase generated encryption keys to manually rebuild KMS. All of the keys can be generated by pass phrases. So if you have recorded all of the pass phrases, then you can recreate the KMS manually from the information you have written down. One way to back up KMS is to place the KMS information on a separate CD, DVD, or USB drive.

Creating a key record

The following procedure shows how to create a key record using a pass phrase and bypassing the prelive state and creating an active key.

Note: If an attempt is made to add a key to a group that already has an active key, the existing key is automatically moved to the inactive state.

To create a key record and create an active key

- 1 To create a key record enter the following command:

```
nbkmsutil -createkey -usepphrase -kgname ENCR_mygroup -keyname  
my_latest_key -activate -desc "key for Jan, Feb, March data"
```

- 2 Enter a pass phrase.

Listing keys from a key group

Use the following procedure to list all or selected keys that you created in a particular key group.

To list the keys in a key group

- ◆ To list the keys in a key group enter the following command:

```
nbkmsutil -listkeys -kgname ENCR_mygroup
```

The `nbkmsutil` outputs the list in the verbose format by default. Following is a non-verbose listing output.

```
KGR ENCR_mygroup AES_256 1 Yes 134220503860000000  
  
134220503860000000 -  
KR my_latest_key Active 134220507320000000 134220507320000000  
key for Jan, Feb, March data  
Number of keys: 1
```

The following options help to list all keys from a specific key group or a specific key from a particular key group:

```
# nbkmsutil -listkeys -all | -kgname <key_group_name> [ -keyname  
<key_name> | -activekey ]  
  
[ -noverbose | -export ]
```

The `-all` option lists down all the keys from all the key groups. The keys are listed in a verbose format.

The `-kgname` option lists the keys from the specified key group.

The `-keyname` option lists a specific key from the specified key group. It must however be used with the option `-kgname`.

The `-activekey` option lists an active key from the specified key group name. It must however be used with the `-kgname` option.

Note: The `-activekey` and `-keyname` options are mutually exclusive.

The `-noverbose` option lists the details of the keys and key groups in a formatted form (non-readable). The default is a verbose list.

The `-export` option generates an output that the `key_file` requires. (The `key_file` is used in `nbkmsutil -export -path <key_container_path> -key_file file`. You can use the output for another `key_file`.)

Run the following command to list all the keys from a specific key group:

```
nbkmsutil -listkeys -kgname <key_group_name>
```

Run the following command to list specific keys from a specific key group:

```
nbkmsutil -listkeys -kgname <key_group_name> -keyname <key_name>
```

Run the following command to list all keys from all groups:

```
nbkmsutil -listkeys -all
```

Run the following command to list all keys from a specific key group:

```
nbkmsutil -listkeys -kgname <key_group_name>
```

Run the following command to list the active keys from a specific key group:

```
nbkmsutil -listkeys -kgname <key_group_name> -activekey
```

Configuring NetBackup to work with KMS

Configuring NetBackup to work with KMS involves the following topics:

- NetBackup getting key records from KMS
See [“NetBackup and key records from KMS”](#) on page 349.
- Setting up NetBackup to use encryption
See [“Example of setting up NetBackup to use tape encryption”](#) on page 349.

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 9-3 NetBackup Administration Console with two volume pools set up to use KMS

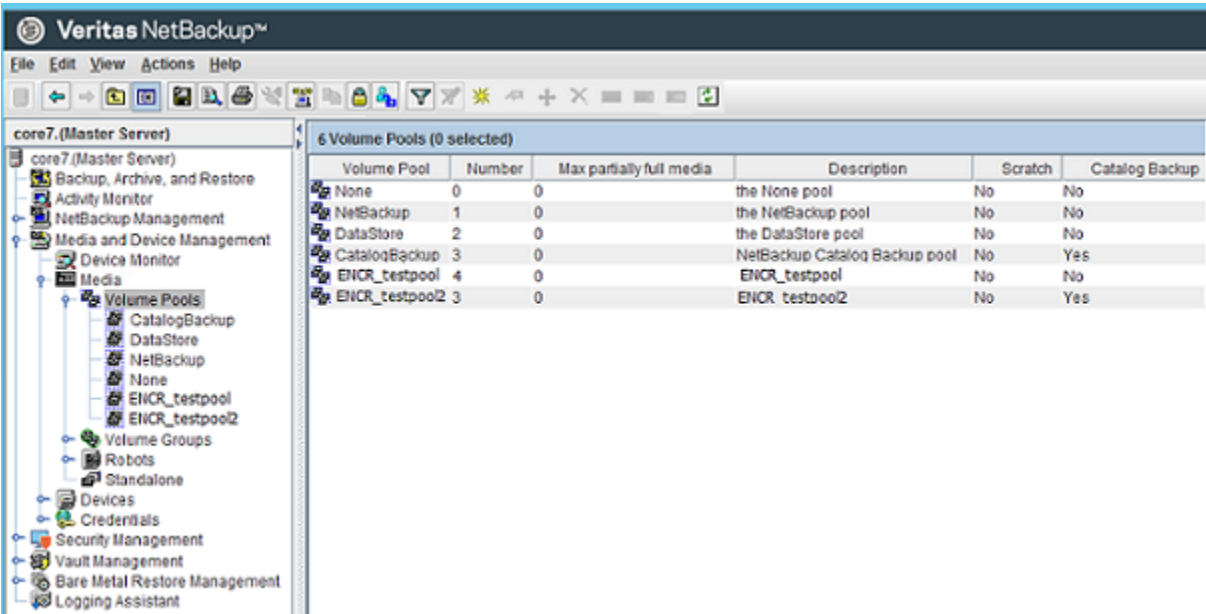
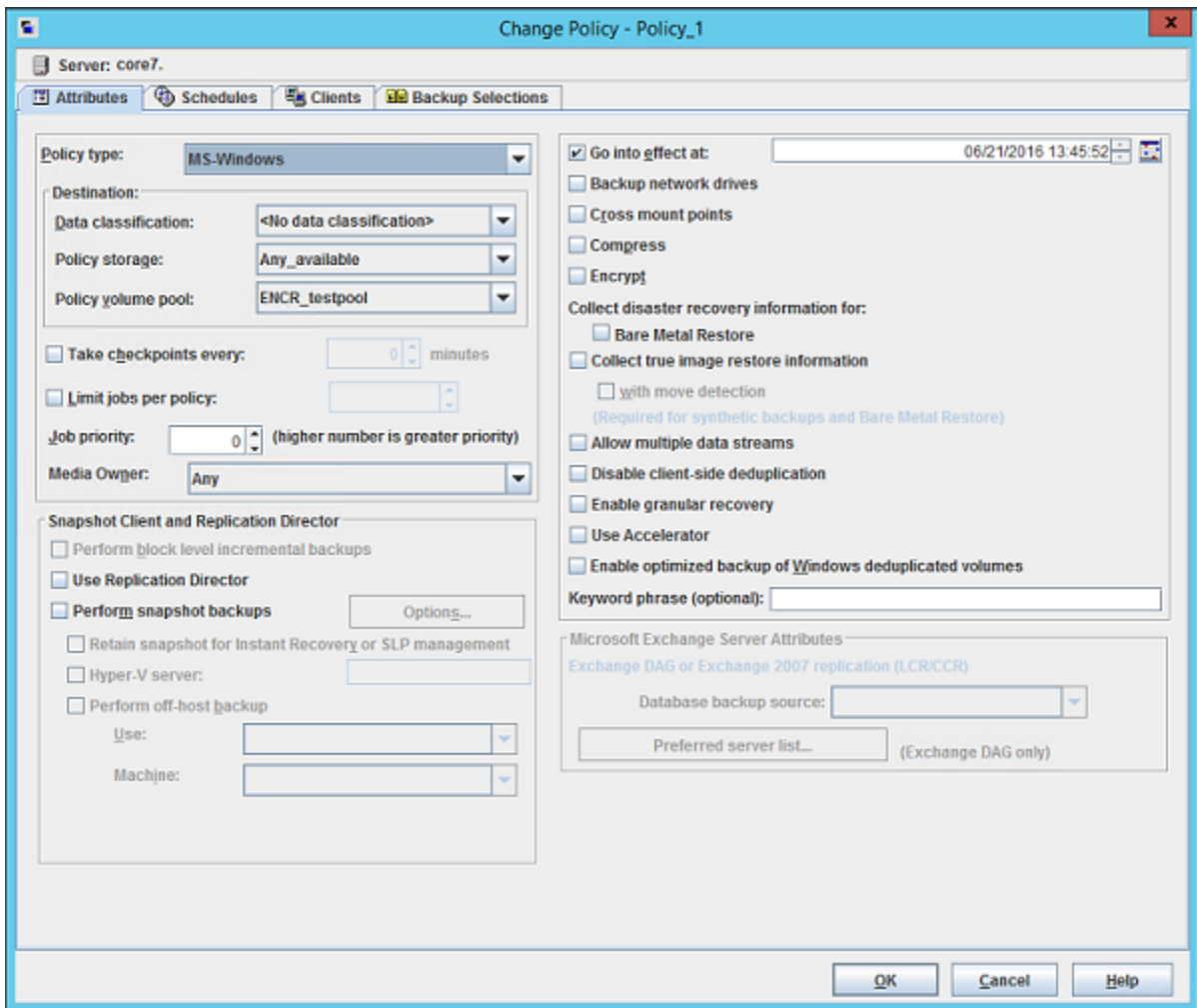


Figure 9-4 shows a NetBackup Policy that is configured to use the volume pool ENCR_testpool, which is the same name as the key group that you configured earlier.

Figure 9-4 NetBackup Change Policy dialog box with KMS volume pool

When a NetBackup image has been encrypted, the key tag is recorded and associated with the image. You can see this information through the **NetBackup Administration Console** reports, or in the output of the `bpimmedia` and `bpimagelist` commands.

About using KMS for encryption

You can use KMS to run an encrypted tape backup, verify an encrypted tape backup, and manage keys. The following topics provide examples for each of these scenarios:

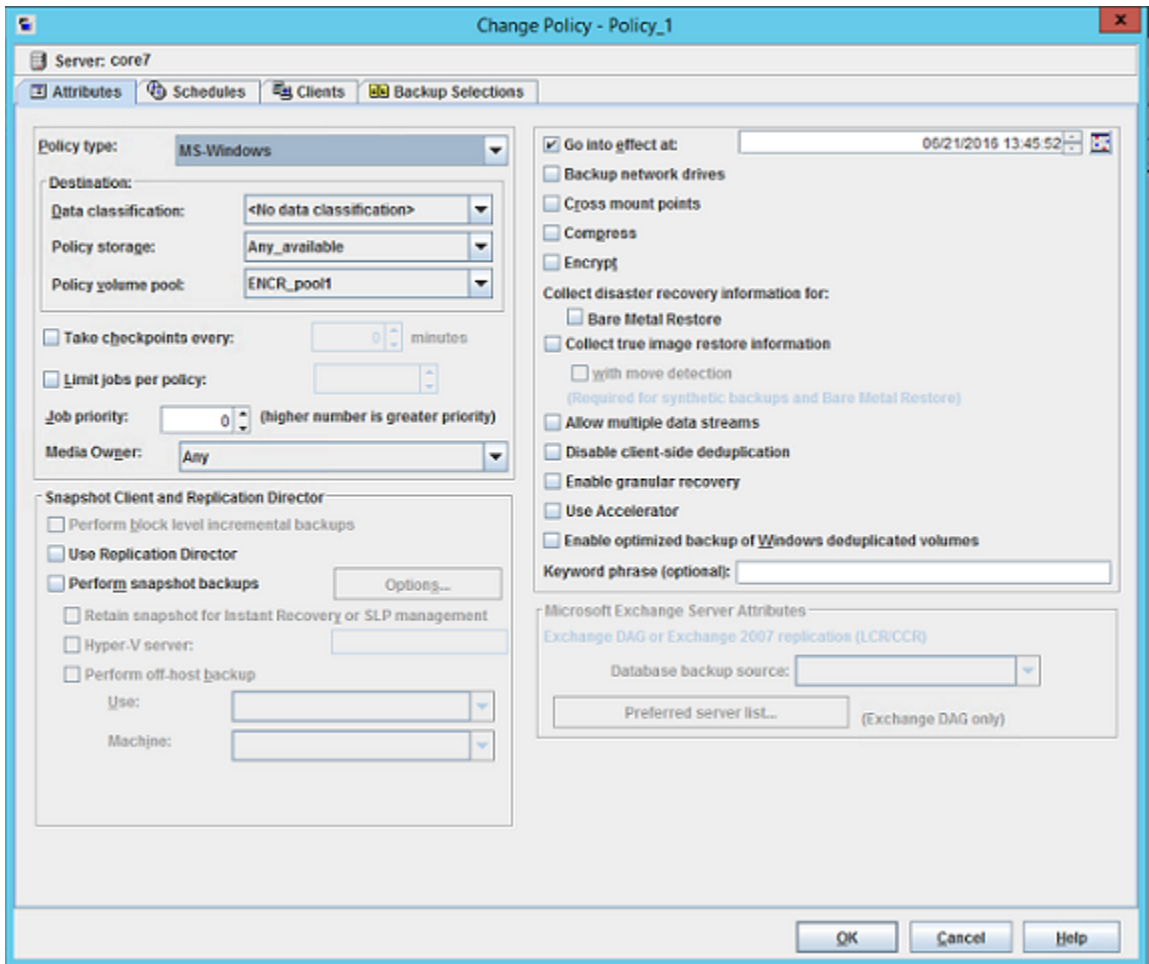
- Example of running an encrypted tape backup
See [“Example of running an encrypted tape backup”](#) on page 352.
- Example of verifying an encryption backup
See [“Example of verifying an encryption backup”](#) on page 353.
- About importing KMS encrypted images
See [“About importing KMS encrypted images”](#) on page 354.

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 9-5](#) shows a NetBackup Policy that you have configured to use the volume pool `ENCR_pool1`.

Figure 9-5 NetBackup Change Policy dialog box with KMS volume pool ENCR_pool1



Example of verifying an encryption backup

When NetBackup runs a tape-encrypted backup, and you view the Images on Media, you see the encryption key tag that is registered with the record. This key tag is your indication that what was written to tape was encrypted. The encryption key tag uniquely identifies which key was used to encrypt the data. You can run a report and read down the policy column to determine whether everything on a particular tape was encrypted.

About importing KMS encrypted images

Importing KMS encrypted images is a two-phase operation. In phase one, the media header and each fragment backup header is read. This data is never encrypted. However, the backup headers indicate if the fragments file data is encrypted with KMS or not. In summary, phase one does not require a key.

Phase two rebuilds the catalog .f file, which requires it to read the encrypted data. The `key-tag` (KAD in SCSI terms) is stored on the tape by the hardware. The NBU/BPTM reads the `key-tag` from the drive, and sends it to KMS for a key lookup. If KMS has a key, then the phase two processes continues to read the encrypted data. If KMS has no key, the data is not readable until the KMS has the key recreated. This is when the pass phrase is important.

If you do not destroy keys, then KMS contains all the keys ever used and you can import any encrypted tape. Move the keystore to your DR site and you do not need to recreate it.

KMS database constituents

The KMS database consists of three files:

- The keystore file (`KMS_DATA.dat`) contains all the key group and key records along with some metadata.
- The KPK file (`KMS_KPKF.dat`) contains the KPK that is used to encrypt the ciphertext portions of the key records that are stored in the keystore file.
- The HMK file (`KMS_HMKF.dat`) contains the HMK that is used to encrypt the entire contents of the keystore file. The keystore file header is an exception. It contains some metadata like the KPK ID and HMK ID that is not encrypted).

Creating an empty KMS database

An empty KMS database can be created by executing the command `nbkms -createemptydb`.

This command prompts you for the following information:

- HMK pass phrase (leave empty for a random HMK)
- HMK ID
- KPK pass phrase (leave empty for a random KPK)
- KPK ID

The KMS database backup and disaster recovery procedures vary for random and pass phrase-generated KPK and HMK as described below.

To recover when the HMK and KPK were generated randomly

- 1 Restore the keystore file from a backup.
- 2 Execute the command `nbkms -info` to find out the KPK ID and HMK ID of the KPK and HMK needed to decrypt this keystore file. The output should also inform you that the HMK and KPK for this keystore file were generated randomly.
- 3 Restore the HMK file corresponding to the HMK ID from a secure backup.
- 4 Restore the KPK file corresponding to the KPK ID from a secure backup.

Importance of the KPK ID and HMK ID

To decipher the contents of a keystore file, it is essential to identify the right KPK and HMK that will do the job. The KPK ID and HMK ID enable you to make this identification. Since these IDs are stored unencrypted in the keystore file header, they can be determined even if you only have access to the keystore file. It is important to choose unique IDs and remember the association of IDs to pass phrases and files to be able to perform a disaster recovery.

About periodically updating the HMK and KPK

The HMK and KPK can be updated periodically using the `modifyhmk` and `modifykpk` options of the KMS CLI. These operations prompt you for a new pass phrase and ID and then update the KPK/HMK. You can choose either a random or a pass phrase-based KPK/HKM at each such invocation.

Note: It is a best practice to use the `-usepphrase` option when modifying the HMK and KPK so that you are required to use a known pass phrase for future recovery. With the `-nopphrase` option, KMS generates a random pass phrase that is unknown and eliminates the possibility of future recovery if needed.

Backing up the KMS keystore and administrator keys

The important KMS data files can be backed up by making copies of the key database `KMS_DATA.dat`, the Host Master Key `KMS_HMKF.dat`, and the Key Protection Key `KMS_HKPKF.dat`.

On Windows these files are as follows:

```
\Program Files\Veritas\kms\db\KMS_DATA.dat
\Program Files\Veritas\kms\key\KMS_HMKF.dat
\Program Files\Veritas\kms\key\KMS_KPKF.dat
```

On UNIX these files are at this location:

```
/opt/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 357.
- Create a new key group
See [“Create a new key group”](#) on page 357.
- Create a new key
See [“Create a new key”](#) on page 358.
- Modify key group attributes
See [“Modify key group attributes”](#) on page 358.
- Modify key attributes
See [“Modify key attributes”](#) on page 359.
- Get details of key groups
See [“Get details of key groups”](#) on page 359.
- Get details of keys
See [“Get details of keys”](#) on page 360.
- Delete a key group
See [“Delete a key group”](#) on page 361.
- Delete a key
See [“Delete a key”](#) on page 361.
- Recover a key
See [“Recover a key”](#) on page 361.
- Modify host master key (HMK)
See [“Modify host master key \(HMK\)”](#) on page 366.
- Get host master key (HMK) ID
See [“Get host master key \(HMK\) ID”](#) on page 366.
- Modify key protection key (KPK)
See [“Modify key protection key \(KPK\)”](#) on page 366.
- Get key protection key (KPK) ID

See [“Get key protection key \(KPK\) ID”](#) on page 366.

- Get keystore statistics
See [“Get keystore statistics”](#) on page 367.
- Quiesce KMS database
See [“Quiesce KMS database”](#) on page 367.
- Unquiesce KMS database
See [“Unquiesce KMS database”](#) on page 367.

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).
----------------------	--

`-cipher` Specifies the type of cipher that is supported by this key group.

Create a new key

To create a new key, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

```
# nbkmsutil -help -createkey
nbkmsutil -createkey [ -nopphrase ]
-keyname <key_name>
-kgname <key_group_name>
[ -activate ]
[ -desc <description> ]
```

Note: The default key state is prelive.

<code>-nopphrase</code>	Creates the key without using a pass phrase. If this option is not specified, the user is prompted for a pass phrase.
<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).

Note: From this release, a salt is generated when you create a new key using a pass phrase. In the event where you try to recover a key, the system prompts you for a salt along with the pass phrase and key tag.

Modify key group attributes

To modify the key group attributes, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

```
# nbkmsutil -help -modifykg
nbkmsutil -modifykg -kgname key_group_name
[ -name <new_name_for_the_key_group> ]
[ -desc <new_description> ]
```

`-kgname` Specifies the name of the key group to be modified.

`-name` Specifies the new name of the key group (should be unique within the keystore).

Modify key attributes

To modify the key attributes use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

```
# nbkmsutil -help -modifykey
nbkmsutil -modifykey -keyname <key_name>
-kgroup <key_group_name>
[ -state <new_state> | -activate ]
[ -name <new_name_for_the_key> ]
[ -desc <new_description> ]
[ -move_to_kgroup <key_group_name> ]
```

Note: The `-state` and `-activate` options are mutually exclusive.

<code>-keyname</code>	Specifies the name of the key to be modified.
<code>-kgroup</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.
<code>-desc</code>	Adds the new description to the key.
<code>move_to_kgroup</code>	Specifies the name of the key group that the key has to be moved to.

Get details of key groups

To get details of key groups, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

```
# nbkmsutil -help -listkgs
nbkmsutil -listkgs [ -kgroup <key_group_name> |
-cipher <type> |
-emptykgs |
-noactive ]
[ -noverbose ]
```

Note: By default all of the key groups are be listed. If no option is specified, the details of all of the key groups are returned.

<code>-kgname</code>	Specifies the name of a key group.
<code>-cipher</code>	Gets the details of all the key groups which support 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.

The `-export` option generates an output that the `key_file` requires. The `key_file` is used in the `nbkmsutil -export -path <key_container_path> -key_file file`. The output can be used for another `key_file`.

```
#nbkmsutil -listkeys -all | -kgname <key_group_name>
[ -keyname <key_name> | -activekey ]
[ -noverbose | -export ]
```

Get details of keys

To get details of the keys, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

#nbkmsutil -help -listkeys

```
nbkmsutil -listkeys -kgname <key_group_name>
[ -keyname <key_name> | -activekey ]
[ -noverbose ]
```

<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>
```

`-kgname` Specifies the name of the key group to be deleted. Only empty key groups can be deleted.

Only empty key groups can be deleted with `-deletekg` option. You can however, also force delete a key group even if it is not empty. Run the following command to force delete a key group:

```
# nbkmsutil -deletekg -kgname <key_group_name> -force
```

Delete a key

To delete a key, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

```
# nbkmsutil -help -deletekey
nbkmsutil -deletekey -keyname <key_name>
-kgroup <key_group_name>
```

Note: Keys in either prelive state or terminated state can be deleted.

`-keyname` Specifies the name of the key to be deleted (to delete, key state has to be in one of prelive, or terminated).

`-kgname` Specifies the name of the key group to which this key belongs.

Recover a key

To recover a key, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

```
# nbkmsutil -help -recoverkey
nbkmsutil -recoverkey -keyname <key_name>
-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 pass phrase).

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

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

Note: From this release, whenever you recover a key, the system prompts you for a salt. A salt is generated for pass phrase derived keys in this version of KMS. To recover the keys that were generated with an older version of KMS, leave the salt field blank.

About exporting and importing keys from the KMS database

The export and import of keys allows the user to quickly sync multiple NetBackup domains to use the same set of keys or quickly move a set of keys from one domain to another domain. This feature is especially helpful for a disaster recovery-induced restore on a different NetBackup domain.

Exporting keys

The `-export` command helps to export keys and keys groups across domains. The following list contains important information about exporting keys and key groups:

- Keys are always exported along with their key group.
- Keys and key groups are exported in an encrypted key container (file) on the host where the Key Management Service (KMS) utility (`nbkmsutil`) is executed. The key container is pass phrase protected.

Note: The same pass phrase must be provided when you want to import the keys and key groups.

- Multiple ways of specifying the export contents are to select specific key groups or to selectively export keys.

Use the `-export` command as specified:

```
nbkmsutil -export -path <secure_key_container>  
[ -key_groups <key_group_name_1 ...> | -key_file <key_file_name> ]
```

By default, the entire keystore is exported.

The `-path` command refers to a fully qualified path where the secure key container is stored.

The `-key_groups` command helps to list the key groups names that separated by spaces.

The `-key_file` command is the file path that lists the keys to be exported in a specific format.

The `<key_group_name>/<key_name>` command helps the user to export keys selectively. You can use a `"*"` to export all the keys from a particular group as shown:

```
<key_group_name>/*
```

You can use the `nbkmsutil -listkeys -export` command to generate an output in a format that this option requires. Refer `nbkmsutil -listkeys -export` for more details.

For more details about listing keys:

See [“Listing keys from a key group”](#) on page 347.

Note: The `-key_groups` and `-key_file` commands are mutually exclusive.

Run the following command to export the entire keystore:

```
nbkmsutil -export -path <secure_key_container>
```

Run the following command to export selected key groups:

```
nbkmsutil -export -path  
<secure_key_container> -key_groups  
<key_group_name_1 key_group_name_2 ...>
```

Run the following command to export selectively export keys:

```
nbkmsutil -export -path  
  
<secure_key_container> -key_file  
  
<key_file_name>
```

Troubleshooting common errors during an export

A set of errors that occur when you export the keys and key groups. This section helps you to troubleshoot them.

- The export can fail when the key container that you specify already exists on the host.
Specify a different key container file and rerun the export operation.
- Export also fails when you mention incorrect keys or key group names.
You must correct the keys or key group names and export them again.

Importing keys

The `-import` command helps to import keys and keys groups across domains. The following list contains important information about importing keys and key groups:

- When importing keys and key groups, you must have the key container file that is created during the export operation. You also need the same pass phrase that is used during the export.
- Importing keys is an atomic operation. It reverts backs all updates on encounter of any error during operation.
- Partial import is not supported.
- A preview of the import output is available. Run the `-preview` command to preview the results of the import.
- The import operation can have two modes, one that includes the `-preserve_kgname` command and another that excludes the `-preserve_kgname` command.
By default, the key groups are imported with following name format:
`< Original_Kgname_<timestamp> >`
You can opt to preserve the key group name by explicitly specifying the `<-preserve_kgname>` option.
- Duplicate keys such as the keys with the same key tag or the same key are not imported.
- The import does not support key group merging.

You can however merge the keys, import the key group without using the `<-preserve_kgname>` command. Run the `nbkmsutil -modifykey -keyname`

`<key_name> -kgname <key_group_name>` command to move key from current group to the required group.

For more information about moving keys:

See [“Modify key attributes”](#) on page 359.

If the same key(s) or key(s) that have the same key tags exist in a key group, they are ignored during import. Run the following commands to import the keys and key groups:

```
# nbkmsutil -import -path <secure_key_container>
[-preserve_kgname]
[ -desc <description> ]
[ -preview ]
```

The `-preserve_kgname` command preserves the key group names during import.

The `-desc <description>` command is a description that is associated with the key groups during import.

The `-preview` command display a preview of the import results.

Run the import operation with the `-preserve_kgname` as follows:

```
nbkmsutil -import -path
<secure_key_container>
[-preserve_kgname]
```

When you run the `-import` command with the `-preserve_kgname` command, the import operation tries to import the original key groups names from the key container. If a key group with the same name exists, the import operation fails.

Run the import operation without the `-preserve_kgname` as follows:

```
nbkmsutil -import -path
<secure_key_container>
```

When you run the `-import` command without the `-preserve_kgname` it imports the key groups, but the key group names are renamed using a suffix, for example a timestamp. Each key group that is renamed always has a unique name.

Troubleshooting common errors during an import

A set of errors that occur when you import the keys and key groups. This section helps you to troubleshoot them.

- During an import, when you import key groups with the `[-preserve_kgname]` option, and if that group already exists in KMS, the entire operation fails. You must either delete or rename the existing key groups or exclude the `[-preserve_kgname]` option and rerun the import operation.
- NetBackup KMS has a limit of 100 key groups. Each group has a limit of 30 keys. The operation fails if more than 100 key groups are imported. You must delete existing unwanted key groups and rerun the import operation.

Modify host master key (HMK)

To modify the host master key, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

The HMK is used to encrypt the keystore. To modify the current HMK, the user should provide an optional seed or pass phrase. An ID (HMK ID) should also be provided that can remind them of the specified pass phrase. Both the pass phrase and HMK ID are read interactively.

```
# nbkmsutil -help -modifyhmk
nbkmsutil -modifyhmk [ -nopphrase ]
```

Get host master key (HMK) ID

To get the HMK ID, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments. The HMK ID is then returned.

```
# nbkmsutil -help -gethmkid
nbkmsutil -gethmkid
```

Get key protection key (KPK) ID

To get the KPK ID, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments. The command returns the current KPK ID.

```
# nbkmsutil -help -getkpkid
nbkmsutil -getkpkid
```

Modify key protection key (KPK)

To modify the key protection key, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

The KPK is used to encrypt the KMS keys. Currently, the KPK is per keystore. To modify the current KPK, the user should provide an optional seed or pass phrase. Also, provide an ID (KPK ID) that can remind us of the specified pass phrase. Both the pass phrase and KPK ID are read interactively.

```
# nbkmsutil -help -modifykpk
nbkmsutil -modifykpk [ -nopphrase ]
```

Get keystore statistics

To get the keystore statistics, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

This command returns the following keystore statistics:

- Total number of key groups
- Total number of keys
- Outstanding quiesce calls

```
# nbkmsutil -help -ksstats
nbkmsutil -ksstats [ -noverbose ]
```

Quiesce KMS database

To quiesce the KMS database, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

This command sends the quiesce request to KMS. If the command succeeds, the current outstanding quiesce count is returned as multiple backup jobs might quiesce the KMS database.

```
# nbkmsutil -help -quiescedb
nbkmsutil -quiescedb
```

Unquiesce KMS database

To unquiesce the KMS database, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

This command sends an unquiesce request to KMS. If the command succeeds, the current outstanding quiesce count is returned. A count of zero (0) means that the KMS database is completely unquiesced.

```
# nbkmsutil -help -unquiescedb
nbkmsutil -unquiescedb
```

Key creation options

Any use of the NetBackup KMS feature should include creating a backup of the `kms/db` and `kms/key` directories. The protection keys and the key database exist in two separate subdirectories to facilitate splitting these when creating a backup copy.

Note: Due to the small size of these files, that they change infrequently, and that they must not be included on any NetBackup tape that itself is encrypted, the files should be manually copied to backup media.

Note: The recommended approach for creating keys with this version of KMS is to always create keys from pass phrases. This includes both the protection keys (Host Master Key and Key Protection Key), and the data encryption keys associated with the key records). It is recommended that the pass phrases used to create the keys are recorded and stored for recovery purposes.

While allowing the KMS system to randomly generate the encryption keys provides a stronger solution, this usage cannot recover from the loss or corruption of all copies of the keystore and protection keys, and therefore is not encouraged.

Troubleshooting KMS

Use the following procedure to initiate troubleshooting for KMS.

To initiate troubleshooting for KMS

- 1 Determine what error code and description are encountered.
- 2 Check to determine if KMS is running and that the following KMS data files exist:

```
kms/db/KMS_DATA.dat  
kms/key/KMS_HMKF.dat  
kms/key/KMS_KPKF.dat
```

If the files do not exist, then KMS has not been configured, or the configuration has been removed. Find out what happened to the files if they do not exist. If KMS has not been configured, the `nbkms` service is not running. If KMS is not running or is not configured, it does not affect NetBackup operation. If you have previously used the `ENCR_` prefix for a volume pool name, this name must be changed as `ENCR_` now has special meaning to NetBackup.

- 3 Get the KMS configuration information:
Get a key group listing by running the command `nbkmsutil -listkgs`. Get a listing of all the keys for a key group by running the command `nbkmsutil -listkeys -kgname key_group_name`.
- 4 Get operational log information such as KMS logs by way of VxUL OID 286 and BPTM logs.
- 5 Evaluate the log information. The KMS errors are handed back to BPTM.
- 6 Evaluate the KMS errors that are recorded in the KMS log.

Solution for backups not encrypting

If tape backups are not encrypted, consider the following solutions:

- Verify that a backup is not encrypted by checking that the encryption key tag field is not set in the image record.
- Verify that the key group and volume pool names are an exact match.
- Verify that there is a key record in the key group with an active state.

Other non-KMS configuration options to look at include:

- Verify that everything that is related to traditional media management is configured properly.
- Is the NetBackup policy drawing a tape from the correct volume pool.
- Does the encryption-capable tape drive have encryption capable media available. For example is LTO4 media installed in the LTO4 tape drive?

Solution for restores that do not decrypt

If the encrypted tape restores are not decrypting, consider the following solutions:

- Verify that the original backup image was encrypted to begin with by viewing the encryption key tag field in the image record.
- Verify that the key record with the same encryption key tag field is in a record state that supports restores. Those states include active or inactive states.
- If the key record is not in the correct state change the key back to the inactive state.

Other non-KMS configuration solution options to consider:

- Verify that the drive and media support encryption.
- Is the encrypted media being read in an encryption-capable tape drive?

Troubleshooting example - backup with no active key record

The following example shows what happens when you attempt a backup when there is no active key record.

Figure 9-6 shows a listing of key records. Three of them have the key group ENCR_mygroup and the same volume pool name. One key group named Q2_2008_key was active. At the end of the command sequence, the state of the Q2_2008_key key group is set to inactive.

Figure 9-6 Listing of key records

```
fel (root) [385]: nbkmsutil -listkeys -kgname ENCR_mygroup
Key Group Name      : ENCR_mygroup
Supported Cipher    : AES_256
Number of Keys      : 3
Has Active Key      : Yes
Creation Time       : Sat Mar 15 10:45:55 2008
Last Modification Time: Sat Mar 15 10:45:55 2008
Description         : -
  Key Tag          : cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d
  Key Name         : Q2_2008_key
  Current State    : Active
  Creation Time    : Sat Mar 15 11:02:46 2008
  Last Modification Time: Sat Mar 15 11:02:46 2008
  Description      : key for Apr, May, & Jun
  Key Tag          : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
  Key Name         : Q1_2008_key
  Current State    : Inactive
  Creation Time    : Sat Mar 15 10:46:51 2008
  Last Modification Time: Sat Mar 15 10:46:51 2008
  Description      : Key for Jan, Feb, & March
  Key Tag          : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe91
  Key Name         : test
  Current State    : Inactive
  Creation Time    : Sat Mar 15 13:12:25 2008
  Last Modification Time: Sat Mar 15 13:12:25 2008
  Description      : -
Number of Keys: 3
fel (root) [383]: nbkmsutil -modifykey -keyname Q2_2008_key -kgname ENCR_mygroup -state
Inactive
Key details are updated successfully
```

Figure 9-7 shows the listing of key records that are produced again, and you can see that the Q2_2008_key state is now listed as inactive.

Figure 9-7 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 9-8 shows the BPTM log output. It logs the message within the 1227 error code in the BPTM log.

Figure 9-8 Output from `bptm` command

```

14:29:16.381 [19978] <2> manage_drive_attributes: MediaPool [ENCR_mygroup], MediaLabel [MEDIA=JRO111;]
14:29:16.384 [19978] <2> manage_drive_attributes: encryption status: nexus scope 0, key scope 0
14:29:16.384 [19978] <2> manage_drive_attributes: encryp mode 0x0, decryp mode 0x0, algorithm index 0, key instance 0
14:29:16.384 [19978] <2> 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 -ORBProtocolFactory PBXIOP_Factory" -ORBSvcConfDirective "static Resource_Factory -ORBProtocolFactory IIOP_Factory" -ORBSvcConfDirective "static PBXIOP_Evaluator_Factory -orb kmslib" -ORBSvcConfDirective "static Resource_Factory -ORBConnectionCacheMax 1024" -ORBEndpoint pbxiop://1556:NB 19978 1536015948517350 -ORBSvcConf /dev/null -ORBSvcConfDirective "static ServerStrategyFactory -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

```

The Job Details dialog box shows the detailed status. You can see a message stating what failed and the detailed status. With the information in the previous diagnostics, you can determine the particular problem or to identify what a given problem is related to.

Troubleshooting example - restore with an improper key record state

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

Figure 9-9 shows that a record you need is set to deprecated. This following shows the listing. The same command is used to change the state from inactive to deprecated.

Figure 9-9 Listing of key records with key group deprecated

```
fel (root) [426]: !385
nbkmsutil -listkeys -kgname ENCR_mygroup

Key Group Name      : ENCR_mygroup
Supported Cipher    : AES_256
Number of Keys      : 3
Has Active Key      : No
Creation Time       : Sat Mar 15 10:45:55 2008
Last Modification Time: Sat Mar 15 10:45:55 2008
Description         : -

Key Tag      : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
Key Name     : Q1_2008_key
Current State : Inactive
Creation Time : Sat Mar 15 10:46:51 2008
Last Modification Time: Sat Mar 15 10:46:51 2008
Description  : Key for Jan, Feb, & March

Key Tag      : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe91
Key Name     : test
Current State : Inactive
Creation Time : Sat Mar 15 13:12:25 2008
Last Modification Time: Sat Mar 15 13:12:25 2008
Description  : -

Key Tag      : cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d
Key Name     : Q2_2008_key
Current State : Deprecated
Creation Time : Sat Mar 15 11:02:46 2008
Last Modification Time: Mon Mar 17 14:52:59 2008
Description  : key for Apr, May, & Jun

Number of Keys: 3
```

Figure 9-10 shows the `bptm` log output with the 1242 error returned.

Figure 9-10 bptm log output with error 1242

```
14:53:48.782 [21109] <2> io_read_back_header: drive index 0, reading backup header
14:53:48.791 [21109] <2> io_position_for_read: successfully positioned JRO111 to file number 3
14:53:48.796 [21109] <2> io_position_for_read: next block encryption status: LON 0x0000000000000009, algorithm
index 1, encryption status 0x6
14:53:48.796 [21109] <2> io_position_for_read: Kad type 0x0, kad length 32 Kad
[cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d]
14:53:48.796 [21109] <2> KMSCLIB::kmsGetKeyAndKadByKeyTag: Entering function...(KMSclib.cpp:655)
14:53:48.796 [21109] <2> KMSCLIB::GetQueryableFacetInstance: Entering function...(KMSclib.cpp:207)
14:53:48.796 [21109] <2> KMSCLIB::InitOrb: Entering function...(KMSclib.cpp:158)
14:53:48.797 [21109] <2> Orb::init: Created anon service name: NB_21109_1537488329610200(Orb.cpp:600)
14:53:48.798 [21109] <2> Orb::init: endpointvalue is : pbxiop://1556:NB_21109_1537488329610200(Orb.cpp:618)
14:53:48.798 [21109] <2> Orb::init: initializing ORB kmslib with: kmslib -ORBSvcConfDirective "-
ORBDottedDecimalAddresses 0" -ORBSvcConfDirective "static PBXIOP_Factory '" -ORBSvcConfDirective "static
EndpointSelectorFactory '" -ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory PBXIOP_Factory'" -
ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory IIOP_Factory'" -ORBSvcConfDirective "static
PBXIOP_Evaluator_Factory '-orb kmslib'" -ORBSvcConfDirective "static Resource_Factory '-ORBConnectionCacheMax 1024
'" -ORBEndpoint pbxiop://1556:NB_21109_1537488329610200 -ORBSvcConf /dev/null -ORBSvcConfDirective "static
Server_Strategy_Factory '-ORBMaxRecvGIOPPayloadSize 268435456'"(Orb.cpp:725)
14:53:48.818 [21109] <2> vnet_cached_gethostbyname: vnet_hosts.c.307: found host in cache: felix.min.veritas.com
14:53:48.818 [21109] <2> vnet_cached_gethostbyaddr_rnl: vnet_hosts.c.506: found IP in cache: 127.0.0.1
14:53:48.842 [21109] <2> db_error_add_to_file: dberrorq.c:midnite = 1205730000
14:53:48.844 [21109] <16> get_encryption_key: NBRMS failed with error status: Operation not allowed for key record
in this state (1242)
```

Index

Symbols

- 40-bit DES key
 - library 298, 300
- 56-bit DES key
 - library 300

A

- Access Control. *See* NetBackup Access Control (NBAC)
 - host properties 167
- access management
 - troubleshooting 174
- Access Management utility 214, 250
- adding a new user to the user group 221
- administration
 - NetBackup access management 153
- Administrator Access Control user group 218
- Alert Notification 132, 138–139
- all NetBackup security
 - multi-datacenter 86
- all security implemented
 - single datacenter 56
- ALLOWED (encryption option) 301, 308
- alternate client restore (see redirected restore) 306, 315
- assigning a user to a user group 222
- attribute for encryption 307, 315
- Audit Manager 119, 132
- audit service (nbaudit) 119–120, 132
- auditing
 - Alert Notification 132, 138–139
 - configuration after upgrade 122
 - enabling 123
 - overview 119
 - report 133, 135
 - viewing current settings 121
- auth.conf 130, 140, 148, 176
- Authentication and Authorization
 - troubleshooting 176
- Authentication Domain tab 168, 172
- authentication port 179

- authorization objects 227
- authorization objects and permissions 224
- authorization port 179
- Authorization Service tab 170
- automatic backup
 - key file 306

B

- backing up KMS database files 344
- backups
 - choosing encryption for 297
 - KMS keystore and administrator keys 355
 - not encrypting, solution for 369
- best practices
 - for key file restoration 305
- bp.conf file
 - auditing changes in 121, 131
 - port usage settings 113
- bpcd 299–300
 - and security deployment 263
 - terminating 318
- BPCD connect-back
 - options 108
- bpclient command
 - specifying 114
- bpinst command 299–300
 - for setting encryption attribute (legacy) 316
 - pushing configuration to clients (legacy) 312
- bpkeyfile command
 - change_netbackup_pass_phrase option 311
 - changing key file pass phrase 318
 - introduction (standard) 299–300
 - managing the key file (legacy) 310
- bpkeyutil command
 - adding pass phrases 302
 - creating the key file 304
 - introduction 298
 - managing the key file 302
 - redirected restore 306, 315
 - standard restore introduction 299

BUAndRest authorization object
permissions 232

C

CA certificate 263

case sensitivity
in command syntax 122–123, 133

catalog
backups, retaining audit records 132
role in deploying host ID-based certificates 258

Certificate Authority (CA) 246, 253, 255, 260, 263–264

certificate deployment security levels 255, 258

Certificate Signing Request (CSR) file 269

certificates
deploying 251
importance of clock sync 262
reissue 256
viewing details 256
where each type is required 246

Change Server 130

changing
client encryption settings from the server 307
client legacy encryption settings 316

checksum of DES key
explanation
legacy encryption 299
legacy restore 301
standard encryption 298
standard restore 300

cipher types 324

class
see policy 307, 315

client
outgoing ports 99

Client Attributes host properties 258

client encryption settings
changing 307

client legacy encryption settings
changing 316

client side encryption
multi-datacenter 69
security 28
single datacenter 47

clients
configuring legacy encryption 308
configuring standard encryption 301
taking offline 131

clock sync for certificates 262

clustered environments

additional key file security (legacy) 317
managing the key file (legacy) 310
managing the key file (standard) 302
pushing configuration (legacy) 313
pushing software (standard) 314

cnpp option 311

Combined world, enterprise, and data center levels 22

command line interface (CLI)

usage help 357
using 356

comparison
encryption options 295

configuration
and clustering (legacy) 312
and clustering (standard) 304
options (legacy) 308
pushing to clients (legacy) 312

configuring
clients for encryption
from client (standard) 306
from server (legacy) 312
from server (standard) 303
legacy encryption from the server 312
ports 106
standard encryption from the server 303

configuring NetBackup
to work with KMS 348

configuring port usage client attribute settings
bpclient command 114

considerations
data at rest encryption 293

Copy Fingerprint to Clipboard option 266

creating
a new key 358
a new key group 357
an empty KMS database 354
key database 338
key file 304
key groups 339
key records 340, 347
new user group 219–220

creating reissue token for a cluster 289

CRYPT option 316

CRYPT_CIPHER option 302

CRYPT_KEYFILE option 299–300, 309–310

CRYPT_KIND option 302, 309

CRYPT_LIBPATH option 309

CRYPT_OPTION 297, 301, 308, 312

CRYPT_STRENGTH option 300, 309, 312

D

- Daemon connection port
 - options 108
- data at rest encryption
 - considerations 293
 - terminology 292
- database constituents
 - KMS 354
- datacenter
 - multi 37
 - single 37
- datacenter-level
 - security 17
- decryption
 - of key file (legacy) 317
 - overview (legacy) 300
 - overview (standard) 299
- deduplication hosts
 - and firewalls 101
- deduplication port usage
 - about 101
- default
 - port numbers
 - NetBackup 95
- Default User Access Control user group 219
- default user groups 218
- deleting
 - a key 361
 - a key group 361
- DENIED (encryption option) 301, 308
- deploying a new host ID-based certificate on a
 - cluster 290
- deploying host ID-based certificate on inactive master
 - server node 287
- deploying host ID-based certificate on media server
 - node 287
- DES
 - key checksum 299–301
 - key checksum for standard encryption 298
- DevHost authorization object
 - permissions 236
- disable
 - random port assignments 107
- DiskPool authorization object
 - permissions 231
- drive authorization object
 - permissions 229

Dynamic Host Configuration Protocol (DHCP) 253

E

- EMM database
 - containing audit records 124, 132
 - role in deploying host ID-based certificates 258
- EMM server
 - outgoing ports 98
- enabling cluster use
 - KMS service 336
- encrypted backup
 - restoring (legacy) 315
 - restoring (standard) 306
- encrypted backup file
 - restoring to another client 306
- encrypted tapes
 - reading 329
 - writing 328
- encryption
 - allow
 - deny. *See* require
 - attribute 299
 - setting 307
 - configuration options (legacy) 308
 - configuring from client (standard) 306
 - confirming the license for 296
 - file containing keys for (legacy) 309
 - installation prerequisites 296
 - kind
 - defining (legacy) 309
 - defining (standard) 302
 - legacy
 - prerequisites 298
 - prerequisites for restoring 300
 - tar header 301
 - libraries
 - defining (legacy) 309
 - managing from client (standard) 301
 - of key file (legacy) 317
 - overview (legacy) 300
 - overview (standard) 299
 - policy attribute 297
 - policy attribute for
 - how to set 307, 315
 - security questions 294
 - standard
 - tar header 300
 - strength
 - defining (legacy) 309

- encryption (*continued*)
 - tar header
 - legacy 299
 - standard 298
 - using KMS 352
 - what is and isn't encrypted (standard) 298
- Encryption attribute
 - in policies 315
- encryption backup
 - running 297
- encryption key files
 - creating on clients 304
- encryption options
 - comparison 295
- encryption, legacy
 - configuring 308
- encryption, standard
 - on clients 301
- Enhanced Auditing 140, 247
 - about 125
 - configuring 127
 - configuring to use Change Server 130
 - connecting to a media server 127
 - disabling 131
 - enabling 126
 - setting up trust between servers 128
 - user authentication 148
 - user management 147
- enterprise level
 - security 15
- Enterprise Media Manager (EMM)
 - database 119
- example
 - running an encrypted tape backup 352
 - setting up NetBackup to use tape encryption 349
 - verifying an encryption backup 353
- exporting keys from KMS 362

F

- fat client authorization object
 - permissions 238
- fat server authorization object
 - permissions 237
- Federal Information Processing Standards (FIPS) 320–321
- fingerprint, finding 265
- firewall connect options
 - on a NetBackup server or client 108

- firewall connect options (*continued*)
 - specifying for a source computer to apply to specific destination computers 111
- firewall connection options
 - on Media Manager 114
- firewall considerations 102
- firewall environment
 - NDMP 116
- firewall problems
 - when using NetBackup with other products 116
- firewalls and deduplication hosts 101

G

- GET_CERT_ALL_MASTERS 267

H

- host ID-based certificates
 - automatic deployment 260
 - cleaning from host before cloning 271
 - deploying 248, 253
 - deploying from multiple master servers 267
 - deploying when client can't connect to master server 256, 269
 - deploying with a token 261
 - deploying without a token 260
 - expiration and renewal 270
 - forcing or overwriting 267–268
 - reissuing 272
 - retaining when reinstalling NetBackup 268
- Host Master Key (HMK) 332, 338, 355, 366
- host master key (HMK)
 - modify 366
- host name-based certificates
 - deploying 247, 251–252
- host properties
 - Access Control 167, 171
 - Authentication Domain tab 168
 - Authorization Service tab 170
 - Network Attributes tab 171
- HostProperties authorization object
 - permissions 235
- hotfix 248, 252

I

- ICMP
 - pinging NDMP 116
- importing
 - KMS encrypted images 354

importing keys from KMS 362

installation

pushing configuration to clients (legacy) 312

pushing pass phrases to clients (legacy) 313

installation prerequisites

for encryption 296

installing

KMS 331, 335

J

Java console

outgoing ports 100

job authorization object

permissions 233

K

key

creating 358

key attributes

modify 359

key creation

options 368

key database, creating 338

key file 298–300

automatic backup 306

backing up (legacy) 311

bpkeyutil command 302

creating (legacy) 310

creating (standard) 304

defining (legacy) 309

encrypting (legacy) 310

encrypting with admin's pass phrase (legacy) 317

encrypting with admin's pass phrase

(standard) 303

explanation (legacy) 313

for redirected restore (standard) 306, 315

in a cluster (legacy) 310, 316–317

in a cluster (standard) 302

legacy 299

managing (standard) 302

pass phrase (legacy) 318

key file pass phrase protection

manual retention 305

key file restoration

best practices 305

key group attributes

modify 358

key groups

creating 339, 357

definition 339

deleting 361

details 359

Key Management Service (KMS)

about 323

configuring 337, 348

considerations 324

database constituents 354

installing 331, 335

NetBackup and key records 349

principles of operation 328

recovering 345

terminology 329

troubleshooting 368

using for encryption 352

with NBAC 335

key pair, changing 275–276

Key Protection Key (KPK) 330, 332, 338, 355, 366

key record states

active 343

considerations 342

deprecated 343

inactive 343

overview 341

prelive 343

terminated 344

key records

creating 340, 347

keys

deleting 361

details 360

listing for a key group 347

recovering 361

keystore statistics 367

KMS Administrator Access Control user group 219

KMS data files

problems backing up 346

solutions for backing up 347

KMS database

creating an empty one 354

quiesce 367

unquiesce 367

KMS database files

backing up 344

KMS encrypted images

importing 354

- Kms group authorization object
 - permissions 239
- KMS keystore and administrator keys
 - backups 355
- KMS service
 - enabling cluster use 336
 - monitored list 337
 - monitoring 336–337

L

- legacy encrypted backup created on another client
 - restoring 315
- legacy encryption
 - backup process 298
 - configuring from the client 308
 - managing 310
- legacy encryption attribute
 - setting in policies 315
- legacy encryption configuration
 - pushing to clients 312
- legacy encryption configuration options
 - managing 308
- legacy encryption from the server
 - configuring 312
- legacy encryption pass phrases
 - pushing to clients 313
- legacy key file security
 - for UNIX clients 316
- libraries
 - defining for encryption (legacy) 309
- license authorization object
 - permissions 235
- logging on as new user 222

M

- managing
 - clients for encryption
 - from client (standard) 301
 - key file (standard) 302
 - legacy encryption key files 310
 - NetBackup encryption key file 302
 - standard encryption configuration options 301
- managing key file (legacy) 310
- master server
 - outgoing ports 96
- master server settings
 - verifying 176

- master, media server, and graphical user interface
 - security
 - NBAC 31
- Maximum Uses Allowed option 273, 278–280
- media authorization object
 - permissions 228
- Media Manager
 - firewall connection options 114
- media manager configuration
 - random port assignments 107
- media server
 - outgoing ports 97
- media server encryption 318
- Media Server Encryption Option (MSEO)
 - security 27
 - single datacenter 44
 - with multi-datacenter 64
- Microsoft Windows Server Failover Cluster 252
- monitoring the KMS service 336–337
- multi-datacenter 37
 - with all NetBackup security 86
 - with client side encryption 69
 - with Media Server Encryption Option (MSEO) 64
 - with NBAC complete 80
 - with NBAC on master and media servers 74
 - with standard NetBackup 60

N

- NBAC
 - master, media server, and graphical user
 - interface security 31
- NBAC (NetBackup Access Control). *See* NetBackup Access Control (NBAC)
- NBAC complete
 - multi-datacenter 80
 - security 32
 - single datacenter 53
- NBAC on master and media servers
 - multi-datacenter 74
 - single datacenter 49
- nbac_cron utility 181
- nbac_cron.exe 181
- nbaudit (NetBackup Audit Service) 119–120, 132, 134
- nbaudit log 138
- nbauditreport 124, 133
- NBU security
 - workgroup 37
- NBU_Admin Access Control user group 218

- NBU_Catalog authorization object
 - permissions 230
- NBU_KMS Admin Access Control user group 219
- NBU_Operator Access Control user group 218
- NBU_Security Admin Access Control user group 219
- NBU_User Access Control user group 219
- NDMP
 - in firewall environment 116
- NetBackup
 - components
 - used in security 17
 - determining access 215
 - hotfix 248, 252
 - ports 93
 - security
 - all 33
 - implementation levels 13
 - security implementation types 23
 - security vulnerabilities 25
- NetBackup Access Control (NBAC) 121, 131, 140
 - and security certificates 247
 - components 17
 - configuration 153–155, 157–158, 160, 240
 - configuring to use Change Server 130
 - default user groups 218
 - individual users 216
 - nbac_cron utility 181
 - nbac_cron.exe 181
 - user groups 216
 - Administrator 218
 - configuring 219
 - Default User 219
 - KMS Administrator 219
 - Operator 218
 - renaming user groups 221
 - SAN Administrator 218
 - Security Administrator 219
 - Vault Operator 219
 - using 150
 - using the Access Management utility 250
- NetBackup access management
 - administration 153
- NetBackup and key records
 - KMS 349
- NetBackup API 249
- NetBackup Audit Manager 119, 132
- NetBackup client encryption 296
- NetBackup CloudStore Service Container 247

- NetBackup Java Application Server Authentication
 - service (bpjava) 281
- NetBackup legacy encryption
 - restore process 300
- NetBackup Request Daemon (BPRD) 249, 251
- NetBackup security
 - standard 26
- NetBackup Service Layer (NBSL) 105, 252–253
- NetBackup standard encryption
 - restore process 299
- NetBackup Vault Manager (nbvault) 252
- NetBackup Web Management Console service
 - (nbwebsvc) 281–282
- NetBackup Web Management Console Service
 - (nbwmc) 254
- Network Attributes tab 171, 173
- Network Time Protocol (NTP) 262

O

- offline
 - taking clients 131
- operating system
 - security 25
- Operator Access Control user group 218
- OpsCenter 119, 121–122, 124, 132
- options
 - BPCD connect-back 108
 - daemon connection port 108
 - ports 108
- outgoing ports
 - client 99
 - EMM server 98
 - Java console 100
 - master server 96
 - media server 97
 - Windows administration console and Java
 - server 99
- overriding or modifying
 - port numbers 93
- overview
 - of legacy restore 300
 - of standard encryption backup 298

P

- pass phrase
 - for encrypting key file (legacy) 310, 317
 - for redirected restore (legacy) 315
 - for redirected restore (standard) 306

- pass phrase *(continued)*
 - pushing to clients (legacy) 313
- passphrase_prompt option 313
- passphrase_stdin option 313
- permissions
 - BUAndRest authorization object 232
 - DevHost authorization object 236
 - DiskPool authorization object 231
 - Drive authorization object 229
 - fat client authorization object 238
 - fat server authorization object 237
 - granting 226
 - HostProperties authorization object 235
 - job authorization object 233
 - Kms group authorization object 239
 - license authorization object 235
 - media authorization object 228
 - NBU_Catalog authorization object 230
 - policy authorization object 228
 - report authorization object 230
 - robot authorization object 231
 - security authorization object 237
 - server group authorization object 239
 - service authorization object 233
 - StorageUnit authorization object 231
 - vault authorization object 238
 - volume group authorization object 235
 - VolumePool authorization object 236
- pinging NDMP
 - ICMP 116
- policy authorization object
 - permissions 228
- port numbers
 - about overriding or modifying 93
 - backup and archive products 103
 - default for NetBackup 95
 - HTTP 104
 - HTTPS 104
 - key OpsCenter components 102
- port usage
 - and deduplication 101
- port usage settings
 - bp.conf 113
- port usage-related Media Manager configuration settings
 - vm.conf 114
- ports
 - about 93
 - authentication 179

- ports *(continued)*
 - authorization 179
 - configuring 106
 - NetBackup 93
 - options 108
- Public Key Infrastructure (PKI) standard 246
- pushing
 - configuration to clients (legacy) 312
 - legacy encryption pass phrases to clients 313
 - pass phrases to clients (legacy) 313
- pushing the legacy encryption configuration to clients 312

R

- random port assignments
 - disable 107
 - in media manager configuration 107
- reading encrypted tape 329
- recovering
 - a key 361
 - KMS 345
- recovering KMS 345
- redirected restore
 - of other client's backup (legacy) 315
 - of other client's backup (standard) 306
 - preventing (legacy) 314
- redirected restores
 - for an encrypted backup file 306
 - of legacy encrypted files 315
- registry
 - auditing changes in 131
- reissue token 270, 275
- reissuing host ID-based certificates 272
- removing CA certificate from cluster 291
- renewing host ID-based certificate on cluster 288
- renewing host ID-based certificates 270
- report authorization object
 - permissions 230
- reports
 - for audit events 132
 - nbauditreport 132
- REQUIRED (encryption option) 301, 308
- restore
 - overview (legacy) 300
- restore process
 - NetBackup legacy encryption 300
 - NetBackup standard encryption 299
- restores not decrypting, solution for 369

- restoring
 - legacy encrypted backup created on another client 315
- revoking a host ID-based certificate from a cluster node 289
- robot authorization object
 - permissions 231
- Root Certificate Fingerprint 264, 266
- running
 - bpkeyfile command 317
 - encryption backup 297

S

- Sarbanes–Oxley Act (SOX) 119
- security
 - client side encryption 28
 - datacenter-level 17
 - enterprise level 15
 - implementation levels 13
 - Media Server Encryption Option (MSEO) 27
 - NBAC complete 32
 - NetBackup
 - all 33
 - operating system 25
 - world-level 14
- Security Administrator Access Control user group 219
- security authorization object
 - permissions 237
- security certificate 127, 130
- security certificate deployment in cluster 284
- security certificates
 - verifying the Certificate Authority 264
- Security Events utility
 - Access History tab 249
 - Certificate Events tab 249
 - Token Events tab 249
- security implementation types
 - NetBackup 23
- Security Management utilities 248
- security vulnerabilities
 - NetBackup 25
- server group authorization object
 - permissions 239
- service authorization object
 - permissions 233
- setting encryption attribute
 - in policies 307
- setuptrust command 165–166

- single datacenter
 - with all security implemented 56
 - with client side encryption 47
 - with Media Server Encryption Option (MSEO) 44
 - with NBAC complete 53
 - with NBAC on master and media servers 49
 - with standard NetBackup 41
- SNMP port 106
- specifying
 - bpclient command 114
- standard
 - NetBackup security 26
- standard encryption
 - backup process 298
- standard encryption from the server
 - configuring 303
- standard NetBackup
 - with multi-datacenter 60
- StorageUnit authorization object
 - permissions 231

T

- tape encryption, setting up NetBackup to use 349
- tar header for legacy encryption 299, 301
- tar header for standard encryption 298, 300
- Targeted Auto Image Replication 247
- terminology
 - data at rest encryption 292
- Token Management 250
- tokens
 - creating 277
 - deleting 279
 - Maximum Uses Allowed option 273, 278–280
 - reissuing 272
 - Valid for option 278, 280
 - viewing details 279
- troubleshooting
 - access management 174
 - Authentication and Authorization 176
 - backup with no active key record 370
 - KMS 368
 - restore with an improper key record state 372

U

- Universally Unique Identifiers (UUIDs) 248
- UNIX clients
 - legacy key file security 316

- updating
 - HMK and KPK 355
- upgrading
 - NetBackup Access Control (NBAC) 240
- upgrading and the auditing configuration 122
- USE_AUTH_CONF_NBAC 176
- user groups 216
 - adding a new user 221
 - Administrator 218
 - assigning a user 222
 - creating 219
 - by copying an existing user group 220
 - Default User 219
 - defining 221
 - KMS Administrator 219
 - Operator 218
 - renaming 221
 - SAN Administrator 218
 - Security Administrator 219
 - Vault Operator 219
 - viewing specific user permissions 225
- user identity in the audit report 125

V

- Valid for option 278, 280
- vault authorization object
 - permissions 238
- Vault Operator User Access Control user group 219
- Vault_Operator Access Control user group 219
- VCS on Windows 251
- verification procedures
 - UNIX 192–193, 196, 198–199, 201
 - Windows 183–184, 188, 190, 205, 208, 210
- verifying an encryption backup 353
- Veritas Cluster Server 252
- viewing certificate details for cluster 290
- vm.conf
 - port usage-related Media Manager configuration settings 114
- volume group authorization object
 - permissions 235
- VolumePool authorization object
 - permissions 236
- VxSS authentication port 179
- VxSS authorization port 179

W

- Windows
 - client verification points 190
 - master server verification points 184
 - media server verification points 188
 - verification points 183
- Windows administration console and Java server
 - outgoing ports 99
- Windows Server Failover Cluster (WSFC) 251
- workgroup
 - NBU security 37
 - with NetBackup 38
- world-level
 - security 14
- writing encrypted tape 328