

NetBackup™ Security and Encryption Guide

UNIX, Windows, and Linux

Release 11.2.0.1

NetBackup™ Security and Encryption Guide

Last updated: 2026-09-09

Legal Notice

Copyright © 2026 Cohesity, Inc. All rights reserved.

© 2026 Cohesity, Inc. All Rights Reserved. Cohesity, the Cohesity Logo and other Cohesity Marks are trademarks of Cohesity, Inc. in the US and/or internationally. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

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. COHESITY 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.

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to [Cohesity Support](#), to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the [Cohesity Support Portal](#) to create a new case.
- Click the (?) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the [Cohesity Knowledge Base](#).
- Log in to the [Cohesity Support Portal](#) to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1	Read this first for secure communications in NetBackup	25
	About secure communication in NetBackup	26
	How NetBackup CA-signed certificates (or host ID-based certificates) are deployed during installation	27
	How secure communication works with primary server cluster nodes	30
	About NetBackup clients installed on nodes of a clustered application	30
	How NetBackup certificates are deployed on hosts during upgrades	31
	When an authorization token is required during certificate deployment	31
	Why do you need to map host names (or IP addresses) to host IDs	32
	How to reset host attributes or host communication status	34
	What has changed for catalog recovery	34
	What has changed with Auto Image Replication	37
	How the hosts with revoked certificates work	37
	Are NetBackup certificates backed up	37
	Can you configure external certificates for primary server	38
	How secure communication works with primary server cluster nodes using external certificates	38
	How revocation lists work for external certificates	38
	How communication happens when a host cannot directly connect to the primary server	38
	How NetBackup 8.1 or later hosts communicate with NetBackup 8.0 and earlier hosts	39
	How communication with legacy media servers happens in the case of cloud configuration	39
	Communication failure scenarios	40
	Failure during communication with 8.0 or earlier hosts	40
	Catalog backup failure	40
	Secure communication support for other hosts in NetBackup domain	40

	Secure communication support for BMR	40
	Configuration for VMware backups that protect SQL Server and backups with SQL Servers that use multiple NICs	41
Chapter 2	Increasing NetBackup security	42
	About NetBackup security and encryption	43
	NetBackup security implementation levels	43
	World-level security	44
	Enterprise-level security	45
	Datacenter-level security overview	47
	NetBackup Access Control (NBAC)	47
	Combined world, enterprise, and datacenter levels	52
	NetBackup security implementation types	53
	Operating system security	54
	NetBackup security vulnerabilities	55
	Standard NetBackup security	55
	Client side encryption security	56
	NBAC on primary, media server, and graphical user interface security	58
	NBAC complete security	60
Chapter 3	Security deployment models	62
	Workgroups	62
	Single datacenters	63
	Multi-datacenters	63
	Workgroup with NetBackup	63
	Single datacenter with standard NetBackup	66
	Single datacenter with client side encryption	68
	Single datacenter with NBAC on primary and media servers	71
	Single datacenter with NBAC complete	75
	Multi-datacenter with standard NetBackup	78
	Multi-datacenter with client side encryption	80
	Multi-datacenter with NBAC on primary and media servers	85
	Multi-datacenter with NBAC complete	89
Chapter 4	Auditing NetBackup operations	94
	About NetBackup auditing	94
	Viewing the current audit settings	98
	About audit events	98
	Viewing audit events	99

	Troubleshooting auditing issues related to the Access History tab	100
	Audit retention period and catalog backups of audit records	100
	Viewing the detailed NetBackup audit report	101
	User identity in the audit report	103
	Disabling auditing	104
	Audit alert notification for audit failures (NetBackup BAR Console)	104
	Send audit events to system logs	105
	SYSLLOG_AUDIT_USE_OCSF_FORMAT for NetBackup primary server	106
Section 1	Identity and access management	107
Chapter 5	About identity and access management	108
	About access control in NetBackup	108
Chapter 6	AD and LDAP domains	110
	Adding AD or LDAP domains in NetBackup	110
	Troubleshooting AD or LDAP domain configuration issues	112
	Certificate authorities trusted by the NetBackup Authentication Service	121
Chapter 7	Access keys	122
	Access keys	122
	Access codes	122
	Request CLI access through web UI authentication	123
	Approve the CLI access request of another user	124
	Edit the settings for command-line access	125
Chapter 8	API keys	126
	About API keys	126
	Creating API keys	127
	Managing an API key	127
	Using an API key	128
	Setting an API key environment variable to run NetBackup commands	128

Chapter 9	Role-based access control	130
	RBAC features	130
	RBAC settings	131
	Configuring RBAC	131
	Role permissions	132
	Notes for using NetBackup RBAC	134
	Add AD or LDAP domains	134
	Default RBAC roles	135
	Add a custom RBAC role for a PaaS administrator	137
	Add a custom RBAC role to restore Azure-managed instances	138
	Add a custom RBAC role	140
	Edit a custom role	142
	View users in RBAC	143
	Add a user to a role (non-SAML)	144
	Add a smart card user to a role (non-SAML, without AD/LDAP)	145
	Add a user to a role (SAML)	145
	Remove a user from a role	146
Chapter 10	NetBackup interface access for OS Administrators	147
	Disable command-line (CLI) access for operating system (OS) administrators	147
	Disable web UI access for operating system (OS) administrators	148
Chapter 11	Smart card or digital certificate	149
	Configure user authentication with smart cards or digital certificates	149
	Configure smart card authentication with a domain	149
	Configure smart card authentication without a domain	151
	Edit the configuration for smart card authentication	152
	Add or delete a CA certificate that is used for smart card authentication	153
	Disable or temporarily disable smart card authentication	154
Chapter 12	Single Sign-On (SSO)	155
	About single sign-on (SSO) configuration	155
	Configure NetBackup for single sign-on (SSO)	157
	Configure the SAML KeyStore	158

Configure the SAML keystore and add and enable the IDP configuration	161
Enroll the NetBackup primary server with the IDP	164
Manage an IDP configuration	165

Chapter 13 NetBackup Access Control Security (NBAC) 168

About using NetBackup Access Control (NBAC)	168
NetBackup access management administration	172
About NetBackup Access Control (NBAC) configuration	172
Configuring NetBackup Access Control (NBAC)	173
NBAC configuration overview	173
Configuring NetBackup Access Control (NBAC) on standalone primary servers	174
Installing the NetBackup primary server highly available on a cluster	175
Configuring NetBackup Access Control (NBAC) on a clustered primary server	176
Configuring NetBackup Access Control (NBAC) on media servers	177
Installing and configuring access control on clients	179
About including authentication and authorization databases in the NetBackup hot catalog backups	179
NBAC configure commands summary	179
Unifying NetBackup Management infrastructures with the setuptrust command	184
Using the setuptrust command	184
Configuring Access Control host properties for the primary and media server	185
Authentication Domain tab	185
Authorization Service tab	186
Network Attributes tab	186
Access Control host properties dialog for the client	186
Authentication Domain tab for the client	186
Network Attributes tab for the client	187
Using NetBackup Access Control (NBAC) with Auto Image Replication	187
Troubleshooting Access Management	188
Troubleshooting NBAC issues	188
Configuration and troubleshooting tips for NetBackup Authentication and Authorization	190
Windows verification points	196
UNIX verification points	205

	Verification points in a mixed environment with a UNIX primary server	212
	Verification points in a mixed environment with a Windows primary server	218
	About the nbac_cron utility	225
	Using the nbac_cron utility	225
	Using the Access Management utility	227
	About determining who can access NetBackup	228
	Individual users	228
	User groups	229
	NetBackup default user groups	229
	Configuring user groups	231
	About defining a user group and users	233
	Upgrading NetBackup Access Control (NBAC)	235
	Configuration requirements if using Change Server with NBAC	235
Chapter 14	Minimizing security configuration risk	237
	About security configuration risk	237
	Security settings to be configured to minimize risk	239
	Set the current posture as security baseline	241
	Manage security baseline	241
	Manage security baseline from Alta View UI	242
Chapter 15	Configuring multifactor authentication	243
	About multifactor authentication	243
	Configure multifactor authentication for your user account	244
	Disable multifactor authentication for your user account	245
	Enforce multifactor authentication for all users	245
	Configure multifactor authentication for your user account when it is enforced in the domain	246
	Reset multifactor authentication for a user	246
Chapter 16	Configuring multiperson authorization	248
	About multiperson authorization	248
	Workflow to configure multiperson authorization for NetBackup operations	250
	RBAC roles and permissions for multiperson authorization	252
	multiperson authorization process with respect to roles	253
	NetBackup operations that need multiperson authorization	255
	Configure multiperson authorization	257
	View multiperson authorization tickets	259

	Manage multiperson authorization tickets	259
	Add exempted users	259
	Schedule expiration and purging of multiperson authorization tickets	260
	Disable multiperson authorization	261
Chapter 17	Configuring freeze mode	262
	About freeze mode in NetBackup	262
	Freeze mode options	263
	Enable freeze mode	263
	Edit freeze mode configuration options	264
	Disable freeze mode	264
	Disable freeze mode using command-line interface	265
Chapter 18	Network access control for the NetBackup web APIs	266
	About controlling network access of the NetBackup web API	266
	Workflow to configure network access control for NetBackup web service	268
	RBAC roles and permissions for network access control configuration	268
	Configure the network access control option	269
Section 2	Encryption of data-in-transit	271
Chapter 19	NetBackup CA and NetBackup certificates	272
	Overview of security certificates in NetBackup	273
	About secure communication in NetBackup	273
	About the Security Management utilities	275
	About login activity	275
	About host management	276
	Hosts tab	277
	Adding host ID to host name mappings	278
	Add or Remove Host Mappings dialog box	279
	Removing host ID to host name mappings	280
	Mappings for Approval tab	281
	Viewing auto-discovered mappings	282
	Mapping Details dialog box	282
	Approving host ID to host name mappings	283
	Rejecting host ID to host name mappings	284
	Adding shared or cluster mappings	284

Add Shared or Cluster Mappings dialog box	286
Resetting NetBackup host attributes	287
Decommission a client	288
Allowing or disallowing automatic certificate reissue	290
Adding or deleting comment for a host	292
About global security settings	293
About secure communication settings	293
Disabling insecure communication	295
About insecure communication with 8.0 and earlier hosts	296
About communication with 8.0 or earlier host in multiple NetBackup domains	296
Automatically mapping host ID to host names and IP addresses	297
About disaster recovery settings	297
Disaster recovery packages	298
Setting a passphrase to encrypt disaster recovery packages	299
Validate the disaster recovery package passphrase	301
About host name-based certificates	302
Deploying host name-based certificates	302
About host ID-based certificates	304
Web login requirements for nbcertcmd command options	304
Using the Certificate Management utility to issue and deploy host ID-based certificates	305
About NetBackup certificate deployment security levels	308
Automatic host ID-based certificate deployment	310
Managing passphrases and passphrase keys for encryption of private key of host ID-based certificates	311
Deploying host ID-based certificates	312
Deploying host ID-based certificates in an asynchronous manner	314
Implication of clock skew on certificate validity	315
Setting up trust with the primary server (Certificate Authority)	317
Forcing or overwriting certificate deployment	320
Retaining host ID-based certificates when reinstalling NetBackup on non-primary hosts	322
Deploying certificates on a client that has no connectivity with the primary server	322
About host ID-based certificate expiration and renewal	323
Deleting sensitive certificates and keys from media servers and clients	324
Cleaning host ID-based certificate information from a host before cloning a virtual machine	325

About reissuing host ID-based certificates	326
About Token Management for host ID-based certificates	330
Creating authorization tokens	331
Deleting authorization tokens	333
Viewing authorization token details	333
About expired authorization tokens and cleanup	334
About the host ID-based certificate revocation list	334
Refreshing the CRL on the primary server	336
Refreshing the CRL on a NetBackup host	336
About revoking host ID-based certificates	337
Removing trust between a host and a primary server	337
Revoking a host ID-based certificate	339
Delete NetBackup CA-signed certificate	341
Determining a NetBackup host's certificate state	342
Getting a list of NetBackup hosts that have revoked certificates	345
Deleting host ID-based certificates	345
Host ID-based certificate deployment in a clustered setup	347
About deployment of a host ID-based certificate on a clustered NetBackup host	347
Deploying host ID-based certificates on cluster nodes	348
Revoking a host ID-based certificate for a clustered NetBackup setup	349
Deploying a host ID-based certificate on a clustered NetBackup setup using reissue token	350
Creating a reissue token for a clustered NetBackup setup	350
Renewing a host ID-based certificate on a clustered NetBackup setup	351
Viewing certificate details of a clustered NetBackup setup	352
Removing CA certificates from a clustered NetBackup setup	352
Generating a certificate on a clustered primary server after disaster recovery installation	353
About the communication between a NetBackup client located in a demilitarized zone and a primary server through an HTTP tunnel	354
Adding a NetBackup host manually	357
Migrating NetBackup CA	357
Setting the required key strength before installation or upgrade using the NB_KEYSIZE environment variable	359
Migrating NetBackup CA when the entire NetBackup domain is upgraded	359
Manually migrating NetBackup CA after installation or upgrade	361

Establishing communication with clients that do not have new CA certificates after CA migration	362
Viewing a list of NetBackup CAs in the domain	362
Viewing the CA migration summary	363
Decommissioning the inactive NetBackup CA	363

Chapter 20 Configuring data-in-transit encryption (DTE) 364

About the data channel	364
Data-in-transit encryption support	365
Workflow to configure data-in-transit encryption	366
Configure the global data-in-transit encryption setting	367
Configure the DTE mode on a client	369
DTE_CLIENT_MODE for clients	369
View the DTE mode of a NetBackup job	370
View the DTE-specific attributes of a NetBackup image and an image copy	370
Configure the DTE mode on the media server	372
Modify the DTE mode on a backup image	373
DTE_IGNORE_IMAGE_MODE for NetBackup servers	374
Media device selection (MDS) and resource allocation	375
How DTE configuration settings work in various NetBackup operations	377
Backup	377
Restore	379
MSDP backup, restore, and optimized duplication	383
Universal-Share policy backup	384
Catalog backup and recovery	385
Duplication	389
Synthetic backup	390
Verify	392
Import	393
Replication	396

Chapter 21 External CA and external certificates 398

About external CA support in NetBackup	399
Command-line options used for external certificate configuration	402
Workflow to use external certificates for NetBackup host communication	402
Configuration options for external CA-signed certificates	404
ECA_CERT_PATH for NetBackup servers and clients	405

ECA_TRUST_STORE_PATH for NetBackup servers and clients	408
ECA_PRIVATE_KEY_PATH for NetBackup servers and clients	409
ECA_KEY_PASSPHRASEFILE for NetBackup servers and clients	410
ECA_CRL_CHECK for NetBackup servers and clients	411
ECA_CRL_PATH for NetBackup servers and clients	412
ECA_CRL_PATH_SYNC_HOURS for NetBackup servers and clients	413
ECA_CRL_REFRESH_HOURS for NetBackup servers and clients	414
ECA_DISABLE_AUTO_ENROLLMENT for NetBackup servers and clients	415
ECA_DR_BKUP_WIN_CERT_STORE for NetBackup servers and clients	416
MANAGE_WIN_CERT_STORE_PRIVATE_KEY option for NetBackup primary servers	417
Limitations of Windows Certificate Store support when NetBackup services are running in Local Service account context	418
About certificate revocation lists for external CA	419
How CRLs from ECA_CRL_PATH are used	420
How CRLs from CDP URLs are used	421
About certificate enrollment	422
About automatic enrollment of an external certificate	422
About viewing enrollment status of primary servers	422
Configure an external certificate for the NetBackup web server	423
Update or renew the external certificate for the web server	425
Remove the external certificate configured for the web server	425
Configuring the primary server to use an external CA-signed certificate	426
Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate after installation	429
Enrolling an external certificate for a remote host	431
Viewing the certificate authorities that your NetBackup domain supports	432
Viewing external CA-signed certificates in the NetBackup web UI	432
Renewing a file-based external certificate	432
Configuring rotation of external CA-issued certificates for host communication	433
Configure rotation of external certificates for a host	436
View certificate renewal status for a host	436

	Delete uploaded certificate artifacts for a host	436
	Removing certificate enrollment	437
	Disabling the NetBackup CA in a NetBackup domain	437
	Enabling the NetBackup CA in a NetBackup domain	439
	Disabling an external CA in a NetBackup domain	439
	Changing the subject name of an enrolled external certificate	440
	About external certificate configuration for a clustered primary server	440
	Workflow to use external certificates for a clustered primary server	441
	Configuration options for external CA-signed certificates for a virtual name	442
	Configuring an external certificate for a clustered primary server	445
Chapter 22	Regenerating keys and certificates	447
	About regenerating keys and certificates	447
	Regenerating NetBackup authentication broker keys and certificates	448
	Regenerating host identity keys and certificates	448
	Regenerating web service keys and certificates	448
	Regenerating nbcertservice keys and certificates	449
	Regenerating web server keys and certificates	449
	Regenerating JWT keys	450
	Regenerating NetBackup gateway certificates	450
	Regenerating web trust store certificates	451
	Regenerating VMware vCenter plug-in certificates	451
	Regenerating NetBackup Administrator Console session certificates	452
	Regenerating NetBackup encryption key file	452
Section 3	Encryption of data at rest	453
Chapter 23	Data at rest encryption security	454
	Data at rest encryption terminology	454
	Data at rest encryption considerations	455
	Destination types for encryption of data at rest	456
	Encryption security questions to consider	457
	Comparison of encryption options	457
	About NetBackup client encryption	458
	Installation prerequisites for encryption security	458

About running an encryption backup	459
NetBackup standard encryption restore process	461
NetBackup legacy encryption restore process	462
Configuring standard encryption on clients	463
Managing standard encryption configuration options	463
Managing the NetBackup encryption key file	464
About configuring standard encryption from the server	466
Restoring an encrypted backup file to another client	468
About configuring standard encryption directly on clients	469
Setting standard encryption attribute in policies	469
Changing the client encryption settings from the NetBackup server	469
Configuring legacy encryption on clients	469
About configuring legacy encryption from the client	470
About configuring legacy encryption from the server	473
Restoring a legacy encrypted backup created on another client	476
About setting legacy encryption attribute in policies	477
Changing client legacy encryption settings from the server	478
Additional legacy key file security for UNIX clients	478

Chapter 24

NetBackup key management service configuration	481
About FIPS enabled KMS	481
About Federal Information Processing Standards (FIPS)	483
Installing KMS	484
Using KMS with NBAC	487
About installing KMS with HA clustering	487
Enabling the monitoring of the KMS service	488
Disabling the monitoring of the KMS service	488
Configuring KMS	488
Creating the key database	489
About key groups and key records	490
Overview of key record states	491
About backing up the KMS database files	494
About recovering KMS by restoring all data files	495
Recovering KMS by restoring only the KMS data file	495
Recovering KMS by regenerating the data encryption key	496
Problems backing up the KMS data files	497
Solutions for backing up the KMS data files	497
Creating a key record	498
Listing keys from a key group	498

Configuring NetBackup to work with KMS	499
Configuring NetBackup KMS using the KMS web application	502
About using KMS for encryption	503
About importing KMS encrypted images	503
Example of running an encrypted tape backup	503
Example of verifying an encryption backup	504
KMS database constituents	505
Creating an empty KMS database	505
Importance of the KPK ID and HMK ID	505
About periodically updating the HMK and KPK	506
Backing up the KMS keystore and administrator keys	506
KMS operations using command-line interface (CLI)	506
CLI usage help	509
Create a new key group	509
Create a new key	510
Modify key group attributes	510
Modify key attributes	511
Get details of key groups	511
Get details of keys	512
Delete a key group	512
Delete a key	513
Recover a key	513
About exporting and importing keys from the KMS database	514
Modify host master key (HMK)	518
Get host master key (HMK) ID	518
Get key protection key (KPK) ID	518
Modify key protection key (KPK)	518
Get keystore statistics	519
Quiesce KMS database	519
Unquiesce KMS database	519
Key creation options	519
Troubleshooting KMS	520
Solution for backups not encrypting	521
Solution for restores that do not decrypt	521
Troubleshooting example - backup with no active key record	521
Troubleshooting example - restore with an improper key record state	524

Chapter 25

External key management service configuration in NetBackup	526
About external KMS	527
Certificate configuration and authorization	527

Workflow for external KMS configuration	527
Validating KMS credentials	528
Configuring KMS credentials	529
Listing KMS credentials	530
Updating KMS credentials	531
Deleting KMS credentials	531
Configuring KMS	531
Listing KMS configurations	532
Updating KMS configuration	532
Deleting KMS configuration	532
Configuring keys in an external KMS for NetBackup consumption	533
Creating keys in an external KMS	534
Listing keys	534
Determining a key group name during storage configuration	534
Working with multiple KMS servers	535
Migrating one KMS server to another KMS server	536
Using a separate KMS server for each storage configuration	536
Working with external KMS during backup and restore	538
Additional security considerations for MSDP media servers	538
FETCH_MSDP_EKMS_KEY for NetBackup servers and clients	539
Checking the compatibility of KMS vendor with NetBackup	540
Key rotation	541
Disaster recovery when catalog backup is encrypted using an external KMS server	541
Alerts for expiration of KMS credentials	542

Chapter 26

Cloud key management service configuration in NetBackup	543
About cloud KMS	543
Workflow to configure cloud KMS in NetBackup	544
Creating credentials in the cloud with permissions to access the created key	545
Add a credential for cloud KMS	546
Configuring proxy server credentials to use with cloud KMS	547
Add a credential for proxy server	547
Configure cloud KMS	548
Configuring a key in NetBackup to use the cloud KMS	549
Add a key in NetBackup to use the cloud KMS server	549
Examples of cloud KMS configuration using <code>nbkmscmd</code> command	550

Chapter 27	Hardware Security Module (HSM) support in NetBackup	552
	Overview of Hardware Security Modules (HSM)	552
	Configuring Hardware Security Module on a NetBackup host	553
	Protecting host ID artefacts in NetBackup using HSM	554
	Moving back to file store-based encryption	554
	Migrating from one HSM to another HSM	555
Chapter 28	Ciphers used in NetBackup for secure communication	556
	Ciphers used in NetBackup	556
Chapter 29	FIPS compliance in NetBackup	561
	About FIPS	561
	About FIPS support in NetBackup	562
	Prerequisites	563
	Specify entropy randomness in NetBackup	564
	Configure FIPS mode in your NetBackup domain	564
	Enable FIPS mode on NetBackup during installation	565
	Enable FIPS mode on a NetBackup host after installation	566
	Enable FIPS mode for the NetBackup Authentication Broker service	567
	Enable FIPS mode for the NetBackup BAR Console	568
	Disable FIPS mode for NetBackup	570
	Disable FIPS mode for a NetBackup host	570
	Disable FIPS mode for NetBackup Authentication broker (<code>nbatd</code>)	571
	Disable FIPS mode for the NetBackup BAR Console	572
	NB_FIPS_MODE option for NetBackup servers and clients	573
	USE_URANDOM for NetBackup servers and clients	574
Chapter 30	Post-Quantum Cryptography (PQC) support in NetBackup	576
	About Post-Quantum Cryptography (PQC)	576
	PQC support for TLS communication	577
	Configuring PQC in NetBackup	577
	Configuring PQC for deduplication	579
	Enabling PQC for MSDP	580
	Disabling PQC for MSDP	580
	Viewing the PQC status for MSDP	581

Chapter 31	STIG compliance support in NetBackup	582
	About STIG compliance support	582
	NBFP_CHECK option for NetBackup servers and clients	583
	Verifying and correcting file permissions using <code>nbfp</code> command	583
Chapter 32	NetBackup web services account	585
	About the NetBackup web services account	585
	Changing the web service user account	586
Chapter 33	Running NetBackup services with non-privileged user (service user) account	589
	About a NetBackup service user account	589
	Important considerations for using a service user account	589
	Configuring a service user account	591
	Changing a service user account after installation or upgrade	591
	Giving access permissions to service user account on external paths	592
	NetBackup services that run with the service user account	593
Chapter 34	Running NetBackup commands with non-privileged user account	595
	Running NetBackup commands using the <code>nbcmdrun</code> wrapper command	595
	Who can run NetBackup commands	596
	How does <code>nbcmdrun</code> function	596
Chapter 35	Immutability and indelibility of data in NetBackup	598
	About immutable and indelible data	598
	Workflow to configure immutable and indelible data	600
	Deleting an immutable image from storage using the <code>bpexpdate</code> command	601
	Removing an immutable image from the catalog using the <code>bpexpdate</code> command	603
Chapter 36	Anomaly detection	604
	About backup anomaly detection	604
	How NetBackup detects backup anomalies	605
	Configure backup anomaly detection settings	606

	Detecting backup anomalies on the primary server	609
	Detecting backup anomalies on the media server	609
	View backup anomalies	610
	About system anomaly detection	612
	Configure system anomaly detection settings	613
	Configure rules-based anomaly detection	614
	Configure risk engine-based anomaly detection	615
	View system anomalies	618
	Anomaly configuration to enable automatic scanning	618
	Computation of entropy and file attributes in NetBackup	621
	Support information for computation of entropy and file attributes	
		622
	COMPUTE_IMAGE_ENTROPY for NetBackup primary servers	
		623
	Disable backup anomaly detection and computation of entropy	
	and file attributes for a client	624
Chapter 37	Compute host	626
	About compute hosts	626
	Add a compute host	626
	Activate a compute host	627
	Deactivate a compute host	627
	Edit a compute host	627
	Delete a compute host	628
	Configure compute host settings	628
Section 4	Malware scanning	629
Chapter 38	Introduction	630
	About malware scanning	630
	Workflow for malware scanning	633
	About dynamic scan	641
	About file hash search with malware hash	641
	Limitations	642
Chapter 39	How to setup Malware scanning	645
	How to set up malware scanning	645

Chapter 40	Instant Access configurations	647
	About Instant Access configurations	647
	MSDP build-your-own (BYO) server prerequisites and hardware requirements to configure Instant Access	648
	Instant Access tuning parameters for malware scanning (BYO)	650
	Configuration for scan instances	650
Chapter 41	Malware tools configurations	652
	Supported malware tools	652
	Configuring NetBackup Malware Scanner (Avira)	653
	Configuration of mirror server for Signature update	654
	Configure a proxy server on Windows or Linux	658
	Configure the NetBackup Malware Scanner on scan host	659
	Configuring Symantec Protection Engine	664
	Configuring Microsoft Defender Antivirus	665
	Configuring Trend Micro Malware Scanner	666
	Configuring NetBackup NextGen Malware Scanner	666
Chapter 42	Scan host configurations	670
	NetBackup malware scan host capabilities	670
	Prerequisites for a scan host	671
	Prerequisites for Windows scan host	672
	Prerequisites for Linux scan host	675
	Limitations and considerations for scan host using NFS share	677
	Configuring scan host	678
	Automated scan host configuration	678
	Manual scan host configuration	682
	Configuring a scan host pool	689
	Prerequisites for scan host pool	689
	Configure a new scan host pool	690
	Add a new host in a scan host pool	690
	Managing a scan host	691
	Add an existing scan host	691
	Validating the scan host pool configuration	692
	Remove the scan host	693
	Activate or deactivate the scan host	693
	Managing credentials for malware scanning	694
	Configure resource limits for malware detection	696

Chapter 43	Performing malware scan	698
	Performing malware scan before recovery	698
	Perform a malware scan	700
	Scanning backup images	702
	Assets by policy type	704
	Assets by workload type	706
Chapter 44	Managing scan tasks for malware and YARA scanning	708
	View the malware scan status	708
	Actions for malware scanned images	710
	Recover from malware-affected images (clients protected by protection plan)	713
	Recover from malware-affected images (clients protected by policies)	714
	Clean file recovery for virtual workload (VMware)	715
Chapter 45	Malware scan configuration parameters	718
	MALWARE_SCAN_OPERATION_TIMEOUT	718
	MALWARE_DETECTION_CLEANUP_PERIOD	719
	MALWARE_DETECTION_TIMEOUT_PERIOD option for NetBackup servers	720
	FAIL_SAFE_SCAN_RETRY_COUNT	721
	Malware hash configuration parameters	721
	MALWARE_DETECTION_MALWARE_JOBS_CLEANUP_PERIOD	722
	MALWARE_DETECTION_WORKLIST_CLEANUP_PERIOD	723
	CLIENT_KEEP_LOG_DAYS	724
	VIRUS_SIGNATURE_UPDATE_INTERVAL	724
Chapter 46	Troubleshooting	726
	Troubleshooting issues with malware scanning	726
Chapter 47	Threat library	738
	About threat library and YARA rule files	738
	Add threat feeds	738

Chapter 48	YARA scanning	740
	About YARA scanning	740
	Workflow to configure YARA scanning	741
	Scanning backup images with YARA scanner	741
	Assets by workload type for YARA scanning	743
Chapter 49	File hash calculation	745
	About file hash calculation	745
	Workflow to configure file hash calculation	746
	Calculate file hashes for backup images	747
	Troubleshooting issues with file hash calculation	748

Read this first for secure communications in NetBackup

This chapter includes the following topics:

- [About secure communication in NetBackup](#)
- [How NetBackup CA-signed certificates \(or host ID-based certificates\) are deployed during installation](#)
- [How secure communication works with primary server cluster nodes](#)
- [About NetBackup clients installed on nodes of a clustered application](#)
- [How NetBackup certificates are deployed on hosts during upgrades](#)
- [When an authorization token is required during certificate deployment](#)
- [Why do you need to map host names \(or IP addresses\) to host IDs](#)
- [How to reset host attributes or host communication status](#)
- [What has changed for catalog recovery](#)
- [What has changed with Auto Image Replication](#)
- [How the hosts with revoked certificates work](#)
- [Are NetBackup certificates backed up](#)
- [Can you configure external certificates for primary server](#)
- [How secure communication works with primary server cluster nodes using external certificates](#)

- [How revocation lists work for external certificates](#)
- [How communication happens when a host cannot directly connect to the primary server](#)
- [How NetBackup 8.1 or later hosts communicate with NetBackup 8.0 and earlier hosts](#)
- [How communication with legacy media servers happens in the case of cloud configuration](#)
- [Communication failure scenarios](#)
- [Secure communication support for other hosts in NetBackup domain](#)
- [Secure communication support for BMR](#)
- [Configuration for VMware backups that protect SQL Server and backups with SQL Servers that use multiple NICs](#)

About secure communication in NetBackup

This chapter provides critical information about secure communication in NetBackup. It is strongly recommended that you read this information before you upgrade NetBackup to a version that supports secure communication (8.1 or later).

NetBackup 8.1 and later hosts can communicate with each other only in a secure mode.

NetBackup uses Transport Layer Security (TLS) protocol for host communication where each host needs to present its security certificate and validate the peer host's certificate against the certificate authority (CA) certificate. NetBackup security certificates that are used to authenticate NetBackup hosts conform to the X.509 Public Key Infrastructure (PKI) standard. NetBackup supports two types of certificates:

- **NetBackup CA-signed certificates:** A NetBackup primary server acts as the certificate authority (CA) and issues digital certificates to hosts.
See [“Overview of security certificates in NetBackup”](#) on page 273.
- **External CA-signed certificates:** Starting with NetBackup 8.2, you can also configure external CA-signed certificates (or external certificates) on the NetBackup hosts.
See [“About external CA support in NetBackup”](#) on page 399.

Depending on the configuration of NetBackup, a host needs one or both types of certificates for successful communication with other hosts.

You can choose to deploy a certificate on a host during NetBackup installation. If, for some reason, a certificate cannot be deployed on a host during installation, the host cannot communicate with other hosts. In that case, you must manually deploy a NetBackup certificate on the host using the `nbcertcmd` command to start host communication after installation.

Alternatively, you can configure external CA-signed certificates.

Secure communication settings are provided in the following places:

- **Security > Host mappings**
- **Settings > Global security**

The following commands provide options to manage certificate deployment and other security settings: `nbhostmgmt`, `nbhostidentity`, `nbcertcmd`, and `nbsecmd`.

If you have NetBackup 8.0 or earlier hosts in your environment, you can enable legacy communication with them.

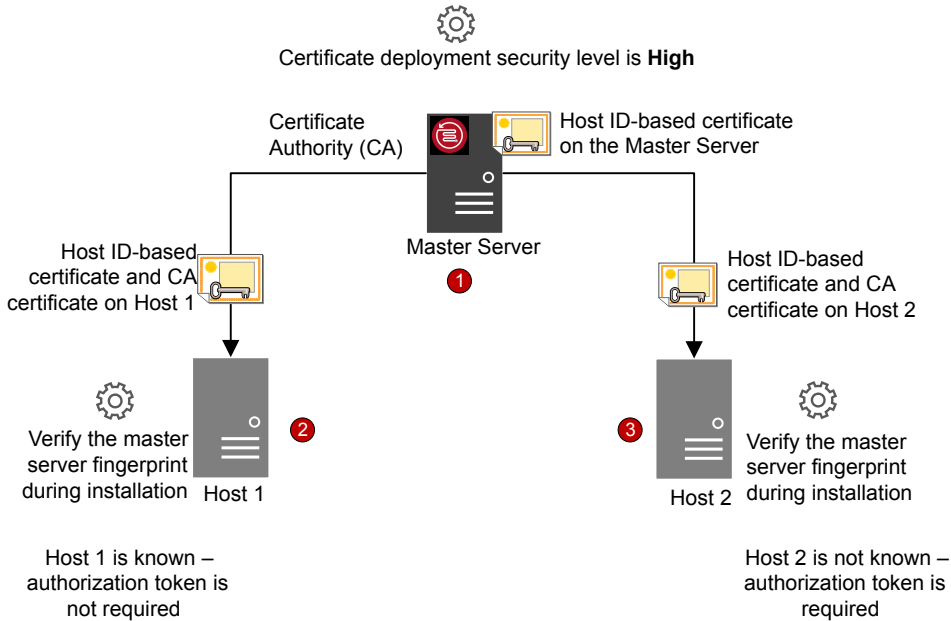
See [“How NetBackup 8.1 or later hosts communicate with NetBackup 8.0 and earlier hosts”](#) on page 39.

Note: A host name-based certificate is required in the following scenarios:

- NetBackup Access Control or NBAC-enabled hosts require host name-based certificates.
- The NetBackup CloudStore Service Container requires that the host name-based certificate be installed on the media server.

How NetBackup CA-signed certificates (or host ID-based certificates) are deployed during installation

The following diagram illustrates how NetBackup CA-signed certificates are deployed on hosts during installation:



NetBackup certificate deployment occurs in the following order:

1. A NetBackup certificate is automatically deployed on the NetBackup primary server during installation. The primary server is the NetBackup CA.
2. A NetBackup certificate is deployed on Host 1 during installation after confirming the CA fingerprint that is made available by the installation wizard or the script.

An authorization token is not required because the certificate deployment security level on the primary server is set to High and Host 1 is known to the primary server.

Note: A fingerprint is used to authenticate the CA of the primary server before it is added to the trust store of a host. The primary server administrator communicates the CA fingerprint to the host administrators by email or file, or publishes it on a website.

Note: An authorization token is used as a mechanism to authorize a host's certificate request that is sent to the NetBackup primary server. An authorization token is confidential and only the primary server administrator can create it. The primary server administrator then passes it on to the administrator of the host where you want to deploy a certificate. A reissue token is a special authorization token that is used to redeploy a certificate on a host to which a certificate was previously issued.

If you continued with the NetBackup installation without confirming the primary server fingerprint, you need to carry out manual steps before backups and restores can occur.

<https://support.cohesity.com/s/article/article-100039650>

3. A NetBackup certificate is deployed on Host 2 during installation after the primary server fingerprint is confirmed. An authorization token is required, because the certificate deployment security level on the primary server is set to High and Host 2 is not known to the primary server.

The host-ID based certificate is generated using the encrypted private key for all the hosts.

The private key of the NetBackup certificate is stored in an encrypted format using AES_256_CBC encryption. The password that is used to encrypt the private keys is stored in file storage and is encrypted using AES_256_GCM encryption.

The form factors of NetBackup such as NetBackup Appliance, NetBackup Flex, NetBackup Flex Scale, NetBackup Scale Out are fully secured on on-disk using the host-ID based certificate. ITA Data Collector 11.4.03 enables the consumption of the encrypted private keys. The ITA Data Collector must be 11.4.03 or later if the collection method is set to the **Data Collector installed on NetBackup Primary Server** option for successful data collections from NetBackup 10.4.1 primary server.

Older versions of ITA Data Collector are able to collect data if the collection method is SSH or WMI protocol to communicate with NetBackup primary server.

How secure communication works with primary server cluster nodes

Review the following scenarios about certificate deployment if you have a clustered primary server:

- In the case of fresh NetBackup installation, the certificate on an active node is deployed automatically. You must manually deploy certificates on all inactive nodes.
The private key of the NetBackup host ID-based certificate is stored in an encrypted format using AES_256_CBC encryption.
- In the case of disaster recovery, certificates for active and inactive nodes are not recovered. After you install NetBackup in a disaster recovery mode after a disaster, you must manually deploy certificates on all nodes using a reissue token.
- In the case of upgrade, active or inactive nodes may already have a certificate. You can verify whether a cluster node has a certificate or not by viewing the certificate details with the `nbcertcmd -listCertDetails` command.
The private key of the host ID-based certificate is stored in an encrypted state, which can be verified using the `nbcertcmd -listCertDetails` command. The 'Private Key Encryption State' field in the command output shows the encrypted status of the private key.

Note: If you have configured NetBackup Access Control (NBAC) on a primary server cluster node, you also need to manually deploy host name-based certificates on all nodes.

In a cluster setup, the same virtual name is used across multiple cluster nodes. Therefore, the virtual name should be mapped with all associated cluster nodes.

About NetBackup clients installed on nodes of a clustered application

Review the following scenarios about secure communication with NetBackup clients installed on nodes of a clustered application:

- For successful communication, you need to simultaneously upgrade all cluster nodes.
- Ensure that the virtual name is mapped to all cluster nodes to avoid backup failures after a failover. Cohesity recommends that you monitor the **Security** >

Host mappings > Mappings for approval tab for any conflicts that are detected and approve the required mappings.

How NetBackup certificates are deployed on hosts during upgrades

During a NetBackup upgrade, NetBackup deploys NetBackup certificates before the upgrade. If the certificates cannot be deployed, you can terminate the upgrade process. The upgrade script retains the existing NetBackup setup that you can use.

If you have upgraded NetBackup from 8.0 to 8.1 or later, NetBackup certificates may already be present on the hosts. In such a case, certificates are not deployed during the upgrade process.

If you have upgraded NetBackup from 8.x to 10.4, the private keys are in an unencrypted state. After the upgrade, the new encrypted private keys are created and certificates are reissued.

Certificates are not deployed during the upgrade process, if the software is upgraded using a utility (that downloads and installs security updates and software patches). You need to manually deploy the certificates.

When an authorization token is required during certificate deployment

The information in this section applies only to NetBackup CA-signed certificates. External CA-signed certificates do not require authorization tokens.

The security level setting determines whether an authorization token is required to deploy a certificate. You can set the security level on the primary server to different levels, depending on your needs. Use the **Settings > Global security > Secure communication** tab.

The following settings are available. The default setting is High.

- **Medium** - The primary server fingerprint must be confirmed during certificate deployment. An authorization token is not required.
- **High** - The primary server fingerprint must be confirmed during certificate deployment. An authorization token is not required if the host is known to the primary server.
- **Very High** - The primary server fingerprint must be confirmed during certificate deployment. An authorization token is mandatory for every host.

Note: Certificate deployment in certain scenarios always requires a token, such as in the case of clients in a demilitarized zone or for certificate reissue.

See [“About NetBackup certificate deployment security levels”](#) on page 308.

Why do you need to map host names (or IP addresses) to host IDs

Hosts can be referenced with multiple names.

For example: In the case of multiple network interfaces or if hosts are referenced by both short names and Fully Qualified Domain Names (FQDN).

For successful secure communication in NetBackup 8.1 or later, you should map all associated host names to the respective host ID. The NetBackup-configured client name of a host (or the primary name) is automatically mapped to its host ID during certificate deployment. Additional host names are discovered during communication and may be automatically mapped to the respective host ID or may appear in the **Mappings for Approval** list. Perform this configuration in the **Hosts > Host properties** on the primary server.

See [“Adding host ID to host name mappings”](#) on page 278.

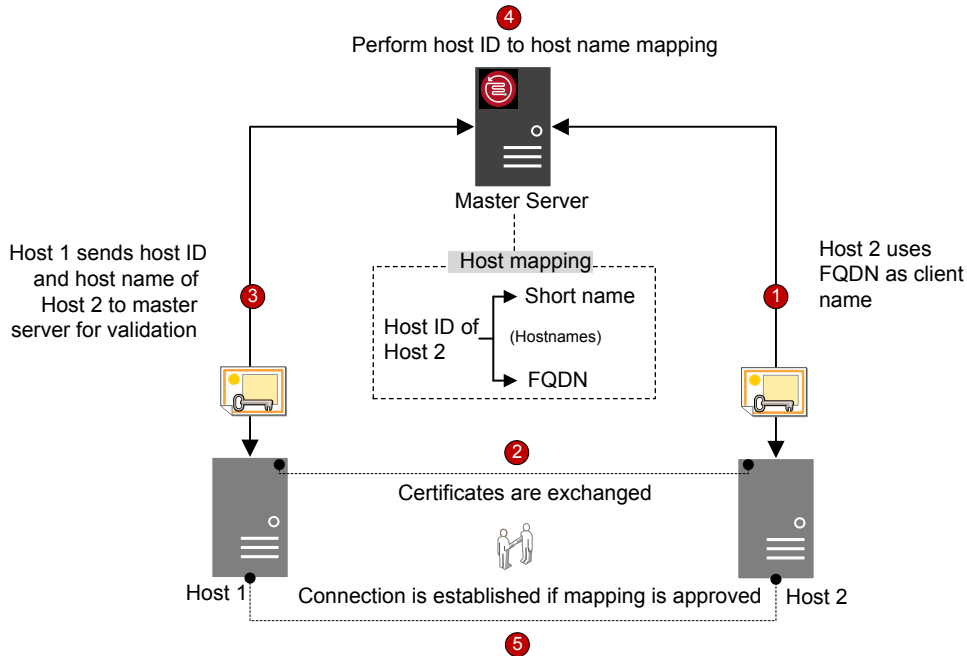
Examples of configurations that have multiple host names include:

- If you have multiple network interfaces, a host has both a public and a private host name.
- A host can have a short name and a fully qualified domain name (FQDN).
- A host can be associated with its IP address.
- For a file system or database that is clustered, a host is associated with its node name and the virtual name of the cluster.

Note the following:

- The Exchange, SharePoint, and SQL Server agents also require that you configure host information in the **Distributed Application Restore Mapping** host properties on the primary server.
- For highly available environments, the SQL Server agent no longer requires a second policy that contains the cluster or AG node names. You also do not need to configure permissions for redirected restores for the cluster or AG nodes. For successful backups and restores of a SQL Server cluster or AG, you need only configure the mappings in the **Host mappings** properties and the **Distributed application restore mapping** host properties.

The following diagram illustrates the host ID-to-host name mapping process:



Host name-to-host ID mapping occurs in the following order:

1. The FQDN of Host 2 is mapped to its host ID during certificate deployment.
2. Host 1 initiates a secure connection to Host 2 using the short name. Both hosts exchange their NetBackup certificates as part of the TLS handshake.
3. Host 1 sends the host ID and short name of Host 2 to the primary server for validation.
4. The primary server looks up the host ID and the short name in its database. Since the provided short host name is not already mapped to the host ID of Host 2, one of the following occurs:
 - If the **Automatically map host ID to host names** option in the **NetBackup web UI** is selected and the short name is not already mapped to another host ID, the discovered short name is automatically mapped to the host ID of Host 2, and Host 1 is instructed to continue the connection.
 - If the **Automatically map host ID to host names** option is not selected or the short name is already mapped to another host ID, the discovered

mapping is added to the pending approval list and Host 1 is instructed to drop the connection. The mapping should be manually approved before any connections to Host 2 using the same short name can succeed.

5. Connection is established between the hosts if the mapping is approved. If the mapping is not approved, the connection is dropped.

How to reset host attributes or host communication status

The **Reset Host Attributes** option deletes host properties and host name-to-host ID mappings information. The primary host name and NetBackup certificate are not deleted.

Resetting host attributes is useful in the following scenarios:

- If you have downgraded a host to 8.0 or earlier to enable insecure (or back-level) communication.
- If you experience host communication issues and you want to delete the host information.

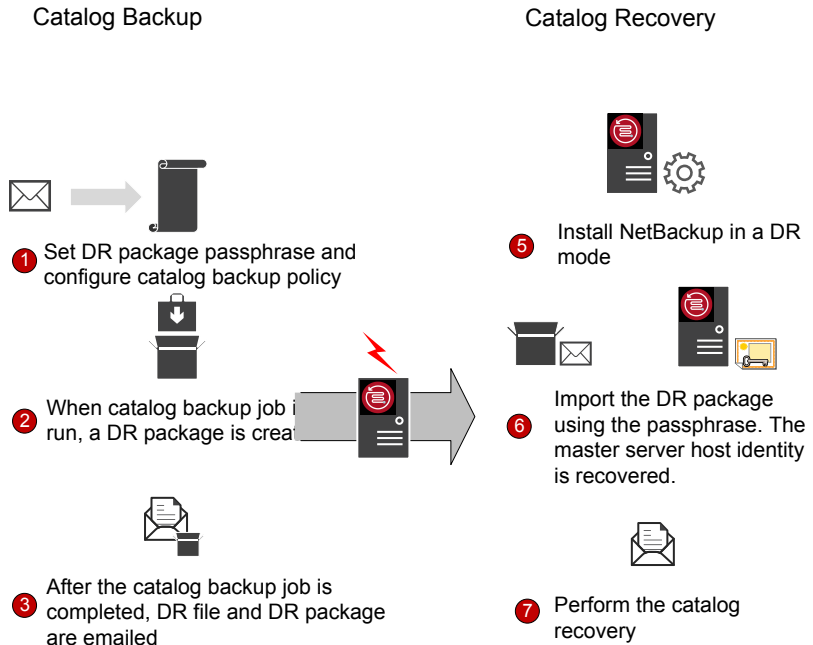
See [“Resetting NetBackup host attributes”](#) on page 287.

What has changed for catalog recovery

In NetBackup 8.1 or later, the primary server requires you to recover its host identity when you restore NetBackup after a disaster. The host identity includes certificate information, security settings, and other information.

With the earlier host identity in place, the primary server can communicate with media server and clients in the new NetBackup instance. A disaster recovery package is created during each catalog backup that retains the primary server host identity. As the disaster recovery package contains sensitive data such as security certificates and security settings, it is encrypted with a passphrase.

The following diagram shows the workflow for the catalog recovery.



1. Set a passphrase for the disaster recovery package and then configure a catalog backup policy. Catalog backups use the passphrase that is configured at the time of policy execution.

To set a passphrase, in the NetBackup web UI open **Settings > Global security**. Then click the **Disaster recovery**.

You can also set the passphrase constraints using the `nbsecmd -setpassphraseconstraints` command option. For more information on the commands, see the [NetBackup Commands Reference Guide](#).

If you do not set the passphrase constraints using the command, the default constraints are applicable: Minimum of 8 and a maximum of 1024 characters.

If you change the passphrase at any time, the passphrase of the disaster recovery packages that were created earlier is not changed. It only changes the passphrase of the disaster recovery packages that are created subsequently.

To recover older catalogs, you must use the corresponding passphrase.

Caution: You must set the passphrase before you configure the catalog backup policy. If the passphrase is not set, catalog backups fail. If the catalog backup policy is upgraded from a version earlier than 8.1, catalog backups continue to fail until the passphrase is set.

2. A disaster recovery package is created during each catalog backup.

To verify that the passphrase after the catalog backup is successful, run the following command:

```
nbhostidentity -testpassphrase -infile dr_package_location
```

3. Disaster recovery packages are stored along with the disaster recovery files and emailed to the recipient that you have specified during policy configuration.
4. Disaster strikes.
5. After a disaster, install NetBackup on the primary server in a disaster recovery mode. This process prompts you to specify the disaster recovery package path and passphrase.
6. If the appropriate passphrase is specified, the primary server host identity is recovered. You must provide the passphrase that corresponds to the disaster recovery package that you want to recover.

If you lost the passphrase, you must deploy security certificates on all NetBackup hosts manually.

For more details, refer to the following article:

<https://support.cohesity.com/s/article/article-100033743>

7. You should perform the catalog recovery immediately after you have recovered the host identity. This action avoids any information loss specific to the certificate-related activities that may take place after the host identity restore. Use the appropriate disaster recovery (DR) file and recover the required catalog.

The passphrase is not recovered during the host identity (or disaster recovery package) restore or during catalog recovery. You must set it again in the new NetBackup instance.

Note: If you need to restore the host identity after the normal NetBackup installation (when the disaster recovery mode is not selected), you can use the `nbhostidentity` command.

To restore the host identity of NetBackup Appliance, you must use the `nbhostidentity` command after the normal installation.

What has changed with Auto Image Replication

To use NetBackup Auto Image Replication (A.I.R.) with secure communications, you must establish trust from both the source and the target primary servers.

When you upgrade both the source and the target primary servers to 8.1 or later, you must update the trust relationship on both primary servers.

Note: After the upgrade, if the trust is not re-established on both the servers, new storage lifecycle policies (SLP) do not work.

You can configure the trust relationship using the **NetBackup web UI** or the `nbseccmd -setuptrustedmaster` command.

For more information on trusted primary servers for Auto Image Replication, refer to the [NetBackup Deduplication Guide](#).

How the hosts with revoked certificates work

NetBackup certificates can be revoked by the primary server administrator for various reasons. A certificate revocation list (CRL) that contains information about the revoked certificates is created by the primary server and is periodically fetched by all hosts. The time interval to update the CRLs is determined by the certificate deployment security level on the primary server.

During communication between hosts, CRLs are verified. The host that uses a revoked certificate is no longer trusted. Communication with such hosts is terminated.

See [“About the host ID-based certificate revocation list”](#) on page 334.

Are NetBackup certificates backed up

For security reasons, NetBackup certificates are not backed up during backups. Certificates are automatically deleted when NetBackup is uninstalled. If required, you can manually back them up along with the respective private keys before you uninstall NetBackup.

See [“Retaining host ID-based certificates when reinstalling NetBackup on non-primary hosts”](#) on page 322.

Can you configure external certificates for primary server

You can use X.509 certificates that your trusted certificate authority (CA) has issued. NetBackup supports file-based certificates and Windows certificate store as sources for external certificates for NetBackup hosts. It supports certificates in PEM, DER, and P7B formats.

See [“Workflow to use external certificates for NetBackup host communication”](#) on page 402.

How secure communication works with primary server cluster nodes using external certificates

You can use X.509 certificates that your trusted certificate authority (CA) has issued, for a clustered primary server.

You should first enable your NetBackup domain to use external CA-signed certificates by configuring the NetBackup web server. You can then configure the NetBackup clustered primary server to use external CA-signed certificates for secure host communication.

See [“Workflow to use external certificates for a clustered primary server”](#) on page 441.

How revocation lists work for external certificates

Certificate revocation list (CRL) for an external certificate authority (CA) contains a list of digital certificates that the external CA has revoked before the scheduled expiration date and should no longer be trusted.

See [“About certificate revocation lists for external CA”](#) on page 419.

How communication happens when a host cannot directly connect to the primary server

In a demilitarized zone (DMZ), NetBackup clients may not be able to directly send requests (for certificate deployment and so on) to the primary server. The HTTP tunnel on the media server is used to accept the web service requests sent by the client hosts and forward them to the primary server. The configuration of the HTTP tunneling is automatic and no setup is required. The NetBackup client and the media server must be 8.1 or later for HTTP tunneling to work.

Irrespective of the certificate deployment security level that is set on the primary server, you require an authorization token to deploy a NetBackup CA-signed certificate on a host in a demilitarized zone.

See [“About the communication between a NetBackup client located in a demilitarized zone and a primary server through an HTTP tunnel”](#) on page 354.

How NetBackup 8.1 or later hosts communicate with NetBackup 8.0 and earlier hosts

NetBackup 8.1 or later hosts can communicate with other 8.1 or later hosts only in a secure mode. For 8.1 or later host to communicate with hosts at 8.0 or earlier, you need to allow insecure communication.

By default, the **Enable insecure communication with NetBackup 8.0 and earlier hosts** option is enabled. The option is available on the **Settings > Global security > Secure communication** tab.

If you disable the option to allow only secure communication, you must restart the NetBackup services on the primary server to terminate any insecure communications and allow only secure communications.

During insecure communication, the NetBackup host first connects to the primary server for host validation. The primary server verifies whether insecure communication is enabled or not. If the option is enabled, the communication between the two hosts is established. If the option is disabled, the communication is dropped.

How communication with legacy media servers happens in the case of cloud configuration

If the **Enable insecure communication with NetBackup 8.0 and earlier hosts** option is disabled, NetBackup cannot communicate with legacy media servers that you use for cloud storage irrespective of the value of the `CSSC_LEGACY_AUTH_ENABLED` cloud configuration option.

The **Enable insecure communication with NetBackup 8.0 and earlier hosts** option is available in the **NetBackup web UI** on the **Setting > Global Security > Secure Communication** tab.

Communication failure scenarios

Review the following scenarios to resolve host communication issues that you may face in NetBackup 8.1 or later.

Failure during communication with 8.0 or earlier hosts

If insecure communication is not allowed in NetBackup, communication with 8.0 and earlier hosts fails. For successful communication with 8.0 and earlier NetBackup hosts, use one of the following methods:

- In the **NetBackup BAR Console** on the primary server host, select the **Settings > Global security > Secure communication > Enable insecure communication with NetBackup 8.0 and earlier hosts** option.
- On the primary server host, run the following command: `nbseccmd -setsecurityconfig -insecurecommunication on`.

Catalog backup failure

If the disaster recovery package passphrase is not set, catalog backups fail with status code 2524. The following error message is displayed:

```
Catalog backup failed because the passphrase for the disaster recovery package is not set.
```

To set a passphrase, use the **Setting > Global Security > Disaster Recovery** tab in **NetBackup web UI**.

Secure communication support for other hosts in NetBackup domain

Use this section to learn about how NetBackup 8.1 supports communication with BMR (Bare Metal Restore) hosts.

Secure communication support for BMR

NetBackup Bare Metal Restore (BMR) 8.1.1 and later versions support NetBackup secure communication. The **Allow Auto Reissue Certificate** option enables the `autoreissue` parameter of a NetBackup host that in turn allows you to deploy a certificate on the host without requiring a reissue token.

See [“Allowing or disallowing automatic certificate reissue”](#) on page 290.

For more information on BMR, refer to the [NetBackup Bare Metal Restore Administrator's Guide](#).

Configuration for VMware backups that protect SQL Server and backups with SQL Servers that use multiple NICs

Certain environments require that you configure host information in the **Distributed Application Restore Mapping** host properties on the primary server. If you have multiple NICs, you must map the hosts in that host property (or, in the altnames directory). For VMware backups, if you use a Primary VM identifier other than VM hostname, then you must map the Primary VM identifier to the client host name.

Increasing NetBackup security

This chapter includes the following topics:

- [About NetBackup security and encryption](#)
- [NetBackup security implementation levels](#)
- [World-level security](#)
- [Enterprise-level security](#)
- [Datacenter-level security overview](#)
- [NetBackup Access Control \(NBAC\)](#)
- [Combined world, enterprise, and datacenter levels](#)
- [NetBackup security implementation types](#)
- [Operating system security](#)
- [NetBackup security vulnerabilities](#)
- [Standard NetBackup security](#)
- [Client side encryption security](#)
- [NBAC on primary, media server, and graphical user interface security](#)
- [NBAC complete security](#)

About NetBackup security and encryption

NetBackup security and encryption provide protection for all parts of NetBackup operations on NetBackup primary 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 43.

See [“NetBackup Access Control \(NBAC\)”](#) on page 47.

See [“Operating system security”](#) on page 54.

See [“Standard NetBackup security”](#) on page 55.

See [“Client side encryption security”](#) on page 56.

See [“NBAC on primary, media server, and graphical user interface security”](#) on page 58.

See [“NBAC complete security”](#) on page 60.

NetBackup security implementation levels

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

[Table 2-1](#) shows how NetBackup security levels can be implemented.

Table 2-1 NetBackup security implementation levels

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

World-level security

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

Figure 2-1 World-level security scope

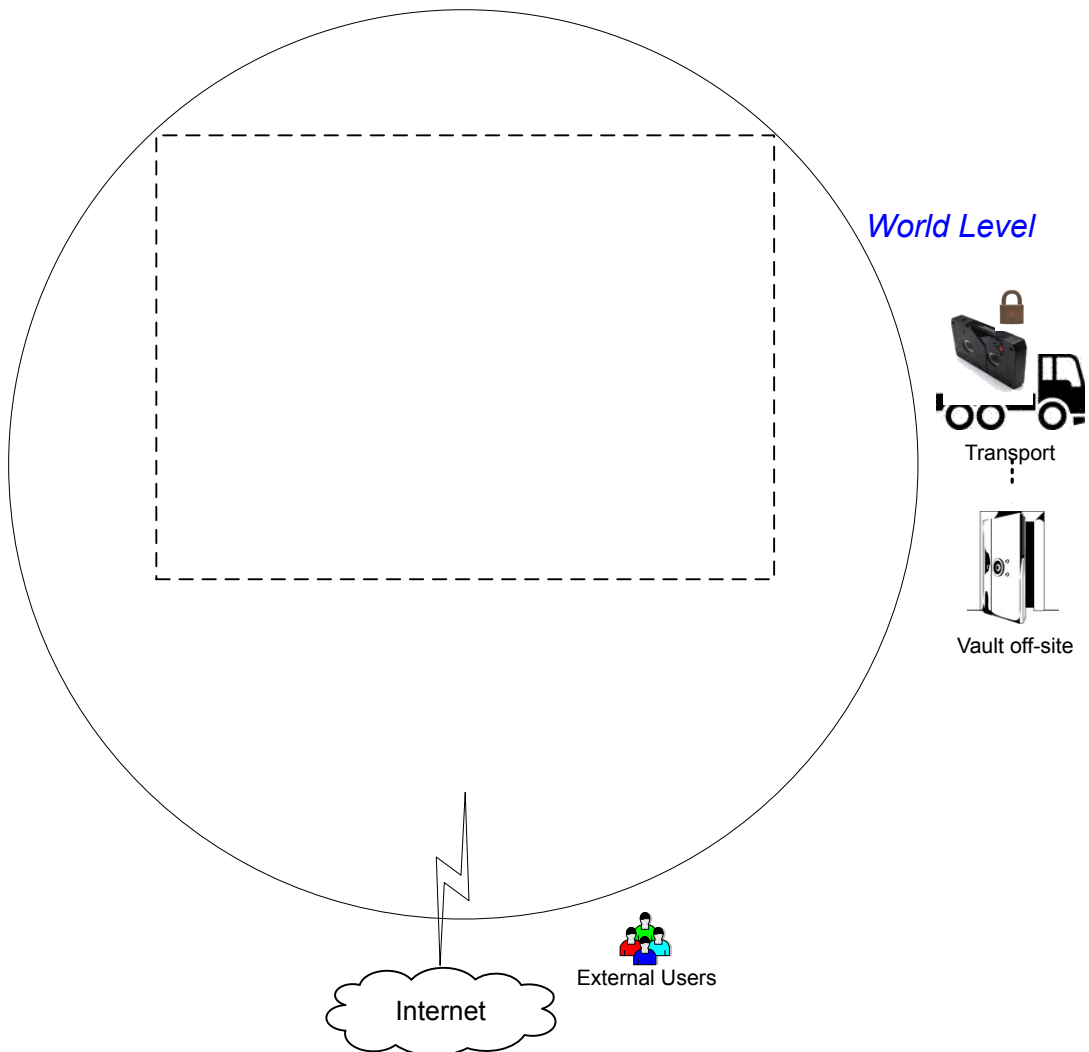


Table 2-2 Types of world-level security

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 datacenter level.

Figure 2-2 Enterprise-level security scope

Security Overview

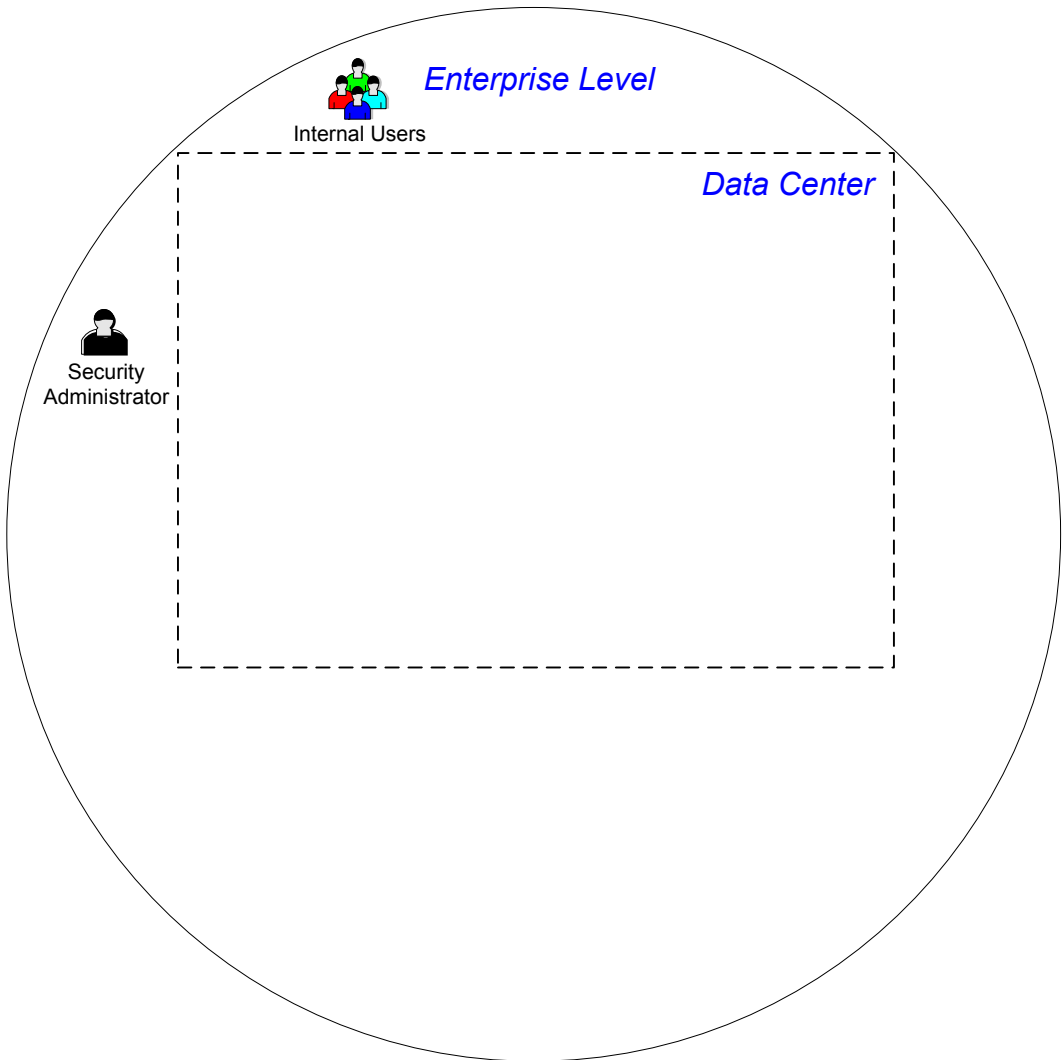


Table 2-3 Types of enterprise-level security

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

Datacenter-level security overview

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

[Table 2-4](#) describes the deployment models unique to datacenter-level security.

Table 2-4 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 43.

NetBackup Access Control (NBAC)

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

See [“About NetBackup security and encryption”](#) on page 43.

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 2-5 NetBackup components used in security

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

Table 2-5 NetBackup components used in security (*continued*)

Component	Description
NetBackup administrator	Specifies a user who has been granted administrator permissions to access and manage the NetBackup functionality from within the data center.
Media server	Communicates with the primary server, root broker and authentication broker, authorization engine, and clients 1 through 6. The media server writes unencrypted data to tape for client 5 and encrypted data to tape for client 6.
Clients	Specifies that clients 1 through 4 are standard NetBackup types. Client 5 is a web server type located in the DMZ. Client 6 is a client side encrypted type also located in the DMZ. All client types are managed by the primary server and have their data backed up to tape through the media server. Clients 5 and 6 communicate to NetBackup using NetBackup only ports through the internal firewall. Client 5 also receives connections from the Internet using HTTP only ports through the external firewall.
Tapes	Specifies that the tape security in NetBackup can be increased by adding the following: ■ Client side encryption ■ Encryption of data at rest Unencrypted and encrypted data tapes are produced in the datacenter. The unencrypted tape data is written for clients 1 through 5 and stored on-site at the datacenter. The encrypted tapes are written for client 6 and are transported off-site to a vault for disaster recovery protection.
Encryption	Specifies that NetBackup encryption can increase security by providing the following: ■ Greater data confidentiality ■ The loss of physical tape is not as critical if all the data is effectively encrypted ■ The best risk mitigation strategy For more information about encryption: See “Encryption security questions to consider” on page 457.

Table 2-5 NetBackup components used in security (*continued*)

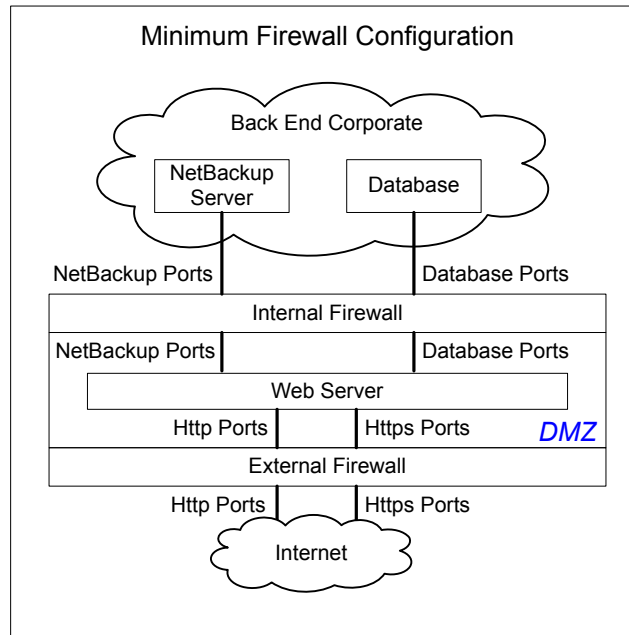
Component	Description
Data over the wire security	Includes the communication between primary servers, media servers, clients, and communication using ports through firewalls and over WANs. For more information about ports, see the NetBackup Network Ports Reference Guide: The data over the wire part of NetBackup can help increase security in the following ways: ■ NetBackup Access Control (NBAC) ■ Classic NetBackup daemons employ authentication when NBAC is enabled ■ CORBA daemons use the fully encrypted channels that support confidentiality, and provide data integrity ■ Firewalls ■ Disabling the unused ports in NetBackup and in other products: ■ PBX and VNETD dedicated ports provide increased NetBackup security ■ Central set of ports to monitor and open through firewalls Note: Communication between NetBackup 8.1 and later hosts is secure. See “About secure communication in NetBackup” on page 273.
Firewall security	Specifies that the NetBackup firewall support can help increase security. Important points about firewall security include the following: ■ It is recommended to use firewall and intrusion detection protection for NetBackup. ■ Firewall protection relates to general network security from a NetBackup standpoint. It focuses on reducing the possible "door locks" for a thief to try to pick. It may be helpful to review the possibility of blocking NFS, telnet, FTP, email ports. They are not strictly needed for NetBackup use and can provide an "open door" for unwanted access. ■ Secure the primary server as much as possible ■ Firewalls can include internal firewalls and external firewalls, as follows: ■ Internal firewall - allows NetBackup to access web server client 5 and encrypted client 6 in the DMZ. Only selected NetBackup ports and possibly other application ports are enabled for data communication through the internal firewall and into and out of the DMZ. The HTTP ports are open in the External Firewall and are not allowed to pass through the internal firewall. ■ External firewall - allows external users to access the web server client 5 located in the DMZ from the Internet over HTTP ports. NetBackup ports are open for web server client 5 to communicate through the internal firewall to NetBackup. The NetBackup ports are not allowed to pass through the external firewall to the Internet. Only the HTTP ports of web server client 5 can pass through the external firewall to the Internet.

Table 2-5 NetBackup components used in security (*continued*)

Component	Description
Demilitarized zone (DMZ)	Specifies that the demilitarized zone (DMZ) increases security as follows: ■ The DMZ is a restricted area in which the number of ports that are allowed for specific hosts is highly controlled ■ The DMZ exists between the external firewall and the internal firewall. The common area in this example is the web server. The external firewall blocks all ports except for the HTTP (standard) and HTTPS (secure) web ports. The internal firewall blocks all ports except for NetBackup and database ports. The DMZ eliminates the possibility of external Internet access to internal NetBackup server and database information. The DMZ provides a "safe" area of operation for the web server client 5 and encrypted client 6 between the internal firewall and external firewall. The web server client 5 in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports. The web server client 5 can also communicate through the external firewall to the Internet using only HTTP ports. Figure 2-3 shows an example internal and external firewall with DMZ.

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

Figure 2-3 Example firewalls and DMZ

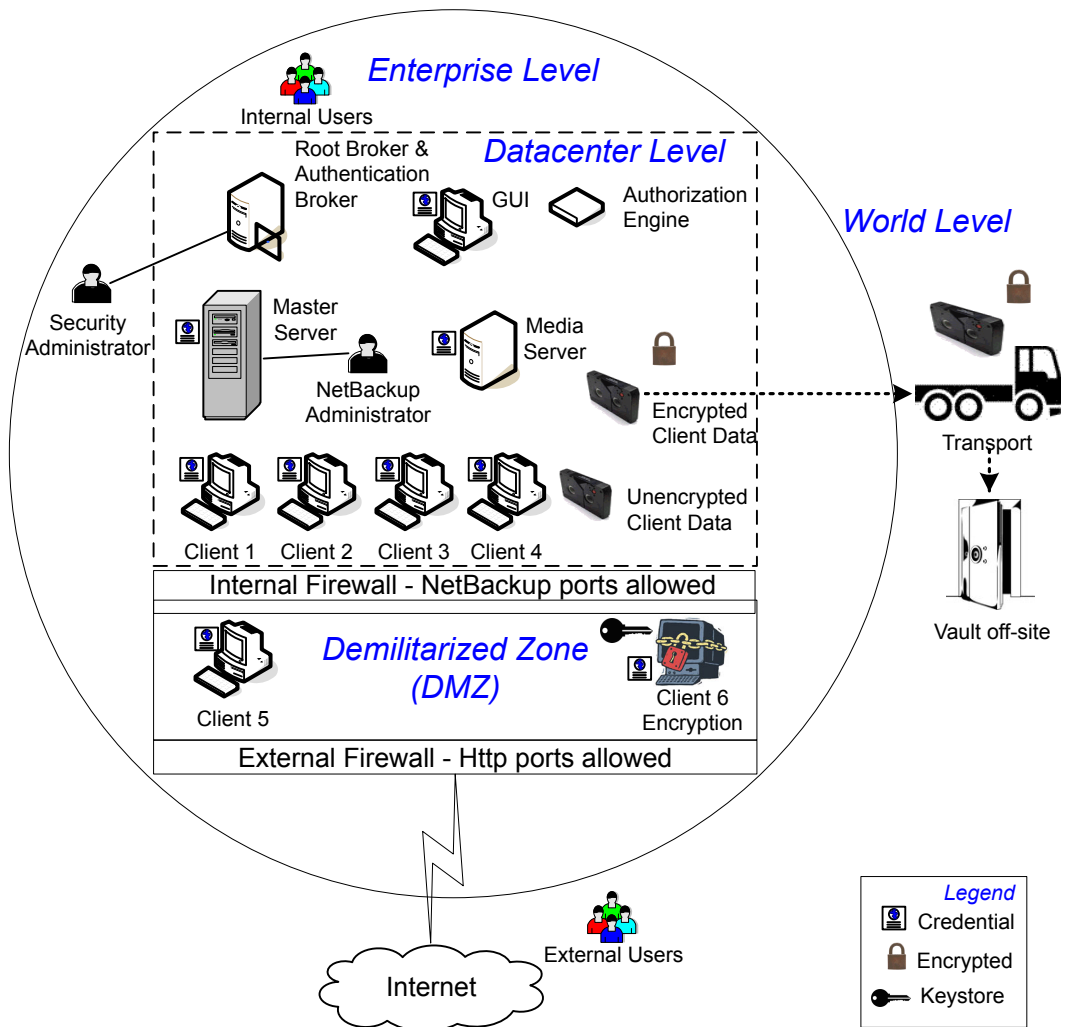


Combined world, enterprise, and datacenter levels

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

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

Figure 2-4 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 2-6 Security implementation types

Security implementation type	Characteristics	Complexity	Security deployment models
See “Operating system security” on page 54.	- Operating system dependent - Varies based on system components	Variable	Workgroup Single datacenter Multi-datacenter
See “Standard NetBackup security” on page 55.	- Manage as root or administrator - Data is not encrypted	Low	Workgroup with NetBackup Single datacenter with standard NetBackup Multi-datacenter with standard NetBackup
See “Client side encryption security” on page 56.	- Data is encrypted on the client - Encrypted data is sent over the wire - Can affect CPU performance on the client - Location of keys	Medium	Single datacenter with client side encryption Multi-datacenter with client side encryption
See “NBAC on primary, media server, and graphical user interface security” on page 58.	- NBAC gives authorization to access primary and media servers - Authenticates the system and users to access primary and media servers	Medium	Single datacenter with NBAC on primary and media servers Multi-datacenter with NBAC on primary and media servers
See “NBAC complete security” on page 60.	- NBAC gives authorization throughout the system - NBAC gives authentication throughout the entire system (servers, clients, and users)	High	Single datacenter with NBAC complete Multi-datacenter with NBAC complete

Operating system security

Operating system security can be enhanced for primary 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

It is recommended to have protective measures 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 following websites for information on possible security vulnerability issues:
<https://support.cohesity.com/s/>
<https://www.veritas.com/security>
- Use email contacts for possible security vulnerability issues:
secure@veritas.com

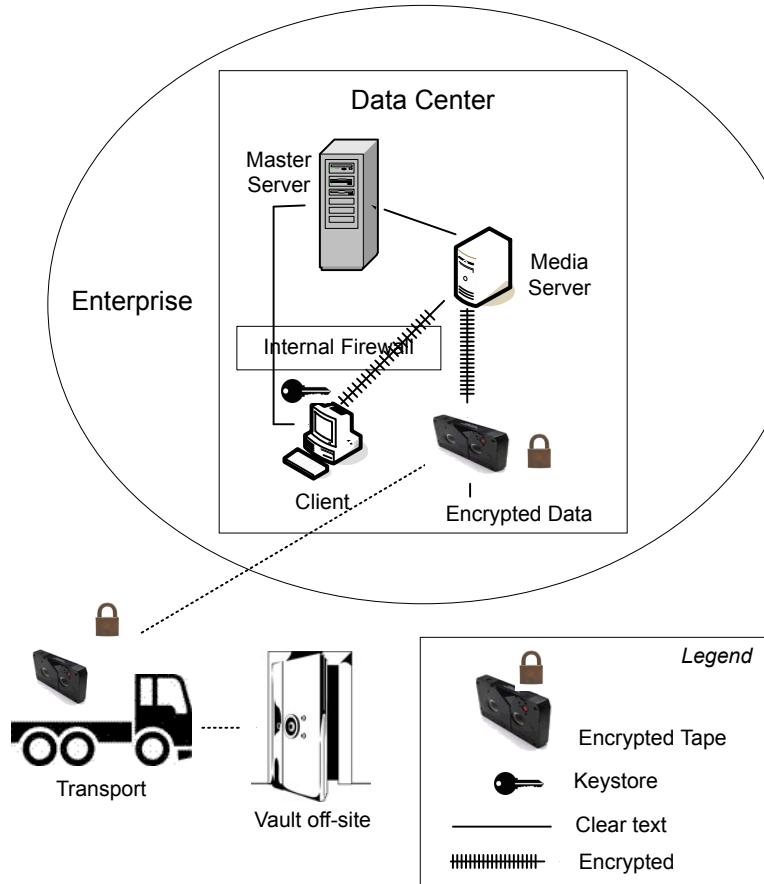
Standard NetBackup security

The standard NetBackup security only includes the security that is offered by the operating system and the hardware components of the datacenter. The authorized NetBackup users administer as root or administrator. Client data is not encrypted. The primary server, media server, and client are all run within a local enterprise datacenter. Unencrypted data is usually stored on site, presenting a relatively high

risk for no disaster recovery plan. Data 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 2-5 Standard NetBackup



Client side encryption security

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

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

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

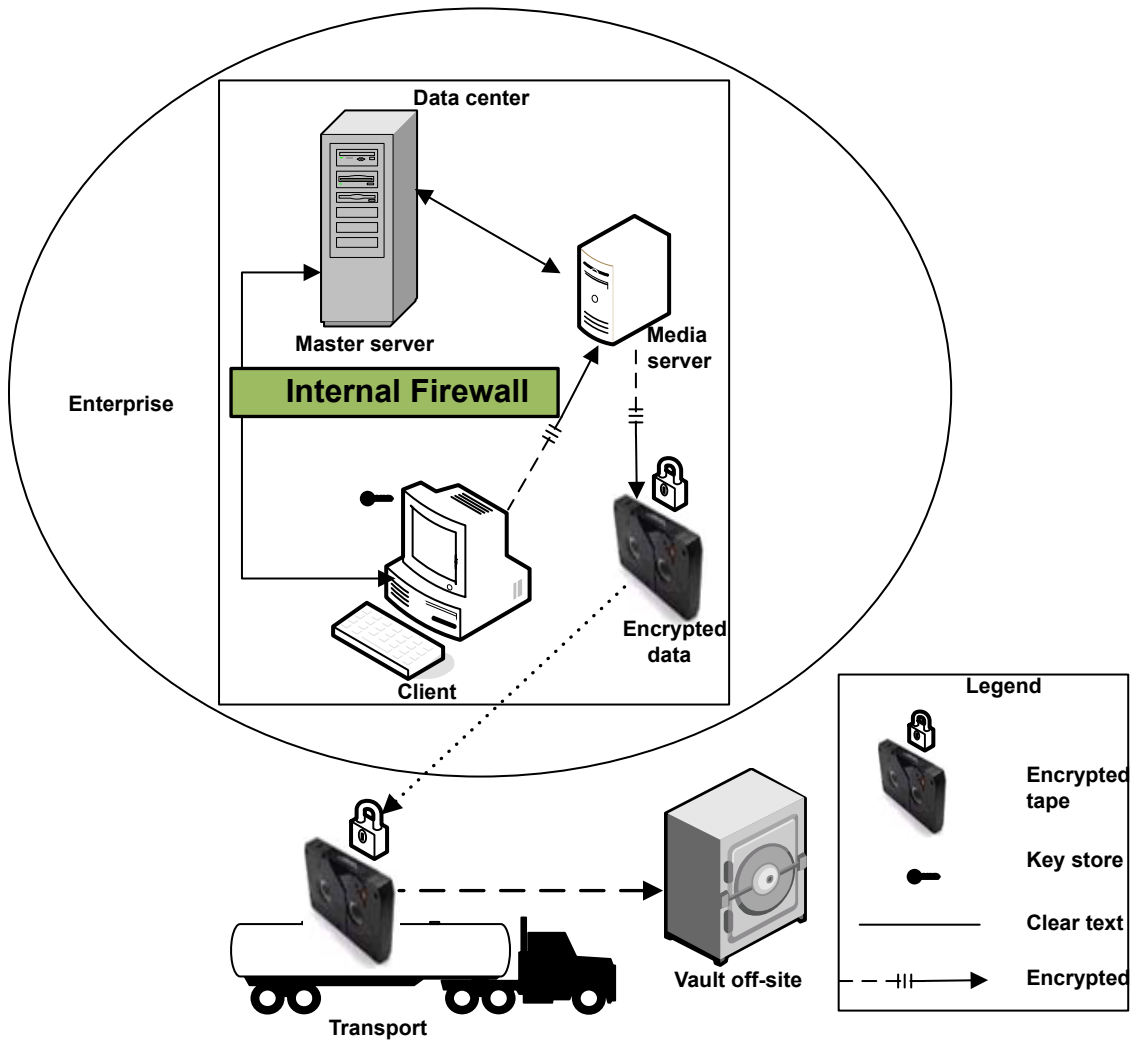
The following backup policy types do not support the Client Encryption Option. You cannot select the encryption check box in the policy attributes interface for these policy types.

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

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

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

Figure 2-6 Client side encryption



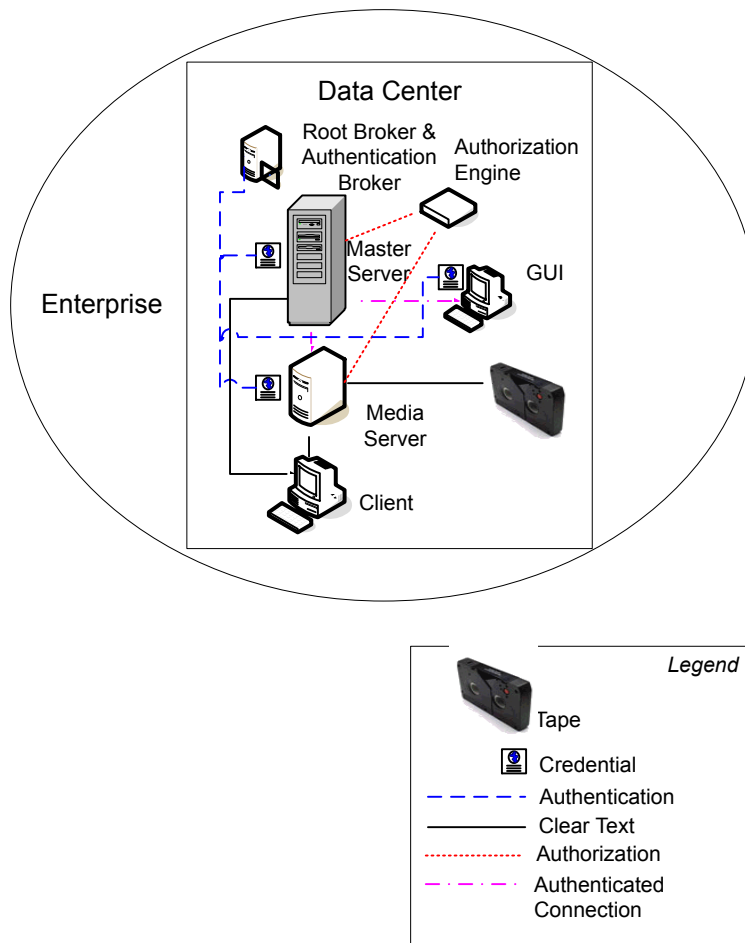
NBAC on primary, media server, and graphical user interface security

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

example uses the NetBackup Access Control on the primary 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 primary and media server configuration.

Figure 2-7 NBAC on primary and media server



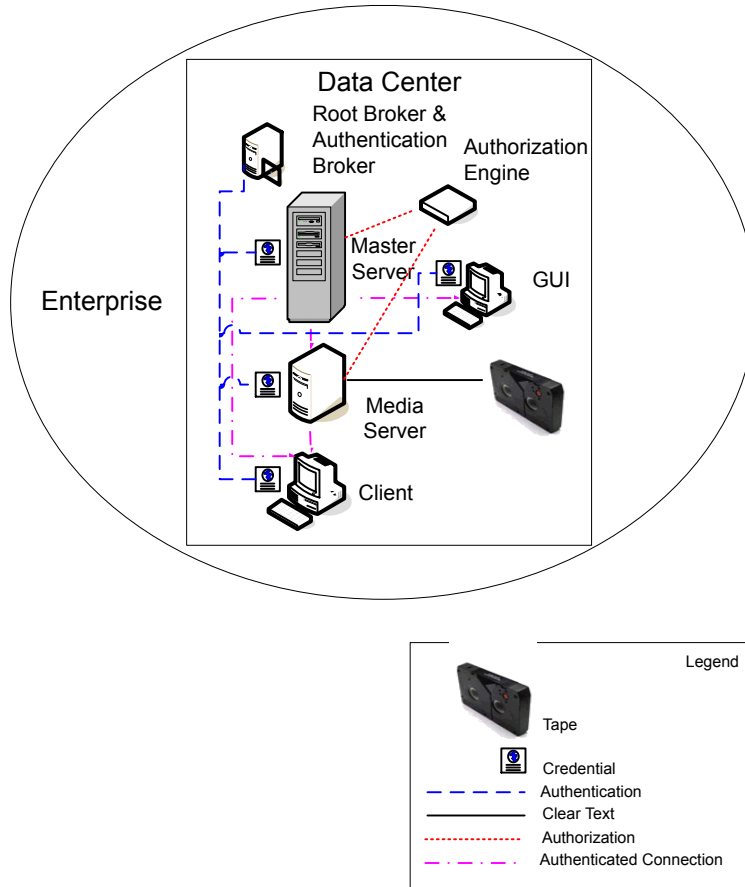
NBAC complete security

The NBAC complete security method uses the authentication broker to provide credentials to the primary server, media server, and client. This environment is very similar to the NBAC primary, 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 2-8 NBAC complete



Security deployment models

This chapter includes the following topics:

- [Workgroups](#)
- [Single datacenters](#)
- [Multi-datacenters](#)
- [Workgroup with NetBackup](#)
- [Single datacenter with standard NetBackup](#)
- [Single datacenter with client side encryption](#)
- [Single datacenter with NBAC on primary and media servers](#)
- [Single datacenter with NBAC complete](#)
- [Multi-datacenter with standard NetBackup](#)
- [Multi-datacenter with client side encryption](#)
- [Multi-datacenter with NBAC on primary and media servers](#)
- [Multi-datacenter with NBAC complete](#)

Workgroups

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

An example workgroup is shown as follows:

- See [“Workgroup with NetBackup”](#) on page 63.

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 66.
- See [“Single datacenter with client side encryption”](#) on page 68.
- See [“Single datacenter with NBAC on primary and media servers”](#) on page 71.
- See [“Single datacenter with NBAC complete”](#) on page 75.

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 78.
- See [“Multi-datacenter with client side encryption”](#) on page 80.
- See [“Multi-datacenter with NBAC on primary and media servers”](#) on page 85.
- See [“Multi-datacenter with NBAC complete”](#) on page 89.

Workgroup with NetBackup

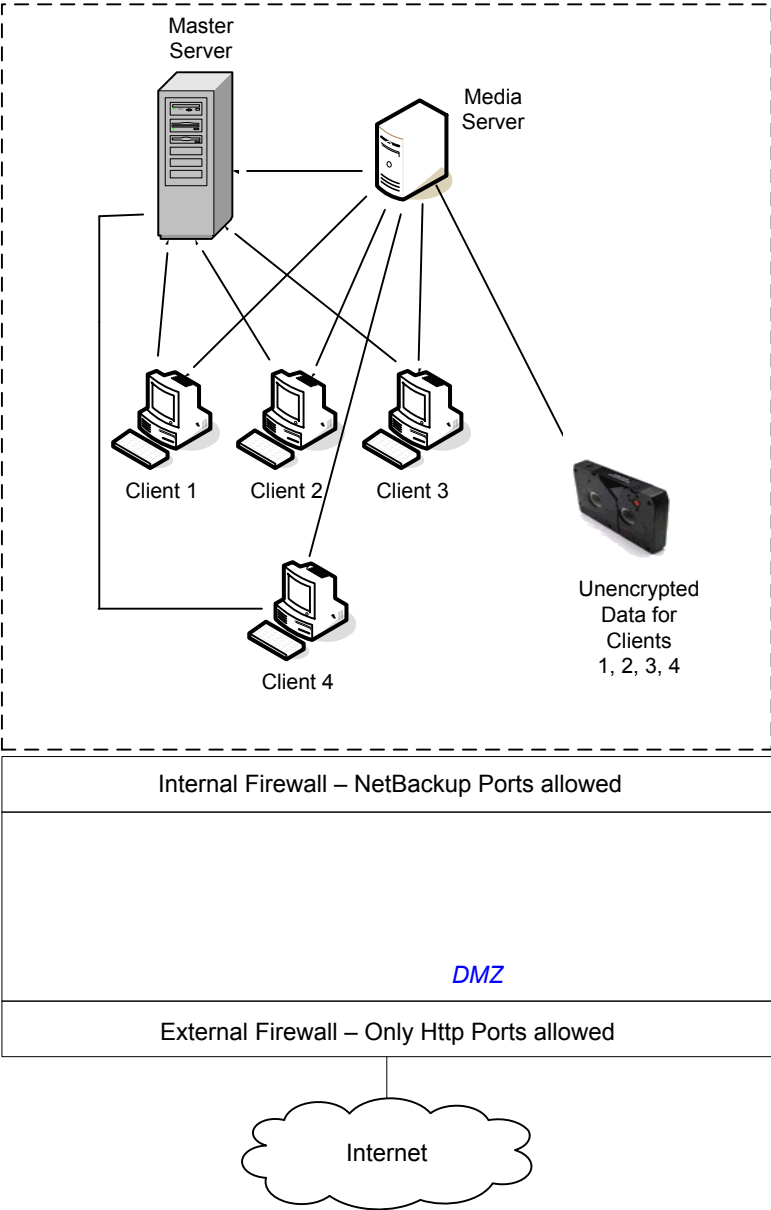
A workgroup with NetBackup is classified as a small group of systems (less than 50). The workgroup is used with NetBackup internally. Typically, this configuration does not have a unified naming service such as NIS or Active Directory. It may not have an authoritative host naming service such as DNS 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 3-1 shows an example workgroup with NetBackup.

Figure 3-1 Workgroup with NetBackup



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

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

Single datacenter with standard NetBackup

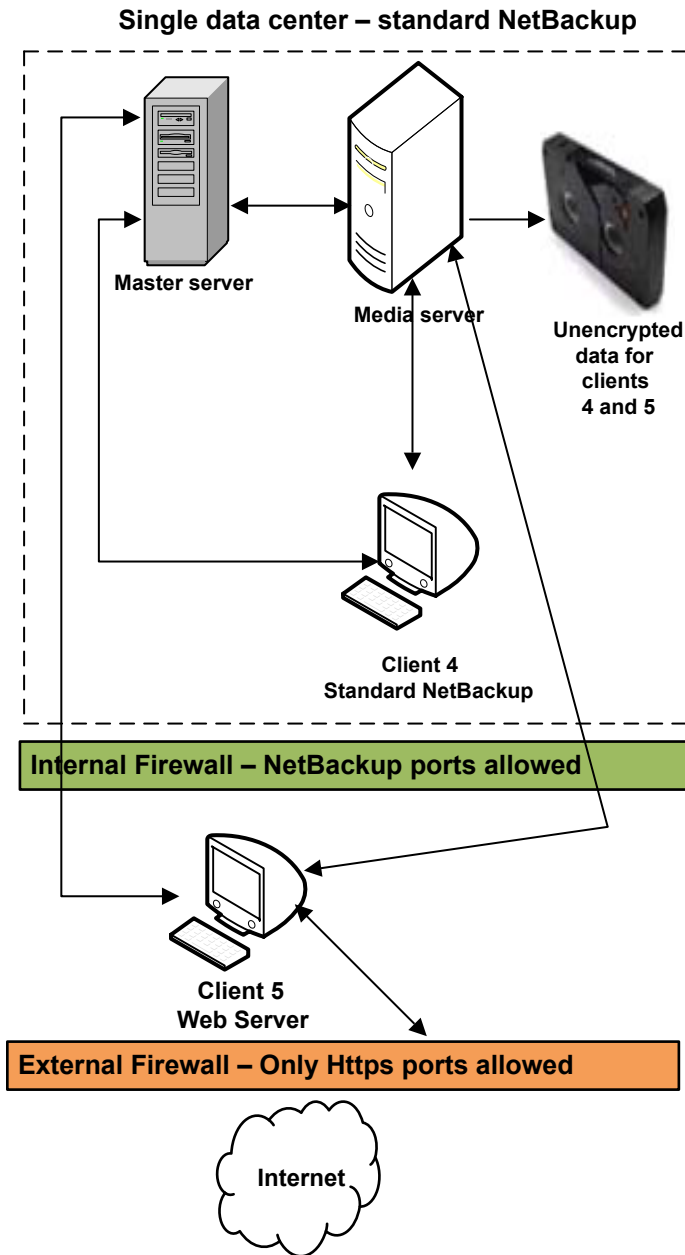
A single datacenter with standard NetBackup is defined as a medium to large group of hosts (greater than 50). It includes the hosts that are both internal only and those that expand through the DMZ to the Internet. This configuration typically has centralized naming service for hosts (such as DNS or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

The single datacenter with standard NetBackup includes the following highlights:

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

[Figure 3-2](#) shows an example single datacenter with standard NetBackup.

Figure 3-2 Single datacenter with standard NetBackup



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

Table 3-2 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 primary 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 primary server manages both clients and have their unencrypted data backed up to tape by the media server. Client 4 exists in the datacenter. Client 5 exists in the DMZ. Client 5 communicates to NetBackup using NetBackup only ports through the internal firewall. Client 5 receives connections from the Internet using HTTP only ports through the external firewall. Note that all NetBackup traffic for the lookup is sent unencrypted over the wire.
Internal firewall	Enables NetBackup to access Web server NetBackup client 5 in the DMZ. Only selected NetBackup ports and possibly other application ports are enabled for data communication into and out of the DMZ. HTTP ports that are open in the external firewall cannot pass through the internal firewall from the Internet.
Demilitarized Zone (DMZ)	Provides a "safe" area of operation for NetBackup client 5, Web server , that exists between the internal firewall and external firewall. Client 5 in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports. The Web server client 5 can communicate through the external firewall to the Internet using HTTP ports.
External firewall	Allows external users to access the Web server client 5 located in the DMZ from the Internet over HTTP ports. NetBackup ports are open for client 5 to communicate through the internal firewall. Caution: NetBackup ports are not allowed to pass through the external firewall to the Internet. Only the HTTP ports to client 5 are open in the external firewall to the Internet.
Internet	Specifies a collection of interconnected computer networks that are linked by copper wires, fiber-optic cables and wireless connections. The Web server client 5 can receive connections over the Internet using HTTP ports through the external firewall.

Single datacenter with client side encryption

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

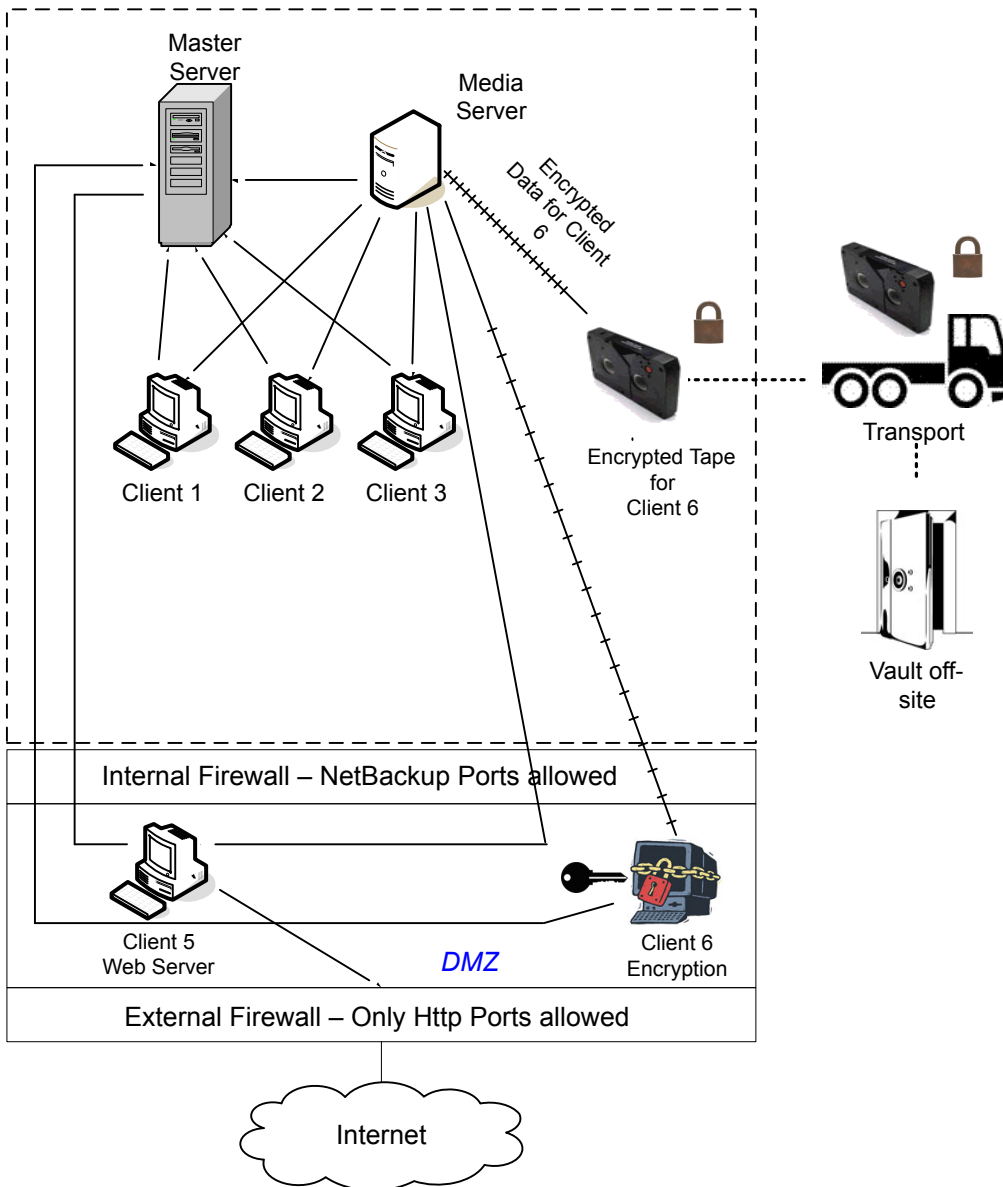
client side encryption mitigates the risk of passive wire tapping within the organization. The risk of data exposure is reduced as tapes are moved off site. This datacenter model assures a medium to large number (greater than 50) of managed hosts. Clients inside the datacenter as well as the DMZ can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

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

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

[Figure 3-3](#) shows an example single datacenter with client side encryption.

Figure 3-3 Single datacenter with client side encryption



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

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

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

Single datacenter with NBAC on primary and media servers

The single datacenter with NBAC on primary servers and media servers example uses the NetBackup Access Control on the primary 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.

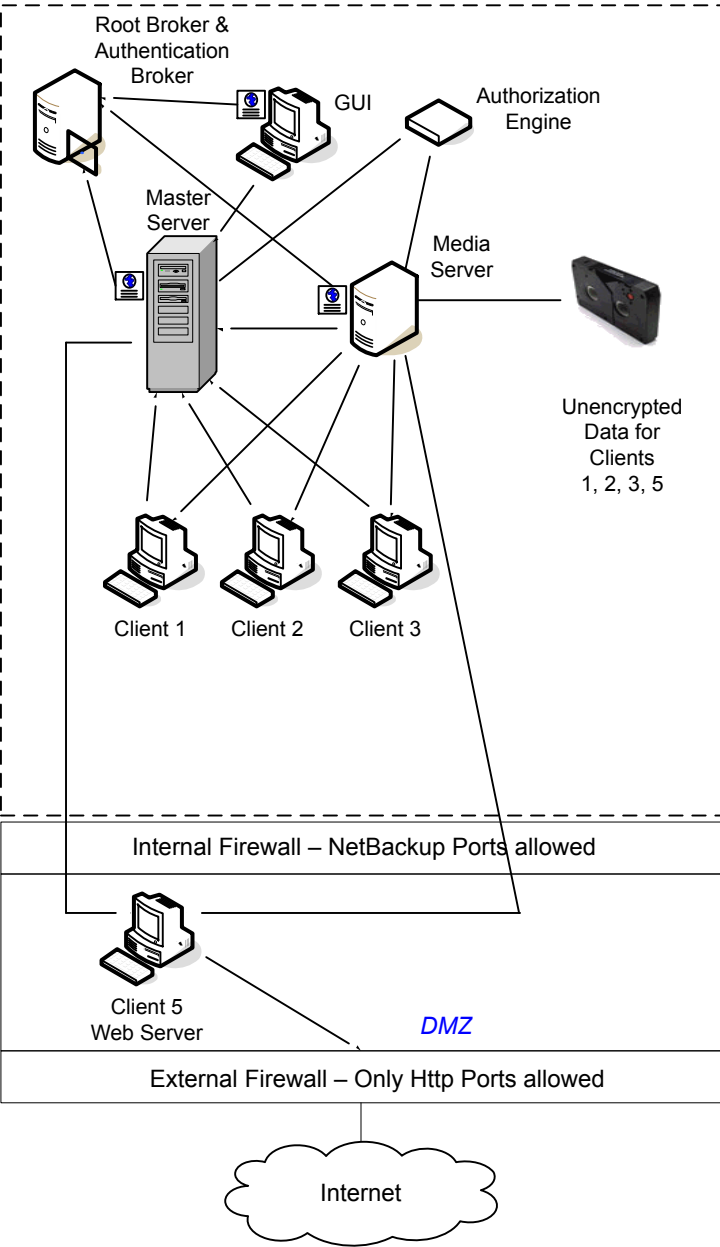
The single datacenter with NBAC on primary and media servers includes the following highlights:

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

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

[Figure 3-4](#) shows an example single datacenter with NBAC on primary and media servers.

Figure 3-4 Single datacenter with NBAC on primary and media servers



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

Table 3-4 NetBackup parts for a single datacenter with NBAC on the primary and media servers

Part	Description
Primary server	Communicates with the media server, root, and authentication broker. It also communicates with the authorization engine, clients 1, 2, 3, and client 5, Web server, in the DMZ. The primary server also communicates with and receives a credential from the authentication broker. When a CLI or GUI accesses a daemon on a primary server, a credential is exchanged to identify the user. The authorization engine is then contacted to determine accessibility to the daemons functions.
Media server	Communicates with the primary server, clients 1, 2, 3, and client 5, Web server, in the DMZ. The media server also communicates with the authorization engine and receives a credential from the authentication broker. The media server enables the writing of unencrypted data to tape for clients 1, 2, 3, and 5. When a CLI or GUI accesses a daemon on a media server, a credential is exchanged to identify the user. The authorization engine is then contacted to determine accessibility to the daemons functions.
GUI	Specifies that this remote administration console GUI receives a credential from the authentication broker. The GUI then uses this credential to gain access to functionality on the media servers and primary 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 primary server, media server, and GUI by establishing credentials with each. If a command prompt is used, the authentication broker also authenticates a user.
Authorization engine	Communicates with the primary server and media server to determine permissions of an authenticated user. These permissions determine the functionality available to the user. It also stores user groups and permissions. Only one authorization engine is needed. Note: The authorization engine resides on the primary server as a daemon process. It is shown in the figure as a separate image for the example only.
Tape	Contains unencrypted backup data that is written for clients 1, 2, 3, and 5.
Clients	Specifies that clients 1, 2, and 3 are standard NetBackup types and client 5 is a Web server type. Both types are managed by the primary 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 3-4 NetBackup parts for a single datacenter with NBAC on the primary 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

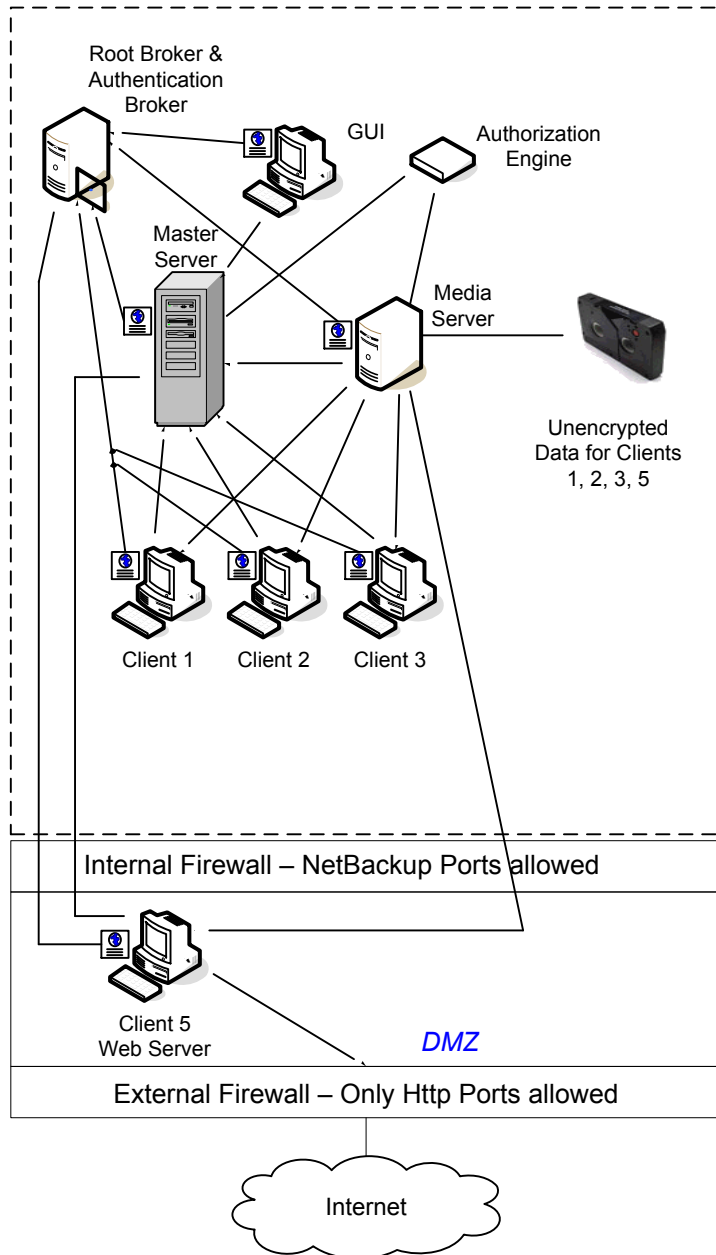
The single datacenter with NBAC complete environment is very similar to the single datacenter with NBAC primary and media server. The main differences are that all of the hosts that participate in the NetBackup environment are reliably identified using credentials. And non-root administrators can manage 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 primary and media server, except for root or administrator on client
- On client systems, non-root / administrator users may be configured to do local backup and restores (setup by default)
- The environment facilitates trusted identification of all hosts participating in NetBackup
- All hosts should have the required NetBackup version

Figure 3-5 shows an example single datacenter with NBAC complete.

Figure 3-5 Single datacenter with NBAC complete



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

Table 3-5 NetBackup parts for a single datacenter with NBAC complete

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

Table 3-5 NetBackup parts for a single datacenter with NBAC complete
(continued)

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

Multi-datacenter with standard NetBackup

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

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

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

- NetBackup spans two or more geographic regions through a WAN
- Centralized naming services typically exist
- Greater than 50 hosts in size
- Simplest to configure; requires only general NetBackup knowledge
- Assumes no fear of passive data interception on the wire as the backup runs

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

Table 3-6 NetBackup parts for a multi-datacenter with standard NetBackup implemented

Part	Description
London datacenter	Contains the primary 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 primary server and media server 2 and client 10.
Primary server	Specifies that it is located in London and communicates with media server 1 in London. The primary server also communicates over the WAN with the media server 2 in Tokyo. The primary 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 primary 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 primary 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.

Table 3-6 NetBackup parts for a multi-datacenter with standard NetBackup implemented (*continued*)

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

Multi-datacenter with client side encryption

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

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

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

- NetBackup spans two or more geographic regions through a WAN
- Useful for protecting off-site data
- Data from client is encrypted and eliminates the passive interception of the data on the wire

- Key management is de-centralized on to the clients
- The original NetBackup encryption option
- Client CPU is used to perform encryption
- Must have the key to get data back. A lost key means lost data.
- Useful when you need to scan tapes off-site or you need confidentiality on the wire

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

Table 3-7 NetBackup parts for a multi-datacenter with client side encryption implemented

Part	Description
London datacenter	Contains the primary 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 primary 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.
Primary server	Specifies that the primary server is located in the London datacenter and communicates with media server 1 and clients 4, 5, and 6. The primary server also uses the WAN to communicate with media server 2, and clients 7, 10, 11, and 12 in Tokyo.

Table 3-7 NetBackup parts for a multi-datacenter with client side encryption implemented (*continued*)

Part	Description
Media servers	Specifies that the multi-datacenter uses two media servers. Media server 1 is located in the London datacenter and media server 2 is located in the Tokyo datacenter. In London, media server 1 communicates with the primary server and clients 4, 5, and 6. Media server 1 also communicates with client 7 in Tokyo. Media server 1 writes unencrypted data to tape for clients 4 and 5. Media server 1 writes encrypted data to tape for clients 6 and 7. Note that client 7 is located in Tokyo but its tape backup is located in London. The encrypted tape for clients 6 and 7 is transported off-site to a vault in London. In Tokyo, media server 2 communicates with the primary 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.
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.
Tapes	Specifies that both unencrypted and encrypted data tapes are produced in the London datacenter and in the Tokyo datacenter. The encrypted tape contains client side encrypted backup data. In London, the unencrypted tape is written for clients 4 and 5 and stored on-site at the London datacenter. The encrypted tape is written for clients 6 and 7. The encrypted tape is transported off-site to a vault in London for disaster recovery protection. In Tokyo, the unencrypted tape is written for clients 10 and 11 and stored on-site at the Tokyo datacenter. The encrypted tape is written for clients 7 and 12. Note that even though client 7 is located in Tokyo and is backed up in Tokyo, client 7 is also backed up in London. The encrypted tape is transported off-site to a vault in Tokyo for disaster recovery protection. Note: To decrypt the data, the key(s) used to encrypt the data must be made available.
Transports	Specifies that the multi-datacenter uses two transports. One transport is located in London and the other is located in Tokyo. The transport truck in London moves the encrypted tape for clients 6 and 7 off-site to a secure London vault facility. The transport truck in Tokyo moves the encrypted tape for clients 7 and 12 off-site to a secure Tokyo vault facility. Note that a backup copy of client 7 is vaulted both in London and in Tokyo. Note: If in the remote case a tape is lost during transport, the datacenter manager has potentially reduced the risk of a data breach. The breach is reduced through the use of client side data encryption.

Table 3-7 NetBackup parts for a multi-datacenter with client side encryption implemented (*continued*)

Part	Description
Vaults off-site	Specifies that the multi-datacenter uses two vaults off-site. One vault is located in London and the other is located in Tokyo. Both vaults provide safe encrypted tape storage facilities off-site at different locations than the datacenters. Note: Storing the encrypted tapes at locations separate from the datacenters promotes good disaster recovery protection.
Clients	Specifies that the clients are located in both the London and Tokyo datacenters. In London, client 4 is a standard NetBackup type. Client 5 is a Web server type located in the DMZ. Client 6 is client side encrypted and is also located in the DMZ. All client types can be managed by the primary server and have their data backed up to tape through media server 1. Clients 5 and 6 communicate to NetBackup using NetBackup only ports through the internal firewall. Client 6 receives connections from the Internet using HTTP only ports through the external firewall. In Tokyo, client 7 is a client side encrypted client but outside of the DMZ. Client 10 is a standard NetBackup type. Client 11 is a Web server type located in the DMZ. Client 12 is client side encrypted also located in the DMZ. All client types can be managed by the primary server in London. Client 7 data is backed up to tape through media server 1 and 2. Client 10, 11, and 12 data is backed up to tape through media server 2. Clients 11 and 12 communicate to NetBackup using NetBackup only ports through the internal firewall. Client 12 receives connections from the Internet using HTTP only ports through the external firewall.
Internal firewalls	Specifies that the multi-datacenter uses two internal firewalls. One internal firewall is located in London and the other is located in Tokyo. In London, the internal firewall allows NetBackup to access Web server client 5 and client side encrypted client 6 in the DMZ. In Tokyo, the internal firewall lets NetBackup access Web server client 11 and client side encrypted client 12 in the DMZ. Only selected NetBackup ports and possibly other application ports are enabled for data communication into and out of the DMZ. HTTP ports that are open in the external firewall cannot pass through the internal firewall.

Table 3-7 NetBackup parts for a multi-datacenter with client side encryption implemented (*continued*)

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

Multi-datacenter with NBAC on primary and media servers

A multi-datacenter with NBAC on the primary 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 primary 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 primary and media servers includes the following highlights:

- NetBackup spans two or more geographic regions through a WAN
- Administer as non-root users
- Administer UNIX with a Windows User ID.
- Administer Windows with a UNIX account.
- Segregate and limit the actions of specific users.
- Root or Administrator or client hosts can still perform local client backups and restores
- Can be combined with other security-related options
- All servers must be NetBackup version 7.7 or later.

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

Table 3-8 NetBackup parts used for a multi-datacenter with NBAC on the primary and media servers

Part	Description
London datacenter	Specifies that the London datacenter contains the root broker, authentication broker 1, GUI 1, authorization engine, primary 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 primary server with GUI 2, media server 2, and clients 10 and 11.
Primary server	Specifies that the primary 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 primary server communicates with clients 4 and 5 in London. The primary server also communicates with GUI 2, media server 2, and clients 10 and 11 in Tokyo.
Media servers	Specifies that in this multi-datacenter example, there are two media servers. Media server 1 is located in the London datacenter and media server 2 is located in the Tokyo datacenter. In London, media server 1 communicates with the primary server, root broker and authentication broker 1, authorization engine, and clients 4 and 5. Media server 1 writes unencrypted data to tape for clients 4 and 5. In Tokyo, media server 2 communicates with the primary 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.
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 primary servers. In London, GUI 1 receives a credential from authentication broker 1. GUI 1 has access to functionality on the primary 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 primary server and media servers 1 and 2.

Table 3-8 NetBackup parts used for a multi-datacenter with NBAC on the primary and media servers *(continued)*

Part	Description
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 primary 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 primary server, media server 1, and GUI 1. All NetBackup servers and clients in Tokyo and London authenticate to authentication broker 1 in London. GUI 1 authenticates to authentication broker 1 in London. GUI 2 authenticates to authentication broker 2 in Tokyo.
Authorization engine	Specifies that in a multi-datacenter installation there is only one authorization engine required. The authorization engine communicates with the primary 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 primary 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 primary server as a daemon process. It is shown in the figure as a separate image for example only.
Tapes	Specifies that unencrypted data tapes are produced in the London datacenter and in the Tokyo datacenter. In London, the unencrypted tape is written for clients 4 and 5 and stored on-site at the London datacenter. In Tokyo, the unencrypted tape is written for clients 10 and 11 and stored on-site at the Tokyo datacenter.

Table 3-8 NetBackup parts used for a multi-datacenter with NBAC on the primary and media servers *(continued)*

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

Table 3-8 NetBackup parts used for a multi-datacenter with NBAC on the primary and media servers (*continued*)

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

Multi-datacenter with NBAC 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 primary 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 primary and media server except for root or administrator on client. The non-root administration of clients and servers is permitted in this configuration.
- On client systems, non-root / administrator users can be configured to perform local backup and restores (setup by default)
- The environment facilitates trusted identification of all hosts participating in NetBackup
- Requires all hosts to be at NetBackup version 7.7 or later.

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

Table 3-9 NetBackup parts used for a multi-datacenter with NBAC complete implemented

Part	Description
London datacenter	Specifies that the London datacenter contains the root broker, authentication broker 1, GUI 1, authorization engine, primary 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 primary server to GUI 2, media server 2, and clients 10 and 11. Finally the WAN connects media server 1 to client 10.
Primary server	Specifies that the primary 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 primary server further communicates with GUI 2 and media server 2, and clients 10 and 11 in Tokyo.

Table 3-9 NetBackup parts used for a multi-datacenter with NBAC complete implemented (*continued*)

Part	Description
Media servers	Specifies that in this multi-datacenter example there are two media servers. Media server 1 is located in the London datacenter and media server 2 is located in the Tokyo datacenter. In London, media server 1 communicates with the primary server, root broker and authentication broker 1, authorization engine, and clients 1, 5, and 10. Media server 1 writes unencrypted data to tape for clients 1, 5, and 10. In Tokyo, media server 2 communicates with the primary server, root broker, and authentication broker 1 and authorization engine in London through the WAN. Media server 2 also communicates with GUI 2, and clients 10 and 11 in Tokyo. Media server 2 writes unencrypted data to tape for clients 10 and 11.
GUIs	Specifies that in this multi-datacenter example, there are two GUIs. GUI 1 is in London and GUI 2 is in Tokyo. These remote administration console GUIs receive credentials from the authentication brokers. The GUIs then use the credentials to gain access to functionality on the media servers and primary servers. In London, GUI 1 receives a credential from authentication broker 1. GUI 1 has access to functionality on the primary 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 primary server and media servers 1 and 2.
Root broker	Specifies that there is only one root broker required in a multi-datacenter installation. Sometimes the root broker is combined with the authentication broker. In this example the root broker and authentication broker are shown as the same component and are located in the London datacenter. In London, the root broker authenticates the authentication broker 1, also in London, and authentication broker 2 in Tokyo. The root broker does not authenticate clients.
Authentication brokers	Specifies that there can be more than one authentication broker in a datacenter installation. Sometimes the authentication broker can be combined with the root broker. In this datacenter installation, there are two authentication brokers. The authentication broker authenticates the primary 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 primary 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.

Table 3-9 NetBackup parts used for a multi-datacenter with NBAC complete implemented (*continued*)

Part	Description
Authorization engine	Specifies that there is only one authorization engine required in a datacenter installation. The authorization engine communicates with the primary 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 primary 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 primary 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.
Clients	Specifies that the clients are located in both the London and Tokyo datacenters. In London, client 1 is a standard NetBackup type. Client 5 is a Web server type located in the DMZ. All client types can be managed by the primary server and have their data backed up to tape through media server 1. Client 5 communicates to NetBackup using NetBackup only ports through the internal firewall. Client 5 also receives connections from the Internet using HTTP only ports through the external firewall. In Tokyo, client 10 is a standard NetBackup type. Client 11 is a Web server type located in the DMZ. All client types can be managed by the primary server and have their data backed up to tape through media server 2. Client 11 communicates to NetBackup using NetBackup only ports through the internal firewall. Client 11 also receives connections from the Internet using HTTP only ports through the external firewall
Internal firewalls	Specifies that there can be two internal firewalls in this multi-datacenter example. One internal firewall is located in London and the other is located in Tokyo. In London, the internal firewall lets NetBackup access Web server client 5 in the DMZ. In Tokyo, the internal firewall lets NetBackup access Web server client 11 in the DMZ. Only selected NetBackup ports and possibly other application ports are enabled for data communication through the internal firewall and into and out of the DMZ. HTTP ports that are open in the external firewall are not allowed to pass through the internal firewall.

Table 3-9 NetBackup parts used for a multi-datacenter with NBAC complete implemented (*continued*)

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

Auditing NetBackup operations

This chapter includes the following topics:

- [About NetBackup auditing](#)
- [Viewing the current audit settings](#)
- [About audit events](#)
- [Audit retention period and catalog backups of audit records](#)
- [Viewing the detailed NetBackup audit report](#)
- [User identity in the audit report](#)
- [Disabling auditing](#)
- [Audit alert notification for audit failures \(NetBackup BAR Console\)](#)
- [Send audit events to system logs](#)
- [SYSLOG_AUDIT_USE_OCSF_FORMAT for NetBackup primary server](#)

About NetBackup auditing

Auditing is enabled by default in new installations. NetBackup auditing can be configured directly on a NetBackup primary server.

Auditing of NetBackup operations provides the following benefits:

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

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

- A method for customers to adhere to internal change management policies.
- Help for NetBackup Support in troubleshooting problems for customers.

About the NetBackup Audit Manager

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

An administrator can search specifically for:

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

Note the following:

- The audit record truncates any entries greater than 4096 characters. (For example, policy name.)
- The audit record truncates any restore image IDs greater than 1024 characters.

Actions that NetBackup audits

NetBackup records the following user-initiated actions.

Activity monitor actions	Canceling, suspending, resuming, restarting, or deleting any type of job creates an audit record.
Alerts and email notifications	If an alert cannot be generated or an email notification cannot be sent for NetBackup configuration settings. For example, SMTP server configuration and the list of excluded status codes for alerts.
Anomalies	When a user reports an anomaly as false positive, the action is audited and logged for that user.
Malware detection	When malware scan is triggered, malware scan status and malware scan configuration actions are audited.
Asset actions	Deleting an asset, such as a vCenter server, as part of the asset cleanup process is audited and logged. Creating, modifying, or deleting an asset group as well any action on an asset group for which a user is not authorized is audited and logged.

Authorization failure	Authorization failure is audited when you use the NetBackup web UI, or the NetBackup APIs.
Catalog information	This information includes: ■ Verifying and expiring images. ■ Read the requests that are sent for the front-end usage data.
Certificate management	Creating, revoking, renewing, and deploying of NetBackup certificates and specific NetBackup certificate failures.
Certificate Verification Failures (CVFs)	Any failed connection attempts that involve SSL handshake errors, revoked certificates, or host name validation failures. For certificate verification failures (CVFs) that involve SSL handshakes and revoked certificates, the timestamp indicates when the audit record is posted to the primary server. (Rather than when an individual certificate verification fails.) A CVF audit record represents a group of CVF events over a time period. The record details provide the start and the end times of the time period as well as the total number of CVFs that occurred in that period.
Disk pools and Volume pools actions	Adding, deleting, or updating disk or volume pools.
Hold operations	Creating, modifying, and deleting hold operations.
Host database	NetBackup operations that are related to the host database.
IRE configuration and states	Adding, updating, and deleting IRE allowed subnets or schedule. IRE external network is opened or closed by IRE schedule or by an administrator.
Logon attempts	Any successful or any failed logon attempts for the NetBackup web UI or the NetBackup APIs.
Policies actions	Adding, deleting, or updating policy attributes, clients, schedules, and backup selections lists.
Restore and browse image user actions	All the restore and browse image content (<code>bplist</code>) operations that a user performs are audited with the user identity. To set an interval to periodically add audit records of the browse image (<code>bplist</code>) operations from the cache into the NetBackup database, use the <code>DATAACCESS_AUDIT_INTERVAL_HOURS</code> configuration option. Setting this configuration option prevents the NetBackup database size from increasing exponentially because of the <code>bplist</code> audit records. See the NetBackup Administrator's Guide Volume I. To add all the <code>bplist</code> audit records from the cache into the NetBackup database, run the following command on the primary server: <pre>nbcertcmd -postAudit -dataAccess</pre>

Security configuration	Information that is related to changes that are made to the security configuration settings.
Starting a restore job	NetBackup does not audit when other types of jobs begin. For example, NetBackup does not audit when a backup job begins.
Starting and stopping the NetBackup Audit Manager (<code>nbaudit</code>).	Starting and stopping of the <code>nbaudit</code> manager is always audited, even if auditing is disabled.
Storage lifecycle policy actions	Attempts to create, modify, or delete a storage lifecycle policy (SLP) are audited and logged. However, activating and suspending an SLP using the command <code>nbslutil</code> are not audited. These operations are audited only when they are initiated from a NetBackup graphical user interface or API.
Storage servers actions	Adding, deleting, or updating storage servers.
Storage units actions	Adding, deleting, or updating storage units. Note: Actions that are related to storage lifecycle policies are not audited.
Token management	Creating, deleting, and cleanup of tokens and specific token issuing failures.
User 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. NetBackup status code 108 is returned (<code>Action succeeded but auditing failed</code>). The NetBackup does not return an exit status code 108 when auditing fails.

Actions that NetBackup does not audit

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

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

Rollback operations	Some operations are carried out as multiple steps. For example, creating an MSDP-based storage server consists of multiple steps. Every successful step is audited. Failure in any of the steps results in a rollback, or rather, the successful steps may need to be undone. The audit record does not contain details about rollback operations.
Host properties actions	Changes made with the <code>bpsetconfig</code> or the <code>nbsetconfig</code> commands, or the equivalent property in host properties, are not audited. Changes that are made directly to the <code>bp.conf</code> file or to the registry are not audited.

Viewing the current audit settings

To view the current audit configuration, use the `nbseccmd` command on the NetBackup primary server.

Alternatively, sign-in to the NetBackup web UI, go to **Global Security settings > Security Controls > Configure audit retention period**, and view the audit retention period.

To view the current audit settings

1 Log on to the primary server.

2 Open the following directory:

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

Linux: `/usr/opensv/netbackup/bin/admincmd`

3 Run the following command:

```
nbseccmd -getsecurityconfig -auditretentionperiod
```

4 The following configuration setting is listed:

Audit Retention Period: 90

About audit events

Events that are specific to the following security parameters are audited:

- Certificate
- Connection
- Host
- Login
- Security Configuration

- Token

See [“Viewing the detailed NetBackup audit report”](#) on page 101.

Viewing audit events

The **Audit Events** tab displays NetBackup events according to the audit categories that you select with the filter. NetBackup records a number of events that occur while you work with the product. For example, a security certificate is issued to a host, an authorization token is deleted, connection between hosts is established and so on.

To view status of audit events

- 1 Open the NetBackup web UI.
- 2 On the left, click **Security > Security events**.
- 3 Click the **Audit events** tab.
- 4 Click the filter icon to select the audit event categories that you want to view.
- 5 The following information is displayed.

Event	A brief description for the audit event that took place.
User	The user name and details related to the audit event.
Description	Full description of the audit event that took place.
Reason	The reason for the audit event, if provided by the user.

- 6 To see the details for an audit event, click on the name of the event.

Note: If you see audit records in the **Connection** category, make sure to review the record details. For certain records in this category, the **Date** field that is displayed in the details indicates when the audit record was posted to the primary server. It does not necessarily indicate when an individual event occurred. This type of audit record (for example, a certificate verification failure (CVF) record) represents a group of events that have occurred over a time period. The audit record details provide the **Beginning Event Time** and **Ending Event Time** of the time period as well as the **Event Count** (the total number of events that occurred in that time period).

Troubleshooting auditing issues related to the Access History tab

In the NetBackup web UI, open **Security** > **Security events**. Click the **Access History** tab. NetBackup displays the details about the login activities that the current user has performed.

If you observe that the required audit records are not being displayed on the **Access History** tab, ensure that the `bprd` service is running on the primary server.

Audit retention period and catalog backups of audit records

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

If no audit retention period is indicated, audit records are retained for 90 days, which is a default value. Set the audit retention period to 0 (zero) if you do not want to delete the audit records.

To configure the audit retention period

- 1 Log on to the primary server.
- 2 Run the following command:

```
bpnbat -login
```

- 3 Open the following directory:

Windows: `install_path\NetBackup\bin\admincmd`

UNIX: `/usr/opensv/netbackup/bin/admincmd`

- 4 Enter the following command:

```
nbseccmd -setsecurityconfig -auditretentionperiod number_of_days
```

The audit report is retained for the value that is specified for the *number_of_days* option.

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

```
nbseccmd -setsecurityconfig -auditretentionperiod 30
```

To ensure that audit records are backed up during catalog backups, configure the catalog backup frequency to be less frequent or equal to the value that you specify for `-auditretentionperiod`.

- 5 To check the current audit retention period, run the following command:

```
nbseccmd -getsecurityconfig -auditretentionperiod
```

Viewing the detailed NetBackup audit report

You can view the actions NetBackup audits from a primary server using the NetBackup web UI. You can see full audit event details with the `nbauditreport` command.

To view the full audit report

- 1 Log on to the primary server.
- 2 Enter the following command to display the audit report in the summary format.

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

UNIX: `/usr/opensv/netbackup/bin/admincmd/nbauditreport`

Or, run the command with the following options.

```
-sdate  
<"MM/DD/YY  
[HH:[MM[:SS]]]">
```

The start date and time of the report data you want to view.

```
-edate  
<"MM/DD/YY  
[HH:[MM[:SS]]]">
```

The end date and time of the report data you want to view.

`-ctgy category`

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

See the [NetBackup Commands Guide](#) for `-ctgy` options.

`-user`

Use to indicate the name of the user for whom you'd like to display audit information.

`<username[:domainname]>`

`-fmt DETAIL`

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

- `[-notruncate]` . Display the old and new values of a changed attribute on separate lines in the details section of the report.
- `[-pagewidth <NNN>]` . Set the page width for the details section of the report.

`-fmt PARSABLE`

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

- `[-order <DTU|DUT|TUD|UDT|UTD>]`. Indicate the order in which the information appears.
 - D (Description)
 - T (Timestamp)
 - U (User)

3 The audit report contains the following details:

DESCRIPTION	The details of the action that was performed.
USER	The identity of the user who performed the action. See "User identity in the audit report" on page 103.
TIMESTAMP	The time that the action was performed.
The following information only displays if you use the <code>-fmt DETAIL</code> or the <code>-fmt PARSABLE</code> options.	
CATEGORY	The category of user action that was performed.
ACTION	The action that was performed.
REASON	The reason that the action was performed. A reason displays if a reason was specified for the operation that created the change.
DETAILS	An account of all of the changes, listing the old values and the new values.

Example of the audit report:

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

Audit records fetched: 5
```

User identity in the audit report

The audit report indicates the identity of the user who performed a specific action. The full identity of the user includes the user name and the domain or the host name that is associated with the authenticated user.

A user's identity appears in the audit report as follows:

- Audit events always include the full user identity. Root users and administrators are logged as "root@hostname" or "administrator@hostname".
- The image browse and image restore events always include the user ID in the audit event.
- The order of the elements for the user principal is "domain:username:domainType:providerId". The domain value does not apply for Linux computers. For that platform, the user principal is :username:domainType:providerId.
- For any operations that do not require credentials or require the user to sign in, operations are logged without a user identity.

Disabling auditing

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

To disable auditing

- 1 Log on to the primary server.
- 2 Open the following directory:

Windows: *install_path\NetBackup\bin\admincmd*

UNIX: */usr/opensv/netbackup/bin/admincmd*

- 3 Enter the following command:

```
nbemmcmd -changesetting -AUDIT DISABLED -machinename primaryserver
```

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

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

Audit alert notification for audit failures (NetBackup BAR Console)

Use the alert notification option to choose if you want to be notified when an auditable action fails to create an audit record. This option is located in the status bar of the NetBackup BAR Console.

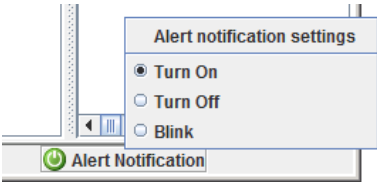


Table 4-1 Audit alert notification options

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

Send audit events to system logs

You can send NetBackup audit events to system logs. You must have the NetBackup Security Administrator role or similar RBAC permissions to perform this task.

By default, NetBackup sends the audit events to system logs in native format. You can now export audit events with the Open Cybersecurity Schema Framework (OCSF) format to Security Information and Event Management (SIEM) platforms.

See [this article](#) for more information.

Use the `SYSLOG_AUDIT_USE_OCSF_FORMAT` configuration option to send the NetBackup audit events to system logs in the OCSF format.

See [“SYSLOG_AUDIT_USE_OCSF_FORMAT for NetBackup primary server”](#) on page 106.

To send audit events to system logs

- 1 Open the NetBackup web UI.
- 2 On the left, select **Security > Security events**.
- 3 On the top right, click **Security event settings**.
- 4 Enable the **Send the audit events to the system logs** option.

- 5 Select **Select audit event** categories. Then select the audit categories for which you want to send the audit events to the system logs.

To send audit events for all audit categories to the system logs, select the **Audit event categories** check box.

- 6 Select **Save**.

You can view NetBackup audit events in the system logs. For example:

On a Windows system, use **Windows Event Viewer** to view NetBackup audit events.

On a Linux system, you can view the system logs on the configured location.

SYSLOG_AUDIT_USE_OCSF_FORMAT for NetBackup primary server

By default, NetBackup sends the audit events to system logs in native format.

Use the `SYSLOG_AUDIT_USE_OCSF_FORMAT` option to send the NetBackup audit events to system logs in the Open Cybersecurity Schema Framework (OCSF) format.

You can view NetBackup audit events in the system logs. For example, on a Windows system, use Windows Event Manager to view NetBackup audit events.

Table 4-2 SYSLOG_AUDIT_USE_OCSF_FORMAT

Usage	Description
Where to use	On NetBackup primary servers.
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: <pre>SYSLOG_AUDIT_USE_OCSF_FORMAT = TRUE</pre>
Equivalent NetBackup web UI property	No equivalent property on the web UI

Identity and access management

- [Chapter 5. About identity and access management](#)
- [Chapter 6. AD and LDAP domains](#)
- [Chapter 7. Access keys](#)
- [Chapter 8. API keys](#)
- [Chapter 9. Role-based access control](#)
- [Chapter 10. NetBackup interface access for OS Administrators](#)
- [Chapter 11. Smart card or digital certificate](#)
- [Chapter 12. Single Sign-On \(SSO\)](#)
- [Chapter 13. NetBackup Access Control Security \(NBAC\)](#)

About identity and access management

This chapter includes the following topics:

- [About access control in NetBackup](#)

About access control in NetBackup

NetBackup provides the following types of access control:

- **Role Based Access Control (RBAC) in the NetBackup web UI**
Beginning with the NetBackup 8.1.2 release, the NetBackup web user interface provides role-based access control for the settings and workloads in NetBackup. Refer to the [NetBackup Web UI Administrator's Guide](#) for more information.
- **Application access in the NetBackup BAR Console (default)**
NetBackup administrators can control who can view the various applications in NetBackup. Root users and administrators have full access to the **NetBackup BAR Console**. A non-root or non-administrator user can access the Backup, Archive, and Restore application. This user can also access additional applications, as defined for that user in the `auth.conf` file.
Access control is view-based, not role-based. The administrator can control the applications that a user can view and manage, but cannot control which tasks a user can perform based on their role in the organization. Access control is limited to the **NetBackup BAR Console**. (Interfaces like the Backup, Archive, and Restore client and the NetBackup MS SQL Client are not affected.)
- **NetBackup Access Control (NBAC)**
NBAC is the original role-based access control provided with NetBackup for the **NetBackup BAR Console** and the CLIs. It is recommended that you use one of the other methods of access control to manage your NetBackup environment.

Access control methods for NetBackup BAR Console and the CLIs

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

Table 5-1

Access and auditing	NetBackup BAR Console and <code>auth.conf</code>
Who can use the NetBackup BAR Console?	Root users and administrators have full access to the BAR Console. Non-root users or non-administrators are limited to the Backup, Archive, and Restore application by default. Otherwise, these users can access the applications that are defined for them in the <code>auth.conf</code> file.
Who can use the CLI?	Root users and administrators have full access to the CLI.
How is a user audited?	As root or administrator

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

AD and LDAP domains

This chapter includes the following topics:

- [Adding AD or LDAP domains in NetBackup](#)
- [Troubleshooting AD or LDAP domain configuration issues](#)
- [Certificate authorities trusted by the NetBackup Authentication Service](#)

Adding AD or LDAP domains in NetBackup

NetBackup supports Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain users.

If an AD domain or an LDAP domain is added in NetBackup, the respective domain users can logon to a NetBackup primary server and Security Administrator can assign role-based access control (RBAC) roles to these domain users.

See [“RBAC features”](#) on page 130.

The following procedure describes how to add an existing AD or LDAP domain in NetBackup and authenticate the domain users to access NetBackup.

To add an AD domain or an LDAP domain in NetBackup

- 1 Run the following command to add an AD domain or an LDAP domain in the NetBackup primary server:

```
vssat addldapdomain -d DomainName -s server_URL -u user_base_DN
-g group_base_DN [-f trusted_CA_file_name] [-tp TLS_protocol_version_to_be_disabled]
[-cs cipher_suite_list] [-t rfc2307 | msad | {-c user_object_class -a user_attribute
-q user_GID_attribute -un user_display_name_attribute -ui user_ID_attribute[:value_type]
-ud user_description_attribute -x group_object_class -y group_attribute
-z group_GID_attribute -gn group_display_name_attribute -gi group_ID_attribute[:value_type]
-gd group_description_attribute [-k DN | UID]]} [-b FLAT | BOB] -m admin_user_DN
[-w admin_user_password] [-p SUB | ONE | BASE] [-F]
```

Note: Ensure that the user name that is specified in the `-m` option has the required rights to query the AD or the LDAP server.

In case of LDAPS, if the Authentication Service (`nbatd`) does not trust the certificate authority (CA) that has signed the server's certificate, use the `-f` option to add the CA certificate in the `nbatd` trust store.

See [“Certificate authorities trusted by the NetBackup Authentication Service”](#) on page 121.

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

Contact your AD administrator for the correct values for these command-line options. The values may vary based on how your AD is setup.

An example to add an AD domain:

```
vssat addldapdomain -d domain1 -s ldap://domain1.veritas.com -u
"CN=Users,DC=domain1,DC=veritas,DC=com" -g "CN=Users,DC=domain1,DC=veritas,DC=com" -t msad -m
"CN=user1,CN=Users,DC=domain1,DC=veritas,DC=com" -b BOB
```

- 2 Run the `vssat validateprpl` command on the primary server to verify whether the specified AD or LDAP domain is successfully added or not.

```
validateprpl -p username -d ldap:domain_name -b
localhost:1556:nbatd
```

An example to validate an AD or LDAP domain:

```
vssat validateprpl -p user1 -d ldap:domain1 -b localhost:1556:nbatd
```

The domain name must match the one that is used in the `addldapdomain` command option.

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

If the AD or LDAP domain is added and the `vssat validateprpl` or `vssat validategroup` command fails, you need to carry out certain troubleshooting steps to resolve the issue.

See [“Troubleshooting AD or LDAP domain configuration issues”](#) on page 112.

Reconfigure the AD/LDAP domain for the nbatd containerized service

This procedure is applicable only for the AD/LDAP domain user. The local OS user and PAM authentication type are not supported.

Starting with NetBackup 10.5, in Cloud Scale deployment, the `nbatd` containerized service runs on a separate Kubernetes Pod cluster server instead of the primary server Kubernetes Pod. Therefore, the existing AD/LDAP domain configuration on the primary server Kubernetes Pod does not work. You must reconfigure the AD/LDAP domain.

To reconfigure the AD/LDAP domain

- 1 Delete the existing AD/LDAP domain from the `nbatd` Kubernetes Pod.
- 2 Add AD/LDAP domains in NetBackup.

See [“Adding AD or LDAP domains in NetBackup”](#) on page 110.

Troubleshooting AD or LDAP domain configuration issues

After you added an AD or LDAP domain configuration, verify the configuration using the `vssat validateprpl` and `vssat validategroup` commands. The commands validate the existing AD / LDAP user and group respectively.

A successful execution of the `vssat validateprpl` and the `vssat validategroup` commands implies that the associated AD or LDAP domain is successfully added.

For information about these commands, see the [NetBackup Commands Reference Guide](#).

If the commands fail, the following error message is displayed:

```
The principal or group does not exist.
```

Validation of AD or LDAP domain can fail because of any of the following reasons:

- Connection cannot be established with the AD or LDAP server
- Invalid user credentials
- Invalid user base DN or group base DN
- Multiple users or groups exist with the same name under the user base DN or the group base DN
- User or group does not exist

Connection cannot be established with the AD or LDAP server

To troubleshoot the issue

- 1 Check if the `nbatd` logs contain the following error:

```
(authldap.cpp) CAuthLDAP::validatePrpl - ldap_simple_bind_s()
failed for user 'CN=Test User,OU=VTRSUsers,DC=VRTS,DC=com', error
= -1, errmsg = Can't contact LDAP server,9:debugmsgs,1
```

2 Check if any of the following scenarios is true and carry out the steps provided for that scenario.

The LDAP server URL (`-s` option) that is provided with the `vssat addldapdomain` may be wrong

Run the following command to validate:

```
ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd> -d
<debug_level> -o nettimeout=<seconds>
```

Example:

```
ldapsearch -H ldaps://example.veritas.com:389 -D "CN=Test
User,OU=VRTSUsers,DC=VRTS,DC=com" -w ***** -d 5 -o
nettimeout=60
```

```
TLS: can't connect: TLS error -8179:Peer's Certificate issuer
is not recognized. ldap_sasl_bind(SIMPLE): Can't contact LDAP
server (-1)
```

The server certificate issuer is not a trusted CA

This is applicable if the `ldaps` option is used and can be validated using the `ldapsearch` command:

```
set env var LDAPTLS_CACERT to cacert.pem
```

```
ldapsearch -H <LDAPS_URI> -D "<admin_user_DN>" -w <passwd> -d
<debug_level> -o nettimeout=<seconds>
```

File path for `cacert.pem`:

On Windows:

```
<Install_path>\NetBackup\var\global\wss\eeb\data\systemprofile\certstore\trusted\plugins\ldap\cacert.pem
```

On Unix:

```
/usr/openw/var/global/wss/eeb/data/root/.VRTSat/profile/certstore/trusted/plugins/ldap/cacert.pem
```

Example:

```
ldapsearch -H ldaps://example.veritas.com:389 -D "CN=Test
User,OU=VRTSUsers,DC=VRTS,DC=com" -w ***** -d 5 -o
nettimeout=60
```

```
TLS: can't connect: TLS error -8179:Peer's Certificate issuer
is not recognized.. ldap_sasl_bind(SIMPLE): Can't contact LDAP
server (-1)
```

The NetBackup Authentication Service (`nbatd`) does not trust the certificate authority that has signed the LDAP server's security certificate

Use the `-f` option of the `vssat addldapdomain` command to add the CA certificate in the Authentication Service (`nbatd`) trust store.

See [“Certificate authorities trusted by the NetBackup Authentication Service”](#) on page 121.

TLS cipher suite list that is provided for the LDAP server may be wrong

By default, NetBackup authentication service communicates with the LDAP server using the cipher suite list:

"ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:

ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:DHE-RSA-AES256-SHA"

Run the following command to view the TLS cipher suite list that is provided for the LDAP server:

On UNIX:

```
/usr/openssl/netbackup/sec/at/bin/vssat listldapdomains
```

On Windows:

```
Install_path\NetBackup\sec\at\bin\vssat listldapdomains
```

Use any utility like `ssllscan` to find out the cipher suites that the LDAP server supports.

Modify the value of TLS cipher suite list as required for the LDAP server by running the following command:

On UNIX:

```
/usr/openssl/netbackup/sec/at/bin/vssregctl -s -f
/usr/openssl/var/global/vxss/eab/data/root/.VRTSat/profile/VRTSatlocal.conf
-b "Security\Authentication\Authentication
Broker\AtPlugins\ldap\ServerInfos\LDAP_server_name" -k
"SSLCipherSuite" -t string -v LDAP_server_supported_cipher_suites
```

On Windows:

```
Install_path\NetBackup\sec\at\bin\vssregctl -s -f
Install_path\NetBackup\var\global\vxss\eab\data\systemprofile\VRTSatlocal.conf
-b "Security\Authentication\Authentication
Broker\AtPlugins\ldap\ServerInfos\LDAP_server_name" -k
"SSLCipherSuite" -t string -v LDAP_server_supported_cipher_suites
```

Example:

```
/usr/openssl/netbackup/sec/at/bin/vssregctl -s -f
/usr/openssl/var/global/vxss/eab/data/root/.VRTSat/profile/VRTSatlocal.conf
-b "Security\Authentication\Authentication
Broker\AtPlugins\ldap\ServerInfos\example.veritas.com" -k
"SSLCipherSuite" -t string -v
"DHE-RSA-AES256-SHA:AES256-GCM-SHA384"
```

TLS protocol version that is disabled for the LDAP server may be wrong

By default, NetBackup authentication service communicates with the LDAP server using the TLS 1.2 or later protocol. TLS protocols with versions earlier than 1.2 are disabled.

Run the following command to view the TLS protocol version that is disabled for the LDAP server.

On UNIX:

```
/usr/opensv/netbackup/sec/at/bin/vssat listldapdomains
```

On Windows:

```
Install_path\NetBackup\sec\at\bin\vssat listldapdomains
```

Modify the value of TLS protocol version that is disabled for the LDAP server using the given command. The specified version and all the earlier versions of the TLS protocol are disabled. Supported values are: "SSLv2", "SSLv3", "TLSv1" and "TLSv1.1".

Run the following command:

On UNIX:

```
/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\AtPlugins\ldap\ServerInfos\LDAP_server_name" -k
"DisableTLSProtocol" -t string -v
TLS_protocol_version_to_be_disabled
```

On Windows:

```
Install_path\NetBackup\sec\at\bin\vssregctl -s -f
Install_path\NetBackup\var\global\vxss\eab\data\systemprofile\VRTSatlocal.conf
-b "Security\Authentication\Authentication
Broker\AtPlugins\ldap\ServerInfos\LDAP_server_name" -k
"DisableTLSProtocol" -t string -v
TLS_protocol_version_to_be_disabled
```

Example:

```
/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\AtPlugins\ldap\ServerInfos\example.veritas.com" -k
"DisableTLSProtocol" -t string -v "TLSv1"
```

Invalid user credentials

To troubleshoot the issue

- 1 Check if the `nbatd` logs contain the following error:

```
CAuthLDAP::validatePrpl - ldap_simple_bind_s() failed for user
'CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com', error = 49, errmsg =
Invalid credentials,9:debugmsgs,1
```

- 2 Check if the following scenario is true and carry out the steps provided for the scenario.

Invalid admin user DN or password provided while adding an LDAP domain using the `vssat`

`addldapdomain` command

Run the following command to validate:

```
ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd> -d
<debug_level> -o nettimeout=<seconds>
```

Example:

```
ldapsearch -H ldap://example.veritas.com:389 -D "CN=Test
User,OU=VRTSUsers,DC=VRTS,DC=com" -w ***** -d 5 -o
nettimeout=60 ldap_bind: Invalid credentials (49)
```

Invalid user base DN or group base DN

To troubleshoot the issue

- 1 Check if the `nbatd` logs contain the following error:

```
CAuthLDAP::validatePrpl - ldap_search_s() error = 10, errmsg =
Referral,9:debugmsgs,1 CAuthLDAP::validatePrpl - ldap_search_s()
error = 34, errmsg = Invalid DN syntax,9:debugmsgs,1
```

- 2 You may see the errors in the logs if user base DN (the `-u` option) or group base DN (the `-g` option) values are incorrect.

Run the following command to validate:

Example:

```
ldapsearch -H ldap://example.veritas.com:389 -D "CN=Test
User,OU=VRTSUsers,DC=VRTS,DC=com" -w ***** -b
"OU=VRTSUsers,DC=VRTS,DC=com" "(&(cn=test
user)(objectClass=user))"

ldapsearch -H ldap://example.veritas.com:389 -D "CN=Test
User,OU=VRTSUsers,DC=VRTS,DC=com" -w ***** -b "VRTS" "(&(cn=test
user)(objectClass=user))"
```

Multiple users or groups exist with the same name under user base DN or group base DN

To troubleshoot the issue

- 1 Check if the `nbatd` logs contain the following error:

```
CAuthLDAP::validateGroup - search returned '2' entries for group
name 'team_noone', even with referrals set to OFF,9:debugmsgs,1
```

- 2 This is applicable if user search attribute (`-a` option) and group search attribute (`-y` option) do not have unique values for the existing user base DN and group base DN respectively.

Validate the number of matching entries for the existing base DN using the `ldapsearch` command.

```
ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd> -d
<debug_level> -o nettimeout=<seconds> -b <BASE_DN> <search_filter>
```

Example:

```
ldapsearch -H ldap://example.veritas.com:389 -D "CN=Test
User,OU=VRTSUsers,DC=VRTS,DC=com" -w ***** -b "DC=VRTS,DC=com"
"(&(cn=test user)(objectClass=user))" # LDAPv3 # base <DC=VRTS,DC=com>
with scope subtree # filter: (cn=Test User) # requesting: ALL # Test
User, VRTSUsers, VRTS.com dn: CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com
# Test User, RsvUsers, VRTS.com dn: CN=Test
User,OU=RsvUsers,DC=VRTS,DC=com # numEntries: 2
```

User or group does not exist

To troubleshoot the issue

- 1 Check if the `nbatd` logs contain the following error:

```
CAuthLDAP::validatePrpl - user 'test user' NOT found,9:debugmsgs,4
CAuthLDAP::validateGroup - group 'test group' NOT
found,9:debugmsgs,4
```

- 2 If a user or group exists in the LDAP domain, but the `vssat validateprpl` or the `vssat validategroup` command fails with this error, validate if the user or the group exists in the current base DN's (`-u` and `-g` options) using the following command.

```
ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd> -d
<debug_level> -o nettimeout=<seconds> -b <BASE_DN> <search_filter>
```

Certificate authorities trusted by the NetBackup Authentication Service

The NetBackup Authentication Service (`nbatd`) trusts the following certificate authorities:

- CyberTrust
- DigiCert GeoTrust
- Certification Services Division
- VeriSign Trust Network
- RSA Security Inc.
- GlobalSign
- Symantec Corporation

Access keys

This chapter includes the following topics:

- [Access keys](#)
- [Access codes](#)
- [Request CLI access through web UI authentication](#)
- [Approve the CLI access request of another user](#)
- [Edit the settings for command-line access](#)

Access keys

NetBackup access keys provide access the NetBackup interfaces through API keys and access codes.

See [“About API keys”](#) on page 126.

See [“Access codes”](#) on page 122.

Access codes

To run certain NetBackup administrator commands, for example `bpererror`, you need to authenticate through the web UI. You need to generate an access code through the command-line interface, get the access request approved from the administrator, and then access the command.

With the web UI authentication for CLI access, NetBackup administrators can delegate the associated privileges to other users. By default, only a root administrator or an administrator can perform NetBackup operations through the command-line interface. The web UI authentication support allows non-root users to administer NetBackup who have CLI access that the Security Administrator has granted. You

can also administer NetBackup with a non-RBAC user role (such as Operating System Administrator) even though you are not registered as a NetBackup user. Each time you need to generate a new access code to access CLIs.

Request CLI access through web UI authentication

To run NetBackup commands using the NetBackup CLI, the following requirements exist for the user:

- The user must have the RBAC role Default NetBackup Command Line (CLI) Administrator or a role with similar permissions.
- The user must submit a request for temporary access to the CLI. By default, a CLI access session is valid for 24 hours.
The command that the user runs for the request depends on whether or not they have access to the NetBackup web UI.
See [the section called “Request CLI access when you have access to the NetBackup web UI”](#) on page 123.
See [the section called “Request CLI access from the security administrator”](#) on page 124.

Request CLI access when you have access to the NetBackup web UI

If you have access to the NetBackup web UI, you can use the web UI to approve a CLI access request using the access code from the `bpnbat` command.

To request CLI access

- 1 Run the following command:

```
bpnbat -login -logintype webui
```


An access code is generated.
- 2 Open the NetBackup web UI.
- 3 On the top right, select the profile icon.
- 4 Select **Approve access request**.
- 5 Enter the CLI access code that was created when you ran the `bpnbat` command. Then select **Review**.
- 6 Review the access request details.
- 7 Select **Approve**.
- 8 After you approve the request, you can use the command-line interface to run the wanted commands.

Request CLI access from the security administrator

If you do not have access to the NetBackup web UI, you must submit a request for a CLI access to the security administrator. A user with the Default Security Administrator role or a role with similar permissions must approve the request.

To request CLI access from the security administrator

- 1 Run the following command:

```
bpnbat -login -logintype webui -requestApproval
```

An access code is generated.

- 2 Contact the security administrator and give them the access code to approve the CLI access request.

See [“Approve the CLI access request of another user”](#) on page 124.

- 3 After the request is approved, you can use the command-line interface to run the wanted commands.

Approve the CLI access request of another user

If you have the Default Security Administrator role or a role with similar permissions, you can approve the request of another user who needs CLI access. Note that to run commands, that user must also have the RBAC role Default NetBackup Command Line (CLI) Administrator or a role with similar permissions.

To approve the CLI access request of another user

- 1 The user that requires CLI access must first run the following command to request approval:

```
bpnbat -login -logintype webui -requestApproval
```

- 2 Sign in to the NetBackup web UI.
- 3 On the left, select **Security > Access keys**. Then select the **Access codes** tab.
- 4 Enter the CLI access code that you have received from the user who requires CLI access and select **Review**.
- 5 Review the access request details.
- 6 (Optional) Provide any comments.
- 7 Select **Approve**.

Edit the settings for command-line access

You can configure the default time that is set for a CLI session when a user requests CLI access.

To edit the settings for command-line access

- 1 Sign in to the web UI.
- 2 On the left, select **Security > Access keys**.
- 3 On the right, select **Access settings**.
- 4 Select **Edit**.
- 5 Enter the time in minutes or hours that you want the CLI access session to be valid. 1 minute is the minimum value and 24 hours is the maximum value.

API keys

This chapter includes the following topics:

- [About API keys](#)
- [Creating API keys](#)
- [Managing an API key](#)
- [Using an API key](#)

About API keys

NetBackup supports user authentication through API keys.

A NetBackup API key is a pre-authenticated token that lets a NetBackup user run NetBackup commands (such as `nbcertcmd -createToken` or `nbcertcmd -revokeCertificate`) or access NetBackup RESTful APIs.

API key operations with multiperson authorization

Note: Starting with NetBackup 10.5, if multiperson authorization is enabled for API key operations, a ticket is generated. After the multiperson authorization ticket is approved, the user needs to execute the ticket using the **Execute ticket** option in the NetBackup web UI and then the required API key operation is executed.

For NetBackup releases earlier than 10.5, if multiperson authorization is enabled, you cannot perform API key operations.

Unlike a password, an API key can exist for a long time and you can configure its expiration. Therefore, operations like automation that need authentication can run for a long time using API keys.

See [“Creating API keys”](#) on page 127.

See [“Using an API key”](#) on page 128.

See [“Managing an API key”](#) on page 127.

Note: It is recommended that you delete an API key that was generated for a principal user after the user becomes inactive, or is blocked, or removed from the authentication system (AD or LDAP).

Creating API keys

A user can have only one API key.

Note: The 'View' RBAC permission is required to create an API key.

You can create API keys in one of the following ways:

- Using the `netbackup/security/api-keys` POST API
Any user can create an API key using the `api-keys` API
- Using the NetBackup web UI
For more details on creating API keys using the web UI or RBAC roles, refer to the *NetBackup Web UI Administrator's Guide*.

See [“Using an API key”](#) on page 128.

See [“Managing an API key”](#) on page 127.

Managing an API key

Each API key is associated with an API key tag. You can update or delete an API key using its API key tag in one of the following ways:

- Using the `netbackup/security/api-keys` API
You can update or delete an API key using its API key tag.
- Using the NetBackup web UI
For more details on managing API keys using the web UI, refer to the *NetBackup Web UI Administrator's Guide*.

See [“Creating API keys”](#) on page 127.

See [“Using an API key”](#) on page 128.

Using an API key

Once an API key is created, you can use it while you access RESTful APIs or run commands:

See [“Creating API keys”](#) on page 127.

Using an API key while accessing NetBackup RESTful APIs

- ◆ Pass the API key in the API request header to access other NetBackup APIs.

Using an API key while you run NetBackup commands

1 Do one of the following:

- Run the following command:

```
bpnbat -Login -LoginType APIKEY
```

You can run NetBackup commands that require authentication for the next 24 hours without requiring to run `bpnbat -Login`.

- Set a new environment variable called `NETBACKUP_APIKEY` for the API key. See [“Setting an API key environment variable to run NetBackup commands”](#) on page 128.

You can run NetBackup commands that require authentication until the API key is valid and the environment variable is set.

2 Run a command such as `nbcertcmd -createToken`.

For more details on NetBackup commands, refer to the *NetBackup Commands Reference Guide*.

Setting an API key environment variable to run NetBackup commands

To use an API key while running NetBackup commands that need user authentication, you need to create an API key and set an environment variable for the API key. Once the environment variable is set, you can run the commands until the API key is valid and the environment variable is set.

On Windows platform, set the API key environment variable in the user context.

Example of an environment variable for an API key:

```
NETBACKUP_APIKEY = MasterServer1:APIKEY1
```

If you want to set multiple API keys, specify the primary server and API key mappings in a comma-separated format.

For example:

```
NETBACKUP_APIKEY =  
MasterServer1:APIKEY1,MasterServer2:APIKEY2,MasterServer3:APIKEY3
```

You can also specify the mappings in a file and the file should be specified with prefix '@'.

For example:

```
NETBACKUP_APIKEY = @file_path/file_name
```

The contents of the file should be as follows:

```
MasterServer1:APIKEY1
```

```
MasterServer2:APIKEY2
```

```
MasterServer3:APIKEY3
```

See [“Creating API keys”](#) on page 127.

Role-based access control

This chapter includes the following topics:

- [RBAC features](#)
- [RBAC settings](#)
- [Configuring RBAC](#)
- [Role permissions](#)
- [Notes for using NetBackup RBAC](#)
- [Add AD or LDAP domains](#)
- [Default RBAC roles](#)
- [Add a custom RBAC role](#)
- [Edit a custom role](#)
- [View users in RBAC](#)
- [Add a user to a role \(non-SAML\)](#)
- [Add a smart card user to a role \(non-SAML, without AD/LDAP\)](#)
- [Add a user to a role \(SAML\)](#)
- [Remove a user from a role](#)

RBAC features

The NetBackup web user interface provides the ability to apply role-based access control in your NetBackup environment. Use RBAC to provide access for the users that do not currently have access to NetBackup. Or, for current NetBackup users

with administrator access you can provide limited access and permissions, based on their role in your organization.

For information on access control and auditing information for root users and administrators, refer to the [NetBackup Security and Encryption Guide](#).

Table 9-1 RBAC features

Feature	Description
Roles allow users to perform specific tasks	Add users to one or more default RBAC roles or create custom roles to fit the role of your users. Add a user to the Administrator role to give full NetBackup permissions to that user. See “ Default RBAC roles ” on page 135.
Users can access NetBackup areas and the features that fit their role	RBAC users can perform common tasks for their business role, but are restricted from accessing other NetBackup areas and features. RBAC also controls the assets that users can view or manage.
Auditing of RBAC events	NetBackup audits RBAC events.
DR ready	RBAC settings are protected with the NetBackup catalog.

RBAC settings

You can configure access control settings based on user roles. The following RBAC settings can be configured:

- Web UI access for Operating System Administrator
- CLI access for Operating System Administrator

Configuring RBAC

To configure role-based access control for the NetBackup web UI, perform the following steps.

Table 9-2 Steps to configure role-based access control

Step	Action	Description
1	Configure any Active Directory or LDAP domains.	Before you can add domain users, Active Directory or LDAP domains must be authenticated with NetBackup. See the NetBackup Security & Encryption Guide .

Table 9-2 Steps to configure role-based access control (*continued*)

Step	Action	Description
2	Determine the permissions that your users need.	Determine the permissions that your users need to perform their daily tasks. You can use the default RBAC roles or use a default role as a template to create a new role. Or, you can create a completely custom role to fit your needs. See “Role permissions” on page 132. See “Default RBAC roles” on page 135. See “Add a custom RBAC role” on page 140.
3	Add users to the appropriate roles.	See “Add a user to a role (non-SAML)” on page 144. See “Add a user to a role (SAML)” on page 145. See “Add a smart card user to a role (non-SAML, without AD/LDAP)” on page 145.
4	Determine the permissions that you want for OS administrators	See “Disable web UI access for operating system (OS) administrators” on page 148. See “Disable command-line (CLI) access for operating system (OS) administrators” on page 147.

Role permissions

Role permissions define the operations that roles users have permission to perform.

For details on individual RBAC permissions and dependencies, refer to the NetBackup API documentation.

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

Table 9-3 Role permissions for NetBackup RBAC

Category	Description
Global	Global permissions apply to all assets or objects. BMR - Configuration and management of BMR. NetBackup Web Management Console Administration - With guidance from Cohesity Support, create diagnostic files to troubleshoot NetBackup and perform JVM garbage collection. These operations are only available from the NetBackup APIs. Refer to the following guides for information on JVM tuning options: NetBackup Installation Guide, NetBackup Upgrade Guide. NetBackup management - Configuration and management of NetBackup. Storage lifecycle policies - Manage storage lifecycle policies (SLPs). Security - NetBackup security settings. Storage - Manage backup storage settings.
Assets	Manage one or more types of assets. For example, VMware assets.
Protection	Manage how backups are performed with policies or protection plans.
Credentials	Manage credentials for assets and for other features of NetBackup.

Table 9-4 Role permissions for NetBackup RBAC

Category	Description
Global	Global permissions apply to all assets or objects. BMR - Configuration and management of BMR. NetBackup Web Management Console Administration - With guidance from Cohesity Support, create diagnostic files to troubleshoot NetBackup and perform JVM garbage collection. These operations are only available from the NetBackup APIs. Refer to the following guides for information on JVM tuning options: NetBackup Installation Guide, NetBackup Upgrade Guide. NetBackup management - Configuration and management of NetBackup. Protection - NetBackup backup policies and storage lifecycle policies. Security - NetBackup security settings. Storage - Manage backup storage settings.
Assets	Manage one or more types of assets. For example, VMware assets.

Table 9-4 Role permissions for NetBackup RBAC (*continued*)

Category	Description
Protection plans	Manage how backups are performed with protection plans.
Credentials	Manage credentials for assets and for other features of NetBackup.

Notes for using NetBackup RBAC

Note the following when you configure the permissions for RBAC roles:

- When you create roles, be sure to enable the minimal number of permissions so the user can sign in to and use the web UI. Some individual permissions do not have a direct correlation with a screen in the web UI. Users that attempt to sign in but that only have a permission of this kind receive an “Unauthorized” message.
- If a user is added to or removed from a role, the user must sign out and sign in again before the user’s permissions are updated.
- Most permissions are not implicit.
 In most cases a **Create** permission does not give a user **View** permission. A **Recovery** permission does not give a user **View** permission or other recovery options like **Overwrite**.
- Not all RBAC-controlled operations can be used from the NetBackup web UI. These types of operations are included in RBAC so a role administrator can create roles for API users as well as for web UI users.
- Some tasks require a user to have permissions in multiple RBAC categories. For example, to establish a trust relationship with a remote primary server, a user must have permissions for both **Remote primary servers** and **Trusted primary servers**.

Add AD or LDAP domains

NetBackup supports Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain users. Before you can add domain users to RBAC roles, you must add the AD or the LDAP domain. A domain also must be added before you can configure that domain for smart card authentication.

You can use the `POST /security/domains/vxat` API or the `vssat` command to configure domains.

For more information on the `vssat` command and more of its options, see the [NetBackup Command Reference Guide](#).

Default RBAC roles

The NetBackup web UI provides the following default RBAC roles with preconfigured permissions and settings.

Table 9-5 Default RBAC roles in the NetBackup web UI

Role name	Description
Administrator	The Administrator role has full permissions for NetBackup and can manage all aspects of NetBackup.
Default AHV Administrator	This role has all the permissions that are necessary to manage Nutanix Acropolis Hypervisor and to back up those assets with protection plans.
Default Apache Cassandra Administrator	This role has all the permissions that are necessary to manage and protect Apache Cassandra assets with protection plans.
Default Cloud Administrator	This role has all the permissions that are necessary to manage cloud assets and to back up those assets with protection plans. Note that a PaaS administrator requires some additional permissions that you can add to a custom role. Cloud administrators also need additional permissions to manage cloud and PaaS assets using intelligent groups. See “Add a custom RBAC role for a PaaS administrator” on page 137.
Default Cloud Object Store Administrator	This role has all the permissions to manage the protection for cloud objects using classic policies.
Default DB2 Administrator	This role provides the ability to view and restore DB2 backups with the <code>nbdb2adutl</code> command. The administrator can also view and manage DB2 jobs.
Default IRE SLP Administrator	Manages IRE (Isolated Recovery Environment) SLP (Storage lifecycle policies) functionalities.
Default Kubernetes Administrator	This role has all the permissions that are necessary to manage Kubernetes and to back up those assets with protection plans. The permissions for this role give a user the ability to view and manage jobs for Kubernetes assets. To view all jobs for this asset type, a user must have the default role for that workload. Or, a similar custom role must have the following option applied when the role is created: Apply selected permissions to all existing and future workload assets .
Default KVM Administrator	This role has all the permissions that are necessary to manage KVM and to back up those assets. The administrator can also view and manage KVM jobs.
Default Microsoft Sentinel Administrator	This role has all the permissions necessary to add Microsoft Sentinel credentials in NetBackup and to send NetBackup audit events to Microsoft Sentinel.

Table 9-5 Default RBAC roles in the NetBackup web UI (*continued*)

Role name	Description
Default Microsoft SQL Server Administrator	This role has all the permissions that are necessary to manage SQL Server databases and to back up those assets with protection plans. In addition to this role, the NetBackup user must meet the following requirements: ■ Member of the Windows administrator group. ■ Have the SQL Server “sysadmin” role.
Default MongoDB Ops Manager	This role has all the permissions that are necessary to manage and protect assets in MongoDB Ops Manager with protection plan.
Default MultiPerson Authorization (MPA) Approver	This role has permissions to manage MPA tickets.
Default MySQL Administrator	This role has all the permissions that are necessary to manage MySQL instances and databases and to back up those assets with protection plans.
Default NAS Administrator	This role has all the permissions that are necessary to perform the backup and restore of NAS volumes using a NAS-Data-Protection policy. To view all jobs for the backups and restores of a NAS volume, a user must have this role. Or, the user must have a custom role with same permissions applied when the role was created.
Default NetBackup Command Line (CLI) Administrator	This role has all the permissions that are necessary to manage NetBackup using the NetBackup command line (CLI). With this role a user can run most of the NetBackup commands with a non-root account. Note: A user that has only this role cannot sign into the web UI.
Default Oracle Administrator	This role has all the permissions that are necessary to manage Oracle databases and to back up those assets with protection plans.
Default PostgreSQL Administrator	This role has all the permissions that are necessary to manage PostgreSQL instances and databases and to back up those assets with protection plans.
Default Resiliency Administrator	This role has all the permissions to protect the rpProductName (VRP) for VMware assets.
Default RHV Administrator	This role has all the permissions that are necessary to manage Red Hat Virtualization computers and to back up those assets with protection plans. This role gives a user the ability to view and manage jobs for RHV assets. To view all jobs for RHV assets, a user must have this role. Or, the user must have a similar custom role with following option applied when the role was created: Apply selected permissions to all existing and future RHV assets.
Default SaaS Administrator	This role has all the permissions to view and manage SaaS assets.

Table 9-5 Default RBAC roles in the NetBackup web UI (*continued*)

Role name	Description
Default Security Administrator	This role has permissions to manage NetBackup security including role-based access control (RBAC), certificates, hosts, identity providers and domains, global security settings, and other permissions. This role can also view settings and assets in most areas of NetBackup: workloads, storage, licensing, and other areas.
Default Storage Administrator	This role has permissions to configure disk-based storage and storage lifecycle policies. SLP settings are managed with the Administrator role. Note: A user that is assigned with this role also has access permissions to Tape vault in Vault management.
Default Universal Share Administrator	This role has the permissions to manage policies and storage servers. It can also manage the assets for filesystem clients (MS-Windows and Standard policies) and for universal shares.
Default VMware Administrator	This role has all the permissions that are necessary to manage VMware virtual machines and to back up those assets with protection plans. To view all jobs for VMware assets, a user must have this role. Or, the user must have a similar custom role with following option applied when the role was created: Apply selected permissions to all existing and future VMware assets.
NetBackup Read-Only Operator	This role provides the read-only permissions to the IT Analytics Operator, Multiperson Authorization Approver, and other operators in NetBackup, with no permissions for security.

Note: Cohesity reserves the right to update the RBAC permissions for default roles in future releases. Any revised permissions are automatically applied to users of these roles when NetBackup is upgraded. If you have copies of default roles these roles are not updated automatically. (Or, if you have any custom roles that are based on default roles.) If you want these custom roles to include changes to default roles, you must manually apply the changes or recreate the custom roles.

Add a custom RBAC role for a PaaS administrator

A PaaS administrator needs additional storage permissions. You can use the **Default Cloud Administrator** role as a template to create a custom role.

To add a custom RBAC role

- 1 On the left, select **Security > RBAC** and click **Add**.
- 2 Select **Default Cloud Administrator**.

- 3 Provide a **Role name** and a description.

For example, you may want to indicate that the role is for any users that are PaaS administrators.

- 4 Under **Permissions**, click **Assign**.

- 5 On the **Global** tab, expand the **Storage** section. Select the following permissions.

Disk pools	View
Storage servers	View
Storage universal shares	View, Create

- 6 On the **Assets** tab, under desired policy type / workload section select the following permissions:
 - Instant access
 - Restore from malware-infected images (Required to restore from malware infected images)
- 7 Click **Assign**.
- 8 Under **Users**, click **Assign**. Then add each user that you want to have access to this custom role.
- 9 When you are done configuring the role, click **Add role**.

Add a custom RBAC role to restore Azure-managed instances

To restore Azure-managed instances, users must have the view permission for these instances. Administrators and similar users can provide other users with a custom role and this permission.

To assign the view permission for Azure-managed instances

- 1 To get the access control ID of the managed instance, enter the following command:

```
GET /asset-service/workloads/cloud/assets?filter=extendedAttributes/managedInstanceName eq 'managedInstanceName'
```

Search for *accessControlId* field in the response. Note down the value of this field.

- 2 To get the role ID, enter the following command:

```
GET /access-control/roles
```

Search for the *id* field in the response. Note down the value of this field.

- 3 Create an access definition, as follows:

```
POST /access-control/managed-objects/{objectId}/access-definitions
```

Request payload

```
{
  "data": {
    "type": "accessDefinition",
    "attributes": {
      "propagation": "OBJECT_AND_CHILDREN"
    },
    "relationships": {
      "role": {
        "data": {
          "id": "<roleId>",
          "type": "accessControlRole"
        }
      },
      "operations": {
        "data": [
          {
            "id": "|OPERATIONS|VIEW|",
            "type": "accessControlOperation"
          }
        ]
      }
    },
    "managedObject": {
      "data": {
        "id": "<objectId>",
```

```

        "type": "managedObject"
      }
    }
  }
}

```

Use the following values:

- `objectId`: Use the value of *accessControlId* obtained from step 1.
- `roleId`: Use the value of *id* obtained from step 2.

Note: For an alternate restore, provide the
`|OPERATIONS|ASSETS|CLOUD|RESTORE_DESTINATION|` permission in the
operations list.

Add a custom RBAC role

Create a custom RBAC role if you want to manually define the permissions and the access that users have to workload assets, policies, protection plans, or credentials.

Create a custom RBAC role if you want to manually define the permissions and the access that users have to workload assets, protection plans, or credentials.

See [“Notes for using NetBackup RBAC”](#) on page 134.

See [“Role permissions”](#) on page 132.

Note: Cohesity reserves the right to update the RBAC permissions for default roles in future releases. Any revised permissions are automatically applied to users of these roles when NetBackup is upgraded. Any copies of default roles (or any custom roles that are based on default roles) are not automatically updated.

To add a custom RBAC role

- 1 Sign in to the NetBackup web UI.
- 2 On the left, select **Security > RBAC**.
- 3 Select **Add**.

4 Select the type of role that you want to create.

You can make a copy of a default role that contains all the preconfigured permissions and settings for that type of role. Or, select **Custom role** to manually configure all the permissions for a role.

5 Provide a **Role name** and a description.

For example, you may want to indicate that the role is for any users that are backup administrators for a particular department or region.

6 Under **Permissions**, select **Edit** or **Assign**.

If you selected a default role type, certain permissions are enabled only if they are required for that type of role. (For example, the **Default Multiperson Authorization (MPA) Approver** does not require policy permissions. The **Default Microsoft SQL Server Administrator** requires credentials.)

The permissions that you select in the **Permissions** card determine the other settings that you can configure for the role.

When you select **Asset** permissions: The **Workloads** card is enabled.

When you select **Protection** permissions for policies or protection plans: The **Protection** card is enabled.

When you select **Credentials** permissions: The **Credentials** card is enabled.

The permissions that you select determine the other settings that you can configure for the role.

- The **Workloads** card is enabled when you select **Asset** permissions.
- **Protection plans** are enabled when you select **Protection plans** permissions.
- **Credentials** are enabled when you select **Credentials** permissions.

7 Under **Protection**, you can select the policies and protection plans that users can manage with this role. For policies, you can apply permissions to all policies, policies of one or more specific types, and specific policies.

8 Under **Users**, select the **Assign**. Then select the users you want to add to the role.

- 9 When you are done configuring the role, select **Save**.

Note: After a role is created, you must edit permissions for assets, policies, protection plans, or credentials directly from the applicable node in the web UI. For example, to edit permissions for all VMware assets, go to **Workloads > VMware** and then select **VMware settings > Manage permissions**. Or, select a VM and select **Manage permissions**.

Note: After a role is created, you must edit permissions for assets, protection plans, or credentials directly from the applicable node in the web UI. For example, to edit permissions for all VMware assets, go to **Workloads > VMware** and then select **VMware settings > Manage permissions**. Or, select a VM and select **Manage permissions**.

- 10 Users that were assigned to the role must sign out and sign in again before each user's permissions are updated.

Edit a custom role

You can edit or remove a custom role when you want to change or remove permissions for users with that role. Default roles cannot be edited or removed. The only action you can perform on default roles is to add or remove users from a role. Permissions for specific assets, policies, protection plans, or credentials directly from the applicable node in the web UI.

For example:

- To edit permissions for all VMware assets, go to **Workloads > VMware** and then select **VMware settings > Manage permissions**.
- To edit permissions for a VM, select a VM and select **Manage permissions**.
- To manage policy permissions, go to **Protection > Policies**. Then at the top right, select **Manage permissions**.
- To manage permissions for a specific policy, select a policy and then select **Manage permissions**.

Note: When you change permissions for a custom role, the changes affect all users that are assigned to that role.

To edit a custom role

- 1 Sign in to the NetBackup web UI.
- 2 On the left, click **Security > RBAC**.
- 3 On the **Roles** tab, locate and click on the custom role that you want to edit.

- 4 To edit the role description, click **Edit name and description**.
- 5 Edit the permissions for the role. You can edit the following details for a role:

Global permissions for the role	On the Global permissions tab, click Edit .
Assets permissions for the role	On the Assets permissions tab, click Edit .
Users for the role	Click the Users tab.
Access definitions for the role	Click the Access definitions tab. Caution: Use caution when removing access definitions. This action may remove critical access to NetBackup for the role's users. You can only remove access definitions from a custom role.

See [“Role permissions”](#) on page 132.

See [“Notes for using NetBackup RBAC”](#) on page 134.

- 6 To add or remove users for the role, click the **Users** tab.
See [“Add a user to a role \(non-SAML\)”](#) on page 144.
See [“Remove a user from a role”](#) on page 146.
- 7 Users that are assigned to the role must refresh their browser to reflect updated role permissions in the web UI.

View users in RBAC

You can view the users that have been added to RBAC and the roles that they are assigned to. The **Users** list is view-only. To edit the users that are assigned to a role, you must edit the role.

To view the users in RBAC

- 1 Sign in to the NetBackup web UI.
- 2 On the left, click **Security > RBAC**.
- 3 Click on the **Users** tab.
- 4 The **Roles** column indicates each role to which the user is assigned.

Add a user to a role (non-SAML)

This topic describes how to add a non-SAML user or group to a role.

Non-SAML users use one of the following sign-in methods: **Sign in with username and password** or **Sign in with smart card**.

To add a user to a role (non-SAML)

- 1
- Sign in to the NetBackup web UI.
- 2
- On the left, click **Security > RBAC**.
- 3
- Click the **Roles** tab.
- 4
- Click on the role name, then click on the **Users** tab.
- 5
- (Conditional) From the **Sign-in type** list, select from the following:

■

Default sign-in. For a user that signs into NetBackup with their username and password.

■

Smart card user. For a user that uses a smart card to sign into NetBackup.

Note: The **Sign-in type** list is only available if there is an IDP configuration available for NetBackup.

- 6
- Enter the user or the group name that you want to add.

For this type of user	Use this format	Example
Local user or group	<i>username</i>	jane_doe
	<i>groupname</i>	admins
Windows user or group	<i>DOMAINusername</i>	WINDOWS\jane_doe
	<i>DOMAINgroupname</i>	WINDOWS\Admins
UNIX user or group	<i>username@domain</i>	john_doe@unix
	<i>groupname@domain</i>	admins@unix

- 7
- Click **Add to list**.
- 8
- Users that are assigned to the role must sign out and sign in again before each user's permissions are updated.

Add a smart card user to a role (non-SAML, without AD/LDAP)

This topic describes how to add a smart card user to a role. In this case the user is a non-SAML user and there is no AD or no LDAP domain association or mapping. User groups are not supported with this type of configuration.

This type of user uses the following sign-in method: **Sign in with smart card**.

To add a smart card user to a role (non-SAML, without AD/LDAP)

- 1 Sign in to the NetBackup web UI.
- 2 On the left, click **Security > RBAC**.
- 3 Click the **Roles** tab.
- 4 Click on the role name, then click on the **Users** tab.
- 5 (Conditional) From the **Sign-in type** list, select **Smart card user**.

Note: The **Sign-in type** list is available only if there is an IDP configuration available for NetBackup. The smart card user option in the **Sign-in type** list is available when the smart card configuration is done without AD or LDAP domain mapping.

- 6 Enter the username that you want to add.
 Provide the exact common name (CN) or the universal principal name (UPN) that is available in the certificate.
- 7 Click **Add to list**.
- 8 Users that are assigned to the role must sign out and sign in again before each user's permissions are updated.

Add a user to a role (SAML)

This topic describes how to add a SAML user or group to a role.

SAML users use one of the following sign-in methods: **SAML user** or **SAML group**.

To add a user to a role (SAML)

- 1 Sign in to the NetBackup web UI.
- 2 On the left, click **Security > RBAC**.
- 3 Click the **Roles** tab.

- 4 Click on the role name, then click on the **Users** tab.
- 5 From the **Sign-in type** list, select the sign-in method **SAML user** or **SAML group**.
- 6 Enter the user or the group name that you want to add.
For example, nbuadmin@my.host.com.

If your Identity Provider (IDP) returns group information in the format of (CN=groupname, DC=domainname) or domainname\groupname, you should add the group using the format groupname@domainname. However, it is also possible to configure SAML Groups in Role-Based Access Control (RBAC) without including the domain name. If your IDP returns group names without domain information, you can add those groups as plain text. Please note that using the email format is not mandatory for SAML groups.
- 7 Click **Add to list**.
- 8 Users that are assigned to the role must sign out and sign in again before each user's permissions are updated.

Remove a user from a role

You can remove a user from a role when you want to remove permissions for that user.

If a user is removed from a role, the user must sign out and sign in again before the user's permissions are updated.

To remove a user from a role

- 1 Sign in to the NetBackup web UI.
- 2 On the left, click **Security > RBAC**.
- 3 Click the **Roles** tab.
- 4 Click on the role that you want to edit, select the **Users** tab.
- 5 Locate the user you want to remove and click **Actions > Remove > Remove**.
- 6 Users that are assigned to the role must sign out and sign in again before each user's permissions are updated.

NetBackup interface access for OS Administrators

This chapter includes the following topics:

- [Disable command-line \(CLI\) access for operating system \(OS\) administrators](#)
- [Disable web UI access for operating system \(OS\) administrators](#)

Disable command-line (CLI) access for operating system (OS) administrators

By default, an OS administrator (user or group member) has access to the NetBackup CLI and does not need to be a member of an RBAC role.

This option prevents OS administrators from accidentally running NetBackup CLIs. A malicious user with the OS administrator access of the primary server can still bypass this restriction.

After you can disable the option, the OS administrator must log in with `bpnbat -login` to access the CLI.

To disable CLI access for OS administrators

- 1 Sign in to the web UI.
- 2 On the top right, click **Settings > Global security**.
- 3 On the **Security controls** tab, turn off the **CLI access for Operating System Administrator** option.

Disable web UI access for operating system (OS) administrators

By default, an OS administrator (user or group member) has access to the NetBackup web UI and does not need to be a member of an RBAC role.

If you do not want an OS administrator to automatically have this access, you can disable it. An OS administrator must then have the RBAC Administrator role to be able to access the web UI.

To disable web UI access control for the OS administrators

- 1 Sign in to the web UI.
- 2 On the top right, click **Settings > Global security**.
- 3 On the **Security controls** tab, turn off the **Web UI access for Operating System Administrator** option.

Smart card or digital certificate

This chapter includes the following topics:

- [Configure user authentication with smart cards or digital certificates](#)
- [Configure smart card authentication with a domain](#)
- [Configure smart card authentication without a domain](#)
- [Edit the configuration for smart card authentication](#)
- [Add or delete a CA certificate that is used for smart card authentication](#)
- [Disable or temporarily disable smart card authentication](#)

Configure user authentication with smart cards or digital certificates

You can map a smart card or certificate with an AD or an LDAP domain for user validation. Alternatively, you can configure a smart card or certificate without an AD or an LDAP domain.

See [“Configure smart card authentication with a domain”](#) on page 149.

See [“Configure smart card authentication without a domain”](#) on page 151.

Configure smart card authentication with a domain

You can configure NetBackup to validate users with smart cards or certificates with an AD or an LDAP domain.

Note the following prerequisites:

- Before you add the authentication method you must add the domain that is associated with your NetBackup users. See the [NetBackup Security & Encryption Guide](#).
- Ensure that you complete the role-based access control (RBAC) configuration for the NetBackup users before you configure smart card or certificate authentication.
See [“Configuring RBAC”](#) on page 131.

To configure smart card authentication with a domain

- 1 Sign in to the NetBackup web UI.
- 2 At the top right, select **Settings > Smart card authentication**.
- 3 Turn on **Smart card authentication**.
- 4 Select the required AD or LDAP domain from the **Select the domain** option.
- 5 Select a **Certificate mapping attribute**: Common name (CN) or Universal principal name (UPN).
- 6 Optionally, enter the **OCSP URI**.
If you do not provide the OCSP URI, the URI in the user certificate is used.
- 7 Select **Save**.
- 8 To the right of **CA certificates**, click **Add**.
- 9 Browse for or drag and drop the **CA certificates** and click **Add**.

Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

Certificate file types must be `.crt`, `.cer`, `.der`, `.pem`, or PKCS #7 format and less than 64KB in size.
- 10 On the **Smart card authentication** page, verify the configuration information.

After configuring smart card authentication, you must restart the NetBackup Web Management Console (nbwmc) service.

- 11 Before users can use a digital certificate that is not installed on a smart card, the certificate must be uploaded to the browser's certificate manager.

See the browser documentation for instructions or contact your certificate administrator for more information.

- 12 When users sign in, they now see an option to **Sign in with certificate or smart card**.

If you do not want users to have this sign-in option yet, turn off **Smart card authentication**. (For example, if all users do not yet have their certificates configured on their hosts.). The settings that you configured are retained even if you turn off smart card authentication.

For such users, the domain name and domain type are smart card.

Configure smart card authentication without a domain

You can configure NetBackup to validate users with smart cards or certificates without an associated AD or LDAP domain. Only users are supported for this configuration. User groups are not supported.

To configure smart card authentication without a domain

- 1 Sign in to the NetBackup web UI.
- 2 At the top right, select **Settings > Smart card authentication**.
- 3 Turn on **Smart card authentication**.
- 4 (Conditional step) If AD or LDAP domain is configured in your environment, select **Continue without the domain** option.
- 5 Select a **Certificate mapping attribute**: Common name (CN) or Universal principal name (UPN).
- 6 Optionally, enter the **OCSP URI**.
If you do not provide the OCSP URI, the URI in the user certificate is used.
- 7 Select **Save**.
- 8 To the right of **CA certificates**, click **Add**.
- 9 Browse for or drag and drop the **CA certificates** and click **Add**.

- 10 Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

Certificate file types must be `.crt`, `.cer`, `.der`, `.pem`, or PKCS #7 format and less than 64KB in size.
- 11 On the **Smart card authentication** page, verify the configuration information.

After configuring smart card authentication, you must restart the NetBackup Web Management Console (nbwmc) service.

Before users can use a digital certificate that is not installed on a smart card, the certificate must be uploaded to the browser's certificate manager.
- 12 When users sign in, they now see an option to **Sign in with certificate or smart card**.

If you do not want users to have this sign-in option yet, turn off **Smart card authentication**. (For example, if all users do not yet have their certificates configured on their hosts.). The settings that you configured are retained even if you turn off smart card authentication.

Edit the configuration for smart card authentication

If the configuration changes for smart card authentication, you can edit the configuration details.

To edit user authentication configuration with domain

- 1 Sign in to the NetBackup web UI.
- 2 At the top right, select **Settings > Smart card authentication**.
- 3 You may want to edit the AD or LDAP domain selection in the following cases:
 - To select a domain that is different than the existing one
 - The existing domain is deleted and you want to select a new domain
 - You want to continue without the domain

Select **Edit**.

- 4 Select a domain.

Only the domains that are configured for NetBackup display in this list.

If you do not want to validate the users with domain, you can select **Continue without the domain**.

- 5 Edit the **Certificate mapping attribute**.
- 6 Leave the **OCSP URI** field empty if you want to use the **URI** value from the user certificate. Or, provide the URI that you want to use.

Add or delete a CA certificate that is used for smart card authentication

Add a CA certificate

Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

To add a CA certificate

- 1 Sign in to the NetBackup web UI.
- 2 At the top right, select **Settings > Smart card authentication**.
- 3 Locate **CA certificates** and select the **Add** button.
- 4 Browse for or drag and drop the **CA certificates**. Then select the **Add** button.

Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

Certificate file types must be in DER, PEM, or PKCS #7 format and no more than 1 MB in size.

Delete a CA certificate

You can delete a CA certificate if it is no longer used for smart card authentication. Note that if a user attempts to use the associated digital certificate or smart card certificate, they are not able to sign in to NetBackup.

To delete a CA certificate

- 1 Sign in to the NetBackup web UI.
- 2 At the top right, select **Settings > Smart card authentication**.
- 3 Select the CA certificates that you want to delete.
- 4 Select **Delete > Delete**.

Disable or temporarily disable smart card authentication

You can disable smart card authentication if you no longer want to use that authentication method for the primary server. Or, if you need to complete other configuration before users can use smart cards.

To disable smart card authentication

- 1 Sign in to the NetBackup web UI.
- 2 At the top right, select **Settings > Smart card authentication**.
- 3 Turn off **Smart card authentication**.

The settings that you configured are retained even if you turn off smart card authentication.

Single Sign-On (SSO)

This chapter includes the following topics:

- [About single sign-on \(SSO\) configuration](#)
- [Configure NetBackup for single sign-on \(SSO\)](#)

About single sign-on (SSO) configuration

You can configure single sign-on (SSO) with any identity provider (IDP) that uses the SAML 2.0 protocol for exchanging authentication and authorization information. Note that you can configure an IDP with more than one Cohesity product. For example, the same IDP can be configured with NetBackup and with APTARE.

Note the following requirements and limitations:

- To use SSO, you must have a SAML 2.0 compliant identity provider configured in your environment.
- Only identity providers that use AD or LDAP directory services are supported.
- Configuration of the IDP requires the NetBackup APIs or the NetBackup command `nbidpcmd`.
- SAML users cannot use the APIs. API keys are used to authenticate a user and therefore cannot be used with a SAML-authenticated user.
- Global logout is not supported.

Figure 12-1 Example NAT configuration: Identity provider in a private network

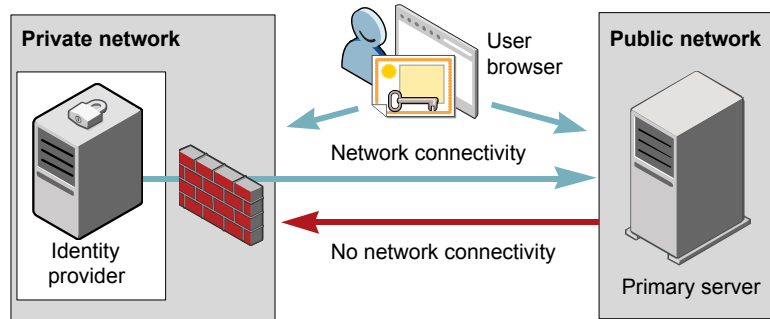


Figure 12-2 Example NAT configuration: Primary server in a private network

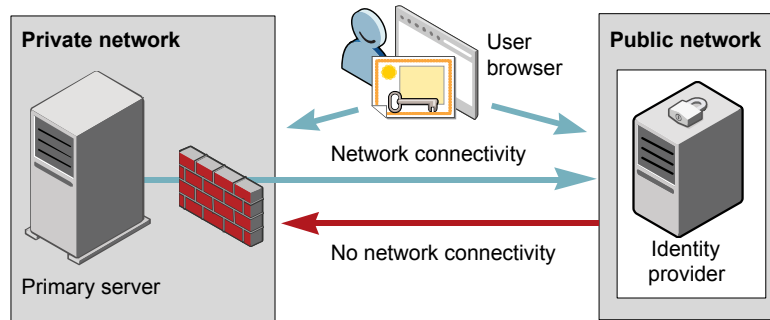


Figure 12-3 Example configuration: Primary server and identity provider in same network

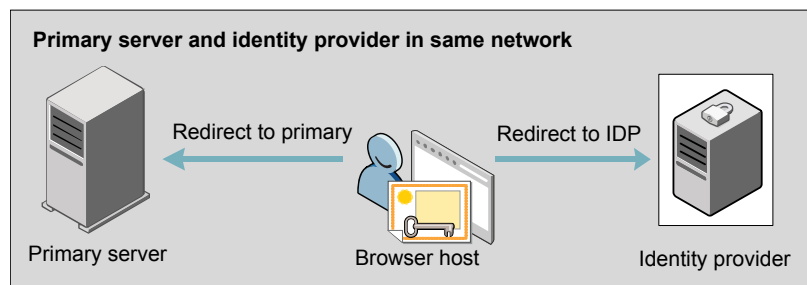
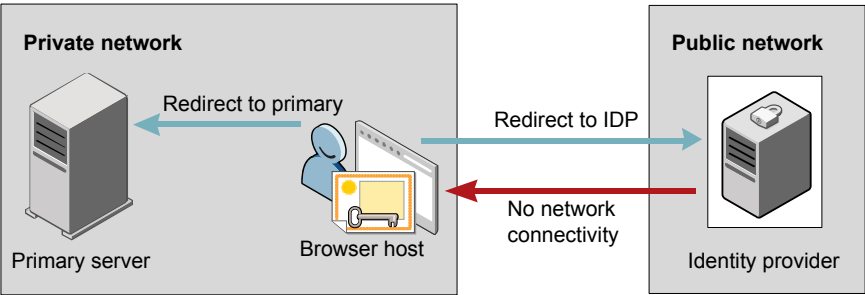


Figure 12-4 Example configuration: Primary server in private network and identity provider in public network



Configure NetBackup for single sign-on (SSO)

This section provides steps to set up trust and exchange configuration information between the IDP and the NetBackup primary server. Before proceeding with the steps, ensure that the following prerequisites are met in your environment:

- An IDP is set up and deployed in your environment.
- The IDP is configured to authenticate domain users of Active Directory (AD) or Lightweight Directory Access Protocol (LDAP).

Table 12-1 Steps to configure NetBackup for single sign-on

Step	Action	Description
1.	Download the IDP metadata XML file	Download and save the IDP metadata XML file from the IDP. SAML metadata that is stored in XML files is used to share configuration information between the IDP and the NetBackup primary server. The IDP metadata XML file is used to add the IDP configuration to the NetBackup primary server.
2.	Configure the SAML keystore, and add and enable the IDP configuration on the NetBackup primary server	See “Configure the SAML KeyStore” on page 158. See “Configure the SAML keystore and add and enable the IDP configuration” on page 161.

Table 12-1 Steps to configure NetBackup for single sign-on (*continued*)

Step	Action	Description
3.	Download the service provider (SP) metadata XML file	The NetBackup primary server is the SP in the NetBackup environment. You can access the SP metadata XML file from the NetBackup primary server by entering the following URL in your browser: <code>https://primaryserver/netbackup/sso/saml2/metadata</code> Where <i>primaryserver</i> is the IP address or host name of the NetBackup primary server.
4.	Enroll the NetBackup primary server as a service provider (SP) with the IDP	See “Enroll the NetBackup primary server with the IDP” on page 164.
5.	Add SAML users and the SAML groups that use SSO to the necessary RBAC roles	SAML users and SAML user groups are available in RBAC only if the IDP is configured and enabled on the NetBackup primary server. For steps on adding RBAC roles, see the following topic. See “Add a user to a role (non-SAML)” on page 144.

After the initial setup, you can choose to enable, update, disable, or delete the IDP configuration.

See [“Manage an IDP configuration”](#) on page 165.

After the initial setup, you can choose to update, renew, or delete the NetBackup CA SAML keystore. You can also configure and manage the ECA SAML keystore.

Configure the SAML KeyStore

To establish a trust between the NetBackup primary server and the IDP server, you must configure an SAML KeyStore on the NetBackup primary server. Depending on whether you are using the NetBackup CA or an external certificate authority (ECA), refer to either of the following sections:

Note: If you are using a combination of an ECA and NetBackup CA in your environment, by default, the ECA is considered while establishing trust with the IDP server.

Note: The SAML KeyStore configuration using batch files, such as `configureCerts.bat`, `configureCerts`, `configureSAMLECACert.bat`, `configureSAMLECACert` and their corresponding options is deprecated.

Configure a NetBackup CA KeyStore

If you are using the NetBackup CA, create the NetBackup CA KeyStore on the NetBackup primary server.

To create a NetBackup CA KeyStore

- 1 Log on to the NetBackup primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -cCert -M master_server -f
```

`-f` is optional. Use the option for the forceful update.

Once the NetBackup CA KeyStore is created, ensure that you update the NetBackup CA KeyStore every time the NetBackup CA certificate is renewed.

To renew the NetBackup CA KeyStore

- 1 Log on to the NetBackup primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -rCert -M master_server
```

- 3 Download the new SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:

`https://primaryserver/netbackup/sso/saml2/metadata`

Where *primaryserver* is the IP address or host name of the NetBackup primary server.

- 4 Upload the new SP metadata XML file to the IDP.

See [“Enroll the NetBackup primary server with the IDP”](#) on page 164.

To remove the NetBackup CA KeyStore

- 1 Log on to the NetBackup primary server as root or administrator.
- 2 Run the following command

```
nbidpcmd -dCert -M master_server
```

- 3 Download the new SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:

`https://primaryserver/netbackup/sso/saml2/metadata`

Where *primaryserver* is the IP address or host name of the NetBackup primary server.

- 4 Upload the new SP metadata XML file to the IDP.
- 5 See “[Enroll the NetBackup primary server with the IDP](#)” on page 164.

Configure an ECA KeyStore

If you are using an ECA, import the ECA KeyStore to the NetBackup primary server.

Note: If you are using a combination of an ECA and the NetBackup CA in your environment, by default, the ECA is considered while establishing trust with the IDP server. To use the NetBackup CA, you must first remove the ECA KeyStore.

To configure an ECA KeyStore

- 1 Log on to the primary server as root or administrator.
- 2 Depending on whether you want to configure SAML ECA keystore using the configured NetBackup ECA KeyStore or you want to provide the ECA certificate chain and private key, run the following commands:
 - Run the following command to use NetBackup ECA configured KeyStore:
`nbidpcmd -cECACert -uECA existing ECA configuration [-f] [-M primary_server]`
 - Run the following command to use ECA certificate chain and private key provided by the user:
`nbidpcmd -cECACert -certPEM certificate chain file -privKeyPath private key file [-ksPassPath Keystore Passkey File] [-f] [-M <master_server>]`
 - Certificate chain file specifies the certificate chain file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
 - Private key file specifies the private key file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
 - KeyStore passkey file specifies the KeyStore password file path and must be accessible to the primary server on which the configuration is being performed.

- Primary server is the host name or IP address of primary server on which you want to perform SAML ECA KeyStore configuration. The NetBackup primary server where you run the command is selected by default.

To remove the ECA KeyStore

- 1 Log on to the primary server as root or administrator.
- 2 Download the new SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:

`https://primaryserver/netbackup/sso/saml2/metadata`

Where *primaryserver* is the IP address or host name of the NetBackup primary server.

- 3 Upload the new SP metadata XML file to the IDP.

See [“Enroll the NetBackup primary server with the IDP”](#) on page 164.

Configure the SAML keystore and add and enable the IDP configuration

Before proceeding with the following steps, ensure that you have downloaded the IDP metadata XML file and saved it on the NetBackup primary server.

To configure SAML keystore and add and enable an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Run the following command.

For IDP and NetBackup CA SAML KeyStore configuration:

```
nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file
[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP user
group field] [-cCert] [-f] [-M primary server]
```

Alternatively for IDP and ECA SAML KeyStore configuration:

Depending on whether you want to configure SAML ECA KeyStore using the configured NetBackup ECA KeyStore or you want to provide the ECA certificate chain and private key, run the following commands:

- Use NetBackup ECA configured keystore:

```
nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata
file[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP
user group field] -cECACert -uECA existing ECA configuration
[-f] [-M Primary Server]
```

- Use ECA certificate chain and private key provided by the user:

```
nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file [-t SAML2] [-e true | false] [-u IDP user field] [-g IDP user group field] -cECACert -certPEM certificate chain file -privKeyPath private key file [-ksPassPath KeyStore passkey file] [-f] [-M primary server]
```

Replace the variables as follows:

- *IDP configuration name* is a unique name provided to the IDP configuration.
- *IDP XML metadata file* is the path to the XML metadata file, which contains the configuration details of the IDP in Base64URL-encoded format.
- *-e true | false* enables or disables the IDP configuration. An IDP configuration must be added and enabled, otherwise users cannot sign in with the single sign-on (SSO) option. Even though you can add multiple IDP configurations on a NetBackup primary server, only one IDP configuration can be enabled at a time.
- The SAML attribute names *IDP user field* and *IDP user group field* are used to map user identity information and group information in the Identity Provider. These fields are optional, and if not provided, they are mapped to the `userPrincipalName` and `memberOf` SAML attributes by default. For instance, if you have customized the attribute mapping in the Identity Provider to use attributes like email and groups, when configuring the SAML configuration, you need to provide the *-u* option for email and *-g* option for groups.

If you have not provided values for these attributes during configuration, ensure that the Identity Provider returns the values against the `userPrincipalName` and `memberOf` attributes.

For Example:

If SAML response is as follows:

```
saml:AttributeStatement <saml:Attribute Name="userPrincipalName">
<saml:AttributeValue>username@domainname</saml:AttributeValue>
</saml:Attribute> <saml:Attribute Name="memberOf">
<saml:AttributeValue>CN=group name,
DC=domainname</saml:AttributeValue> </saml:Attribute>
</saml:AttributeStatement>
```

It implies that you need to map the *-u* and *-g* options against the fields "saml:Attribute Name".

Note: Ensure that the SAML attribute values are returned in the format of *username@domainname* for the field mapped to the `-u` option that defaults to `userPrincipalName`. If you include the domain name when returning group information, it should follow the format "(CN=group name, DC=domainname)" or "(domainname\groupname)".

However, if you return the group name as plain text without domain information, it should be mapped without the domain name in the SAML RBAC group.

- *primary Server* is the host name or IP address of primary server to which you want to add or modify the IDP configuration. The NetBackup primary server where you run the command is selected by default.
- *Certificate Chain File* is the certificate chain file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
Private Key File is the private key file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
KeyStore Passkey File is the KeyStore passkey file path and must be accessible to the primary server on which the configuration is being performed.

If your Identity Provider is already configured with SAML attribute names as `userPrincipalName` and `memberOf`, you do not have to provide the `-u` and `-g` option while configuration. If you are using any other custom attributes name, provide those names against `-u` and `-g` as follows:

For example:

If the Identity Provider SAML attribute names are mapped as "email" and "groups", use the following command for configuration:

```
nbidpcmd -ac -n cohesity_configuration -mxp file.xml -t SAML2 -e true -u email -g groups -cCert -Mprimary_server.abc.com
```

`-u` and `-g` are optional and it depends on the Identity Provider configuration. Ensure that you specify the same parameter values that you have provided at the time of configuration.

Enroll the NetBackup primary server with the IDP

The NetBackup primary server must be enrolled with the IDP as a service provider (SP). For step-by-step procedures that are specific to a particular IDP, see the following table:

Table 12-2 IDP-specific steps for enrolling the NetBackup primary server

IDP name	Link to steps
ADFS	https://support.cohesity.com/s/article/article-100047744
Okta	https://support.cohesity.com/s/article/article-100047745
PingFederate	https://support.cohesity.com/s/article/article-100047746
Azure	https://support.cohesity.com/s/article/article-100047748
Shibboleth	https://www.veritas.com/docs/00047747

Enrolling an SP with an IDP typically involves the following operations:

Uploading the SP metadata XML file to the IDP

The SP metadata XML file contains the SP certificate, the entity ID, the Assertion Consumer Service URL (ACS URL), and a log out URL (SingleLogoutService). The SP metadata XML file is required by the IDP to establish trust, and exchange authentication and authorization information with the SP.

Mapping the SAML attributes to their AD or LDAP attributes

Attribute mappings are used to map SAML attributes in the SSO with its corresponding attributes in the AD or LDAP directory. The SAML attribute mappings are used for generating SAML responses, which are sent to the NetBackup primary server. Ensure that you define SAML attributes that map to the `userPrincipalName` and the `memberOf` attributes in the AD or LDAP directory. The SAML attributes must adhere to the following formats:

Table 12-3

Corresponding AD or LDAP attribute	SAML attribute format
<code>userPrincipalName</code>	<code>username@domainname</code>
<code>memberOf</code>	<code>(CN=group name, DC=domainname)</code>

Note: While adding the IDP configuration to the NetBackup primary server, the values entered for the user (-u) and user group (-g) options must match the SAML attribute names that are mapped to the `userPrincipalName` and the `memberOf` attributes in the AD or LDAP.

See [“Configure the SAML keystore and add and enable the IDP configuration”](#) on page 161.

Manage an IDP configuration

You can manage the identity provider (IDP) configurations on the NetBackup primary server by using the enable (-e true), update (-uc), disable (-e false), and delete (-dc) options of the `nbidpcmd` command.

Enable an IDP configuration

By default, an IDP configuration is not enabled in the product environment. If you did not enable the IDP when you added it, you can use the `-uc -e true` options to update and enable the IDP configuration.

To enable an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -uc -n IDP configuration name -e true
```

Where *IDP configuration name* is a unique name provided to the IDP configuration.

Note: Even though you can configure multiple IDPs on a NetBackup primary server, only one IDP can be enabled at a time.

Update an IDP configuration

You can update the XML metadata file associated with an IDP configuration.

To update the IDP XML metadata file in an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -uc -n IDP configuration name -mxp IDP XML metadata file
```

Replace the variables as described below:

- *IDP configuration name* is a unique name provided to the IDP configuration.

- *IDP XML metadata file* is the path to the XML metadata file, which contains the configuration details of the IDP in Base64URL-encoded format.

If you want to update the IDP user or IDP user group values in an IDP configuration, you must first delete the configuration. The single sign-on (SSO) option is not available for users until you re-add the configuration with the updated IDP user or IDP user group values.

To update IDP user or IDP user group in an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Delete the IDP configuration.

```
nbidpcmd -dc -n IDP configuration name
```

Where *IDP configuration name* is a unique name provided to the IDP configuration.

- 3 To add and enable the configuration again, run the following command:

```
nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file  
[-t SAML2] [-e true | false] [-u IDP user] [-g IDP user group  
field] [-M Master Server]
```

Replace the variables as described below:

- *IDP configuration name* is a unique name provided to the IDP configuration.
- *IDP XML metadata file* is the path to the XML metadata file, which contains the configuration details of the IDP in Base64URL-encoded format.
- *-e true | false* enables or disables the IDP configuration. An IDP must be available and enabled otherwise users cannot sign in with the single sign-on (SSO) option. Even though you can add multiple IDP configurations on a NetBackup primary server, only one IDP configuration can be enabled at a time.
- *Master Server* is the host name or IP address of the primary server to which you want to add or modify the IDP configuration. The NetBackup primary server where you run the command is selected by default.

Disable an IDP configuration

If an IDP configuration is disabled in the product environment, the single sign-on (SSO) option of that IDP is not available for users when they sign in.

To disable an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -uc -n IDP configuration name -e false
```

Where *IDP configuration name* is a unique name provided to the IDP configuration.

Delete an IDP configuration

If an IDP configuration is deleted, the single sign-on (SSO) option of that IDP is not available for users when they sign in.

To delete an IDP configuration

- 1 Log on to the primary server as root or administrator.
- 2 Run the following command:

```
nbidpcmd -dc -n IDP configuration name
```

Where *IDP configuration name* is a unique name provided to the IDP configuration.

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 primary and media server](#)
- [Access Control host properties dialog for the client](#)
- [Using NetBackup Access Control \(NBAC\) with Auto Image Replication](#)
- [Troubleshooting Access Management](#)
- [Using the Access Management utility](#)
- [About determining who can access NetBackup](#)
- [Upgrading NetBackup Access Control \(NBAC\)](#)
- [Configuration requirements if using Change Server with NBAC](#)

About using NetBackup Access Control (NBAC)

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

The NetBackup Access Control (NBAC) is the role-based access control that is used for primary 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 13-1 NBAC considerations

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

Table 13-1 NBAC considerations (*continued*)

Consideration or issue	Description or resolution
Determine if the primary server, media server, or client is to be upgraded	Determine if the primary server, media server, or client is to be upgraded as follows: ■ Some features are provided by upgrading primary servers, some by media servers, and some from upgrading clients. ■ NetBackup works with a higher revision primary server and lower revision clients and media servers. ■ Feature content determines what is deployed. ■ Deployment can be step wise if required.
Information about roles	Determine the roles in the configuration as follows: ■ Who administers the hosts (root permission on primary server equals head administrator). ■ Determine roles to start and then add on the roles as required.
NBAC license requirements	No license is required to turn on the access controls.
NBAC and KMS permissions	Typically when using NBAC and when the <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.
Windows Server Failover Clustering (WSFC) error messages while unhooking shared security services from PBX	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.
Possible cluster node errors	In a clustered environment when the command <code>bpnbaz -setupmaster</code> is run in the context of local Administrator the <code>AUTHENTICATION_DOMAIN</code> entries may not contain the other cluster node entries. In such case these entries must be manually added from Host Properties into the <code>bp.conf</code> file.

Table 13-1 NBAC considerations (*continued*)

Consideration or issue	Description or resolution
Catalog recovery fails when NBAC is set to REQUIRED mode	NetBackup does not support catalog recovery when NBAC is set to the REQUIRED mode. To perform catalog recovery, you must first ensure that the NBAC setting on the primary server and all media servers is configured to PROHIBITED or AUTOMATIC.
Policy validation fails in NBAC mode (USE_VXSS = REQUIRED)	Back up, restore, and verification of policy for snapshot can fail in NBAC enabled mode if one of the following has been done. ■ Authenticated Principle is removed from the NBAC group: NBU_Users group ■ Back up and restore permissions of NBU_User group have been removed
The bpnbaz -setupmaster command fails with an error "Unable to contact Authorization Service"	If a user other than an Administrator tries to modify NetBackup security, the bpnbaz -setupmaster fails. Only a user 'Administrator' who is a part of the Administrator's group has permissions to modify the NetBackup security and enable NBAC.
Failure of authentication broker configuration during installation.	Invalid domain name configuration of the system causes failure during configuration of authentication broker. To correct this problem, use the <code>bpnbaz -configureauth</code> command to configure the authentication broker. For information about the <code>bpnbaz</code> command, see the <i>NetBackup Commands Reference Guide</i>:
NetBackup GUI errors may occur if NBAC is enabled on a system that previously had Enhanced Auditing enabled.	When switching the NetBackup server from Enhanced Auditing to NBAC, make sure that all directories that are named after users are deleted in the following directory: Windows: <code>install_path\NetBackup\logs\user_ops</code> UNIX, Linux: <code>/usr/openv/netbackup/logs/user_ops</code> The following topic contains more details: See "Troubleshooting NBAC issues" on page 188.

Table 13-1 NBAC considerations (*continued*)

Consideration or issue	Description or resolution
NBAC requires the Reverse Hostname Lookup option to be set to Allowed	For NBAC to function properly and to allow communication with NBAC-enabled systems, do the following on the primary server, media servers and all clients: ■ In the NetBackup BAR Console, go to Host Properties > Network Settings. In the NetBackup web UI, go to Host Properties > Edit client > Network settings. ■ Ensure that the Reverse Hostname Lookup option is set to Allowed.

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 BAR Console** to function, the user must have permission to log on to the system remotely.

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

About NetBackup Access Control (NBAC) configuration

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

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

- If required, build a cluster for the primary 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 Primary Server Administrator's Guide](#).

- Configure NBAC for operation by using the instructions provided.
See [“Configuring NetBackup Access Control \(NBAC\)”](#) on page 173.

Configuring NetBackup Access Control (NBAC)

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

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

Configuring NetBackup Access Control (NBAC)

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

See [“Configuring NetBackup Access Control \(NBAC\) on standalone primary servers”](#) on page 174.

Note: The primary 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 177.

- 3 Configure clients for NBAC.

See [“Installing and configuring access control on clients”](#) on page 179.

NBAC configuration overview

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

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

See [“NBAC configure commands summary”](#) on page 179.

Since the configuration is done from the primary server, ensure that operational communications links exist between the primary server, the media servers, and the clients. Review the prerequisites to ensure that you have noted all the associated media servers, clients, and the addresses to communicate with them.

See [“About using NetBackup Access Control \(NBAC\)”](#) on page 168.

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. See the following topic for troubleshooting information:

See [“Configuration and troubleshooting tips for NetBackup Authentication and Authorization”](#) on page 190.

Configuring NetBackup Access Control (NBAC) on standalone primary servers

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

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

Table 13-2 Example host names

Host name	Windows	UNIX
Primary servers	win_primary	unix_primary
Media servers	win_media	unix_media
Clients	win_client	unix_client

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

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

Configuring NBAC on standalone primary servers

- 1 Complete all of the NetBackup primary 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 177.

Installing the NetBackup primary server highly available on a cluster

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

Installing NetBackup with clustering

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

Note: In a Windows clustered environment, after setting up primary server, 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 workaround for this issue is to add the local node name as authentication domain into the `AUTHENTICATION_DOMAIN` on passive nodes after setting up primary server (before failover). Before updating the value of `AUTHENTICATION_DOMAIN`, get the current value using the `bpgetconfig` command. Then add the local node name as authentication domain in the existing domain list using the `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 primary server.

Configuring NetBackup Access Control (NBAC) on a clustered primary 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
`install_path\NetBackup\bin\admincmd`.
- 4 Run `bpnbaz -setupmaster` on the active node.
- 5 Log on to the administration console on the primary server.
- 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 primary server.

Note: Use `-setupmedia set USE_VXSS = AUTOMATIC` on the primary server. If `USE_VXSS = REQUIRED` is set on the primary server and an attempt is made to configure NBAC on media server, the following error can occur: NetBackup primary 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 primary 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 179.

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 179.

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 13-3 NBAC configure commands summary

Command	Description
<pre>bpbaz -GetConfiguredHosts [target.server.com [-out file] -all [-outfile] -file progress.file]</pre>	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. The syntax is: ■ <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 13-3 NBAC configure commands summary (continued)

Command	Description
<code>bpbaz -SetupMaster [-fsa [<domain type>:<domain name>:]<user name>]</code>	The <code>bpbaz -SetupMaster</code> command is run to set up the primary server for using NBAC. The authorization server and authentication broker are expected to be installed and running on the primary server. 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: ■ <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. Note: The user is verified for the existence in the specified domain. Existing behavior of provisioning the logged-on Administrator or root as NBU Admin is preserved.

Table 13-3 NBAC configure commands summary (*continued*)

Command	Description
<pre>bpnbaz -SetupMedia [media.server.com [-out file] -all [-out file] -file progress.file] [-dryrun] [-disable]</pre>	The <code>bpnbaz -SetupMedia</code> command is run by an NBU_Administrator group member on the primary server. It should not be run until a <code>bpnbaz -SetupMaster</code> has been completed successfully. It expects connectivity between the primary server and target media server systems. Either the <code>-all</code> or <code>target.server.com</code> options are required for this command. The syntax is: ■ <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 13-3 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>	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 primary server. It expects connectivity between the primary server and target client systems. Either the <code>-all</code> or <code>target.server.com</code> options are required for this command. The syntax is: ■ <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 primaries, 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

The Cohesity 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.

Details on the `setuptrust` command are described in the [NetBackup Commands Reference Guide](#). See “Using the `setuptrust` command” on page 184.

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 [-F]
```

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.

Use the `-F (--enable_fips)` option to run the `vssat` command in the FIPS mode. By default, the FIPS mode is disabled.

Configuring Access Control host properties for the primary and media server

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

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

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

Authentication Domain tab

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

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

Add the domain that you want users to authenticate against.

The following examples contain six authentication domains.

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

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

Authorization Service tab

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

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

Network Attributes tab

View the **Access Control** host properties on the **Network Attributes** tab. Add the primary 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 primary needs to have the **Access Control** properties configured. These properties are configured on both itself and the primary. This configuration can be done through the host properties on the primary server.

Access Control host properties dialog for the client

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

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

Authentication Domain tab for the client

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

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

Network Attributes tab for the client

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

Using NetBackup Access Control (NBAC) with Auto Image Replication

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

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

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

- In the source primary server domain:
The administrator should make sure that the target primary server has the permissions set correctly before configuration for the operation begins.
- In the target primary server domain:
The security administrator in the target domain must give the administrator in the source domain the correct set of permissions. The source domain administrator needs Browse, Read, and Configure permissions on the following objects: **HostProperties**, **DiskPool**, and **DevHost**.
The source domain administrator can be added as a member to any existing group which has all three permissions.

Consider the following example:

Two NBAC domains each contain a primary server:

- Replication source NBAC domain: *DomainA* contains *Master-A*
- Replication target NBAC domain: *DomainB* contains *Master-B*

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

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

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

- **HostProperties**
- **DiskPool**
- **DevHost**

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

Troubleshooting Access Management

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

See [“Configuration and troubleshooting tips for NetBackup Authentication and Authorization”](#) on page 190.

These verification points include:

- Windows verification points
See [“Windows verification points”](#) on page 196.
- UNIX verification points
See [“UNIX verification points”](#) on page 205.
- Verification points in a mixed environment with a UNIX primary server
See [“Verification points in a mixed environment with a UNIX primary server”](#) on page 212.
- Verification points in a mixed environment with a Windows primary server
See [“Verification points in a mixed environment with a Windows primary server”](#) on page 218.

Troubleshooting NBAC issues

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

Table 13-4 NBAC issues

Issue and Cause	Solution
A user directed backup or restore fails A user-directed backup or restore fails with NBAC in the automated mode. The Backup, Archive, and Restore interface shows some errors in the Windows interface when NBAC is configured. A backup or restore failure can happen when a NetBackup setup on a UNIX primary server is configured with NBAC and you try to use the Windows interface without first configuring the interface for such a setup. Another reason may be that there is an expired certificate in the home directory.	Configure the Windows interface to support the setup. There should be at least one Microsoft Windows system that acts as an Authentication Broker to authenticate users from the Active Directory domain. Refer to the TECH199281 for steps to configure the Windows interface to make use of existing users from Active Directory to manage or operate or use a NetBackup environment that is primarily on UNIX/Linux platforms. After you correctly configure the setup run the <code>bnpbat -logout</code> command to log out from the setup before you restart the interface.
Authentication failure with error 116 The authentication fails with 'error 116-VxSS authentication' when you try to set up NBAC on a target host.	Check whether NBAC authentication is configured correctly and also if you have a valid usable credential for the target host.
Error when a non-admin user from the NBU_Operator group tries to use Access Management A non-admin user is added to the NBU_Operator group. Read, Browse, and Configure permissions are assigned along with the permission to configure the Host Properties. However, when the user tries to open the Access Management utility, an error displays.	The users from the NBU_Operator group have limited permissions. The user would require a different set of permissions to use the Access Management utility. For the required permissions, add the user to the NBU_Security_Admin group. For more information about user groups: See "NetBackup default user groups" on page 229.
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.	

Table 13-4 NBAC issues (*continued*)

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

Configuration and troubleshooting tips for NetBackup Authentication and Authorization

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

Table 13-5 Configuration and troubleshooting tips for NetBackup Authentication and Authorization

Topic	Configuration tips
Verifying primary server settings	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. <pre>bpnbat -whoami -cf "install_path\netbackup\var\vxss\credentials\ primary.company.com "Name: primary.company.com Domain: NBU_Machines@primary.company.com Issued by: /CN=broker/OU=root@primary.company.com/O=vx Expiry Date: Oct 31 20:17:51 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.</pre> If the domain listed is not <code>NBU_Machines@primary.company.com</code>, consider running <code>bpnbat -addmachine</code> for the name in question (primary). The command is run on the computer that serves the <code>NBU_Machines</code> domain (primary). Then, on the computer where you want to place the credentials, run: <code>bpnbat -loginmachine</code>
Establishing root credentials	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>. Use the following command to detect the current value: <pre>echo \$HOME</pre> This value should agree with <code>root</code>'s home directory, which can be typically found in the <code>/etc/passwd</code> file. Note that when switching to <code>root</code>, you may need to use: <pre>su -</pre> instead of only <code>su</code> to correctly condition the <code>root</code> environment variables.
Expired credentials message	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: <pre>Supplied credential is expired or incorrect. Please reauthenticate and try again.</pre> Run <code>bpnbat -Login</code> to update an expired credential.

Table 13-5 Configuration and troubleshooting tips for NetBackup Authentication and Authorization (*continued*)

Topic	Configuration tips
Useful debug logs	The following logs are useful to debug NetBackup Access Control: On the primary: admin, bpcd, bprd, bpdbm, bpjjobd, bpsched On the client: admin, bpcd Access control: nbatd, nbazd. See the NetBackup Troubleshooting Guide for instructions on proper logging.
Where credentials are stored	The NetBackup Authentication and Authorization credentials are stored in the following directories: UNIX: User credentials: \$HOME/.vxss Computer credentials: /usr/opensv/var/vxss/credentials/ Windows: <user_home_dir>\Application Data\VERITAS\VSS
How system time affects access control	Credentials have a birth time and death time. Computers with large discrepancies in system clock time view credentials as being created in the future or prematurely expired. Consider synchronizing system time if you have trouble communicating between systems.

Table 13-5 Configuration and troubleshooting tips for NetBackup Authentication and Authorization *(continued)*

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

Table 13-5 Configuration and troubleshooting tips for NetBackup Authentication and Authorization (*continued*)

Topic	Configuration tips
Stopping NetBackup Authentication and Authorization daemons for Shared Services	When the NetBackup Authentication and Authorization services are stopped, stop authorization first, then stop authentication. UNIX -Use the following commands. To stop authorization use the term signal as shown in the example: <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> To stop authentication use the term signal as shown in the example: <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> Windows Use the Services utility that Windows provides, since these services do not appear in the NetBackup Activity Monitor.
If you lock yourself out of NetBackup	
Backups of storage units on media servers might not work in an NBAC environment	The host name of a system in NetBackup domain (primary server, media server, or client) and host name that is specified in the <code>bp.conf</code> file should be the same.
Using the <code>nbac_cron</code> utility	Use the <code>nbac_cron.exe</code> utility to create identities under which to run cron or at jobs. For more information about the <code>nbac_cron</code> utility: See “About the nbac_cron utility” on page 225. <code>nbac_cron.exe</code> is found in the following location: UNIX <code>-/opt/openv/netbackup/bin/goodies/nbac_cron</code> Windows <code>-install_path\netbackup\bin\goodies\nbac_cron.exe</code> For detailed information about using the <code>nbac_cron</code> utility: See “Using the nbac_cron utility” on page 225.

Table 13-5 Configuration and troubleshooting tips for NetBackup Authentication and Authorization (*continued*)

Topic	Configuration tips
Enabling NBAC after a recovery on Windows	Use the following procedure to manually enable NBAC after a recovery on Windows. ■ 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. Note: On a cluster run the <code>bpclusterutil -enableSvc nbatd</code> and <code>bpclusterutil -enable nbazd</code> commands.
In cluster installations the <code>setupmaster</code> might fail	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.
Known issue on a cluster if shared security services (<code>vxatd</code> or <code>vxazd</code>) are clustered along with the primary server	A known issue exists on a cluster if shared security services (<code>vxatd</code> or <code>vxazd</code>) are clustered along with the primary 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.
Known issue in a clustered primary server upgrade with NBAC, that all the <code>AUTHENTICATION_DOMAIN</code> entries in the <code>bp.conf</code> file are updated with the primary server virtual name as the authentication broker	A known issue exists where in a clustered primary server upgrade with NBAC, all the <code>AUTHENTICATION_DOMAIN</code> entries in the <code>bp.conf</code> file are updated with the primary server virtual name as the authentication broker. If any domain entry is present that refers to a different authentication broker other than the primary server (and the primary server does not service that domain), that entry needs to be manually removed from the <code>bp.conf</code> file.
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>bpnbaz -GetDomainInfosFromAuthBroker</code> returns none. In upgrades, the <code>bp.conf</code> file is updated to have the NetBackup virtual name.

Table 13-5 Configuration and troubleshooting tips for NetBackup Authentication and Authorization (*continued*)

Topic	Configuration tips
Known issue of multiple instances of <code>bpcd</code> causing a possible error	A known issue exists where the <code>bpnbaz -SetupMedia</code> command, <code>bprd</code> uses the <code>AT_LOGINMACHINE_RQST</code> protocol to talk with <code>bpcd</code> on the destination box. A new instance of <code>bpcd</code> is spawned. After the command completes it tries to free a <code>char</code> array as a regular pointer possibly causing <code>bpcd</code> to core dump on the client side. Functionality should not be lost as this <code>bpcd</code> instance is only created temporarily and exits normally. The parent <code>bpcd</code> is unaffected.
Known issue with clusters using shared AT with configuration files on the shared drive	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 <code>NBAZDB</code>	A known issue exists in which some database utilities support and other database utilities do not. The following database utilities support <code>NBAZDB</code>: <code>nbdb_backup</code>, <code>nbdb_move</code>, <code>nbdb_ping</code>, <code>nbdb_restore</code>, <code>nbdb_unload</code>, and <code>nbdb_admin</code>. The <code>dbadm</code> utility does not support <code>NBAZDB</code>.

Windows verification points

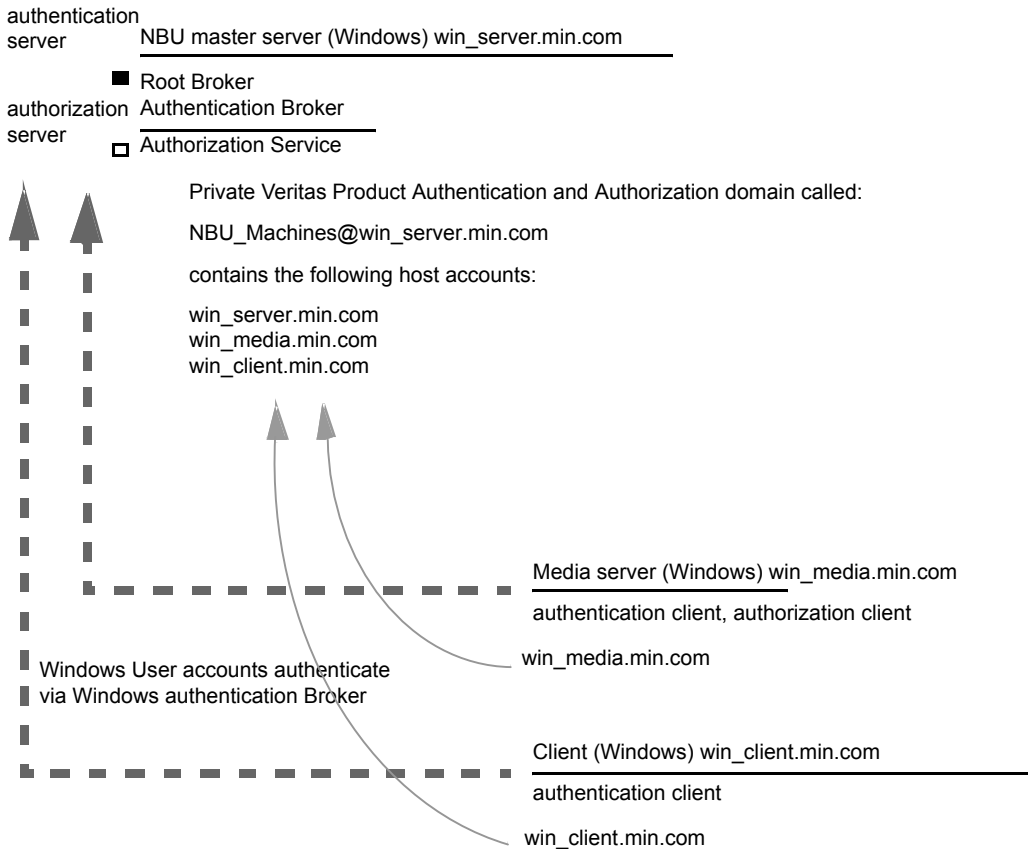
The following configuration procedures can help you verify that the primary server, media server, and client are configured correctly for access control.

These Windows verification points include:

- See [“Primary server verification points for Windows”](#) on page 197.
- See [“Media server verification points for Windows”](#) on page 201.
- See [“Client verification points for Windows”](#) on page 203.

[Figure 13-1](#) shows an example configuration containing Windows systems only.

Figure 13-1 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.

Primary server verification points for Windows

The following topics describe procedures to:

- Verify Windows primary 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 primary server verification procedures for Windows.

Table 13-6 Primary server verification procedures for Windows

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

Table 13-6 Primary server verification procedures for Windows (*continued*)

Procedure	Description
Verify which computers are present in the authentication broker	To verify which computers are present in the authentication broker, log on as a member of the Administrators group and run the following command: <pre>bpnbat -ShowMachines</pre> This command shows the computers for which you have run <code>bpnbat -AddMachine</code>. Note: If a host is not on the list, run <code>bpnbat -AddMachine</code> from the primary. Then run <code>bpnbat -loginMachine</code> from the host in question.
Verify which computers are permitted to perform authorization lookups	To verify which computers are permitted to perform authorization lookups, log on as a member of the Administrators group and run the following command: <pre>bpnbaz -ShowAuthorizers</pre> This command shows that <code>win_primary</code> and <code>win_media</code> (primary 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_primary.company.com</code>. 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. <pre>bpnbaz -ShowAuthorizers ===== Type: User Domain Type: vx Domain:NBU_Machines@win_primary.company.com Name: win_primary.company.com ===== Type: User Domain Type: vx Domain:NBU_Machines@win_primary.company.com Name: win_media.company.com Operation completed successfully.</pre> If a primary server or media server is not on the list of authorized computers, run <code>bpnbaz -allowauthorization server_name</code> to add the missing computer.

Table 13-6 Primary server verification procedures for Windows (*continued*)

Procedure	Description
Verify that the database is configured correctly	To make sure that the database is configured correctly, run <code>bpnbaz -listgroups</code>: <pre> bpnbaz -listgroups NBU_Operator NBU_Admin NBU_SAN Admin NBU_User NBU_Security Admin Vault_Operator Operation completed successfully. </pre> 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>.
Verify that the <code>nbatd</code> and <code>nbazd</code> processes are running	Use the Windows Task Manager to make sure that <code>nbatd.exe</code> and <code>nbazd.exe</code> are running on the designated host. If necessary, start them.
Verify that the host properties are configured correctly	In the access control host properties, verify that the NetBackup Authentication and Authorization property is set correctly. (The setting should be either Automatic or Required, depending on whether all computers use NetBackup Authentication and Authorization or not. If all computers do not use NetBackup Authentication and Authorization, set it to Automatic. The host properties can also be verified by looking at <code>USE_VXSS</code> in the registry at: <pre> HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\NetBackup\ CurrentVersion\config. </pre> Figure 13-2 shows an example of the host properties settings on the Authentication domain tab. In the Access Control host properties, verify that the listed authentication domains are spelled correctly and point to the proper servers (valid authentication brokers). If all of the domains are Windows-based, they should point to a Windows computer that runs the authentication broker.

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

Figure 13-2 Host properties settings

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

Media server verification points for Windows

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

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

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

Table 13-7 Media server verification procedures for Windows

Procedure	Description
Verify the media server	To determine which authentication broker the media server is authenticated against, run <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. For example: <pre>bpnbat -whoami -cf "c:\Program Files\Veritas\Netbackup\var\vxss\credentials\ win_media.company.com" Name: win_media.company.com Domain: NBU_Machines@win_primary.company.com Issued by: /CN=broker/OU=root@win_primary.company.com/ O=vx Expiry Date: Oct 31 20:11:40 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.</pre> If the domain listed is not <code>NBU_Machines@win_primary.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_primary</code>). Then, on the computer where we want to place the certificate (<code>win_media</code>), run: <pre>bpnbat -loginmachine</pre>

Table 13-7 Media server verification procedures for Windows (*continued*)

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

Client verification points for Windows

The following topics describe the client verification procedures for Windows:

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

The following table describes the client verification procedures for Windows.

Table 13-8 Client verification procedures for Windows

Procedure	Description
Verify the credential for the client	Check that the credential for the client is indeed for the correct client and comes from the correct domain. Run <code>bpnbat -whoami</code> with <code>-cf</code> for the client's credential file. For example: <pre>bpnbat -whoami -cf "install_path \Netbackup\var\vxss\credentials\ win_client.company.com " Name: win_client.company.com Domain: NBU_Machines@win_primary.company.com Issued by: /CN=broker/OU=root@win_primary.company.com/ O=vx Expiry Date: Oct 31 20:11:45 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.</pre> If the domain listed is not <code>NBU_Machines@win_primary.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_primary</code>). Then, on the computer where we want to place the certificate (<code>win_client</code>), run: <pre>bpnbat -loginmachine</pre>
Verify that the authentication client libraries are installed	Note: Run <code>bpnbat -login</code> on the client to verify that the authentication client libraries are installed. <pre>bpnbat -login Authentication Broker: win_primary Authentication port [Enter = default]: Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd) : WINDOWS Domain: ENTERPRISE Name: Smith Password:Operation completed successfully.</pre> If the libraries are not installed, a message displays: The NetBackup Authentication and Authorization libraries are not installed. This verification can also be done by looking at the Windows Add/Remove Programs.

Table 13-8 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.

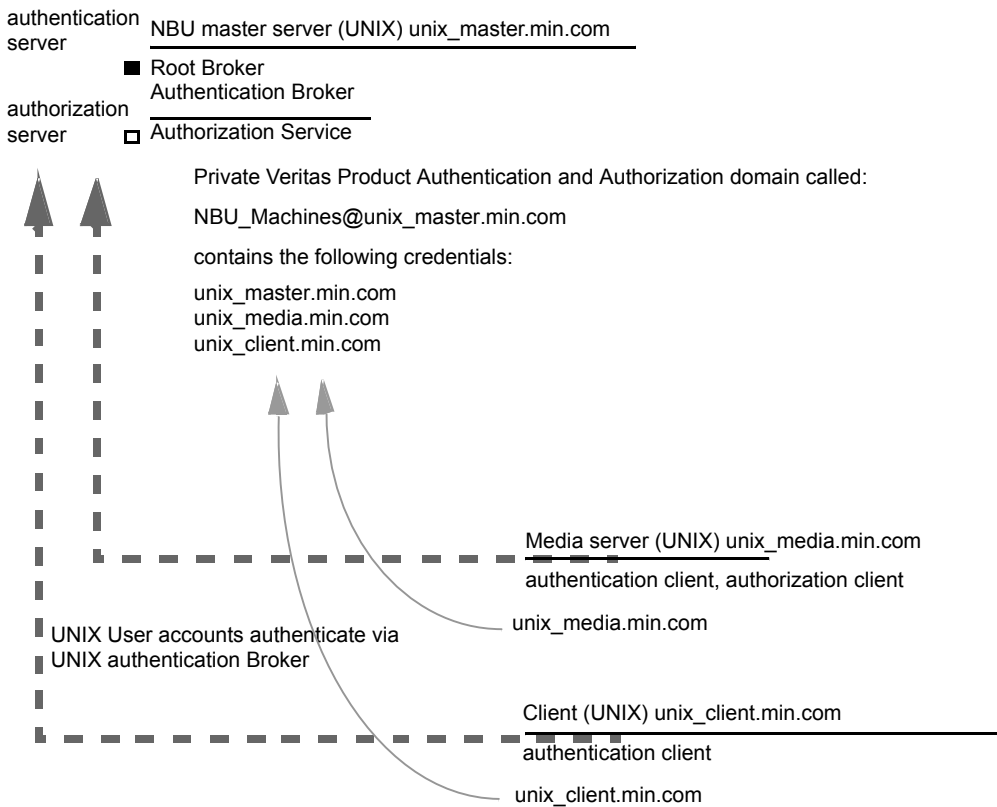
UNIX verification points

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

- UNIX primary server verification
See “[UNIX primary server verification](#)” on page 206.
- UNIX media server verification
See “[UNIX media server verification](#)” on page 209.
- UNIX client verification
See “[UNIX client verification](#)” on page 211.

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

Figure 13-3 Example configuration containing UNIX systems only



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

UNIX primary server verification

Use the following procedures to verify the UNIX primary server:

- Verify UNIX primary 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 primary server.

Table 13-9 Verification process for the UNIX primary server

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

Table 13-9 Verification process for the UNIX primary server (*continued*)

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

Table 13-9 Verification process for the UNIX primary server (*continued*)

Process	Description
Verify that the nbatd and nbazd processes are running	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. For example: <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	In the Access Control host properties, verify that the NetBackup Authentication and Authorization property is set correctly. (The setting should be either Automatic or Required, depending on whether all of the computers use NetBackup Authentication and Authorization or not. If all computers do not use NetBackup Authentication and Authorization, set it to Automatic.) In the Access Control host properties, verify that the authentication domains on the list are spelled correctly. Also make sure that they point to the proper servers (valid authentication brokers). If all domains are UNIX-based, they should point to a UNIX machine that is running the authentication broker. This process can also be verified in <code>bp.conf</code> using <code>cat</code>. <pre>cat bp.conf SERVER = unix_primary SERVER = unix_media CLIENT_NAME = unix_primary AUTHENTICATION_DOMAIN = company.com "default company NIS namespace" NIS unix_primary 0 AUTHENTICATION_DOMAIN = unix_primary "unix_primary password file" PASSWD unix_primary 0 AUTHORIZATION_SERVICE = unix_primary.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 13-10 Verification process for the UNIX media server

Process	Description
Verify the media server	To determine which authentication broker the media server is authenticated against, run <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. For example: <pre> bpnbat -whoami -cf /usr/opensv/var/vxss/credentials/unix_media.company.com Name: unix_media.company.com Domain: NBU_Machines@unix_primary.company.com Issued by: /CN=broker/OU=root@unix_primary.company.com/ O=vx Expiry Date: Oct 31 14:48:08 2007 GMT Authentication method: Veritas Private Security Operation completed successfully. </pre> If the domain listed is not <code>NBU_Machines@unix_primary.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_primary</code>). Then, on the computer where we want to place the certificate, run (<code>unix_primary</code>): <pre> bpnbat -loginmachine </pre>
Verify that the server has access to the authorization database	To make sure that the media server is able to access the authorization database as it needs, run <code>bpnbaz -ListGroup</code> "machine_credential_file" For example: <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> If this command fails, run <code>bpnbaz -AllowAuthorization</code> on the primary server that is the authorization server (<code>unix_primary</code>). Note that you need to run as root or administrator.

Table 13-10 Verification process for the UNIX media server (*continued*)

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

UNIX client verification

The following procedures are used to verify the UNIX client:

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

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

Table 13-11 Verification procedures for the UNIX client

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

Table 13-11 Verification procedures for the UNIX client (*continued*)

Procedures	Description
Verify that the authentication client libraries are installed	Run <code>bpbnet -login</code> on the client to verify that the authentication client libraries are installed. <pre> bpbnet -login Authentication Broker: unix_primary.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	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. This process can also be verified in <code>bp.conf</code> using <code>cat (1)</code>. <pre> cat bp.conf SERVER = unix_primary SERVER = unix_media CLIENT_NAME = unix_primary AUTHENTICATION_DOMAIN = min.com "default company NIS namespace" NIS unix_primary 0 AUTHENTICATION_DOMAIN = unix_primary.company.com "unix_primary password file" PASSWD unix_primary 0 AUTHORIZATION_SERVICE = unix_primary.company.com 0 USE_VXSS = AUTOMATIC </pre>

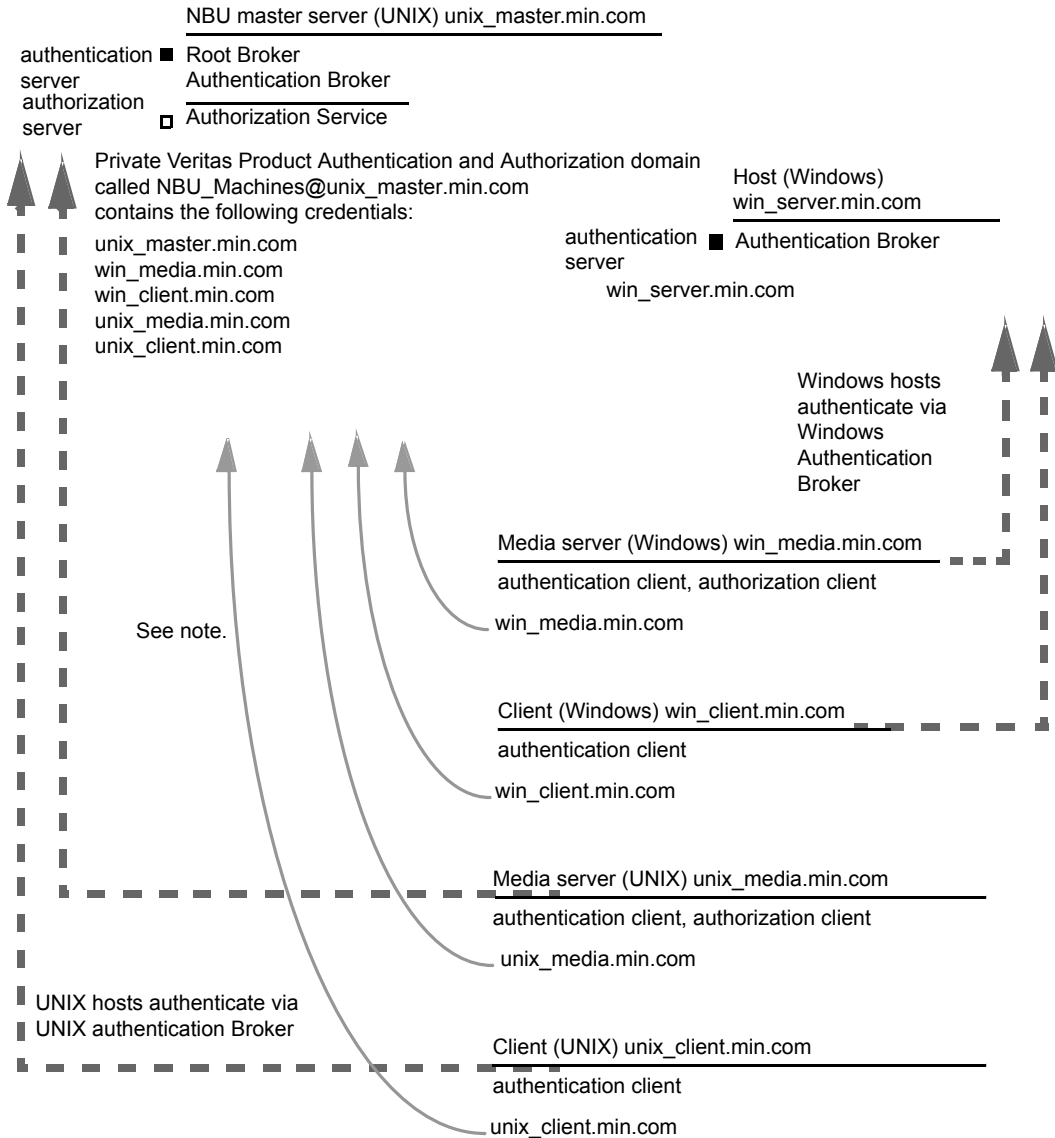
Verification points in a mixed environment with a UNIX primary server

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

- Primary server verification points for mixed UNIX primary
- Media server verification points for mixed UNIX primary
- Client verification points for mixed UNIX primary

Figure 13-4 is an example of a mixed configuration that contains a UNIX primary server.

Figure 13-4 Example mixed configuration containing a UNIX primary 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.

Primary server verification points for a mixed UNIX primary server

See the following topic for the verification procedure for a UNIX primary server:
See [“UNIX primary server verification”](#) on page 206.

Media server verification points for a mixed UNIX primary server

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

Table 13-12 Verification procedures for a mixed UNIX primary 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 209.
Verify the Windows media server	Check that the computer certificate comes from the root authentication broker, which is found on the UNIX primary server (unix_primary). If there is a missing certificate, run the following commands to correct the problem: ■ <code>bpnbat -addmachine</code> on the root authentication broker (in this example, <code>unix_primary</code>) ■ <code>bpnbat -loginmachine</code> (in this example, <code>win_media</code>) For example: <pre>bpnbat -whoami -cf "install_path \Netbackup\var\vxss\credentials\ win_media.company.com" Name: win_media.company.com Domain: NBU_Machines@unix_primary.company.com Issued by: /CN=broker/OU=root@ unix_primary.company.com/O=vx Expiry Date: Oct 31 20:11:04 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.</pre>

Table 13-12 Verification procedures for a mixed UNIX primary server
(continued)

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

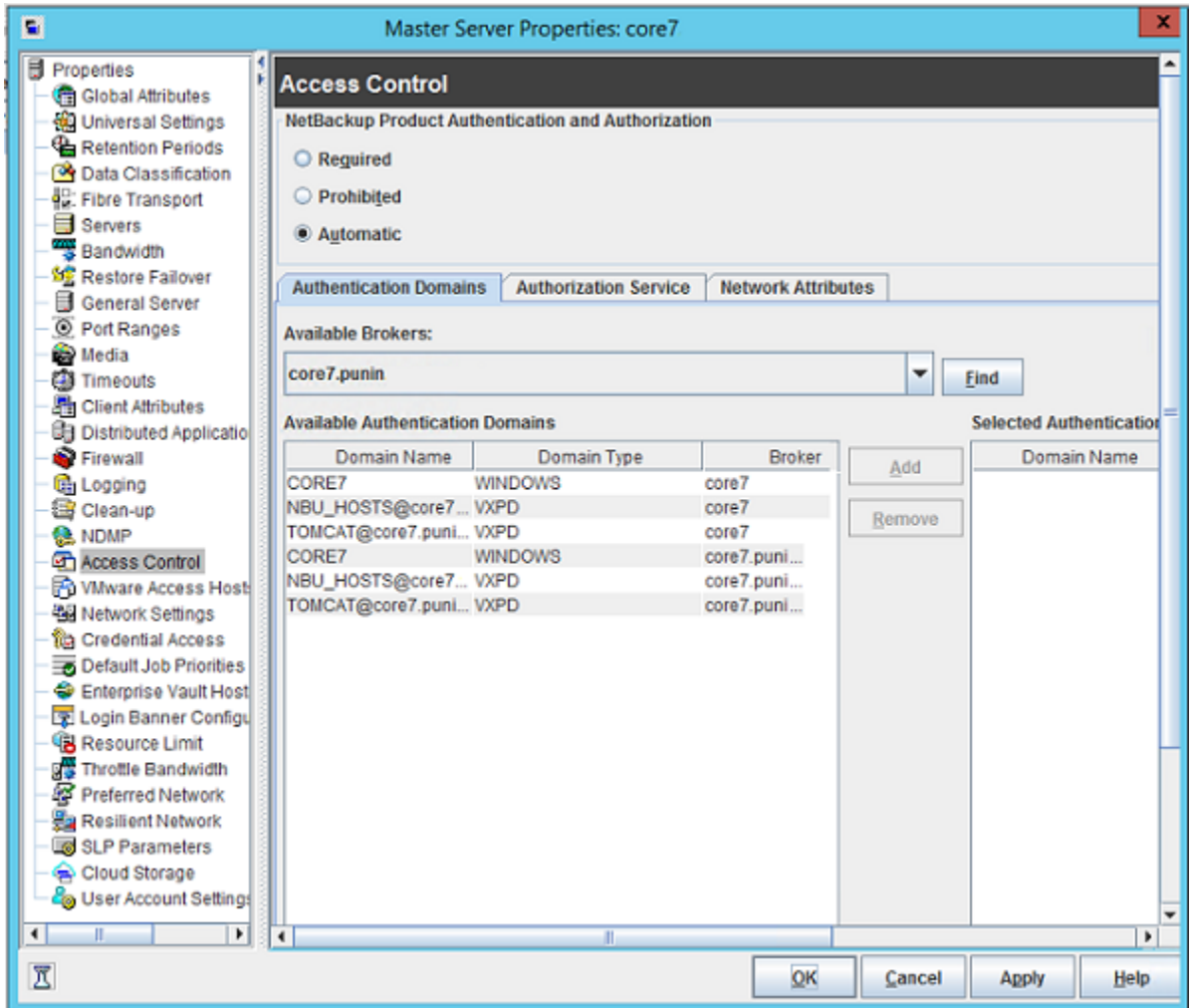
Table 13-12

Verification procedures for a mixed UNIX primary server

(continued)

Procedure	Description
Cross platform authentication domains	Take extra care in mixed environments to ensure that the appropriate domain types point to the correct authentication brokers. The example Authentication domain tab shows available authentication Windows domains that can be added to the Windows broker. In this case, it is not a mixed environment as both systems are Windows based. If there were a combination of Windows and UNIX domains it is important to match the brokers to the most useful authentication domains. Figure 13-5 for a display on how to match the platform to the most useful authentication domains.

Figure 13-5 Cross platform authentication domains



Client verification points for a mixed UNIX primary server

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

See [“UNIX client verification”](#) on page 211.

The following table describes the procedures to verify Windows clients.

Table 13-13 Procedures to verify Windows clients

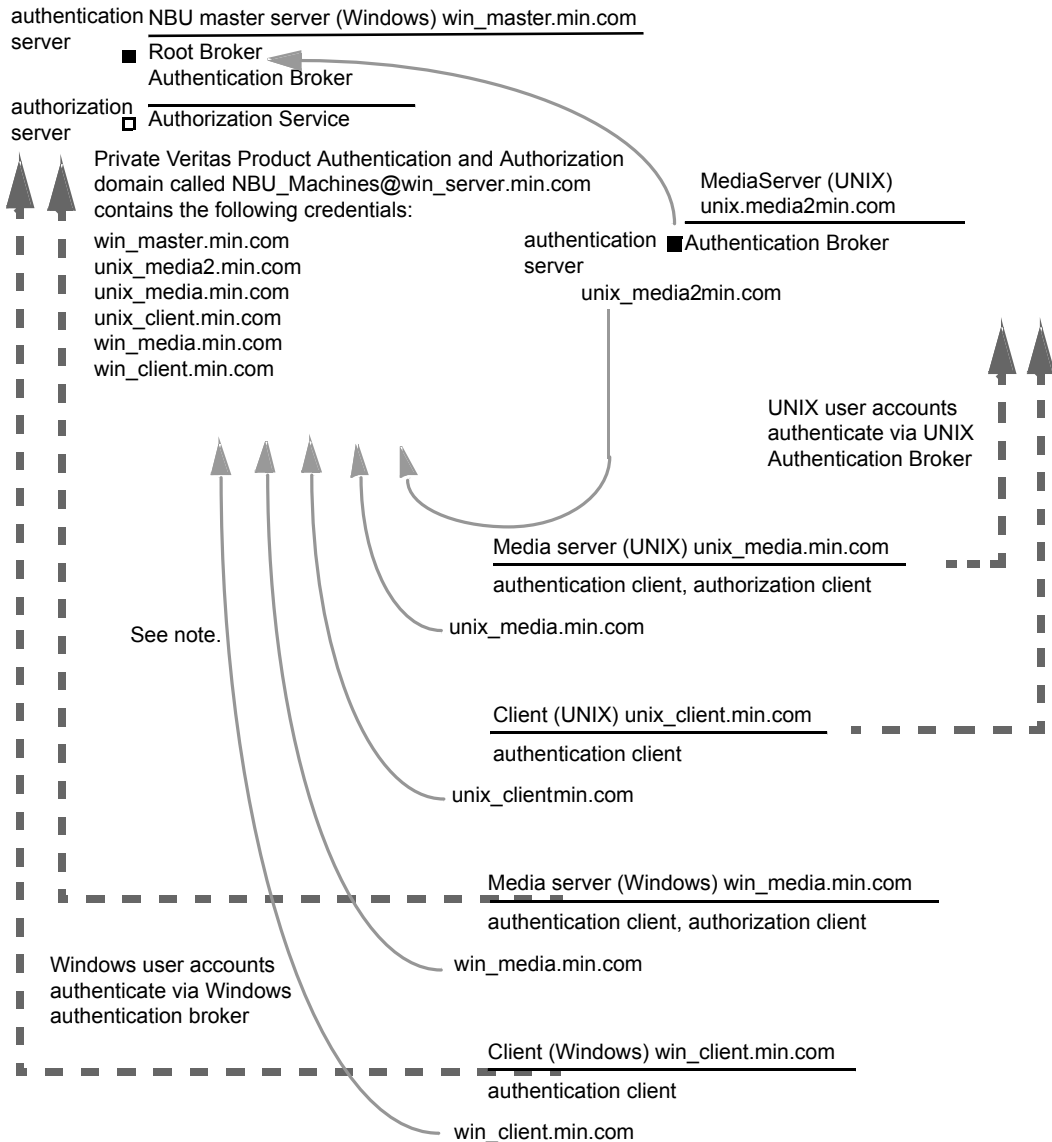
Procedures	Description
Verify the credential for the Windows client	Check that the credential for the client is indeed for the correct client and comes from the correct domain. Run <code>bpnbat -whoami</code> with <code>-cf</code> for the client's credential file. For example: <pre> bpnbat -whoami -cf "c:\Program Files\Veritas\Netbackup\var\vxss\credentials\ win_client.company.com Name: win_client.company.com Domain: NBU_Machines@unix_primary.company.com Issued by: /CN=broker/OU=root@unix_primary.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	Run <code>bpnbat -login</code> on the client to verify that the authentication client libraries are installed. For example: <pre> bpnbat -login Authentication Broker: unix_primary.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	Ensure that the Windows authentication broker has mutual trust with the main UNIX authentication broker. Also, make sure that the broker uses the UNIX broker as its root broker.

Verification points in a mixed environment with a Windows primary server

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

- Primary server verification points for mixed Windows primary
See [“Primary server verification points for a mixed Windows primary server”](#) on page 221.
 - Media server verification points for mixed Windows primary
See [“Media server verification points for a mixed Windows primary server”](#) on page 221.
 - Client verification points for mixed Windows primary
See [“Client verification points for a mixed Windows primary server”](#) on page 223.
- [Figure 13-6](#) is an example configuration that contains a Windows primary server.

Figure 13-6 Example mixed configuration containing a Windows primary 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.

Primary server verification points for a mixed Windows primary server

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

See [“Primary server verification points for Windows”](#) on page 197.

Media server verification points for a mixed Windows primary server

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

Table 13-14 Media server verification procedures for a mixed Windows primary server

Procedure	Description
Verify the Windows media server for a mixed Windows primary server	See the following topic for the verification procedures for a Windows media server: See “Media server verification points for Windows” on page 201.
Verify the UNIX media server	Check that the computer certificate is issued from the root authentication broker, found on the Windows primary server (win_primary). 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/openv/var/vxss/credentials/unix_media.company.com Name: unix_media.company.comDomain: NBU_Machines@ win_primary.company.com Issued by: /CN=broker/OU=root@win_primary.company.com/ O=vx Expiry Date: Oct 31 14:48:08 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.</pre>

Table 13-14 Media server verification procedures for a mixed Windows primary server (*continued*)

Procedure	Description
Verify that the server has access to the authorization database	To make sure that the media server is able to access the authorization database it needs to perform authorization checks. Run <code>bpnbaz -ListGroup -CredFile "/usr/opensv/var/vxss/credentials/<hostname>"</code> For example: <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> If the media server is not allowed to perform authorization checks, run <code>bpnbaz -allowauthorization</code> on the primary server for the media server name in question.
Unable to load library message	Verify the media server and that it has access to the proper database indirectly. This verification informs us that the NetBackup Authentication and Authorization client libraries for both authentication and authorization are properly installed. If either of these procedures fail with a message "unable to load libraries": Check to make certain the authentication client libraries and authorization client libraries are installed.

Table 13-14 Media server verification procedures for a mixed Windows primary server (*continued*)

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

Client verification points for a mixed Windows primary server

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

Table 13-15 Verification procedures for a mixed Windows primary server

Procedure	Description
Verify the credential for the Windows client	See the following topic for the verification procedures for Windows clients: See “Client verification points for Windows” on page 203.

Table 13-15 Verification procedures for a mixed Windows primary server
(continued)

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

About the nbac_cron utility

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

The utility is found in the following location:

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

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

See [“Using the nbac_cron utility”](#) on page 225.

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 primary 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 Cohesity 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 BAR 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 BAR 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 BAR Console > Access Management > NBU user groups** window.

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

UNIX

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

Windows

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

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

```
bpnbaz -ListGroups
NBU_User
NBU_Operator
```

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

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

About determining who can access NetBackup

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

- The permissions of individual users.
See ["Individual users"](#) on page 228.
- The creation of user groups.
See ["User groups"](#) on page 229.

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

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

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

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

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

Individual users

The NetBackup **Access Management** utility uses your existing OS-defined users, groups, and domains. The **Access Management** utility maintains no list of users

and passwords. When members of groups are defined, the Security Administrator specifies existing OS users as members of user groups.

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

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

User groups

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

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

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

NetBackup default user groups

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

The following table describes each NetBackup default user group.

Table 13-16 NetBackup default user groups

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

Table 13-16 NetBackup default user groups (*continued*)

Default user group	Description
Vault operator (Vault_Operator)	The Vault_Operator user group is the default user group that contains permissions to perform the operator actions necessary for the Vault process.
KMS Administrator (NBU_KMS Admin)	By default, members of the NBU_KMS Admin user group have full permissions to browse, read, operate and configure encryption key management properties. These permissions make sure that you can configure the KMS environment and NetBackup's interaction with it.
Additional user groups	The Security Administrator (member of NBU_Security Admin or equivalent) can create user groups as needed. The default user groups can be selected, changed, and saved. It is recommended 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 BAR 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 234.

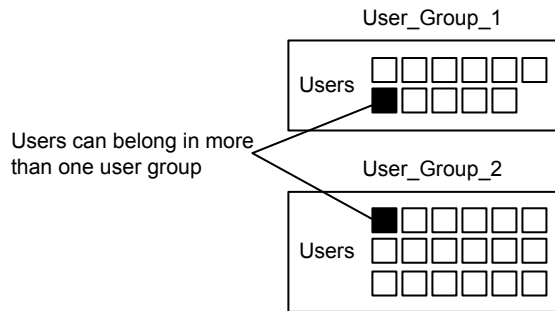
About defining a user group and users

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

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

Figure 13-7 shows defining a user group.

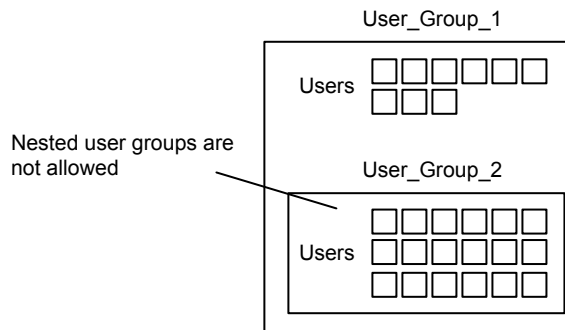
Figure 13-7 Defining a user group



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

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

Figure 13-8 Nested user groups are not allowed



Logging on as a new user

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

To log on as a new user

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

Assigning a user to a user group

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

To add a user to a user group

- 1 As a member of the NBU_Security Admin user group (or equivalent), expand **Access Management > NBU User Groups**.
- 2 Double-click on the user group to which you want to add a user.
- 3 Select the **Users** tab and click **Add User**.
- 4 Enter the user name and the authentication domain. Select the domain type of the user: NIS, NIS+, PASSWD, Windows, or Vx.
- 5 Select the **Domain Type** of the user:
 - NIS
Network Information Services
 - NIS+
Network Information Services Plus
 - PASSWD
UNIX password file on the authentication server
 - Windows
Primary domain controller or Active Directory
 - Vx
Cohesity 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 BAR Console** tree.

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

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

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

- **Browse/Read**
- **Operate**
- **Configure**

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

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 primary 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 Cohesity product uses them.

Configuration requirements if using Change Server with NBAC

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

The following steps assume that NBAC 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 primary servers):
 - Use the `vssat` command to set up trust between the primary servers of *fromServer* and *toServer*.
 - Add the primary 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.

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 primary server by using either the `vssat` command or explicitly log on to each server at least once.

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

Minimizing security configuration risk

This chapter includes the following topics:

- [About security configuration risk](#)
- [Security settings to be configured to minimize risk](#)
- [Set the current posture as security baseline](#)
- [Manage security baseline](#)
- [Manage security baseline from Alta View UI](#)

About security configuration risk

Security configuration risk depends on the status of the security settings in your NetBackup domain. A high configuration risk score implies that more number of security settings need to be configured in the domain. To minimize the risk, enable all the required security settings.

The security risk score is also determined based on the active status of each host in the domain. A host is considered to be active if it has participated in secure communication within the domain during the last seven days.

Risk score for the following settings is determined based on the active status of the hosts:

- Secure data-in-transit encryption (DTE)
See [“Data-in-transit encryption support”](#) on page 365.
- Service user configuration
See [“Configuring a service user account”](#) on page 591.

See [“Security settings to be configured to minimize risk”](#) on page 239.

For more information on how to minimize the security configuration risk, see the [article](#).

The NetBackup web UI dashboard shows the security configuration risk score. When you change any of the security settings, the risk score is updated on the dashboard.

The following parameters help you learn the current security scenario in your domain and how you can minimize the security configuration risk.

Use the NetBackup web UI dashboard to see these parameters.

Current posture

Current posture comprises the current values of NetBackup security settings. It is recommended that you enable all security settings to minimize the security configuration risk.

See [“Security settings to be configured to minimize risk”](#) on page 239.

Security baseline

Security baseline is a collection of recommended security settings for your NetBackup domain. For the first time, you configure the security settings as per the recommendation, and use this current posture as your security baseline.

By default, security baseline is not configured.

See [“Security settings to be configured to minimize risk”](#) on page 239.

See [“Set the current posture as security baseline”](#) on page 241.

The security baseline is managed by the NetBackup Administrator or the Security Administrator.

For primary servers that are registered with Cohesity Alta View server, the security baseline is managed by the Cohesity Alta View Administrator.

Recommended values

Recommended values for any given setting represents the possible values of the setting which are considered secure. It is highly recommended to align the current posture of every setting as per the recommended values in order to observe the most secure environment.

Compliance status

If a NetBackup security setting (current posture) does not comply with the security baseline, it is shown in the compliance status as 'Not compliant with the baseline'.

You should review the compliance status and modify the security settings to minimize the risk.

RBAC roles and permissions

To view the **Security configuration risk** card on the NetBackup web UI dashboard, you should have the following roles and permissions:

See [“Configuring RBAC”](#) on page 131.

RBAC roles

Custom

Permissions

View, update global security settings

Security settings to be configured to minimize risk

Configure the following security settings to minimize the security configuration risk.

See [“About security configuration risk”](#) on page 237.

Table 14-1

Security settings	Description
Insecure communication with 8.0 and earlier hosts	This setting determines if insecure communication with 8.0 and earlier hosts is enabled or not. It is recommended that you disable the setting to ensure only the secure communication in the domain.
Security level for certificate deployment	Determines the checks that are performed before the NetBackup CA issues a certificate to a NetBackup host. It is recommended that you set it to High or Very High. See “About NetBackup certificate deployment security levels” on page 308.
Multifactor authentication (MFA)	This setting adds an additional layer of protection in addition to passwords that significantly reduces the risk of malicious access. Enforcing multifactor authentication for all users is recommended. See “Enforce multifactor authentication for all users” on page 245.
Secure data-in-transit encryption (DTE)	This setting determines the global data-in-transit encryption (DTE) mode. It is recommended that you set it to Enforced or Preferred On. See “Configure the global data-in-transit encryption setting” on page 367.
Percent of hosts with DTE enabled	This setting determines the percentage of active hosts in the domain that are participating in DTE.

Table 14-1 (continued)

Security settings	Description
Multiperson authorization (MPA)	This setting ensures that critical actions or decisions are approved by multiple authorized individuals, minimizing the risk of errors, fraud, or misuse of privileges. Enabling this setting is recommended. See “Configure multiperson authorization” on page 257.
Malware detection	This setting determines if malware detection is configured or not. Malware detection scans backup images and detects malware. Configuring malware detection is recommended.
Anomaly detection	This setting detects any unusual deviation in backup job or system attributes and notifies it as an anomaly. Enabling backup and system anomaly detection is recommended. See “Configure backup anomaly detection settings” on page 606. See “Configure system anomaly detection settings” on page 613.
Percent of hosts with service user configured	Measures the percentage of active hosts that are configured to run NetBackup services under a service user account. Having NetBackup services configured to run under a service user (non-privileged user) account is highly recommended. Security configuration risk can be reduced if more hosts are configured to run NetBackup services under service user account. Active primary server, media server, and client hosts are considered for service user configuration.
Percent of encryption-enabled backup storage	This setting identifies the percentage of total active backup storage that is configured to encrypt the data at rest.
Immutable backup storage	This setting identifies if there is at least one active WORM backup storage to be configured. It can either be a storage unit or a tape volume.
Percent of servers with version (primary version) or later	This setting represents the percentage of active hosts (primary and media servers) with NetBackup version later or same as the primary server.
Percent of other hosts with version (primary version) or later	This setting represents the percentage of active hosts (other than primary and media servers) with NetBackup version later or same as the primary server.
CLI access to OS administrator	This setting enables or disables the CLI access for the operating system administrator. It is recommended to disable the setting.
Web UI access to OS administrator	This setting enables or disables web UI access for the operating system administrator. It is recommended to disable the setting.
Client-initiated redirected restores	This setting determines if client-initiated redirected restores are allowed in the domain. It depends on the presence of the <code>No.Restrictions</code> file. It is recommended to remove this file if it exists.

Set the current posture as security baseline

Current posture comprises the current values of NetBackup security settings. It is recommended that you enable all security settings to minimize the security configuration risk.

See [“About security configuration risk”](#) on page 237.

Security baseline is a collection of recommended security settings for your NetBackup domain. For the first time, you configure the security settings as per the recommendation, and use this current posture as your security baseline.

Note: If API is used to set the security baseline, ensure that you provide at least one attribute. Rest of the attributes are set to null. Use the current posture values as security baseline.

At any point in time, a user with the view and update global security settings permissions can set the current configuration posture as the security baseline.

Set the current posture as security baseline

- 1 Enable the security settings to minimize the security configuration risk.
See [“Security settings to be configured to minimize risk”](#) on page 239.
- 2 On the **Global security settings > Overview** tab, click **Set security baseline**.
After the security baseline is set, if a NetBackup security setting is modified and therefore it no longer complies with the security baseline, it is flagged in the compliance status on the **Global security settings > Overview** tab.

Manage security baseline

You can manage or modify the security baseline that you have set earlier.

See [“Set the current posture as security baseline”](#) on page 241.

You can import, export or remove the security baseline. You can also manage the security baseline from the Alta View UI if the associated Alta View server is registered with NetBackup.

Note: The security baseline cannot be modified if it is managed by Alta View administrator. In this case, you can only use the **Export security baseline** option.

To manage security baseline

1 Click **Settings > Global security**.

2 On the **Global security settings > Overview** tab, click **Manage security baseline**.

If you have not set the security baseline earlier, the **Manage security baseline** option is not visible.

3 On the **Manage security baseline** pop-up screen, use one of the following options:

- **Use current posture values as security baseline** - The current posture (security settings values) is set as security baseline.
- **Import security baseline** - An authorized user can set the security baseline by using the import option. This option allows you to provide a JSON file with the security baseline data. The JSON file is created by exporting the security baseline that is set for a NetBackup domain. Select a JSON file with a size that is within the allowed range of 10 KB.
- **Export security baseline** - An authorized user can export the current security baseline into a JSON file. This JSON file can further be used to set the security baseline by providing this file for the import option.
- **Remove the current security baseline** - An authorized user can delete the security baseline. If a security baseline is set by an Alta View user, it can be modified only by the Alta View user.
If security baseline is deleted, notifications are not generated for any changes in the security risk.

Manage security baseline from Alta View UI

If a security baseline is set by an Alta View user, it cannot be modified or deleted by NetBackup users. Only Alta View users can modify the security baseline.

If the baseline is set by an Alta View user, the **Manage security baseline** option is disabled for NetBackup users.

See [“Manage security baseline”](#) on page 241.

Configuring multifactor authentication

This chapter includes the following topics:

- [About multifactor authentication](#)
- [Configure multifactor authentication for your user account](#)
- [Disable multifactor authentication for your user account](#)
- [Enforce multifactor authentication for all users](#)
- [Configure multifactor authentication for your user account when it is enforced in the domain](#)
- [Reset multifactor authentication for a user](#)

About multifactor authentication

Multifactor authentication is a multiple-step account login process that requires you to enter a 6-digit one-time password along with your password.

It is strongly recommended that you configure multifactor authentication to protect the security of your environment.

Note: User logins that are based on the following authentication types do not support multifactor authentication: SAML, smart card, and API keys.

See [“Configure multifactor authentication for your user account”](#) on page 244.

If multifactor authentication is configured, you may need to reauthenticate yourself by entering the one-time password that you see in the authenticator application on your smart device before you perform the following operations:

- Manage the global security settings for the primary server
- Adding an API key

If multifactor authentication is enforced in the NetBackup domain, all users must configure multifactor authentication for their user accounts for successful sign-in.

See [“Configure multifactor authentication for your user account when it is enforced in the domain”](#) on page 246.

Configure multifactor authentication for your user account

For enhanced security, you can configure multifactor authentication for your user account. You must first install and configure authenticator application on your smart device that provides you with the one-time password.

Configuring multifactor authentication in NetBackup does not require internet connectivity on your smart device.

If the NetBackup administrator has enforced multifactor authentication in the NetBackup domain, you must configure it for your user account for successful sign-in.

See [“Disable multifactor authentication for your user account”](#) on page 245.

To configure multifactor authentication for your user account

- 1 Sign in to the NetBackup web UI.
- 2 On the top right, click the profile icon and click **Configure multifactor authentication**.
- 3 On the **Configure multifactor authentication** screen, click **Configure**.
- 4 On the next screen, follow the given steps.

Install and configure authenticator application on your smart device. It generates one-time password and sends it on your smart device.

[Supported authenticator applications](#)

- 5 Scan the QR code with the authenticator application or enter the key manually.

- 6 Enter the one-time password that you see in the authenticator application on your smart device.

- 7 Select **Configure**.

At the time of next sign-in, you need to enter the one-time password along with the username and password.

Disable multifactor authentication for your user account

If multifactor authentication is not enforced, you can disable it for your user account. However, it is strongly recommended that you configure multifactor authentication to protect the security of your account.

See [“Configure multifactor authentication for your user account”](#) on page 244.

To disable multifactor authentication for your user account

- 1 Sign in to the NetBackup web UI.
- 2 On the top right, click the profile icon and select **Configure multifactor authentication**.
- 3 If you have already configured multifactor authentication for your user account, you can see the **Disable** option.
- 4 Select **Disable**.
- 5 Enter the one-time password and click **Confirm**.

Enforce multifactor authentication for all users

Only the NetBackup administrator can enforce multifactor authentication for all NetBackup users.

To enforce multifactor authentication for all users

- 1 Sign in to the NetBackup web UI.
- 2 On the top right, click **Settings > Global security**.
- 3 On the **Security controls** tab, turn on **Enforce multifactor authentication**.
Select **Confirm** to enforce multifactor authentication for all NetBackup users.
Notify all users that they must configure multifactor authentication for their user accounts to be able to successfully sign in.

See [“Configure multifactor authentication for your user account”](#) on page 244.

Configure multifactor authentication for your user account when it is enforced in the domain

After multifactor authentication is enforced in the domain, you must configure it for your user account if you have not already configured it. If you do not configure multifactor authentication for your account after the enforcement, you cannot sign-in.

To configure multifactor authentication after the enforcement

- 1 Open a web browser and go to the following URL.
`https://primaryserver/webui/login`
The *primaryserver* is the host name or IP address of the NetBackup primary server that you want to sign in to.
- 2 Go to the NetBackup sign-in screen.
- 3 Enter the **Username** and **Password**.
- 4 Select **Sign in**. The **Configure multifactor authentication** screen is displayed.
- 5 On the next screen, follow the given steps.
Install and configure an authenticator application on your smart device. It generates a one-time password and sends it to your smart device.
[Supported authenticator applications](#)
- 6 Scan the QR code with the authenticator application or enter the key manually.
- 7 Enter the one-time password that you see in the authenticator application on your smart device.
- 8 Select **Configure**.
Successful configuration takes you back to the sign-in screen.
Enter the username, password, and one-time password for successful sign-in.

Reset multifactor authentication for a user

Only the NetBackup administrator can reset multifactor authentication for other NetBackup users.

To reset multifactor authentication for a NetBackup user

- 1 Sign in to the NetBackup web UI.
- 2 On the top right, click **Settings > Global security**.
- 3 Go to the **Security controls** tab.

- 4** Locate the section **Reset multifactor authentication for a user**. Then select **Reset**.
- 5** Select the user for whom you want to reset multifactor authentication.
- 6** Select **Reset**.
- 7** At the prompt, enter the one-time password and select **Confirm**.

Configuring multiperson authorization

This chapter includes the following topics:

- [About multiperson authorization](#)
- [Workflow to configure multiperson authorization for NetBackup operations](#)
- [RBAC roles and permissions for multiperson authorization](#)
- [multiperson authorization process with respect to roles](#)
- [NetBackup operations that need multiperson authorization](#)
- [Configure multiperson authorization](#)
- [View multiperson authorization tickets](#)
- [Manage multiperson authorization tickets](#)
- [Add exempted users](#)
- [Schedule expiration and purging of multiperson authorization tickets](#)
- [Disable multiperson authorization](#)

About multiperson authorization

NetBackup Security Administrator can configure multiperson authorization that helps protect primary servers from an undesirable or a malicious act, in a proactive manner. Multiperson authorization ensures that a second authorized user approves actions before they are performed.

To configure multiperson authorization in NetBackup, you need to have two users: one is the requester and the other is the approver.

A requester cannot be an approver of their own tickets.

Support information

- Multiperson authorization is not supported in a domain where NetBackup Access Control (NBAC) is enabled.
- Multiperson authorization is not supported for catalog maintenance operations by certain database agents.

As part of the database catalog synchronization, the database may initiate an image expiration request through command-line or other interfaces to the NetBackup catalog, which does not generate multiperson authorization ticket.

To prevent the direct expiration of backup images by database agents see the 'About preventing the direct expiration of backup images' topic in the [NetBackup for Oracle Administrator's Guide](#).

Terminology

- Ticket - Ticket is a multiperson authorization request to perform a critical operation.
- Requester - A requester is a user who wants to perform a critical operation that requires multiperson authorization.
- Approver - An approver is an individual who reviews and allows an operation that requires multiperson authorization by approving a ticket.
- Exempted user - An exempted user is not required to go through the multiperson authorization workflow. This user must only be used to perform critical operations like image expiration and image hold removal.

For additional security, it is recommended that there are no exempted users.

Command-line options that need multiperson authorization

The following operations and the associated command-line options need multiperson authorization:

- Expiring images expiration:
 - `bpexpdate`
 - `nbdecommission`
 - `bpimage -deleteCopy`
- Removing image hold:
 - `nbholdutil -delete`

Workflow to configure multiperson authorization for NetBackup operations

- Modifying global security settings:
 - `nbcertcmd -setsecconfig`
 - `nbseccmd -setsecurityconfig`
- Managing encryption key
 - `nbkmscmd`
 - `nbkmsutil`

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

Multiperson authorization is supported for the following commands that are run with the `nbcmdrun` command:

- `bpplcatdrinfo`
- `bpplclients`
- `bppldelete`
- `bpplsched`
- `bpplininclude`
- `bpplininfo -set`
- `bpplsched`
- `bpplschedrep`
- `bpplschedwin`
- `bpolicynew`

Multiperson authorization in a NetBackup and Alta View setup

If an Alta View user has requested a NetBackup operation that needs multiperson authorization, on a registered primary server, multiperson authorization must be enabled in Alta View. Else, NetBackup rejects this Alta View request and the respective user operation fails.

Workflow to configure multiperson authorization for NetBackup operations

Here are the high-level steps to configure multiperson authorization for NetBackup operations:

Table 16-1

Step	Description
Step 1	Identify critical NetBackup operations that require multiperson authorization. See “NetBackup operations that need multiperson authorization” on page 255.
Step 2	Identify the approvers who can approve requests or multiperson authorization tickets.
Step 3	Assign the Default multiperson authorization approver RBAC role to the approvers. See “RBAC roles and permissions for multiperson authorization” on page 252.
Step 4	Configure multiperson authorization using the NetBackup web UI. See “Configure multiperson authorization” on page 257.
Step 5	When a user or a requester tries to perform an operation that requires multiperson authorization (for example, expiring an image), a ticket is generated. Initially, the ticket is in the pending state.
Step 6	The ticket is visible to all multiperson authorization approvers in the NetBackup web UI where they can review the ticket information and approve or reject the ticket.
Step 7	When the approver approves or rejects the ticket, the requester is notified. If the ticket is approved, the associated operation is executed. Note: For API key operations, the requester needs to execute the operation using the web UI after the ticket is approved.

Multiperson authorization configuration begins when the Administrator or the Security Administrator enables critical operations that require multiperson authorization and specifies other settings like expiration period and purge period.

A multiperson authorization configuration ticket is generated. After the approver approves the ticket, multiperson authorization configuration comes into effect.

Initial multiperson authorization configuration

Configuring multiperson authorization for the first time involves adding users to the Default multiperson Authorization Approver role. To start using the multiperson

authorization for additional data security, the Security Administrator must enable the multiperson authorization for critical pre-defined operations that require an additional approval from a user with the Default multiperson Authorization Approver role.

Initially, the Security Administrator should configure multiperson authorization that results into a multiperson authorization ticket. After the approver approves the ticket, multiperson authorization becomes mandatory for the specified NetBackup operation (such as image expiry). The Administrator or Security Administrator can add users to the Default multiperson Authorization Approver role at any point in time.

RBAC roles and permissions for multiperson authorization

multiperson authorization configuration requires the users to be assigned to the following RBAC roles:

- Administrator
- Default Security Administrator
- Default multiperson Authorization Approver

Users with these RBAC roles should have the following permissions.

Table 16-2

RBAC role	Permissions
Administrator	View, update multiperson authorization configuration, and delegate the configuration permissions to other users. View, update tickets, and delegate ticket permissions to other users.
Default Security Administrator	View, update multiperson authorization configuration, and delegate the configuration permissions to other users.
Default multiperson Authorization Approver	View and update tickets.
Default Operator	View all NetBackup entities.

multiperson authorization process with respect to roles

Users can be requesters and approvers at the same time, however they cannot approve their own tickets.

The multiperson authorization process flow with respect to roles is as follows:

Table 16-3

Component	Description
multiperson authorization ticket	When a requester performs a critical NetBackup operation that is protected by multiperson authorization, a ticket is generated that requires an approval from the approver before a specific action can be executed. This ticket is used within NetBackup to ensure that critical actions undergo thorough review process by multiple people before they are executed. The following sample flow is for the image expiry operation that requires multiperson authorization: 1 A requester expires an image using the NetBackup web UI. 2 A ticket is created. 3 The ticket is pending for approval. 4 Approvers review the ticket. 5 Approvers either approve or reject the ticket. 6 After the approval, the ticket is scheduled by NetBackup and finally marked Done after the execution. 7 The ticket activity log, request, and response details can be viewed by the approver or the requester using the web UI, on the Ticket details page. 8 A ticket is expired after it ages beyond the expiration period. Such tickets cannot be approved unless they are renewed by the Requester. 9 Tickets in the Done, Rejected, Expired, and Canceled states are purged when no action is performed on them for the specified purge period in days.

Table 16-3 (continued)

Component	Description
Requester role	1 A requester is a user who initiates an operation that requires multiperson authorization. 2 A ticket is created for the operation if the user is not in the exempted users' list. 3 The ticket requires an approval from an approver before the operation is performed. 4 A requester is not allowed to self approve even if the requester is also an approver, an Administrator, or a Security Administrator. 5 Once the ticket is created it is in the Pending state. 6 The requester can cancel a ticket only if it is in the Pending state. 7 If the ticket ages beyond the expiry period, the ticket is moved to the Expired state. 8 Only the requester can renew such tickets. A new expiry period is calculated for the renewed ticket based on the configuration settings multiperson authorization.
Approver role	1 An approver is an authorized individual who reviews and provides approval for tickets. 2 The approver evaluates the details of the ticket and either approves or rejects the ticket based on the assessment. 3 After the approval, the ticket is scheduled for execution. 4 To be an approver, the user should have RBAC permissions like Update Ticket, View Ticket or the user should have the Default Multiperson Authorization Approver role. 5 When a ticket is in the Pending State, it can be approved or rejected.

Table 16-3 (continued)

Component	Description
Exempted users	1 An exempted user is an individual who does not need multiperson authorization for operations except the following: ■ To modify multiperson authorization configuration ■ To modify security properties 2 User groups cannot be exempted. 3 This eliminates the necessity for any approvals, however it must be used with caution. 4 If the exempted user account is hacked, the multiperson authorization process can be of no use as it is bypassed for this user. 5 For example, if user1 is an exempted user and she attempts to expire an image (an operation that needs multiperson authorization), the image expires without ticket generation and additional approvals.

NetBackup operations that need multiperson authorization

The following operations require multiperson authorization and therefore a ticket is generated for these operations:

- Configuring multiperson authorization
- Enabling and disabling operations that require multiperson authorization
- Adding exempted users
- Changing any multiperson authorization settings
- Expiring images
- Updating image expiration time
- Changing the MSDP WORM configuration
- Removing the MSDP WORM retention lock
- Removing hold applied on the images
- Updating CLI expiration period
- Adding, updating, deleting, and re-issuing API key
- Adding, updating, and deleting KMS configuration, keys, and key groups

- Importing, exporting, and recovering encryption keys
- Adding, updating, deleting malware scan host
- Adding, updating, deleting, copying backup and deployment policies
- Enabling, updating, or disabling freeze mode, which restricts certain configuration changes during a security incident or maintenance window
- Configuring network access control
- Updating the following global security settings:
 - Enabling and disabling NetBackup host communication with insecure hosts
 - Adding host aliases with or without NetBackup administrator's approval
 - Setting automatic deployment of certificates on a host
 - Enabling and disabling CAC/PIV authentication
 - Setting values for CAC/PIV certificate mapping attribute
 - Setting the value of the CAC/PIV certificate mapping attribute that is used to perform a search in active directory
 - Setting the value of the CAC/PIV certificate mapping attribute that is used to perform a search in LDAP directory
 - Enabling and disabling AD/LDAP domain mapping
 - Setting the value of the domain name that is used for user look-ups in active directory or LDAP
 - Setting the value of the OCSP URI that is used for certificate revocation checks with respect to CAC/PIV authentication
 - Enabling and disabling the data-in-transit encryption (DTE)
 - Setting unique identifier for external certificates
 - Allowing or disallowing the NetBackup web UI access to Operating System Administrators
 - Allowing or disallowing the default CLI access to OS administrators
 - Pausing client protection
 - Pausing client image expiration
 - Enabling and disabling TLS session resumption
 - Enabling and disabling rule engine for anomaly detection
 - Changing multifactor authentication configuration settings
 - Setting audit retention period for audit report

Even if multiperson authorization is configured for image expiry, the following operations do not require multiperson authorization:

- Changing values for image retention level
- Modifying retention levels in policy and SLP
- Canceling incomplete SLPs using the `nbstlutil` command:
Refer to the *NetBackup Commands Reference Guide*.

Configure multiperson authorization

The configuration of multiperson authorization for NetBackup operations is supported only from the NetBackup web UI. A user with the Administrator or the Security Administrator role can configure multiperson authorization for critical NetBackup operations.

To configure multiperson authorization for NetBackup operations

- 1 Sign into the NetBackup web UI using the security administrator account.
- 2 On the left, select **Security > multiperson authorization**.
- 3 At the top right, select the option **Configure multiperson authorization**.
- 4 Go to **Operations for multiperson authorization**. Then select **Edit**.
- 5 Select all or any of the following critical operations for which you want to configure multiperson authorization.
 - Images
 - Image expiry
 - Remove image hold
 - Security
 - Global security settings
 - Encryption key management
 - API keys

Note: If multiperson authorization is enabled for API key operations, a ticket is generated. After the multiperson authorization ticket is approved, the user needs to execute the ticket using the **Execute ticket** option in the NetBackup web UI and then the required API key operation is executed.

For NetBackup releases earlier than 10.5, if multiperson authorization is enabled, you cannot perform API key operations.

- Malware scan host management

Note: Starting with NetBackup 11.0, if multiperson authorization is enabled for this operation, a ticket is generated.

- Protection
 - Policy management

Note: Starting with NetBackup 11.0, if multiperson authorization is enabled for this operation, a ticket is generated. If there is an existing ticket for a policy that is pending for approval, you cannot perform any operations on the same policy until the existing ticket is either approved, rejected, canceled, or expired.

- MSDP WORM
 - WORM retention lock removal
 - WORM configuration change

6 Select **Save**.

7 Configure the users to be exempted from multiperson authorization.

Starting with 11.0, you can exempt users from multiperson authorization for specific operation and action for specific time frame.

8 Configure email notifications that you want to send to approvers and other email recipients. You can specify additional email recipients to whom you want to send email notifications.

Click **Configure** to configure the SMTP server for emails.

9 Go to **Schedules**. Then select **Edit**.

- 10 Specify when you want to expire and purge the multiperson authorization tickets.
- 11 Select **Save**.
- 12 Select **Configure**.

View multiperson authorization tickets

Users can view their own multiperson authorization tickets.

- 1 Sign into the NetBackup web UI.
- 2 On the left pane, click **Security > Multiperson authorization**. The list of multiperson authorization tickets is displayed.

Select the ticket ID to see more details.

Manage multiperson authorization tickets

Users with the approver role can approve or reject the multiperson authorization tickets.

To manage multiperson authorization tickets

- 1 Sign into the NetBackup web UI.
- 2 On the left pane, click **Security > Multiperson authorization**. The list of multiperson authorization tickets is displayed.
- 3 Select the ticket ID to view the request details.
- 4 Select **Review ticket** and enter the respective ticket ID to approve or reject the ticket.
- 5 Add comments and click **Approve** or **Reject**.

Add exempted users

Your organization may need to exempt certain users from multiperson authorization so that operations like image expiry and image hold removal can proceed without second-level approval.

Add such users to the exempted users' list.

Note: User groups cannot be added to the exempted list. Only individual users can be exempted.

The exempted users also need to go through the multiperson authorization workflow for the following operations:

- Modifying multiperson authorization configuration
- Modifying global security settings
- Modifying risk engine-based anomaly detection configuration

An exempted user is generally an automation user or a script that does not require multiperson authorization. By default, multiperson authorization configuration does not have exempted users and that is a recommended security setting.

To add exempted users

- 1 Sign into the NetBackup web UI.
- 2 On the left pane, select **Security > Multiperson authorization**.
- 3 On the top right, select **Configure Multiperson authorization**.
- 4 In the **Exempted users** section, select the **Add** button.
- 5 Specify the name of the user whom you want to exempt from the multiperson authorization process.
- 6 Select **Add to list** and then **Save**.
- 7 Select **Save**.

Schedule expiration and purging of multiperson authorization tickets

Expiration period is configurable option defines the duration for which a multiperson authorization ticket can be in the Pending state. A ticket expires if it is in the Pending state for more than the configured expiry period.

For multiperson authorization configuration, expiration period can vary from minimum 24 hours to 168 hours. By default, tickets expire after 72 hours.

Purge period is a configurable option defines the duration for which a ticket resides in the tickets database. Purging a ticket ensures that the database does not grow exponentially. Purge period can vary from minimum 3 days to 30 days.

By default, tickets purge after 72 hours. All the Done, Expired, Rejected, and Canceled tickets are purged after the given purge period.

To schedule expiration and purging of tickets

- 1 Sign into the NetBackup web UI.
- 2 On the left pane, click **Security > Multiperson authorization**.

- 3 On the top right, click **Configure Multiperson authorization**.
- 4 In the **Schedules** section, click **Edit**.
- 5 Specify the expiration period (in hours) for the **Expire ticket after** option.
Specify the purge period (in days) for the **Purge ticket after** option.
- 6 Select **Save**.
- 7 Select **Save**.

Disable multiperson authorization

In certain cases, you may need to temporarily disable multiperson authorization for the associated operations.

To disable multiperson authorization for all the associated operations, run the following command after `bpnbat -login -loginType WEB` using the root or Administrator account.

```
nbseccmd -disableMPA
```

You can disable multiperson authorization for a specific operation using the NetBackup web UI

To disable multiperson authorization for a specific operation

- 1 Sign into the NetBackup web UI.
- 2 On the left pane, click **Security > Multiperson authorization**.
- 3 On the top right, click **Configure Multiperson authorization**.
- 4 In the **Operations for multiperson authorization** section, click **Edit**.
- 5 Clear the check box for the operation for which you want to disable multiperson authorization.
- 6 Select **Save**.
- 7 Select **Save**.

This generates a ticket that is shown on the ticket details page with the operation name as MPA Configuration.

Multiperson authorization will be disabled for the associated operation only after the approval of the respective ticket.

Configuring freeze mode

This chapter includes the following topics:

- [About freeze mode in NetBackup](#)
- [Freeze mode options](#)
- [Enable freeze mode](#)
- [Edit freeze mode configuration options](#)
- [Disable freeze mode](#)
- [Disable freeze mode using command-line interface](#)

About freeze mode in NetBackup

In certain scenarios, you can enable freeze mode to prevent users from making changes to NetBackup for security reasons. In freeze mode, you cannot change NetBackup configurations and cannot use certain functionality based on the freeze mode options that are configured.

It is recommended that organizations identify scenarios (for example, malware attack) when they need to enable freeze mode, beforehand.

Important notes

- Freeze mode can be enabled only on primary servers.
- After freeze mode is enabled, it is advised that you restrict users from accessing the primary server using shell and console.
- Do not upgrade NetBackup primary server if freeze mode is enabled or the process is still in progress.
- You must have Security Administrator permissions to enable and disable freeze mode.

- On NetBackup hosts earlier than 10.0, freeze mode may not be fully supported and NetBackup operations may be affected.
Freeze mode is supported on primary servers with NetBackup version 11.1 or later.
- You can enable multiperson authorization to enable and disable freeze mode, and edit freeze mode options. Ensure one or more MPA approvers are available in the given NetBackup domain.
- If NetBackup catalog was backed up during freeze mode, restoring such catalog backup enables freeze mode on the NetBackup the primary server after catalog recovery.
If catalog backup was taken when freeze mode was not enabled and it was recovered during freeze mode, freeze mode is reset.
- In Flex Scale web UI, the cluster management tab manages the Flex Scale cluster. Freeze mode in NetBackup does not impact cluster management operations. Freeze mode is applicable only for NetBackup operations. Underlying platform operations do not have any impact during freeze mode.

Freeze mode options

You can enable freeze mode for the following NetBackup configurations and operations:

- Updates to configurations (example: add, update, delete policies)
 - Updates to NetBackup configurations are blocked.
 - Updates to NetBackup objects by NetBackup interfaces are blocked.
- Backups and storage lifecycle policy operations (example: duplication, replication)
 - Automated and manual backups, and SLP operations are blocked
- Restore operations - Restore operations are blocked
- Image expiry operations - The following operations are blocked:
 - Scheduled image expiry
 - User-initialed image expiry

Enable freeze mode

You can enable freeze mode using the web UI.

To enable freeze mode

- 1 Click **Settings** > **Global security**.
- 2 On the **Freeze mode** tab, turn on the **Freeze mode** option.
- 3 On the **Enable freeze mode options** dialog box, select the following options:
 - Updates to configurations (example: add, update, delete policies)
 - Backups and storage lifecycle policy operations (example: duplication, replication)
 - Restore operations
 - Image expiry operations
- 4 Enter 'enable' in the given text box.
- 5 Click **Save**.

Edit freeze mode configuration options

You can edit the freeze mode configuration options.

To edit freeze mode configurations

- 1 Click **Settings** > **Global security**.
- 2 On the **Freeze mode** tab, click **Edit freeze mode options**.
- 3 You can disable freeze mode.
- 4 On the **Edit freeze mode options dialog** box, select the following options:
 - Updates to configurations (example: add, update, delete policies)
 - Backups and storage lifecycle policy operations (example: duplication, replication)
 - Restore operations
 - Image expiry operations
- 5 Enter 'edit' in the given text box.
- 6 Click **Save**.

Disable freeze mode

You can disable freeze mode

To disable freeze mode

- 1 Click **Settings > Global security**.
- 2 On the **Freeze mode** tab, turn off the **Freeze mode** option.

Disable freeze mode using command-line interface

In a scenario where you want to disable freeze mode and NetBackup web UI is not accessible, you can use the command-line interface.

To disable freeze mode using the command-line interface

- 1 Run the following command on the primary server using the system administrator privileges:

```
nbseccmd -disableFreezeMode
```

- 2 Restart all NetBackup services using the NetBackup administrator privileges.

Network access control for the NetBackup web APIs

This chapter includes the following topics:

- [About controlling network access of the NetBackup web API](#)
- [Workflow to configure network access control for NetBackup web service](#)
- [RBAC roles and permissions for network access control configuration](#)
- [Configure the network access control option](#)

About controlling network access of the NetBackup web API

The network access control option provides an additional security layer that restricts access to the NetBackup web APIs based on IP addresses. This option ensures that only trusted networks can interact with the NetBackup web APIs. By enabling this option with the NetBackup web UI or API, you can specify IP addresses or IP address ranges that can or cannot access web APIs.

Important notes

- By default, none of the IP addresses can access NetBackup APIs. You must add them in network access control configuration to have the access.
See [“Configure the network access control option”](#) on page 269.
- The network access control feature is not supported in NetBackup Flex Scale.
- All user interactions that use NetBackup web APIs are impacted by the network access control feature. Such as:
 - IT Analytics and database agent hosts that are used to generate reports

- Scripts that are invoked by hosts using API key and commands
- System-originated interactions (by NetBackup client, media server, or primary server) that use machine certificates to interact with web service API are not impacted by the network access control feature.
- Interaction of NetBackup primary server with Alta View is not impacted by the network access control feature because the primary server establishes an outbound connection with the Alta View server.

Network access control terminology

Classless Inter-Domain Routing (CIDR) or IP address range

- CIDR - Is a way to specify a range of IP addresses with a single entry instead of listing each address one by one. For example:
 192.168.1.0/24
 fd00:abcd:1234::/48
- Allowed IP addresses or IP address ranges
 These IP addresses or the IP addresses in these ranges are allowed to access the web service.
- Denied IP addresses or IP address ranges
 These IP addresses or the IP addresses in these ranges cannot access the web service.

How the network access control option decides providing access

Note: After you enable the network access control option, your IP address must be added and saved.

- Check the IP addresses or ranges that are denied the access. The 'Deny' action takes precedence over the 'Allow' action.
- Check if the IP address is part of denied IP addresses or IP address ranges.
- Check if the IP address is part of allowed IP addresses or IP address ranges.
- If the IP address is neither part of the denied list nor allowed list, the access is denied.

Workflow to configure network access control for NetBackup web service

Here are the high-level steps to configure network access control for NetBackup web service:

Table 18-1

Step	Description
Step 1	Identify the IP addresses or IP address ranges that must have access or that must not have access. Use the nbauditreport -ctgy LOGIN command to check which IP addresses or IP address ranges can be part of the network access control configuration. For information commands, see the NetBackup Commands Reference Guide
Step 2	Configure network access control using theNetBackup web UI or API. The IP address or range that needs access to the NetBackup web service must be added in the allowed list. The IP address or range that needs to be blocked from accessing the NetBackup web service must be added in the denied list. See “Configure the network access control option” on page 269.
Step 3	Network access control configuration supports multiperson authorization. For additional security, you can configure multiperson authorization for network access control configuration update. With this configuration, any updates to network access control configuration needs approval from MPA approvers. Note: Ensure that one or more MPA approvers are available in your environment. See “About multiperson authorization” on page 248.

RBAC roles and permissions for network access control configuration

To view and update the network access control options, the users should be assigned with the following RBAC roles:

Table 18-2

RBAC role	Permissions
Default Security Administrator	View and update network access control and delegate the configuration permissions to other users. Namespace: ' SECURITY NETWORK-ACCESS-CONTROL '
Custom role	View and update network access control and delegate the configuration permissions to other users. Namespace: ' SECURITY NETWORK-ACCESS-CONTROL '

Configure the network access control option

By default, none of the IP addresses can access web APIs. You must add them in network access control configuration to have the access.

You can use the network access control option to specify IP addresses or IP address ranges that must not have the access to web APIs.

Configure the network access control option

- 1 Sign into the NetBackup web UI using the security administrator account.
- 2 On the **Global security settings > Security controls** tab, on the **Network access control** card, click **Configure**.
- 3 On the **Network access control** page, select the **Enable network access control** check box.

Warning: After you enable the **Network access control** option, you must add your address or IP address range and allow the access and save the configuration.

- 4 Click **Add** in the table.

- 5 In the **Add IP address or IP address range** dialog box, add an IP address or an IP address range that should or should not have the access of web APIs.

Example of an IP address range: 10.0.0.0/16

Enter the purpose of adding this IP address or range in the **Comment** field.

For example, for an IP address that should have the access, you can enter the following comments: Used by finance team.

For an IP address that should not have the access, you can enter the following comments: Blocked for abuse reports.

Note: Ensure that the allowed IP address or range is not a subset of any of the denied IP addresses or ranges.

- 6 Select the action type of the access control for the specified IP address or range.

Note: The 'Deny' action takes precedence over the 'Allow' action.

Select **Allow network access** if the specified IP address or range must have the access to web APIs.

Select **Deny network access** if the specified IP address or range must not have the access to web APIs.

- 7 Click **Save and add another** to add more IP addresses or ranges.

Click **Save** after you are done with adding all the required IP addresses or ranges for the network access control configuration.

Encryption of data-in-transit

- [Chapter 19. NetBackup CA and NetBackup certificates](#)
- [Chapter 20. Configuring data-in-transit encryption \(DTE\)](#)
- [Chapter 21. External CA and external certificates](#)
- [Chapter 22. Regenerating keys and certificates](#)

NetBackup CA and NetBackup certificates

This chapter includes the following topics:

- [Overview of security certificates in NetBackup](#)
- [About secure communication in NetBackup](#)
- [About the Security Management utilities](#)
- [About host management](#)
- [About global security settings](#)
- [About host name-based certificates](#)
- [About host ID-based certificates](#)
- [About Token Management for host ID-based certificates](#)
- [About the host ID-based certificate revocation list](#)
- [About revoking host ID-based certificates](#)
- [Deleting host ID-based certificates](#)
- [Host ID-based certificate deployment in a clustered setup](#)
- [About the communication between a NetBackup client located in a demilitarized zone and a primary server through an HTTP tunnel](#)
- [Adding a NetBackup host manually](#)
- [Migrating NetBackup CA](#)

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 primary server acts as the Certificate Authority (CA) and issues digital certificates to hosts.

Any security certificates that were generated before NetBackup 8.0 are referred to as host name-based certificates. NetBackup is in the process of replacing these older certificates with newer host ID-based certificates. The transition will be completed in future releases and the use of host name-based certificates will be eliminated.

However, the transition is on-going and NetBackup continues to require the older host name-based certificates for some operations. The following table lists various operations where host name-based certificate is required.

Note: All NetBackup 8.1 hosts must have a host ID-based certificate.

Table 19-1 Host name-based certificate requirements for NetBackup 8.1 hosts

Operation or component	Type of certificate required
NetBackup Access Control (NBAC)	If NBAC is enabled on a NetBackup host, the host requires a host name-based certificate. These are automatically deployed when NBAC is enabled.
Cloud storage	This is applicable to NetBackup media server versions 8.0 to 8.1.2 only. The NetBackup CloudStore Service Container requires that the host name-based certificate be installed on the media server. If the certificate is not installed, the Service Container cannot start. See "Deploying host name-based certificates" on page 302.

About secure communication in NetBackup

NetBackup 8.1 and later hosts can communicate with each other only in a secure mode. NetBackup 8.1 hosts must have a Certificate Authority (CA) certificate and a host ID-based certificate for successful communication. NetBackup uses Transport Layer Security (TLS) protocol for host communication where each host needs to present its security certificate and validate the peer host's certificate against the Certificate Authority (CA) certificate.

All control communication (or control channel) between NetBackup hosts are secured using Transport Layer Security (TLS) protocol version 1.2 and X.509 certificates.

The NetBackup software uses Control communication to initiate, control, and monitor backup, archive, and restore operations.

Data communication consists of the data that is backed up using NetBackup. The security policies require the Backup Administrators to ensure that the channel on which NetBackup clients send metadata and data to NetBackup servers be secure. In NetBackup 10.0 and later, the backup images and metadata are encrypted over the wire by secure communications. This feature is referred to as Data Channel Encryption or Data In-Transit Encryption (DTE).

The following channels are classified as data channels:

- **Tar stream (client to media server):** This channel is the channel over which the tar or the data stream flows between the client and the media server. During a backup operation, the media server receives the data from the client and sends it to storage (for example, by an OST plug-in). The direction is reversed during a restore.
- **Tar stream (media server to media server):** This channel is used during duplication.
- **Catalog Info (client to media server):** This channel is the channel over which the catalog information and control commands flow between the client and the media server. The amount of data that is transmitted over this channel is proportional to the number of files and directories that are part of the backup. The media server sends the catalog information that is received from the client to the primary server.
- **Catalog Info (media server to primary server):** This channel is the channel over which the catalog information flows from the media server to the primary server.

Secure communication settings are available in **Settings > Global security**.

See [“About host management”](#) on page 276.

See [“Adding host ID to host name mappings”](#) on page 278.

See [“About global security settings”](#) on page 293.

See [“About secure communication settings”](#) on page 293.

See [“About disaster recovery settings”](#) on page 297.

Two commands, `nbhostmgmt` and `nbhostidentity`, along with enhancements to `nbcertcmd` and `nbseccmd`, provide options to manage certificate deployment and other security settings.

About the Security Management utilities

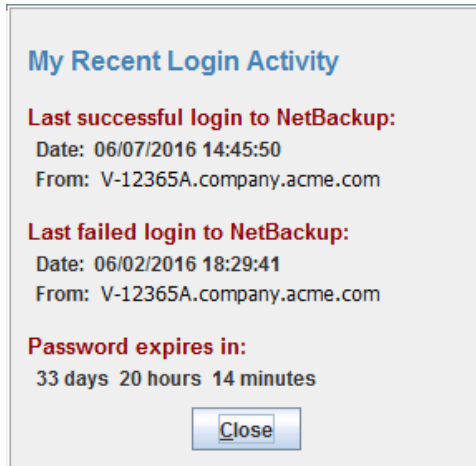
The **NetBackup BAR Console > Security Management** node is visible only to administrators on the NetBackup primary server.

Security Management contains the utilities to view login activity, manage host ID-based certificates, and configure secure communications in the domain.

- Use **Security Events** to view the login details about the current administrator and the user-initiated changes that are made to certificates, tokens, hosts, and security configurations. You can also view details about host connections.
- Use the **Host Management** node to carry out NetBackup host operations, such as adding or approving host ID to host name mappings, resetting host, or adding comments for a host.
 See [“Hosts tab”](#) on page 277.
- Use the **Certificate Management** node to carry out operations specific to certificates such as viewing, revoking, or reissuing.
 See [“Using the Certificate Management utility to issue and deploy host ID-based certificates”](#) on page 305.
- Use the **Global Security Settings** node to configure security settings like enable insecure communication, disaster recovery package passphrase, certificate deployment level and so on.
 See [“About global security settings”](#) on page 293.

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 BAR 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 primary server using the single sign-on (SSO) feature of the **NetBackup Administration Console**
- If you have logged in to the UNIX or Linux primary server using the **NetBackup Administration Console**

Note: The login and the password expiration details are displayed only after the first successful login and logout from the **NetBackup Administration Console**.

The login details are not automatically refreshed. You must log off from the **NetBackup Administration Console** and log in again to view the latest information about the last login details.

This information is also displayed in **Security Events** on the **Access History** tab.

About host management

The **Security Management > Host Management** node lets you map host names to their respective host IDs. Appropriate mapping between host ID-to-host names is important for secure host communication.

See [“About secure communication in NetBackup”](#) on page 273.

See [“Adding host ID to host name mappings”](#) on page 278.

See [“Resetting NetBackup host attributes”](#) on page 287.

Hosts tab

The **Hosts** tab provides the following information:

Host	The name of the host. Note: The Host Management node shows only those hosts that have a host ID.
Mapped Host Names / IP Addresses	Host names or IP addresses that are mapped to the host ID of the selected client. See “Add or Remove Host Mappings dialog box” on page 279.
Version	The NetBackup version that is installed on the host.
Allow Auto Reissue Certificate Validity	The time until which certificate can be reissued on the host without requiring a reissue token. By default, the Allow Auto Reissue Certificate option has a validity of 48 hours. See “Allowing or disallowing automatic certificate reissue” on page 290.
Operating System	The operating system version that is installed on the host.
OS Type	The type of operating system (Windows or UNIX) that is installed on the host.
CPU Architecture	The architecture of the central processing unit that is used on the host.
Secure	States whether the communication status of the host is secure or not. If the host is 8.1, the communication status is secure and it can communicate securely.
Comment	Comment or additional information that you have added for the host.
Hardware Description	The hardware that is used on the host.
NetBackup Host ID	A unique identifier for the host.
NetBackup EEBs	States whether the NetBackup EEBs (Emergency Engineering Binary) are installed or not.
Servers	Additional servers that are associated with the host.

Master Server	Primary server host that is associated with the host.
Issued On	Date when the host ID-based certificate was issued to the host.
Last Updated On	Date when the host ID-based certificate was updated.
VxUpdate Platform	Identifies the VxUpdate package that is needed to upgrade the host.
Installed Packages	The NetBackup packages that are installed on the host.

Adding host ID to host name mappings

Hosts may have multiple host names or IP addresses associated with them. For successful communication between hosts, all relevant host names and IP addresses need to be mapped to the respective host IDs.

During communication, NetBackup may detect new host names or IP addresses with respect to a host ID. These host names or IP addresses can be automatically or manually mapped to the respective host ID for successful communication.

The host names or IP addresses that NetBackup detects are automatically mapped to the respective host ID, if the **Automatically map host names to their NetBackup host ID** option is selected in **Settings > Global security > Secure communication**.

See [“Automatically mapping host ID to host names and IP addresses”](#) on page 297.

Important notes

Review the following notes specific to host ID to host name mappings:

- In the case of DHCP (Dynamic Host Configuration Protocol) hosts, NetBackup may detect dynamic IP addresses during communication and added as host ID to host name mappings. You should delete such mappings.
- In the case of a cluster setup, host name, and FQDN (Fully Qualified Domain Name) of virtual name are discovered during host communication.
- You may choose to redeploy a certificate on a host using a host name that is not mapped with the existing host ID. In this case a new certificate is deployed and a new host ID is issued to the host. This action occurs because NetBackup considers it as a different host. To avoid this situation, you should map all available host names with the existing host ID.
- When you register NetBackup Snapshot Manager to NetBackup, the certificates that are generated are exchanged between them. Hence the NetBackup Snapshot Manager's **Host Mapping** displays the details of the NetBackup Snapshot Manager container instead of the NetBackup Snapshot Manager host.

Use the following procedure to manually map a specific host ID to the corresponding host names or IP addresses.

See [“Add or Remove Host Mappings dialog box”](#) on page 279.

See [“Removing host ID to host name mappings”](#) on page 280.

To add host ID to host name mappings

- 1 On the left, select **Security > Host mappings**.
- 2 On the **Hosts** tab, locate the host that you want to modify.
- 3 Select **Actions > Manage mappings**.

The host ID of the client host is displayed along with the existing mappings.

- 4 Select **Add**.
- 5 Provide the following details:

Mapping name	Specify the host ID-to-host name mapping. Note: The host ID-to-host name mappings are not case-sensitive.
Audit reason	For auditing purposes, specify the reason or additional information for why you want to add this mapping.

To add a host ID to host name mapping using the command-line interface

- 1 Run the following command to authenticate your web services login:

```
bpnbat -login -loginType WEB
```

- 2 Run the following command to add a host ID to host name mapping:

```
nbhostmgmt -add -hostid host_ID -mappingname mapping_name
```

Add or Remove Host Mappings dialog box

Hosts may have multiple host names or IP addresses associated with them. For successful communication between hosts, all relevant host names and IP addresses need to be mapped to the respective host IDs.

On the **Security Management > Host Management > Hosts** tab, right-click the host that you want to modify, and click the **Add or Remove Host Mappings** option to open the dialog box.

Only System Administrator can access the **Add or Remove Host Mappings** properties for a NetBackup host.

See [“Adding host ID to host name mappings”](#) on page 278.

See [“Removing host ID to host name mappings”](#) on page 280.

The **Add or Remove Host Mappings** dialog box contains the following properties.

NetBackup Host ID	Displays the host ID of the selected host.
Mapped Host Names / IP Addresses	Lists host names and IP addresses that are mapped to the host ID of the client host.
Auto-discovered	States whether the mapped host name or IP address was automatically discovered by the system or not.
Created On	Date and time when the mapping was created.
Last Updated On	Date and time when the mapping was last updated.
Add	Click to add new host ID to host name mappings for the client host. The Add Mapping dialog box is displayed. See “Adding host ID to host name mappings” on page 278.
Remove	Click to remove the selected host ID to host name mapping for the client host. The Remove Mapping dialog box is displayed. See “Removing host ID to host name mappings” on page 280. Note: The operations that you carry out on the Add Mapping and Remove Mapping dialog boxes directly update the NetBackup database.
Close	Click to close the Add or Remove Host Mappings dialog box.
Help	Click to see help.

Removing host ID to host name mappings

Use the following procedure to remove host ID to host name mappings.

See [“Add or Remove Host Mappings dialog box”](#) on page 279.

See [“Adding host ID to host name mappings”](#) on page 278.

To remove host ID to host name mappings

- 1 In the **NetBackup BAR Console**, expand **Security Management > Host Management**.
- 2 In the details pane, on the **Hosts** tab, right-click the client host that you want to modify.
- 3 Click the **Add or Remove Host Mappings** option.

- 4 On the **Add or Remove Host Mappings** screen, host ID of the selected client host is displayed along with the existing mappings.
- 5 Select the mapping that you want to remove.
- 6 Click **Remove**.
- 7 On the **Remove Mapping** dialog box, specify the audit reason for removing the selected mapping for auditing purpose.
- 8 Click **Yes**.

To remove host ID to host name mapping using the command-line interface

- 1 Run the following command to authenticate your web services login:

```
bpnbat -login -loginType WEB
```

- 2 Run the following command to remove a host ID to host name mapping:

```
nbhostmgmt -delete -hostid host_ID-mappingname mapping_name
```

Mappings for Approval tab

Use the **Security Management > Host Management > Mappings for Approval** tab to view host ID-to-host name mappings that are pending for approval.

The following options are available on the **Mappings for Approval** tab:

Host	Name of the selected host.
Auto-discovered Mapping	Host ID-to-host name mapping that was discovered with respect to the host during communication.
Conflict	States if there is any conflict in the mappings. For example, in a cluster setup, a mapping can be shared across host IDs.
Discovered On	Date and time when the mapping was discovered by the system.
NetBackup Host ID	Host ID of the host.

See [“Viewing auto-discovered mappings”](#) on page 282.

See [“Add or Remove Host Mappings dialog box”](#) on page 279.

Note: If the **Automatically map host ID to host names** option on the **Security Management > Global Security Settings > Secure Communication** tab is selected, the **Mappings for Approval** tab shows only conflicting mappings.

See [“Automatically mapping host ID to host names and IP addresses”](#) on page 297.

Viewing auto-discovered mappings

During communication, NetBackup may detect new host names or IP addresses with respect to a host ID. You can view the host ID-to-host name mappings that are automatically discovered.

See [“Add or Remove Host Mappings dialog box”](#) on page 279.

To view auto-discovered host ID-to-host name mappings

- 1 In the **NetBackup BAR Console**, expand **Security Management > Host Management**.
- 2 In the details pane, click the **Mappings for Approval** tab.

See [“Mappings for Approval tab”](#) on page 281.

Note: If the **Automatically map host ID to host names** option on the **Security Management > Global Security Settings > Secure Communication** tab is selected, the **Mappings for Approval** tab shows only conflicting mappings.

See [“Automatically mapping host ID to host names and IP addresses”](#) on page 297.

Mapping Details dialog box

Use the **Mapping Details** dialog box to approve or reject the pending host ID-to-host name mappings.

On the **Security Management > Host Management > Mappings for Approval** tab, right-click the host ID-to-host name mapping that you want to approve or reject, and click **Mapping Details** to open the dialog box.

See [“Add or Remove Host Mappings dialog box”](#) on page 279.

See [“Approving host ID to host name mappings”](#) on page 283.

See [“Rejecting host ID to host name mappings”](#) on page 284.

See [“Mappings for Approval tab”](#) on page 281.

The following options are available on the dialog box:

Host	Displays name of the host for which you want to approve or reject the mapping.
Mapped Host Names / IP Addresses	Lists the existing mappings that are associated with the host.

NetBackup Host ID	Displays the host ID of the host.
Conflict in mapping - Shared with hosts	Note: This information is displayed if the selected mapping is already associated with other hosts. This table lists information of all hosts across which the selected mapping is shared. For example, in a cluster set up, multiple host IDs share the same virtual name. If a mapping is added for a host ID and if the same mapping is discovered against a different host ID, it is listed on the Mappings for Approval tab. You can either approve this mapping or reject it using the Mapping Details dialog box. ■ Host - Displays the name of the host with which the selected mapping is already associated. ■ NetBackup Host ID - Displays host ID of the host with which the selected mapping is already associated. See “About shared or cluster mapping scenarios” on page 285.
Reason	Provide the reason for approving or rejecting the mapping.
Approve	Click to approve the pending mapping.
Reject	Click to reject the pending mapping.
Close	Click to close the dialog box without saving the changes.
Help	Click to see help.

Approving host ID to host name mappings

This section provides a procedure for approving host ID to host name mappings that are pending for approval.

See [“Add or Remove Host Mappings dialog box”](#) on page 279.

See [“Rejecting host ID to host name mappings”](#) on page 284.

To approve host ID to host name mapping

- 1 In the **NetBackup BAR Console**, expand **Security Management > Host Management**.
- 2 In the details pane, click the **Mappings for Approval** tab.

- 3 Select the mapping that you want to approve and right-click.
- 4 On the right-click options, click **Approve**. The selected mappings are approved.
Alternatively, click **Mapping Details** on the right-click options. Use the **Mapping Details** dialog box to approve the selected mapping.
See [“Mapping Details dialog box”](#) on page 282.

Rejecting host ID to host name mappings

This section provides a procedure for rejecting host ID to host name mappings that are pending for approval.

See [“Add or Remove Host Mappings dialog box”](#) on page 279.

See [“Approving host ID to host name mappings”](#) on page 283.

To reject host ID to host name mapping

- 1 In the **NetBackup BAR Console**, expand **Security Management > Host Management**.
- 2 In the details pane, click the **Mappings for Approval** tab.
- 3 Select the mapping that you want to reject and right-click.
- 4 On the right-click options, click **Reject**. The selected mappings are rejected.
Alternatively, click **Mapping Details** on the right-click options. Use the **Mapping Details** dialog box to reject the selected mapping.

Adding shared or cluster mappings

In certain scenarios, host ID to host name mappings are shared across host IDs. For example, in a cluster setup, virtual name is shared across all nodes. You need to add these shared mappings using the **NetBackup BAR Console** so that the primary server can successfully communicate with the nodes.

See [“Add or Remove Host Mappings dialog box”](#) on page 279.

To add shared mappings

- 1 In the **NetBackup BAR Console**, expand **Security Management > Host Management**.
- 2 On the **Hosts** tab, in the details pane, right-click to view the options.
- 3 On the right-click options, select **Add Shared or Cluster Mappings**.
- 4 On the **Add Shared or Cluster Mappings** dialog box, specify the shared mapping name.

See [“Add Shared or Cluster Mappings dialog box”](#) on page 286.

- 5 Select host IDs to be mapped with the specified shared mapping name.
- 6 Click **Save**.

About shared or cluster mapping scenarios

Host ID to host name mappings can be shared across multiple hosts in the following scenarios:

- If multiple hosts from different domains use the same host name
- In a cluster setup where the same virtual name is used by multiple cluster nodes

However, in a scenario where the associated hosts do not have the same communication status (some are 8.0 or earlier and can communicate insecurely and some are 8.1 or later and communicate securely), communication may fail.

See [“Add or Remove Host Mappings dialog box”](#) on page 279.

Scenario 1 - If multiple hosts from different domains use the same host name

Consider the following example:

- Host1 – abc.secure.domain1.com, version – 8.1, policy – P1
- Host2 – abc.insecure.domain2.com, version – 7.7.3, policy – P2
- Host1 and Host 2 use the same name – abc – as their host name. Security Administrator adds abc as a shared mapping for Host2.
See [“Adding shared or cluster mappings”](#) on page 284.
- Insecure communication with 8.0 and earlier hosts is enabled.
See [“About insecure communication with 8.0 and earlier hosts”](#) on page 296.
- When Host2 initiates communication with another host, the primary server validates the communication status of host2 (which is insecure), which is different than Host1 (which is secure). Because both hosts use the same host name, but their communication status do not match, the communication with Host2 fails.
- Recommendation – Host2 should be upgraded to 8.1 or later.

Scenario 2 - In a cluster setup where the same virtual name is used by multiple cluster nodes

Consider the following example:

- Host1 – abc.secure.domain1.com, active cluster node, version – 8.1
- Host2 – abc.secure.domain1.com, inactive cluster node, version – 8.0
- Host1 and Host2 use the same virtual name that is abc. Security Administrator adds abc as a shared or cluster mapping for Host2.

See [“Adding shared or cluster mappings”](#) on page 284.

- Insecure communication with 8.0 and earlier hosts is enabled.
See [“About insecure communication with 8.0 and earlier hosts”](#) on page 296.
- Host1 fails over to Host2. The primary server validates the communication status of host2 (that is insecure), which is different than Host1 (that is secure). Because communication status for both hosts do not match, the communication with Host2 fails.
- Recommendation – Host2 should be upgraded to 8.1.
- Workaround – Delete the host ID-to-host name mapping abc for Host1. In case of shared mapping, if the associated hosts do not have the same communication status (secure), communication fails for the host that has insecure communication status.

Add Shared or Cluster Mappings dialog box

Use this option to add shared or cluster mappings. On the **Security Management > Host Management > Hosts** tab, on the right-click options, click **Add Shared or Cluster Mappings** to open the dialog box.

The following options are available on the **Add Shared or Cluster Mappings** dialog box:

Shared mapping name or virtual name of cluster	Enter the mapping name that needs to be shared by multiple host IDs.
Select Hosts	Click the button to list all hosts and select the ones that you want to map with the specified mapping name. The Select Hosts pop-up screen lists all available hosts. Select the required hosts and click Add to list . The selected hosts appear in the list on the Add Shared or Cluster Mappings dialog box.
Host	Name of the host that you want to map with the specified shared name.
NetBackup Host ID	Host ID of the host that you want to map with the specified shared name.
Save	Click to save the mapping.
Cancel	Click to close the dialog box without saving the changes.
Help	Click to see help.

See [“Adding shared or cluster mappings”](#) on page 284.

See [“About shared or cluster mapping scenarios”](#) on page 285.

Resetting NetBackup host attributes

In certain scenarios, you may need to clean up or reset host attributes: For example, you have downgraded the host.

In such cases, you need to reset host ID to host name mapping information, communication status and so on for successful communication.

Review the following notes before resetting host attributes

- You must reset the host attributes of the downgraded host if you want the primary server to communicate with the host in an insecure mode.
- Resetting host attributes resets host ID to host name mapping information, communication status and so on. It does not reset the host ID, host name, or security certificates of the host.
- After you reset the host attributes, the connection status (is secure flag) is set to insecure state. At the time of the next host communication, the connection status is updated appropriately.
- If you have inadvertently used the **Reset Host Attributes** option, you can undo the changes by restarting the `bpcd` service. Else the host attributes are automatically updated with the appropriate values after 24 hours.

See [“Add or Remove Host Mappings dialog box”](#) on page 279.

About resetting host attributes

NetBackup 8.1 primary server can communicate securely with all 8.1 hosts. However, it communicates insecurely with 8.0 and earlier hosts.

In certain scenarios, you may need to downgrade a NetBackup client from 8.1 version to 8.0 or earlier. After the downgrade, the primary server cannot communicate with the client, because the communication status for the client is still set to secure mode. The communication status is not automatically updated to insecure mode after the downgrade.

Use one of the following options to reset a host:

To reset a host using the NetBackup BAR Console

- 1 Expand **Security Management > Host Management**.
- 2 On the **Hosts** tab, in the details pane, right-click the host that you have downgraded and which you want to reset, and click **Reset Host Attributes**.

Note: To resume insecure communication with downgraded hosts, ensure that the **Enable insecure communication with 8.0 and earlier hosts** option on the **Security Management > Global Security Settings > Secure Communication** tab is selected.

To reset host attributes using the command-line interface

- 1 Run the following command to authenticate your web services login:

```
bpnbat -login -loginType WEB
```

- 2 Run the following command to reset the host:

```
nbenmcmd -resethost
```

Decommission a client

This operation is applicable only for NetBackup clients.

To decommission a host with special roles like media server, remote primary server, or Flex WORM storage server, you should first downgrade its role and then decommission the host.

When you decommission a client, NetBackup removes the client from the domain by revoking its identity. It resets the host's communication status and other attributes like Operating System version, NetBackup machine type and so on for that client. Primary servers and media servers from the same domain cannot communicate with the decommissioned client.

Review the following notes before decommissioning a client host:

- If the specified client is configured with NetBackup certificate, the associated certificates are revoked.
- If the specified client is configured with external certificate, its enrollment is removed.
- You should remove the client that needs to be decommissioned from the policies and protection plan, and expire the associated images of that client.

- Alternatively, you can use the `-force` option to decommission the client irrespective of the associated policies or images. With the `-force` option, you do not need to delete the data.

A user with the following RBAC roles can decommission a host:

- NetBackup Administrator
- Default Security Administrator
- A custom role with the 'Decommission host' permission

To decommission a client using the NetBackup web UI

- 1 On the left, select **Security > Host mappings**.
- 2 Locate the host and click **Actions > Decommission client**.
- 3 Enter the reason to decommission the client.

Decommission a client using RESTful APIs

To decommission a client, use the following API: `POST - /config/hosts/{hostId}/decommission`

To list decommissioned clients, use the following API: `GET - /config/hosts`

Use the filter 'decommissionedDateTime'

Decommission a client using the command-line interface

To decommission a client using command-line interface

- ◆ Run the following command:

```
nbhostmgmt {{-dh | -decommissionhost}} {{-i | -hostid}} <hostid> |
  {-n | -host} <host> {{-r | -reason}} "<reason>" [-f | -force]
  [{-j | -json} | { -jc | -json_compact}]
```

Recommission a client

If you want to recommission a previously decommissioned client with host ID-based (NBCA) certificate, provision a new certificate on that client host.

To recommission a client with NetBackup certificate

- ◆ Run the following command on the client:

```
Install_Path/bin/nbcertcmd -getCertificate -reissue -token value
-force
```

To recommission a client with external certificate

- ◆ Run the following command on the client:

```
Install_Path/bin/nbcertcmd -enrollCertificate -force
```

After a client is recommissioned, restart the NetBackup services on the client host or run the following command:

```
Install_Path/bin/nbhostdbcmd -update -force
```

Allowing or disallowing automatic certificate reissue

This section provides the procedures for allowing and disallowing automatic certificate reissue.

The **Allow Auto Reissue Certificate** option enables the `autoreissue` parameter of a host that in turn allows you to deploy a certificate on the host without requiring a reissue token.

See [“Deploying host ID-based certificates”](#) on page 312.

By default, the `autoreissue` parameter is enabled for 2880 minutes (or 48 hours or 2 days). After this duration, the parameter is disabled and the certificate reissue operation requires a reissue token.

See [“Configuring validity of the `autoreissue` parameter for a host”](#) on page 291.

To manually disable the `autoreissue` parameter, use the **Disallow Auto Reissue Certificate** option.

Note: During the Bare Metal Restore (BMR) process, the `autoreissue` flag is automatically set.

For more information about Bare Metal Restore, refer to the *NetBackup Bare Metal Restore Administrator's Guide*.

To allow automatic certificate reissue using the NetBackup BAR Console

- 1 Expand **Security Management > Host Management**.
- 2 In the right pane, select the host for which you want to allow automatic certificate reissue.
- 3 Right-click the host and select the **Allow Auto Reissue Certificate** option.

To allow automatic certificate reissue using the command-line interface

- 1 Run the following command to authenticate your web services login:

```
bpnbat -login -loginType WEB
```

- 2 Run the following command to enable the `autoreissue` parameter, which in turn allows automatic certificate reissue:

```
nbhostmgmt -allowautoreissuecert -hostid host_ID -autoreissue 1
```

To disallow automatic certificate reissue using the NetBackup BAR Console

- 1 Expand **Security Management > Host Management**.
- 2 In the right pane, select the host for which you want to disallow automatic certificate reissue.
- 3 Right-click the host and select the **Disallow Auto Reissue Certificate** option.

To disallow automatic certificate reissue using the command-line interface

- 1 Run the following command to authenticate your web services login:

```
bpnbat -login -loginType WEB
```

- 2 Run the following command to disable the `autoreissue` parameter, which in turn disallows automatic certificate reissue:

```
nbhostmgmt -allowautoreissuecert -hostid host_ID -autoreissue 0
```

Configuring validity of the `autoreissue` parameter for a host

When you allow automatic reissue of a host ID-based certificate, the `autoreissue` parameter is by default enabled for 2880 minutes (or 48 hours or 2 days). After this duration, the parameter is reset and the certificate reissue operation requires a reissue token.

You can configure the duration for automatic reissue of certificate or the time-to-live (TTL) setting for the `autoreissue` parameter by updating the `web.conf` file.

To configure validity of the `autoreissue` parameter or the TTL setting

- 1 Open the `web.conf` file. Location for the file is as follows:

On Windows: `Install_Path\var\global\wsl\config\web.conf`

On Linux: `/usr/opensv/var/global/wsl/config/web.conf`

- 2 Configure the TTL setting for the `autorissue` parameter in minutes. For example:

```
ttn.autoReissue.minutes = 1440
```

Note: Valid range for the `autoreissue` TTL setting is 0 min to 43200 min (or 30 days).

If the TTL value that you have configured is not within the valid range, the server continues using the last configured TTL value.

- 3 For the new `autoreissue` TTL value to take effect, do one of the following:

- Restart the NetBackup Web Management Console (WMC) service.

- Run the following command:

On Windows: `Install_Path/bin/nbhostdbcmd -reloadconfig -host`

On UNIX: `NETBACKUP_INSTALL_DIR/bin/nbhostdbcmd -reloadconfig -host`

Adding or deleting comment for a host

You can provide additional information about a NetBackup host using the **Add or Edit Comment** dialog box. For example, if a host is decommissioned, you can add a comment to explain why and when it was decommissioned.

To add or edit a comment for a host

- 1 Expand **Security Management > Host Management**.
- 2 On the **Hosts** tab, in the details pane, right-click the host for which you want to provide additional information, and click **Add or Edit Comment**.
- 3 On the **Add or Edit Comment** dialog box, in the **Comment** pane, enter the required information or comments.

Click **Save**.

To delete a comment for a host

- 1 Expand **NetBackup Management > Security Management > Host Management**.
- 2 On the **Hosts** tab, in the details pane, right-click the host for which you want to delete comment, and click **Delete Comment**.

About global security settings

The options in **Settings > Global security** let you configure the settings that are crucial for secure communication in NetBackup.

See [“About secure communication in NetBackup”](#) on page 273.

See [“About disaster recovery settings”](#) on page 297.

See [“About secure communication settings”](#) on page 293.

About secure communication settings

NetBackup provides settings that you can configure for secure communication between hosts.

Table 19-2 Secure communication settings

Setting	Description
Certificate Authority	Displays the certificate authorities that your NetBackup domain supports. The NetBackup web server can be configured to enable the NetBackup domain to use: ■ NetBackup CA-signed certificates only ■ External CA-signed certificates only ■ NetBackup CA-signed certificates and external CA-signed certificates Use the <code>-configureWebServerCerts</code> command for certificate configuration for the web server. For more information, refer to the NetBackup Commands Reference Guide.

Table 19-2 Secure communication settings (*continued*)

Setting	Description
Enable communication with 8.0 and earlier hosts	NetBackup communicates insecurely with 8.0 and earlier hosts. For increased security, upgrade all your hosts to the current version and disable this setting. This ensures that only secure communication is possible between NetBackup hosts. The option allows NetBackup to communicate with hosts including 8.0 and earlier hosts that may be present in the existing NetBackup environment. This option also allows communication between NetBackup 8.1 or later primary server. See “Disabling insecure communication” on page 295. See “About insecure communication with 8.0 and earlier hosts” on page 296. If you have configured Auto Image Replication, ensure the following before you clear the option: The trusted primary server that you have specified for image replication is of the version that is later than NetBackup 8.0. For more information, refer to the NetBackup Administrator's Guide, Volume I.
Automatically map NetBackup host ID to host names	Hosts may have multiple host names or IP addresses associated with them. For successful communication between hosts, all relevant host names and IP addresses need to be mapped to the respective host IDs. During communication, NetBackup may detect new host names or IP addresses with respect to a host ID. Select this option to automatically map the host ID to host names or IP addresses that are detected by the system. By default, the option is selected. For increased security, clear this option so that the NetBackup Administrator can manually verify the mappings and approve them. See “Automatically mapping host ID to host names and IP addresses” on page 297.

Table 19-2 Secure communication settings (*continued*)

Setting	Description
Security level for certificate deployment	Based on the security level that is configured on the NetBackup primary server, the certificate deployment approach is determined. For example, if the security level is set to Very High, an authorization token is a must for certificate deployment. Note: Security levels for certificate deployment are specific to NetBackup CA-signed certificates. If the NetBackup web server is not configured to use NetBackup certificates for secure communication, this option cannot be accessed. See “About NetBackup certificate deployment security levels” on page 308. See “Configuring the certificate deployment security levels” on page 310.

Disabling insecure communication

NetBackup communicates with 8.0 and earlier hosts in an insecure manner. For increased security, you should upgrade all hosts to the current version and disable NetBackup communication with 8.0 and earlier hosts.

See [“About secure communication settings”](#) on page 293.

To disable insecure communication

- 1 On the right pane, select **Setting > Global security**.
- 2 In the **Global security settings** page, select **Secure Communication** tab
- 3 Turn off the **Enable insecure communication with 8.0 and earlier hosts** option.
- 4 Click **Save**.

Note: If you disable insecure communications, it is recommended that you restart services to ensure that the insecure connections that are already established are terminated.

About insecure communication with 8.0 and earlier hosts

NetBackup communicates insecurely with 8.0 or earlier hosts.

If you have NetBackup 8.0 or earlier hosts in your environment, you can allow insecure communication with them using the **Enable insecure communication with 8.0 and earlier hosts** option in the **NetBackup BAR Console**.

The option is available on the **Setting > Global Security > Secure communication** tab.

This option also allows communication between NetBackup 8.1 or later primary server .

For increased security, you should upgrade all hosts to the current version and disable communication with 8.0 and earlier hosts.

See [“Disabling insecure communication”](#) on page 295.

See [“About communication with 8.0 or earlier host in multiple NetBackup domains”](#) on page 296.

Note: If you have configured Auto Image Replication, ensure the following before you disable insecure communication: The trusted primary server that you have specified for image replication is of the version that is later than NetBackup 8.0.

See [“About secure communication in NetBackup”](#) on page 273.

About communication with 8.0 or earlier host in multiple NetBackup domains

This section provides information on what is the impact of the **Enable insecure communication with 8.0 and earlier hosts** option on the host communication when one of the NetBackup hosts is in multiple domains.

Consider the following scenario:

- Host A is of version 8.1, which is present in multiple NetBackup domains called M1 and M2.
- Host B is of version 8.0, which is present in a NetBackup domain called M3.
- The **Enable insecure communication with 8.0 and earlier hosts** option is cleared on primary server M1, which means hosts that are associated with M1 cannot communicate with hosts that are 8.0 or earlier.
- The **Enable insecure communication with 8.0 and earlier hosts** option is selected on primary server M2, which means hosts that are associated with M2 can communicate with hosts that are 8.0 or earlier.

- The configuration file (`bp.conf` file on UNIX or registry keys on Windows) for Host A contains 'M2' as the first entry in the primary server list.

When Host A initiates communication with Host B, the status of the **Enable insecure communication with 8.0 and earlier hosts** option is verified for the first primary server that appears in the configuration file of Host A, which is M2. As per the option set for M2, communication with 8.0 or earlier hosts is allowed. Therefore, communication between Host A and Host B is successful.

Automatically mapping host ID to host names and IP addresses

For successful communication between NetBackup hosts, all relevant host names and IP addresses need to be mapped to the respective host IDs. You can choose to automatically map the host ID to the respective host names (and IP addresses) or allow the NetBackup Administrator to verify the mappings before approving them.

See [“Add or Remove Host Mappings dialog box”](#) on page 279.

Note: For increased security, clear this option so that the NetBackup Administrator can manually verify the mappings and approve them.

To automatically map host ID to host names or IP addresses

- 1 At the top right, select **Settings > Global security**.
- 2 Select the **Secure Communication** tab.
- 3 Select the **Automatically map NetBackup host ID to host names** option.
- 4 Click **Save**.

See [“About secure communication settings”](#) on page 293.

About disaster recovery settings

For increased security, a disaster recovery package is created during each catalog backup.

See [“Disaster recovery packages”](#) on page 298.

During each catalog backup, a disaster recovery package is created and encrypted with the passphrase that you set. You need to provide this encryption passphrase while you install NetBackup on the primary server in a disaster recovery mode after a disaster.

The following options are displayed on the **Disaster recovery** tab:

Table 19-3 Disaster recovery settings

Setting	Description
Enter passphrase	Enter the passphrase to encrypt disaster recovery packages. - By default, the passphrase must contain a minimum of 8 and a maximum of 1024 characters. You can set the passphrase constraints using the <code>nbseccmd -setpassphraseconstraints</code> command option. - The existing passphrase and the new passphrase must be different. - Only the following characters are supported for the passphrase: White spaces, uppercase characters (A to Z), lowercase characters (a to z), numbers (0 to 9), and special characters. Special characters include: ~ ! @ # \$ % ^ & * () _ + - = ` { } [] : ; ' , . / ? < > "
Confirm passphrase	Re-enter the passphrase for confirmation.

Caution: Ensure that the passphrase contains only the supported characters. If you enter a character that is not supported, you may face problems during disaster recovery package restore. The passphrase may not be validated and you may not be able to restore the disaster recovery package.

Note the following before you modify the passphrase for the disaster recovery packages:

- Subsequent disaster recovery packages are encrypted with the new passphrase that you set.
- If you change the passphrase anytime, it is not changed for the previous disaster recovery packages. Only new disaster recovery packages are associated with the new passphrase.
- The passphrase that you provide when you install NetBackup on the primary server in the disaster recovery mode after a disaster must correspond to the disaster recovery package from which you want to recover the primary server host identity.

Disaster recovery packages

For increased security, a disaster recovery package is created during each catalog backup. The disaster recovery package file has `.drpkg` extension.

The disaster recovery (DR) package stores the identity of the primary server host. NetBackup requires this package to get the identity of the primary server back after a disaster. Once you have recovered the host identity, you can perform the catalog recovery.

The disaster recovery package contains the following information:

- NetBackup CA-signed certificates and private keys of the primary server certificate and the NetBackup certificate authority (CA) certificate
- Information about the hosts in the domain
- Security settings
- External CA-signed certificates
External CA-signed certificates from Windows certificate store, if applicable
- NetBackup configuration options that are specific to external CA-signed certificates
- Key management service (KMS) configuration

Note: By default, the KMS configuration is not backed up during catalog backup. Set the KMS_CONFIG_IN_CATALOG_BKUP configuration option to 1 to include the KMS configuration as part of the disaster recovery package during catalog backup.

Note: You must set a passphrase for the disaster recovery package for the catalog backups to be successful.

Setting a passphrase to encrypt disaster recovery packages

During each catalog backup, a disaster recovery package is created and encrypted with the passphrase that you set.

See [“Disaster recovery packages”](#) on page 298.

Workflow to set a passphrase to encrypt disaster recovery packages and use it after a disaster:

Review the following workflow to learn about disaster recovery package restore:

1. Set an encryption passphrase for disaster recovery packages.
2. Create a catalog policy.

Consider the following scenarios:

- If you have not set the passphrase earlier, NetBackup prevents you from configuring a new catalog backup policy.
- If the catalog backup policy is upgraded from a previous version, catalog backups continue to fail until the passphrase is set.

Note: Catalog backups may fail with status code 144 even though the passphrase is set. This issue occurs because the passphrase may be corrupted. To resolve this issue, you must reset the passphrase.

3. After a disaster, when you install NetBackup on the primary server in a disaster recovery mode, provide the passphrase that you have set earlier. NetBackup decrypts the disaster recovery package using this passphrase and gets the identity of the primary server back during installation.

Caution: Special action is required if you fail to provide the appropriate passphrase when you install NetBackup on the primary server after a disaster. You may need to redeploy the security certificates on all NetBackup hosts. For more details, refer to the following article:

<https://support.cohesity.com/s/article/article-100033743>

4. Once the primary server identity is back in place, the secure communication between the primary server and the media server is established and you can perform catalog recovery.
5. After successful catalog recovery, you must set the disaster recovery package passphrase again, because the passphrase is not recovered during the catalog recovery. Catalog backups that you configure in a new NetBackup instance continue to fail until you set the passphrase.

To set or modify a passphrase

- 1 Open the NetBackup web UI.
- 2 At the top right, select **Settings > Global security**.
- 3 Select **Disaster recovery**.
See [“About disaster recovery settings”](#) on page 297.
- 4 Enter and confirm a passphrase.
Review the following password rules:

- The existing passphrase and the new passphrase must be different.

- By default, the passphrase must contain a minimum of 8 and a maximum of 1024 characters.

You can set the passphrase constraints using the `nbseccmd -setpassphraseconstraints` command option.

- Only the following characters are supported for the passphrase: White spaces, uppercase characters (A to Z), lowercase characters (a to z), numbers (0 to 9), and special characters. Special characters include: ~ ! @ # \$ % ^ & * () _ + - = ` { } [] | : ; ' , . / ? < > "

Caution: If you enter a character that is not supported, you may face problems during disaster recovery package restore. The passphrase may not be validated and you may not be able to restore the disaster recovery package.

- 5 Select **Save**. If the passphrase already exists, it is overwritten.

To set or modify a passphrase using the command-line interface

- 1 The NetBackup administrator must be logged on to the NetBackup Web Management Service to perform this task. Use the following command to log on:

```
bpbnet -login -loginType WEB
```

- 2 Run the following command to set a passphrase to encrypt disaster recovery packages:

```
nbseccmd -drpkgpassphrase
```

- 3 Enter the passphrase.

If a passphrase already exists, it is overwritten.

Validate the disaster recovery package passphrase

Cohesity strongly recommends that you validate the disaster recovery (DR) package passphrase every 30 days. It helps you recall the passphrase when you need to recover the primary server identity using the DR package.

If validation fails, the specified passphrase is set as your DR package passphrase.

To validate the disaster recovery package passphrase

- 1 At the top right, select **Settings > Global security**.
- 2 Go to the **Disaster recovery** tab.
- 3 Locate the **Passphrase Validation** section and select **Validate**.

- 4 Enter and confirm the passphrase that you set earlier.
- 5 Select the check box **Notify me to validate passphrase every 30 days**. This option is recommended.
- 6 Select **Validate**.

About host name-based certificates

By default, individual NetBackup primary servers are provisioned with a host name-based certificate during installation. To provision a host name-based certificate on a media server or client, the NetBackup administrator runs the `bpnbaz` command on the primary server to push the certificate to other hosts.

See [“Overview of security certificates in NetBackup”](#) on page 273.

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 19-4 Deploying host name-based certificates

Procedure	Description and link to procedure
Deploying a host name-based security certificate for a primary server in a cluster	Use this procedure to deploy the host name-based security certificates on all of the nodes in a NetBackup primary server cluster.
Deploying a host name-based security certificate for media servers or clients	This procedure uses IP address verification to identify the target NetBackup host and then deploy the certificate. With this procedure, you can deploy a host name-based certificate for an individual host, for all media servers, or for all clients.

Note: Deploying a host name-based certificate is a one-time activity for a host. If a host name-based certificate was deployed for an earlier release or for a hotfix, it does not need to be done again.

Deploying a host name-based certificate for a primary server in a cluster

Use this procedure to deploy host name-based certificates on all cluster nodes.

Ensure the following before you deploy a host-name based certificate:

- All nodes of the cluster have a host ID-based certificate.
- All Fully Qualified Domain Names (FQHN) and short names for the cluster nodes are mapped to their respective host IDs.

To deploy a host name-based security certificate for a NetBackup primary server in a cluster

- 1 Run the following command on the active node of the primary 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 primary server.

Deploying a host name-based certificate on media servers or clients

This procedure works well when you deploy host name-based security certificates to many hosts at one time. As with NetBackup deployment in general, this method assumes that the network is secure.

To deploy a host name-based security certificate for media servers or clients

- 1 Run the following command on the primary 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/opensv/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 primary server. To do so, run the following NetBackup `bpclient` command on the primary server:

On Windows: `Install_path\NetBackup\bin\admincmd\bpclient -L -All`
 On UNIX: `/usr/opensv/netbackup/bin/admincmd/bpclient -L -All`

About host ID-based certificates

Each host in a NetBackup domain has a unique identity, which is referred to as a host ID or a Universally Unique Identifier (UUID). The primary server is the Certificate Authority (CA). It assigns host ID-based certificates to hosts and stores the host information in the `nbdb` database. The CA maintains a list of all of the host IDs that have certificates (or revoked certificates). The host ID is used in many certificate management operations to identify the host.

Host IDs are randomly generated by the system and are not tied to any property of the hardware.

NetBackup provides a list of host ID-based certificates that you have revoked.

See [“About the host ID-based certificate revocation list”](#) on page 334.

See [“Overview of security certificates in NetBackup”](#) on page 273.

Only a NetBackup administrator can control the settings that are related to certificate deployment and revocation.

The host ID remains the same even when the host name changes.

If a host obtains certificates from multiple NetBackup domains, it has multiple host IDs that correspond to each NetBackup domain.

When the primary server is configured as part of a cluster, each node in the cluster receives a unique host ID. An additional host ID is assigned for the virtual name. For example, if the primary server cluster is comprised of N nodes, the number of host IDs that are allocated for the primary server cluster is $N + 1$.

Web login requirements for `nbcertcmd` command options

The `nbcertcmd` command can be used to perform all of the operations that are associated with host-ID based certificates. However, some of the `nbcertcmd` options require that the user first logs in to the NetBackup Web Management Service (`nbwmc`).

- To log in to the NetBackup Web Management Service, run the following command:

```
bpnbat -login -logintype WEB
```

The account must have NetBackup administrator privileges.

The following shows an example `WEB` login:

```
bpnbat -login -LoginType WEB
Authentication Broker: server.domain.com
Authentication port [0 is default]: 0
Authentication type (NIS, NISPLUS, WINDOWS, vx, unixpwd, ldap): unixpwd
```

```
Domain: server.domain.com
Login Name: root
Password: *****
Operation completed successfully.
```

- The `bpnbat -login -logintype AT` command creates a session with the NetBackup Authentication Broker (`nbatd`). (The NetBackup Authentication Broker may not always be the primary 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 primary server.)

Note: The authentication broker for a `WEB` login is the primary server as the `nbwmc` service runs only on the primary server.

The [NetBackup Commands Reference Guide](#) lists the privilege details that each `nbcertcmd` option requires. This guide also contains detailed information about running the `bpnbat` command.

Using the Certificate Management utility to issue and deploy host ID-based certificates

The process for host ID-based certificate deployment varies based on the certificate deployment security level configured on the primary server. The levels are **Medium**, **High**, and **Very High**. By default, the security level is **High**.

A host ID-based certificate is automatically deployed on the primary server during upgrade or installation.

Host ID-based certificates are deployed on hosts after confirming the fingerprint. Whether an authorization token is required or not depends on the security level.

These levels determine the nature of the Certificate Authority (CA) checks that are performed when the CA receives a certificate request from a NetBackup host. Select the certificate deployment level according to the security requirements of your NetBackup environment.

See [“About NetBackup certificate deployment security levels”](#) on page 308.

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 19-5 Deployment requirements at each certificate deployment level or scenario

Certificate deployment level or scenario	Is an authorization token required?	Deploy host ID-based certificate?
Certificate deployment level setting at Very High	Yes. All certificate requests require an authorization token. The primary server administrator creates a token to be used on the non-primary host: See “Creating authorization tokens” on page 331.	The host administrator of the non-primary server host must obtain an authorization token from the primary server administrator and use it to deploy the host ID-based certificate. See “Deploying host ID-based certificates” on page 312.
Certificate deployment level setting at High (default)	Maybe. Certificates are deployed without tokens on hosts that are known to the primary server. The following topic explains what it means to be known to the primary server: See “About NetBackup certificate deployment security levels” on page 308. If the host is not known to the primary server, the certificate must be deployed using an authorization token. The primary server administrator creates a token to be used on the non-primary server host. See “Creating authorization tokens” on page 331.	If a host ID-based certificate is deployed, no further action is required. If a token is required, the host administrator of the non-primary server host must to obtain one from the primary server administrator and use it to deploy the host ID-based certificate. See “Deploying host ID-based certificates” on page 312.
Certificate deployment level setting at Medium	No. Certificates may be deployed on all hosts that request one. See “Automatic host ID-based certificate deployment” on page 310. Note: A certificate may not be deployed if the primary server cannot verify that the requested host name matches the IP from which the certificate request originated.	If a host ID-based certificate is deployed, no further action is required. If the primary server cannot verify the host name, a host ID-based certificate must be deployed using a token. See “Deploying host ID-based certificates” on page 312.

Table 19-5 Deployment requirements at each certificate deployment level or scenario (*continued*)

Certificate deployment level or scenario	Is an authorization token required?	Deploy host ID-based certificate?
Certificate reissue	Yes. A certificate reissue requires a reissue token in most cases.	See “Creating a reissue token” on page 327.
Hosts that cannot communicate with the primary server directly (an example of this is NetBackup hosts in a demilitarized zone (DMZ)).	Yes. NetBackup can automatically detect whether a host has connectivity with the primary server or not. If there is no connectivity, NetBackup attempts to use the built-in HTTP tunnel on a media server to route the certificate request to the primary server. See “About the communication between a NetBackup client located in a demilitarized zone and a primary server through an HTTP tunnel” on page 354.	See “Deploying certificates on a client that has no connectivity with the primary server” on page 322.
Certificate deployment and generation for NAT clients	Yes. During NetBackup certificate deployment on a NAT client, you must provide an authorization token is must, irrespective of the certificate deployment security level that is set on the primary server. This is because, the primary server cannot resolve the host name to the IP address from which the request is sent.	For more information about the support for NAT clients in NetBackup, refer to the NetBackup Administrator's Guide, Volume I .

Viewing host ID-based certificate details

Details for each host ID-based certificate can be viewed in the **NetBackup web UI** or with the `nbcertcmd` command or the NetBackup APIs.

To view certificate details in the NetBackup web UI

- 1 Open the NetBackup web UI.
- 2 On the left, click **Security > Certificates**.
The certificate details are displayed in the right pane.
- 3 Select the host name and click **View details**.

To view certificate details using the `nbcertcmd` command

- ◆ To view all of the host IDs that are assigned to a host from different primary servers, run the following command on a NetBackup host:

```
nbcertcmd -listCertDetails
```

About NetBackup certificate deployment security levels

Security levels for certificate deployment are specific to NetBackup CA-signed certificates. If the NetBackup web server is not configured to use NetBackup certificates for secure communication, the security levels cannot be accessed.

The NetBackup certificate deployment level determines the checks that are performed before the NetBackup CA issues a certificate to a NetBackup host. It also determines how frequently the NetBackup Certificate Revocation List (CRL) is refreshed on the host.

NetBackup certificates are deployed on hosts during installation (after the host administrator confirms the primary server fingerprint) or with the `nbcertcmd` command. Choose a deployment level that corresponds to the security requirements of your NetBackup environment.

Note: During NetBackup certificate deployment on a NAT client, you must provide an authorization token irrespective of the certificate deployment security level that is set on the primary server. This is because, the primary server cannot resolve the host name to the IP address from which the request is sent.

For more information about NAT support in NetBackup, refer to the [NetBackup Administrator's Guide, Volume I](#).

See [“Using the Certificate Management utility to issue and deploy host ID-based certificates”](#) on page 305.

See [“Configuring the certificate deployment security levels”](#) on page 310.

Table 19-6 Description of NetBackup certificate deployment security levels

Security level	Description	CRL refresh
Very High	An authorization token is required for every new NetBackup certificate request. See “Creating authorization tokens” on page 331.	The CRL that is present on the host is refreshed every hour. See “About the host ID-based certificate revocation list” on page 334.

Table 19-6 Description of NetBackup certificate deployment security levels
(continued)

Security level	Description	CRL refresh
High (default)	No authorization token is required if the host is known to the primary server. A host is considered to be known to the primary server if the host can be found in the following entities: 1 The host is listed for any of the following options in the NetBackup configuration file (Windows registry or the <code>bp.conf</code> file on UNIX): ■ APP_PROXY_SERVER ■ DISK_CLIENT ■ ENTERPRISE_VAULT_REDIRECT_ALLOWED ■ MEDIA_SERVER ■ NDMP_CLIENT ■ SERVER ■ SPS_REDIRECT_ALLOWED ■ TRUSTED_MASTER ■ VM_PROXY_SERVER ■ MSDP_SERVER For more details on the NetBackup configuration options, refer to the NetBackup Administrator's Guide, Volume I. 2 The host is listed as a client name in the <code>altnames</code> file (<code>ALTNAMEESDB_PATH</code>). 3 The host appears in the EMM database of the primary server. 4 At least one catalog image of the client exists. The image must not be older than 6 months. 5 The client is listed in at least one backup policy. 6 The client is a legacy client. This is a client that was added using the Client Attributes host properties. See “Creating authorization tokens” on page 331.	The CRL that is present on the host is refreshed every 4 hours.
Medium	The certificates are issued without an authorization token if the primary server can resolve the host name to the IP address from which the request was originated.	The CRL that is present on the host is refreshed every 8 hours.

Configuring the certificate deployment security levels

Use the **NetBackup web UI** or the `nbcertcmd` command to configure the certificate deployment security level in the NetBackup domain.

These security levels are specific to NetBackup CA-signed certificates.

To configure the certificate deployment level

- 1 At the top right, click **Settings > Global security**.
- 2 Click the **Secure communication** tab.
- 3 Under **Security level for certificate deployment**, select the security level: **Very High**, **High** (default), or **Medium**.
- 4 Click **Save**.

To configure the certificate deployment level using the command line

- 1 The primary server administrator must be logged in to the NetBackup Web Management Service to perform this task. Use the following command to log in:

```
bnpbat -login -logintype WEB
```

See [“Web login requirements for nbcertcmd command options”](#) on page 304.

- 2 Run the following command to view the current security level:

```
nbcertcmd -getSecConfig -certDeployLevel -server  
primary_server_name
```

- 3 Run the following command to change the security level:

```
nbcertcmd -setSecConfig -certDeployLevel 0-2 -server  
primary_server_name
```

Where 0 is Very High, 1 is High (default), and 2 is Medium.

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

Automatic host ID-based certificate deployment

A host ID-based certificate is automatically deployed on the NetBackup primary server as part of NetBackup installation.

These certificates are deployed on other NetBackup hosts (after confirming the fingerprint) depending on the certificate deployment level.

The Certificate Authority (CA) on the NetBackup primary server can accept or reject the certificate request depending on the certificate deployment level and the ability of the primary server to verify the host information.

You can check the list of the deployed certificates on any NetBackup host by using the following command:

```
nbcertcmd -listCertDetails
```

When a certificate request is rejected, the host administrator must request the NetBackup administrator to generate and share an authorization token to deploy the certificate manually.

See [“Creating authorization tokens”](#) on page 331.

See [“About NetBackup certificate deployment security levels”](#) on page 308.

Managing passphrases and passphrase keys for encryption of private key of host ID-based certificates

Randomly-generated passphrases are used to encrypt and decrypt the private keys of NetBackup host ID-based certificates. Passphrase keys are used to encrypt and decrypt these passphrases. There is one passphrase - passphrase key pair that is used to encrypt and decrypt all the private keys in a keystore. The passphrase that is used to encrypt the private keys is itself encrypted using another passphrase key. The passphrase - passphrase key pair is generated when the first key in the keystore is created and stored.

Using a passphrase key to encrypt passphrases adds an additional layer of security as only those users who have access to the passphrase key can decrypt and access the encrypted passphrases. A passphrase key protects a passphrase from unauthorized access and enables centralized management of passphrases. With easy rotation of passphrases, organizations can maintain the security in their NetBackup environment.

Passphrase rotation is the process of updating the existing passphrases. The process makes the system more secure by ensuring that the compromised private keys or passphrases are updated. Rotating the passphrase also encrypts the private keys that are currently in plain text.

Rotating passphrases is essential to reduce the risk of unauthorized access by limiting the time an attacker can exploit a compromised passphrase. It helps protect against brute-force attacks and mitigates the impact of insider threats. Additionally, regular passphrase rotation is often a requirement for compliance with various security standards and regulatory frameworks that helps organizations maintain a secure and compliant environment.

Advantages of 2-level encryption

Rotation of a passphrase key: This allows to re-encrypt the passphrase with new passphrase key at regular intervals without hampering the ongoing NetBackup operations.

Rotation of passphrase: If the administrators encounter a security threat, they can rotate the passphrase. This creates a new passphrase - passphrase key pair. Re-encrypt all private keys with the new passphrase. All NetBackup services must be stopped before this operation.

Rotating a passphrase

To rotate a passphrase

- 1 Stop the NetBackup services.

Ensure that all NetBackup services are stopped before you proceed.

- 2 Run the following command to rotate passphrase:

```
nbcertcmd -rotatePassphrase
```

Note: The default passphrase length is 64 characters.

Run the following command to specify the passphrase length:

```
nbcertcmd -rotatePassphrase -length 1023
```

The length ranges from 32 to 1023.

- 3 Start the NetBackup services.

Rotating a passphrase key

To rotate the passphrase key

- ◆ Run the following command:

```
nbcertcmd -rotatePassphraseKey
```

Deploying host ID-based certificates

Depending on the certificate deployment security level, a non-primary host may require an authorization token before it can obtain a host ID-based certificate from the Certificate Authority (primary 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.

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-primary 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-primary host to establish that the primary server can be trusted:

```
nbcertcmd -getCACertificate
```

- 2 Run the following command on the non-primary host:

```
nbcertcmd -getCertificate
```

Note: To communicate with multiple NetBackup domains, the administrator of the host must request a certificate from each primary server using the `-server` option.

Run the following command to get a certificate from a specific primary server:

```
nbcertcmd -getCertificate -server primary_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-primary host to establish that the primary server can be trusted:

```
nbcertcmd -getCACertificate
```

- 3 Run the following command on the non-primary 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 primary server using the `-server` option.

If the administrator obtained the token in a file, enter the following:

```
nbcertcmd -getCertificate -file authorization_token_file
```

- 4 To verify that the certificate is deployed on the host, run the following command:

```
nbcertcmd -listCertDetails
```

Use the `-cluster` option to display cluster certificates.

Deploying host ID-based certificates in an asynchronous manner

Host ID-based certificates are automatically deployed on NetBackup hosts during installation or upgrade. For successful automatic certificate deployment, the host where the certificate needs to be deployed should be connected to the primary server.

In certain scenarios, you may want to create, sign, and deploy host ID-based certificates in an asynchronous manner where the host and the primary server do not need to be connected at the time of certificate deployment.

To deploy host ID-based certificate in an asynchronous manner

- 1 This command can be run only by the host administrator.

Create a certificate signing request. Run the following command on the non-primary server host where you want to deploy the certificate:

```
nbcertcmd -createCertRequest -requestFile request_file_name  
-server primary_server_name
```

Optionally, copy the Certificate Signing Request (CSR) file to any NetBackup host.

- 2 Get a signed certificate from the primary server on the host. An authorization token is mandatory. If the host already has a certificate, a reissue token is required.

Run the following command on the host:

```
nbcertcmd -signCertificate -requestFile request_file_name  
-certificateFile certificate_file_name -token
```

Note: Be sure to use the `-signCertificate` option on a host with the same or higher NetBackup version where the certificate signing request (CSR) was generated.

- 3 Copy the signed certificate that is generated in step 2 and provide it to the host administrator.
- 4 This command can be run only by the host administrator.

To deploy the signed certificate on the host, run the following command on the client:

```
nbcertcmd -deployCertificate -certificateFile  
certificate_file_name
```

Implication of clock skew on certificate validity

When a primary server issues a certificate, it determines for how long the certificate will be valid for the host to use. The primary 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 primary 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, it is recommended 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 primary 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 primary server issued a fresh certificate, it could be treated as expired.
- If the host clock is behind the primary server, a fresh certificate issued by the primary server could be considered as unusable by the host because the host considers the certificate as not yet valid.

To determine whether the primary 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 primary server clock:

```
nbcertcmd -checkClockSkew -server primary_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 primary server.
```
- If the current host is behind the primary server, the command reports the difference in seconds:

```
The current host clock is behind the primary server by 36 seconds(s) .
```
- If the current host is ahead of the primary server, the command reports the difference in seconds:

```
The current host clock is ahead of the primary server by 86363 second(s) .
```
- If the command is run on the primary 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 primary server (Certificate Authority)

Each NetBackup host must first trust the NetBackup primary 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 primary server.

See [“Automatic host ID-based certificate deployment”](#) on page 310.

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 primary servers that the host already trusts.

To establish trust with the primary 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 primary 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 the certificate authority”](#) on page 319.

- 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 primary 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 312.

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

Adding a CA certificate via message in the NetBackup BAR Console

The **Backup, Archive, and Restore** console communicate with NetBackup hosts (primary 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 19-1](#) displays in the **NetBackup BAR Console** in the following situation: A user is running the **NetBackup BAR Console** on a NetBackup host. The user tries to connect to another NetBackup host (a target host) using the **NetBackup BAR 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 19-1 Message inquiring whether to add a Certificate Authority (CA) to the trust store



To verify the CA fingerprint that the dialog displays, see the following topic:

See [“Finding and communicating the fingerprint of the certificate authority”](#) on page 319.

If the user selects **Yes** in this message, the CA is added to the trust store of the host where the console is running. This host will then trust all hosts that have a certificate signed by the CA that is listed in the message.

Finding and communicating the fingerprint of the certificate authority

The primary 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.

Both SHA-1 or SHA-256 fingerprints are supported.

To find the fingerprint of the CA certificate

- 1 The primary server administrator can find the fingerprint using the NetBackup web UI or the command line:

Using the **NetBackup web UI**:

- Select **Security > Certificates**.
- Select **Certificate Authority**.
- The following information is displayed:

Subject name	Identifies the certificate for the desired primary server.
--------------	--

Start date	The date when the certificate is activated.
Expires	The date when the certificate expires.
SHA-1 fingerprint	The hash value of the certificate that is calculated using the SHA-1 algorithm. Click Copy to clipboard to help the administrator communicate the fingerprint to the host administrator.
SHA-256 fingerprint	The hash value of the certificate that is calculated using the SHA-256 algorithm. Click Copy to clipboard to help the administrator communicate the fingerprint to the host administrator.

Using the command line:

- Run the following command on the primary server to view the Root Certificate Fingerprint:

```
nbcertcmd -listCACertDetails
```

If multiple CA certificates are displayed, use the **Subject name**.

- 2 The primary server administrator communicates the fingerprint to the host administrator by email, by file, or on an internal web site.

The host administrator uses the fingerprint value to verify the fingerprint that is displayed when the host runs `nbcertcmd -getCACertificate`. This verifies the authenticity of the CA certificate.

Using the vssat command to view the CA certificate fingerprint

The `vssat` command can also be used to view the CA certificate fingerprint. Use `vssat` with the following options:

```
vssat showcred -p nbatd
```

However, note the following differences between using `nbcertcmd -listCACertDetails` and `vssat`:

- `vssat` displays the fingerprint as a hash and does not include colon separators.
- If the host trusts multiple Certificate Authorities, the `nbcertcmd` command displays all CA certificates. The **Subject Name** displays the identity of the CA.

Forcing or overwriting certificate deployment

In some situations it may be necessary to use the `-force` option with the `nbcertcmd -getCertificate` command. For example, to force certificate deployment to a host

or to overwrite the existing host ID-based certificate information and fetch a new certificate.

Forcing certificate deployment

A host may already have a host ID-based certificate, but needs to overwrite the old certificate with a new one. This is required, for example, when a primary 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-primary host:

```
nbcertcmd -getCertificate -server primary_server_name -force
```

- Depending on the security setting on the primary server, a token may also need to be specified.
See [“Creating authorization tokens”](#) on page 331.
- 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-primary 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-primary host:

```
nbcertcmd -getCertificate -force
```

- Depending on the security setting on the primary server, a token may also need to be specified.
See [“Creating authorization tokens”](#) on page 331.
- Use the `-cluster` option to deploy a cluster certificate.

Retaining host ID-based certificates when reinstalling NetBackup on non-primary 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 including the hidden files:
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 primary server

NetBackup can detect whether a host has connectivity with the primary server or not. If there is no connectivity, NetBackup automatically attempts to use the built-in HTTP tunnel on a media server to route the connection request to the primary server.

If NetBackup cannot automatically detect the host connectivity with the primary server or find an appropriate media server to route the connection request, you need to manually configure the HTTP tunnel options.

See [“About the communication between a NetBackup client located in a demilitarized zone and a primary server through an HTTP tunnel”](#) on page 354.

To deploy a certificate on a client that has no connectivity with the primary server, refer to the following topic:

See [“Deploying host ID-based certificates”](#) on page 312.

Note: As the request is routed via a different host, the primary server cannot validate the authenticity of the certificate request, therefore an authorization token is a must.

About host ID-based certificate expiration and renewal

NetBackup host ID-based certificates expire one year after their issue date. They are automatically renewed 180 days before the expiration date. A certificate renewal request is sent periodically until a certificate is successfully renewed. Automatic renewal ensures that the renewal process is transparent to the users.

Note: You can disable automatic renewal of host-ID based certificates using the `DISABLE_CERT_AUTO_RENEW` parameter from the NetBackup configuration file (the Windows registry or the `bp.conf` file on UNIX).

For more information, see the *NetBackup Administrator's Guide, Volume I*.

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-primary host:

```
nbcertcmd -renewCertificate
```

- Certificates corresponding to NetBackup domains other than the primary domain can be manually renewed by specifying the `-server` option.
- Use the `-cluster` option to renew the cluster certificate of NetBackup clustered server.

In a scenario where the certificate has expired, the administrator of the host must manually reissue the certificate.

See [“About reissuing host ID-based certificates”](#) on page 326.

Deleting sensitive certificates and keys from media servers and clients

In the cloning process, use the following command to remove certain sensitive certificates and keys from NetBackup media servers and clients in the following scenarios:

- Run the command on the cloned virtual machine, which is cloned from an active NetBackup host.
- Run the command before creating a gold image of a virtual machine for cloning.

```
nbcertcmd -deleteAllCertificates
```

Note: This command is allowed only on media servers and clients. The command is not allowed on primary servers.

This operation deletes or shreds the appropriate sensitive information (certificates and keys) from the following locations:

On Windows:

- *Install_Path\NetBackup\var\VxSS\certmapinfo.json*
- *Install_Path\NetBackup\var\VxSS\credentials\<certificate>*
 For example:
Install_Path\NetBackup\var\VxSS\credentials\6d92d4dd-ed2d-43de-adb1-bf333aa2cc3c
- *Install_Path\NetBackup\var\VxSS\credentials\keystore\PrivKeyFile.pem*
 (shredded)
- *Install_Path\NetBackup\var\VxSS\at\systemprofile\certstore\<certificate>*
 For example:
Install_Path\NetBackup\var\VxSS\at\systemprofile\certstore\9345b05e-lilycl2nb!1556!nbatd!1556.0
- *Install_Path\NetBackup\var\VxSS\at\systemprofile\certstore\keystore\PrivKeyFile.pem*
 (shredded)
- *Install_Path\NetBackup\var\VxSS\at\systemprofile\certstore\keystore\PubKeyFile.pem*

On UNIX:

- /usr/opensv/var/vxss/certmapinfo.json
- /usr/opensv/var/vxss/credentials/<certificate>
For example:
 /usr/opensv/var/vxss/credentials/
 f4f72ef3-2cfc-42a4-ab5a-65fd09e8b63e
- /usr/opensv/var/vxss/credentials/keystore/PrivKeyFile.pem (shredded)
- /var/vxss/at/root/.VRTSat/profile/certstore/<certificate>
- /var/vxss/at/root/.VRTSat/profile/certstore/keystore/PubKeyFile.pem
- /var/vxss/at/root/.VRTSat/profile/certstore/keystore/PrivKeyFile.pem (shredded)

Cleaning host ID-based certificate information from a host before cloning a virtual machine

Cloning a virtual machine can present the opportunity for identity theft. Multiple hosts should not have the same key pair. This procedure ensures that each copy of the host gets a unique key pair and identity.

Perform the following procedure before cloning a virtual machine (or before creating a gold image of a machine for cloning) if it is a one-time operation.

To clean the host ID-based certificate information from a host before cloning

- 1 Stop all NetBackup services on the host.
- 2 Delete all files and directories from the following locations:

On Windows:

*Install_path\NetBackup\var\VxSS\at**

*Install_path\NetBackup\var\VxSS\credentials**

*Install_path\NetBackup\var\webtruststore**

On UNIX:

*/usr/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, and you later determine that you can trust that host again.
- The certificate expired.
- NetBackup was reinstalled on the host where a certificate was already issued.
- The name of the host was changed.
- The key pair for the host was changed.

Reissuing a certificate is one way to prevent malicious users from assuming the identity of an existing NetBackup host that is already registered with the NetBackup primary server. In most cases, a reissue token is required for certificate reissue.

- Reissuing a host ID-based certificate for a NetBackup host is different from deploying the certificate for the first time. Use the following procedure to reissue a certificate.

See [“Creating a reissue token”](#) on page 327.

- 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 312.

When the primary 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-primary host is already registered with the primary 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

- 1 Open the NetBackup web UI.
- 2 On the left, select **Security > Certificates**.
- 3 Select the host that requires a reissue token.
- 4 Click **Generate Reissue Token**.
- 5 Enter the name for the token.
- 6 Select a date for token validity from the **Valid for** option.
- 7 In the **Reason** field, enter a reason for the reissue token. The reason appears in the log as an audit event.
- 8 Click **Generate**.
- 9 Click **Copy to clipboard** to copy the token value.
- 10 Convey the token value to the administrator of the non-primary 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-primary 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 312.

To create a reissue a token using the `nbcertcmd` command

- 1 The primary 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 304.

- 2 Run one of the following commands on the primary server:

Use the host name for which the certificate needs to be reissued:

```
nbcertcmd -createToken -name token_name -reissue -host host_name
```

Note: You must provide the primary name of the host for which you want to reissue the certificate. If you provide any of the host ID-to-host name mappings that are added for the host, the certificate cannot be reissued.

Use the host ID for which the certificate needs to be reissued:

```
nbcertcmd -createToken -name token_name -reissue -hostId host_id
```

Additional parameters can be used to indicate validity duration and the reason for creation.

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

Additional steps to request a certificate for a renamed NetBackup host

In addition to reissuing a token, the following steps are required to request a certificate for a renamed NetBackup host.

To request a certificate for a host after a host name change

- 1 The NetBackup administrator of the primary server generates a reissue token for the renamed NetBackup host.
- 2 Add the new host name as one of the approved host ID-to-host name mappings by using **NetBackup web UI**.

See [“Adding host ID to host name mappings”](#) on page 278.

Alternatively, you can use the `nbhostmgmt -add` command-line interface option.

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

- 3 The NetBackup administrator must revoke the host ID-based certificate for the renamed host.

See [“Revoking a host ID-based certificate”](#) on page 339.

Note: After the certificate is revoked, the host is unable to communicate with the NetBackup Web Management Console service (`nbwmc`). When the host obtains a new certificate using the reissue token, the host can communicate with `nbwmc` again.

- 4 After the certificate is revoked, the administrator of the non-primary host must use the reissue token to get a certificate for the renamed host.

See [“Deploying host ID-based certificates”](#) on page 312.

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 primary server, only a non-primary server host.

To change a key pair for a host

- 1 The NetBackup host administrator backs up the following directories:

On Windows: `Install_path\NetBackup\var\VxSS\at\systemprofile`

On UNIX: `/usr/openv/var/vxss/at/root`

- 2 The NetBackup host administrator removes the directory from the host.
- 3 Restart the NetBackup services on the host.
- 4 The primary server administrator performs the following steps:

- Log in to the NetBackup Web Management Service:

```
bpbnet -login -logintype WEB
```

See [“Web login requirements for nbcertcmd command options”](#) on page 304.

- 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 327.

- Deploy a new host name-based certificate:

```
bpnbaz -ProvisionCert host_name
```

- 5 The NetBackup host administrator uses the reissue token to deploy a new host ID-based certificate with an updated key pair.

Use the following command to enter the token directly:

```
nbcertcmd -getCertificate -force -token
```

Use the following command if the token is in a file:

```
nbcertcmd -getCertificate -force -file /directory/token_file
```

- 6 If the host has more than one primary server, repeat the process beginning at step 4 for each primary server.
- 7 Restart the NetBackup services on the NetBackup host where the key was changed.

About Token Management for host ID-based certificates

Master server administrators use the **Token Management** utility to perform the following tasks:

- Create new authorization tokens
 Depending on the security level, an authorization token may be required for a non-primary NetBackup host to obtain a host ID-based certificate. The NetBackup administrator of the primary server generates the token and shares it with the administrator of the non-primary host. That administrator can then deploy the certificate without the presence of the primary server administrator.
 See [“Creating authorization tokens”](#) on page 331.
- Delete authorization tokens
 See [“Deleting authorization tokens”](#) on page 333.
- View authorization token details
 See [“Viewing authorization token details”](#) on page 333.
- Clean up invalid or expired authorization tokens
 See [“About expired authorization tokens and cleanup”](#) on page 334.

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 (primary server).

See [“Creating a reissue token”](#) on page 327.

- 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 primary server. If the host is not known to the primary 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 primary server, see the following topic:
 See [“About NetBackup certificate deployment security levels”](#) on page 308.
- 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 primary 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 primary server.

See [“Deploying certificates on a client that has no connectivity with the primary server”](#) on page 322.

Note: Do not use this procedure to create an authorization token for a NetBackup host whose current certificate is not in a valid state because it is lost, corrupt, or expired. In these cases, a reissue token must be used.

See [“About reissuing host ID-based certificates”](#) on page 326.

The NetBackup administrator of the primary server can use the NetBackup web UI or the command line to create the token.

To create a token using the NetBackup web UI

- 1 On the left, select **Security > Tokens**.
- 2 Select **Add**.

- 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 primary_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 primary 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** Select the **Copy to clipboard** button to save the token value to the clipboard.
- 9** Convey the token value to the administrator of the non-primary 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-primary 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 312.

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 web UI** 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 web UI

- 1 On the left pane, select **Security > Tokens**.
- 2 In the right pane, select the token to be deleted.
- 3 Click **Delete**.
- 4 Click **Yes** in the confirmation dialog box to delete the token.

To delete a token using the command line

- ◆ Run the `nbcertcmd -deleteToken` command (with additional parameters).

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

Viewing authorization token details

Details for each authorization token can be viewed in the **NetBackup BAR Console** or from the command line.

To view token details using the NetBackup Administration web UI

- 1 On the left pane, select **Security > Tokens**.
- 2 On the **Token Management** page, the token details will be displayed.

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 primary 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 token is used for **Maximum Uses Allowed** requests.

An expired authorization token remains in the token database, but cannot be used to authorize certificate deployment requests.

Expired tokens can be deleted one by one, or they can be cleaned up all at once by using the **Cleanup** operation. The **Cleanup** operation deletes all expired tokens from the token database.

To clean up expired authorization tokens using the NetBackup Administration web UI

- 1 On the left pane, select **Security > Tokens**.
- 2 On the **Token Management** page, select **Cleanup**.
- 3 Click **Yes** 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 333.

About the host ID-based certificate revocation list

The NetBackup certificate revocation list (CRL) is a list of host ID-based digital security certificates that have been revoked before their expiration date. The hosts that own revoked certificates should no longer be trusted.

The NetBackup certificate revocation list conforms to the Certificate Revocation List profile that the Internet Engineering Task Force publishes in RFC 5280 at <https://www.ietf.org>. The NetBackup certificate authority signs the CRL. The NetBackup primary server is the certificate authority. The CRL is public and does not require secure transmission. The CRL endpoint is open, free for anyone to access.

Every NetBackup host must have a valid security certificate and a valid CRL so that it can communicate with other NetBackup hosts.

How often NetBackup generates a new CRL

The NetBackup primary server generates a new CRL as follows:

- On startup.
- Sixty minutes since the CRL was last generated.
- NetBackup checks every 5 minutes for a newly revoked certificate. It can take NetBackup up to 5 minutes to update the web server after a certificate is revoked.

A CRL expires after 7 days.

How often a NetBackup host gets a CRL

A NetBackup host obtains a CRL when NetBackup is installed on the host. A NetBackup host also obtains a fresh CRL during an upgrade of the NetBackup software.

After installation or upgrade, each host requests a new CRL on a time interval since the host was started. (NetBackup uses a pull method to refresh host CRLs.) The NetBackup primary server certificate deployment security level determines the time interval, as shown in the following table.

Table 19-7 CRL refresh interval

Security level	CRL refresh interval
Very high	Hourly
High	4 hours
Medium	8 hours

See [“About NetBackup certificate deployment security levels”](#) on page 308.

You can get a new CRL before its scheduled refresh period.

See [“Refreshing the CRL on the primary server”](#) on page 336.

See [“Refreshing the CRL on a NetBackup host”](#) on page 336.

For more information

See [“Overview of security certificates in NetBackup”](#) on page 273.

See [“About host ID-based certificates”](#) on page 304.

See [“About revoking host ID-based certificates”](#) on page 337.

Refreshing the CRL on the primary server

Use the following procedure to refresh the CRL on the primary server. The procedure gets the current CRL from the NetBackup certificate authority and copies it to the primary server. If a host in the environment was recently revoked, you must wait up to 5 minutes before the CRL reflects that the host was revoked.

See [“About the host ID-based certificate revocation list”](#) on page 334.

To refresh the CRL on the primary server

- 1 Log in to the primary server as an administrator.

For a clustered primary server, log in to the active node.

- 2 For a clustered primary server, run the following command:

```
nbcertcmd -getCRL -cluster [-server primary_server_name]
```

To get a CRL from a NetBackup domain other than the default, specify the `-server primary_server_name` option and argument.

- 3 Run the following command:

```
nbcertcmd -getCRL [-server primary_server_name]
```

Refreshing the CRL on a NetBackup host

Use the following procedure to refresh the CRL on a NetBackup host. The procedure gets the current CRL from the NetBackup certificate authority and copies it to the local host. If a host in the environment was recently revoked, you must wait up to 5 minutes before the CRL reflects that the host was revoked.

See [“About the host ID-based certificate revocation list”](#) on page 334.

To refresh the CRL on a NetBackup host

- 1 Log on as an administrator on the NetBackup host that requires a fresh CRL.

- 2 Run the following command:

```
nbcertcmd -getCRL [-server primary_server_name]
```

To get a CRL from a NetBackup domain other than the default, specify the `-server primary_server_name` option and argument.

About revoking host ID-based certificates

When you revoke a NetBackup digital security certificate, NetBackup revokes any other certificates for that host. NetBackup ceases to trust the host, and it no longer can communicate with other NetBackup hosts.

If you revoke a certificate, you must select one of the following reasons:

Affiliation Changed	The host changes affiliation to a different NetBackup domain.
CA Compromise	The certificate authority is compromised.
Cessation of Operation	The host ceases to be a NetBackup host. For example, you decommission a NetBackup media server or client.
Key Compromise	The certificate key is compromised.
Superseded	A new certificate supersedes the certificate to be revoked.
Unspecified	Other, unspecified reasons. Perhaps you want to suspend privileges temporarily while you investigate a security event.

If you revoke a certificate and later determine that you can trust the host, provision a new certificate on that host. You do so by using a reissue token.

See [“About reissuing host ID-based certificates”](#) on page 326.

Note: Do not revoke a certificate of the primary server. If you do, NetBackup operations may cease.

After you revoke a host’s certificate, you should consider doing the following actions in NetBackup:

- Remove the host from backup policies.
- For a NetBackup media server, deactivate it.

You should also consider any actions that are not related to NetBackup to ensure that someone with malicious intent cannot use the certificate and key.

See [“About the host ID-based certificate revocation list”](#) on page 334.

Removing trust between a host and a primary server

A NetBackup host can trust multiple Certificate Authorities (primary servers) at any time. For various reasons, it may be necessary for a NetBackup host to remove trust from a primary server that previously had been trusted.

For example, if a NetBackup client is moved from one primary server to another, it is advisable to remove trust from the first primary 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 primary 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 primary server

- 1 The administrator of the non-primary host runs the following command on the host to determine the CA certificate fingerprint of the primary server:

```
nbcertcmd -listCACertDetails
```

In this example output, the host has certificates from two primary 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 primary 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 BAR Console** on the primary 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 primary server web services.

See [“About revoking host ID-based certificates”](#) on page 337.

Security best practices suggest that the administrator explicitly revoke the certificates for any host that is no longer active, regardless of whether the certificate is still deployed on the host, or whether it has been successfully removed from the host.

Note: Do not revoke a certificate of the primary server. If you do, NetBackup operations may cease.

To revoke a host ID-based certificate using the NetBackup Administration web UI

- 1** On the left pane, select **Security > Certificates**.
- 2** On the NetBackup certificates tab, select the certificate to be revoked.
- 3** Select **Revoke Certificate**.
- 4** Select a reason from the drop-down list and click **Yes**.
- 5** After you revoke a host’s certificate, do the following actions in NetBackup:
 - Remove the host from backup policies.
 - For a NetBackup media server, deactivate it.

To revoke a host ID-based certificate using the command line

- 1** The primary 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 304.

- 2** Run one of the following commands to revoke the certificate using the host name or the host ID.

Revoke using the host name:

```
nbcertcmd -revokeCertificate -host host_name
```

Note: You must provide the primary name of the host for which you want to revoke the certificate. If you provide any of the host ID-to-host name mappings that are added for the host, the certificate cannot be revoked.

Revoke using the host ID:

```
nbcertcmd -revokeCertificate -hostID host_id
```

Additional parameters can be used to indicate a revocation reason code and the primary server.

- 3** After you revoke a host's certificate, do the following actions in NetBackup:
 - Remove the host from backup policies.
 - For a NetBackup media server, deactivate it.

Note: Revoking a certificate does not delete the certificate from the local store of the non-primary host.

Delete NetBackup CA-signed certificate

When you delete a NetBackup CA-signed certificate, NetBackup revokes all NetBackup certificates for that host and marks all of them as deleted.

Consider the following scenario: An external certificate authority (ECA)-only environment is configured in your domain. Because of the presence of NetBackup CA-signed certificates on hosts, primary server receives notifications like 'certificate expiry' for the hosts. In such scenario, you can choose to delete the NetBackup CA-signed certificates to stop receiving unwanted notifications.

Users with the following RBAC roles can delete a NetBackup CA-signed certificate:

- NetBackup Administrator
- Default Security Administrator

To delete NetBackup CA-signed certificates of a host using the NetBackup web UI

- 1** On the left, go to **Security > Certificates**. Select the **NetBackup certificates** tab.
- 2** Select the host that is associated with the certificate that you want to delete. Select **Delete Certificate**.
- 3** Enter the reason to delete the certificate.
- 4** Click **Yes**.

Delete NetBackup CA-signed certificates of the host using RESTful APIs

Use the following API to delete the NetBackup CA-signed certificate:

```
DELETE - /security/certificates/{serial_number} -
```

Use the following API to list the deleted NetBackup CA-signed certificates:

```
GET- /security/certificates/
```

Use the filter 'isCertDeleted'.

Delete NetBackup CA-signed certificates of a host using the command-line interface

To delete NetBackup CA-signed certificates of a host using the command-line interface

- ◆ Run the following command:

```
nbcertcmd -deleteNBCACertificate -hostId host_id | -host host_name
-deletionReason value [-server master_server_name]
```

Determining a NetBackup host's certificate state

If NetBackup CA-signed certificate is used

You can determine the state of a NetBackup certificate: Active or Revoked. Doing so may help troubleshoot connection and communication problems. Three methods exist to determine a certificate state, as follows:

Verify a host certificate from the host itself	The method uses the NetBackup <code>nbcertcmd</code> command. See “To verify the host's certificate state from the host” on page 343.
Verify a host certificate from a NetBackup server	The method uses the NetBackup <code>bptestbpcd</code> command. See “To verify from a NetBackup server if a different host's certificate is revoked” on page 343.
Verify a host certificate from the host itself	See “To verify a host's certificate” on page 344.

See [“About the host ID-based certificate revocation list”](#) on page 334.

To verify the host's certificate state from the host

- 1 Optionally, on the NetBackup host run the following command as an administrator to get the most recent certificate revocation list:

UNIX: `/usr/opensv/netbackup/bin/nbcertcmd -getCRL [-server primary_server_name]`

Windows: `install_path\NetBackup\bin\nbcertcmd -getCRL [-server primary_server_name]`

To get a CRL from a NetBackup domain other than the default, specify the `-server primary_server_name` option and argument.

- 2 On the NetBackup host, run the following command as an administrator:

UNIX: `/usr/opensv/netbackup/bin/nbcertcmd -hostSelfCheck [-cluster] [-server primary_server_name]`

Windows: `install_path\NetBackup\bin\nbcertcmd -hostSelfCheck [-cluster] [-server primary_server_name]`

Use one or both of the following options if necessary:

- `-cluster` Use this option on the active node of a NetBackup primary server cluster to verify the certificate of the virtual host.
- `-server` Use this option with the *primary_server_name* argument to verify a certificate from a primary server other than the default.

- 3 Examine the command output. The output indicates that either the certificate is or is not revoked.

To verify from a NetBackup server if a different host's certificate is revoked

- 1 As an administrator on the NetBackup primary server or a NetBackup media server, run the following command:

UNIX: `/usr/opensv/netbackup/bin/admincmd/bptestbpcd -host hostname -verbose`

Windows: `install_path\NetBackup\bin\admincmd\bptestbpcd -host hostname -verbose`

For `-host hostname`, specify the host for which you want to verify the certificate.

- 2 Examine the command output. If the certificate on the specified host is revoked, the command output includes the string `The Peer Certificate is revoked`. If the command output does not include that string, the certificate is valid.

To verify a host's certificate

- 1 Open the NetBackup web UI.
- 2 On the left, click **Security > Certificates**.
- 3 Click the certificate name to examine the status of the certificate.

If external CA-signed certificate is used

You can determine the state of an external CA-signed host certificate: Active or Revoked. Doing so may help troubleshoot connection and communication problems.

Two methods exist to determine a certificate state, as follows:

Verify a host certificate from the host itself See ["To verify a host certificate from the host itself"](#) on page 344.

Verify a host certificate from a NetBackup server See ["To verify from a NetBackup server if a different host's certificate is revoked"](#) on page 345.

To verify a host certificate from the host itself

- 1 Refresh the CRLs in the NetBackup CRL cache.
- 2 On the NetBackup host, run the following command as an administrator:
 UNIX: `/usr/opensv/netbackup/bin/nbcertcmd -hostSelfCheck [-cluster]`
 Windows: `install_path\NetBackup\bin\nbcertcmd -hostSelfCheck [-cluster]`
 Use the `-cluster` option on the active node of a clustered primary server to verify the certificate of the virtual name.
- 3 Examine the command output. The output indicates whether the certificate is revoked or not.

To verify from a NetBackup server if a different host's certificate is revoked

- 1 As an administrator on the NetBackup primary server or a NetBackup media server, run the following command:

UNIX: `/usr/opensv/netbackup/bin/admincmd/bptestbpcd -host hostname -verbose`

Windows: `install_path\NetBackup\bin\bptestbpcd -host hostname -verbose`

For `-host hostname`, specify the host for which you want to verify the certificate.

- 2 Examine the command output. If the certificate on the specified host is revoked, the command output includes the string 'The Peer Certificate is revoked'. If the command output does not include that string, the certificate is valid.

Getting a list of NetBackup hosts that have revoked certificates

Use the following procedure to obtain a list of NetBackup hosts that have a revoked certificate.

See [“About the host ID-based certificate revocation list”](#) on page 334.

To get a list of NetBackup hosts with revoked certificates

- 1 In a command window, log on to the **NetBackup Web Management Service** on the primary server, as follows (the logon account must have NetBackup administrator privileges):

UNIX: `/usr/opensv/netbackup/bin/bpnbat -login -loginType WEB`

Windows: `install_path\NetBackup\bin\bpnbat -login -loginType WEB`

- 2 Run the following command to extract from the CRL a list of certificates that are not expired and then filter the results for the word “Revoked”:

UNIX: `/usr/opensv/netbackup/bin/nbcertcmd -listAllDomainCertificates | grep Revoked`

Windows: `install_path\NetBackup\bin\nbcertcmd -listAllDomainCertificates | findstr Revoked`

Deleting host ID-based certificates

Use this topic to manually delete host ID-based certificate of a NetBackup host. You may need to delete certificates in certain scenarios, for example: A NetBackup host is moved from one NetBackup domain to another NetBackup domain. In this scenario, the current host ID-based certificate needs to be deleted and the host

must have a certificate issued by the new Certificate Authority (CA) that is the new primary server.

Caution: Manually deleting the host ID-based certificates may adversely impact NetBackup functionality.

Note: During NetBackup software removal, host ID-based certificates are automatically deleted.

To delete a host ID-based certificate from a NetBackup host

- 1 Run the following command on the NetBackup host to view the details of all associated host ID-based certificates.

UNIX: `/usr/opensv/netbackup/bin/nbcertcmd -listCertDetails`

Windows: `install_path\NetBackup\bin\nbcertcmd -listCertDetails`

- 2 To delete a certificate, run the following command on the host:

UNIX: `/usr/opensv/netbackup/bin/nbcertcmd -deleteCertificate -hostid host_ID`

Windows: `install_path\NetBackup\bin\nbcertcmd -deleteCertificate -hostid host_ID`

To delete a host ID-based certificate from an active node in a cluster setup

- 1 Run the following command on the active node to view the details of all associated host ID-based certificates.

UNIX: `/usr/opensv/netbackup/bin/nbcertcmd -listCertDetails -cluster`

Windows: `install_path\NetBackup\bin\nbcertcmd -listCertDetails -cluster`

- 2 To delete a certificate, run the following command on the active node of the cluster:

`nbcertcmd -deleteCertificate -hostid host_ID -cluster`

UNIX: `/usr/opensv/netbackup/bin/nbcertcmd -hostid host_ID -cluster]`

Windows: `install_path\NetBackup\bin\nbcertcmd -hostid host_ID -cluster`

Host ID-based certificate deployment in a clustered setup

This section provides information on deployment of host name-based and host ID-based certificates in a NetBackup clustered setup.

For more information about NetBackup clusters, see the *NetBackup Clustered Primary Server Administrator's Guide*.

About host ID-based certificate deployment on a NetBackup cluster

In a clustered NetBackup primary 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 primary server.

Note: Only primary servers can be clustered in NetBackup.

About host name-based certificate deployment on a NetBackup cluster

In a clustered NetBackup primary 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 302.

About deployment of a host ID-based certificate on a clustered NetBackup host

Review the following scenarios for certificate deployment on cluster nodes:

- In case of fresh NetBackup installation, certificate on an active node is deployed automatically. You must manually deploy certificates on all inactive nodes.
- In case of disaster recovery, certificates for active and inactive nodes are not recovered. After you install NetBackup in a disaster recovery mode after a disaster, you must manually deploy certificates on all nodes.
 See [“Generating a certificate on a clustered primary server after disaster recovery installation”](#) on page 353.

Note: In case of upgrade, active or inactive nodes may already have a certificate. You can verify whether a cluster node has a certificate or not.

See [“Viewing certificate details of a clustered NetBackup setup”](#) on page 352.

See [“Host ID-based certificate deployment on the active primary server node”](#) on page 348.

See [“Host ID-based certificate deployment on inactive primary server nodes”](#) on page 348.

Host ID-based certificate deployment on the active primary server node

During NetBackup installation, host ID-based certificates are deployed on the active primary 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 primary server nodes

Certificates on inactive nodes are not deployed during installation. You must manually deploy certificates on all inactive nodes after the installation.

See [“Deploying host ID-based certificates on cluster nodes”](#) on page 348.

Deploying host ID-based certificates on cluster nodes

You must manually deploy certificates on all inactive nodes.

In certain scenarios, you need to manually deploy host ID-based certificates also on active nodes.

To manually deploy a host ID-based certificate on a primary server cluster node

- ◆ Run the following commands on the primary server cluster node:

- `nbcertcmd -getCACertificate`
- `nbcertcmd -getCertificate [-file authorization_token_file]`

See [“About Token Management for host ID-based certificates”](#) on page 330.

Revoking a host ID-based certificate for a clustered NetBackup setup

NetBackup administrators may consider revoking a host ID-based certificate under various conditions. For example, if the administrator detects that client security has been compromised, if a client is decommissioned, or if NetBackup is uninstalled from the host. A host with a revoked certificate cannot communicate with other hosts. Every NetBackup host must have a valid security certificate and a valid Certificate Revocation List (CRL) for successful communication.

See [“About the host ID-based certificate revocation list”](#) on page 334.

The NetBackup administrator can revoke certificates for a cluster node or the virtual name from any host in a NetBackup domain.

Ensure that you revoke the appropriate certificate.

After the certificate is revoked, you may need to deploy a new host ID-based certificate. Create a reissue token on the clustered node and deploy a new certificate using the reissue token.

See [“Creating a reissue token for a clustered NetBackup setup”](#) on page 350.

See [“Deploying a host ID-based certificate on a clustered NetBackup setup using reissue token”](#) on page 350.

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 304.

- 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 339.

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 339.

Deploying a host ID-based certificate on a clustered NetBackup setup using reissue token

After a host ID-based certificate is revoked, you can deploy new certificates on a clustered NetBackup setup using reissue tokens.

See [“Creating a reissue token for a clustered NetBackup setup”](#) on page 350.

To deploy a new host ID-based certificate on a cluster node

- ◆ Run the following command to deploy a new certificate on the cluster node using the reissue token:

```
nbcertcmd -getCertificate -file reissue_token_file -force
```

To deploy a new host ID-based certificate for the virtual name

- ◆ Run the following command to deploy a new certificate for the virtual name using the reissue token:

```
nbcertcmd -getCertificate -file reissue_token_file_virtual -force  
-cluster
```

Creating a reissue token for a clustered NetBackup setup

You need to reissue a certificate to a host in certain scenarios, for example a certificate is revoked for a host and you need to reissue a new certificate to the host.

See [“Deploying a host ID-based certificate on a clustered NetBackup setup using reissue token”](#) on page 350.

You need a reissue token to reissue a new certificate to a host.

See [“About Token Management for host ID-based certificates”](#) on page 330.

To create a reissue token for a cluster node

- 1 Log in to the NetBackup Web Management Service with the following command:

```
bpnbat -login -logintype WEB
```

See [“Web login requirements for nbcertcmd command options”](#) on page 304.

- 2 Run the following command to create a reissue token for the required cluster node:

```
nbcertcmd -createToken -name token_name -reissue -host host_name
```

See [“Creating a reissue token”](#) on page 327.

To create a reissue token for the virtual name

- 1 Log in to the NetBackup Web Management Service with the following command:

```
bpnbat -login -logintype WEB
```

See [“Web login requirements for nbcertcmd command options”](#) on page 304.

- 2 Run the following command to create a reissue token for the virtual name.

```
nbcertcmd -createToken -name token_name_virtual -reissue -host  
virtual_name
```

See [“Creating a reissue token”](#) on page 327.

Renewing a host ID-based certificate on a clustered NetBackup setup

Host ID-based certificates for the cluster nodes and the virtual name are automatically renewed. The certificates are automatically renewed 180 days before the expiration date.

You can also renew the certificates manually, if required.

See [“About host ID-based certificate expiration and renewal”](#) on page 323.

To manually renew certificate for a cluster node

- ◆ Run the following command from a cluster node to renew the certificate for the node:

```
nbcertcmd -renewCertificate
```

To manually renew certificate for the virtual name

- ◆ Run the following command on the active node to manually renew the certificate for the virtual name:

```
nbcertcmd -renewCertificate -cluster
```

Viewing certificate details of a clustered NetBackup setup

Run the following commands to view the certificate details of a cluster node or the virtual name.

To view certificate details of a cluster node

- ◆ Run the following command on a cluster node:

```
nbcertcmd -listCertDetails
```

See [“Viewing host ID-based certificate details”](#) on page 307.

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 307.

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 primary server node can adversely impact the NetBackup functionality.

To remove the CA certificates from a cluster node

- 1 Run the following command on a cluster node to view the fingerprints of the CA certificates:

```
nbcertcmd -listCACertDetails
```

- 2 Run the following command to remove the CA certificate by providing the appropriate fingerprint:

```
nbcertcmd -removeCACertificate -fingerprint fingerprint
```

To remove the CA certificates for the virtual name

- 1 Run the following command on the active node to view the fingerprints of the CA certificates for the virtual name:

```
nbcertcmd -listCACertDetails -cluster
```

- 2 Run the following command on the active node to remove the CA certificate for the virtual name by providing the appropriate fingerprint:

```
nbcertcmd -removeCACertificate -fingerprint fingerprint_virtual -cluster
```

Generating a certificate on a clustered primary server after disaster recovery installation

After you complete the disaster recovery of a clustered primary server, you must generate a certificate on the active node as well as all inactive nodes. Additionally, failover to the secondary node is expected behavior in a cluster environment. This procedure is required for successful backups and restores of the cluster.

For additional information on deploying certificates on primary server nodes see the [NetBackup Security and Encryption Guide](#).

Generating the local certificate on each cluster node after disaster recovery installation

- 1 Add all inactive nodes to the cluster.

If all the nodes of the cluster are not currently part of the cluster, start by adding them to the cluster. Consult with your operating system cluster instructions for assistance with this process.

More information about supported cluster technologies is available. See the [NetBackup Clustered Primary Server Administrator's Guide](#).

- 2 Run the `nbcertcmd` command to store the Certificate Authority certificate.

UNIX: `/usr/openv/netbackup/bin/nbcertcmd -getCACertificate`

Windows: `install_path\NetBackup\bin\nbcertcmd -getCACertificate`

- 3 Use the `bpnbat` command as shown to authorize the necessary changes. When you are prompted for the authentication broker, enter the virtual server name, not the local node name.

```
bpnbat -login -loginType WEB
```

- 4 Use the `nbcertcmd` command to create a reissue token. The *hostname* is the local node name. When the command runs, it displays the token string value. A unique reissue token is needed for each cluster node.

```
nbcertcmd -createtoken -name token_name -reissue -host hostname
```

- 5 Use the reissue token with the `nbcertcmd` command to store the host certificate. This command prompts you for the token string value. Enter the token string from the `nbcertcmd -createToken` command.

```
nbcertcmd -getCertificate -token
```

About the communication between a NetBackup client located in a demilitarized zone and a primary server through an HTTP tunnel

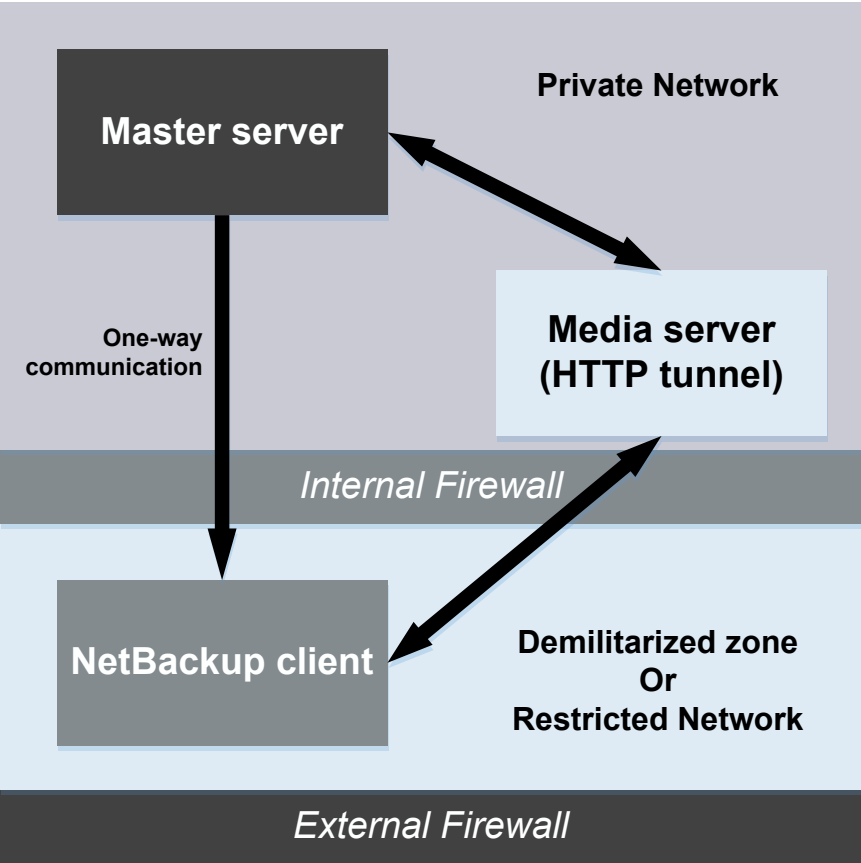
In a NetBackup deployment setup, the client computers can be in a demilitarized zone (DMZ) where the communication takes place only through specific web ports.

All NetBackup clients must be able to communicate with the web management service on the primary server to deploy security certificates and authorize peers for secure connections. For example, the NetBackup client sends requests to the primary server for deploying certificates, which is essential for secure NetBackup communication. In a DMZ setup, the client might not be able to send web service requests directly to the primary server. In this scenario, a NetBackup client sends a connection request and a web service request to the HTTP tunnel on the media server by the HTTP CONNECT proxy method. The HTTP tunnel accepts the connection request and forwards the web service request to the primary server.

The HTTP tunneling feature allows the NetBackup clients in a DMZ to send web service requests to the primary server. The NetBackup media server forms an HTTP tunnel that forwards the web service request from the NetBackup client to the primary server. The further web service communication uses Secure Socket Layer (SSL).

Note: The port number 1556 on the media server must be accessible by the NetBackup client for sending web service requests.

Figure 19-2 NetBackup client and primary server communication in a DMZ setup



In a single domain or multi-domain environment, when the NetBackup client in a DMZ tries to send a web service connection request to the primary server, it follows a particular sequence::

Table 19-8 Sequence to send a connection request

Sequence	Description
1. The NetBackup client tries to send the connection request directly to the primary server.	In a DMZ, the web service connection request might not succeed.

Table 19-8 Sequence to send a connection request (continued)

Sequence	Description
2. If the direct connection fails, then the client checks if a media server is specified to use HTTP tunneling to send the web service connection request to the primary server.	
3. If a media server is not specified, then the client refers to a list of media servers that is available in the NetBackup configuration and uses them for sending web service connection requests.	NetBackup client maintains an internal cache file (<code>websvctunnels.cache</code>) that contains a list of media servers that are automatically updated based on previous successful connections. The cache file is available in the same location as the <code>bp.conf</code> file for both Windows and UNIX.

Additional information

- The following additional options are available for configuring the HTTP Tunnel feature:
 - WEB_SERVER_TUNNEL_USE** - You can use this option on the NetBackup clients to configure the default communication behavior using the HTTP Tunnel.
 - WEB_SERVER_TUNNEL_ENABLE** - By default, HTTP Tunnel is enabled on the media server. You can use this option on the media servers to disable the HTTP Tunnel feature.
For more information, refer to the *NetBackup Administrator's Guide Volume I*.
- If your NetBackup client configuration does not contain information about the media servers in the domain, run the `nbsetconfig` command on the primary server. The registry on a Windows client or the `bp.conf` file on a UNIX client includes the primary and the media servers that the client selects to send connection and web service requests.
- If you use the `nbcertcmd -getCertificate` command on the NetBackup client in a DMZ, and if you see one of the following errors:
 - EXIT STATUS 5955:** The host name is not known to the primary server.
 - EXIT STATUS 5954:** The host name could not be resolved to the requesting host's IP address.
Use a token to deploy the security certificate because the primary server cannot match the IP address of the HTTP tunnel to the identity of the host that requests the certificate.

- NetBackup audit report lists the media server as the user if an HTTP tunnel is used to send a certificate request to the primary server.

Adding a NetBackup host manually

It is not recommended to manually add a host in the host database except for specific scenarios. For example, you may need to manually add a host when you recover a Bare Metal Restore (BMR) client to other NetBackup domain using Auto Image Replication (AIR).

For more information about Bare Metal Restore, refer to the *NetBackup Bare Metal Restore Administrator's Guide*.

Note: Before adding a host, you must ensure that the host entry that you want to add does not already exist in the host database.

You can add a host using the command-line interface only.

To add a host in the host database using the command-line interface

- 1 Run the following command to authenticate your web services login on the primary server:

```
bpnbat -login -loginType WEB
```

- 2 Run the following command to add a host:

```
nbhostmgmt -addhost -host host name -server primary server
```

Migrating NetBackup CA

In certain scenarios, you may need to migrate your existing NetBackup certificate authority (CA) hierarchy to a new one. NetBackup supports migrating the existing NetBackup CA. This chapter provides information on the NetBackup CA migration process.

NetBackup security certificates that are used to authenticate NetBackup hosts conform to the X.509 Public Key Infrastructure (PKI) standard. A NetBackup primary server acts as the certificate authority (CA) and issues digital certificates to hosts. NetBackup uses the NetBackup authentication daemon (NBATD) as its PKI provider. NBATD and its client implementation generate the RSA private key that is used for authentication.

NetBackup now supports certificate authorities with the following key strengths: 2048 bits, 3072 bits, 4096 bits, 8192 bits, and 16384 bits.

Note: After NetBackup primary server installation or upgrade, by default a new root CA with 2048-bits key strength is deployed. With upgrade, you need to migrate the existing CA to a new CA.

Table 19-9 NetBackup CA migration procedures for various use cases

Use case	Description
When you need a NetBackup CA with a key strength other than the default one (2048 bits)	See “Setting the required key strength before installation or upgrade using the NB_KEYSIZ e” on page 359. See “Manually migrating NetBackup CA after installation or upgrade” on page 361.
When you want to migrate the existing NetBackup CA after the entire NetBackup domain is upgraded to 8.3	See “Migrating NetBackup CA when the entire NetBackup domain is upgraded” on page 359.

The NetBackup CA migration process comprises the following phases:

1. Initiating NetBackup CA migration

Note: Run the following command:

```
vssat setuptrust --broker nb_master_server_name:1556:nbatd
--securitylevel high
```

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

The `vssat` command resides at the following location:

Windows	<code>INSTALL_PATH\NetBackup\sec\at\bin\vssat</code>
UNIX	<code>/usr/opensv/netbackup/sec/at/bin</code>

2. Activating the new NetBackup CA
3. Completing NetBackup CA migration
4. Decommissioning the old NetBackup CA

Note: Decommissioning the old NetBackup CA is an optional clean-up task.

See the video *NetBackup CA migration* for details.

Setting the required key strength before installation or upgrade using the NB_KEYSIZE environment variable

After NetBackup installation or upgrade, by default a new root CA with 2048-bits key strength is deployed. If you want a larger key strength, you can set an environment variable to a value larger than 2048 bits before installation or upgrade.

To have a NetBackup CA with a key strength larger than 2048 bits

- 1 Set the `NB_KEYSIZE` environment variable on the primary server before you start NetBackup installation or upgrade.

For example: `NB_KEYSIZE = 4096`

The `NB_KEYSIZE` environment variable can have the following values: 2048, 3072, 4096, 8192, or 16384.

Note: If the FIPS mode is enabled on the primary server, you can specify only 2048 and 3072 bits as a value for the `NB_KEYSIZE` environment variable.

Caution: You should carefully choose the key size for your environment. Choosing a large key size may reduce performance. A key size of 2048 offers security for most use cases.

- 2 Install or upgrade NetBackup on hosts.

In case of upgrade, continue with the CA migration.

See [“Migrating NetBackup CA when the entire NetBackup domain is upgraded”](#) on page 359.

Migrating NetBackup CA when the entire NetBackup domain is upgraded

With NetBackup 8.3 upgrade, by default a new root CA with 2048 bits key strength is deployed and the CA migration process is automatically initiated. You can also set the `NB_KEYSIZE` environment variable to a value larger than 2048 bits before installation or upgrade.

See [“Setting the required key strength before installation or upgrade using the NB_KEYSIZE environment variable”](#) on page 359.

Note: If you have media servers earlier than NetBackup 8.2 that are configured as cloud storage servers, the CA migration process is not initiated. Ensure that all NetBackup hosts are upgraded to 8.3 or later for successful host communication.

When all hosts in your NetBackup domain are upgraded to NetBackup 8.3 or later, use the following procedure to complete the CA migration process:

To migrate NetBackup CA when all hosts are upgraded to NetBackup 8.3

- 1 Run the following command to ensure that all hosts have the new CA certificates in their trust stores.

```
nbseccmd -nbcaMigrate -hostsPendingTrustPropagation
```

- 2 Ensure that the command returns zero (0) hosts as the output.

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

- 3 **Warning:** If one or more NetBackup hosts are at 8.2 or earlier versions, backups of such hosts fail after activation. Therefore, you must ensure that all NetBackup hosts in the domain are upgraded to 8.3 before activating the new CA.
-

Run the following command to activate the new CA that can start issuing NetBackup certificates going forward:

```
nbseccmd -nbcaMigrate -activateNewCA
```

- 4 Run the following command to ensure that all hosts have certificates that the new CA has renewed:

```
nbseccmd -nbcaMigrate -hostsPendingRenewal
```

Ensure that the command returns zero (0) hosts as the output.

- 5 Restart the NetBackup Messaging Broker (`nbmqbroker`) service on this host.
- 6 Run the following command to complete the CA migration process:

```
nbseccmd -nbcaMigrate -completeMigration
```

- 7 After completing the NetBackup CA migration process and ensuring that the hosts use certificates that the new CA has issued, you can safely decommission the old NetBackup CA.

This clean-up task is optional.

See “[Decommissioning the inactive NetBackup CA](#)” on page 363.

Manually migrating NetBackup CA after installation or upgrade

With fresh NetBackup installation or upgrade, by default a new root CA with 2048-bits key strength is deployed. However, if you want to use a CA with a different key size or move to a new CA after installation or upgrade, you should manually initiate the CA migration process.

See [“Setting the required key strength before installation or upgrade using the NB_KEYSIZESIZE environment variable”](#) on page 359.

To migrate NetBackup CA after installation or upgrade

- 1 Run the following command to initiate the CA migration process:

```
nbseccmd -nbcaMigrate -initiateMigration -keysize key_value
```

A new NetBackup CA is deployed with this command.

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

- 2 Run the following command to reissue certificates to the host.

```
nbcertcmd -reissueCertificates
```

- 3 Stop the NetBackup Web Management Console (`nbwmc`) service before reissuing the certificate to the NetBackup web server.

- 4 Run the following command to reissue the certificate to the NetBackup web server:

```
configureCerts -renew_webserver_keys
```

- 5 Start the `nbwmc` service.

- 6 Run the following command to ensure that all hosts have the new CA certificates in their trust stores.

```
nbseccmd -nbcaMigrate -hostsPendingTrustPropagation
```

- 7 Ensure that the command returns zero (0) hosts as the output.

- 8 **Warning:** If one or more NetBackup hosts are at 8.2 or earlier versions, backups of such hosts fail after activation. Therefore, you must ensure that all NetBackup hosts in the domain are upgraded to 8.3 before activating the new CA.

Run the following command to activate the new CA that can start issuing NetBackup certificates going forward:

```
nbseccmd -nbcaMigrate -activateNewCA
```

- 9 Run the following command to renew host certificates using the new CA.

```
nbcertcmd -renewCertificate
```

- 10 Run the following command to ensure that all hosts have certificates that the new CA has renewed:

```
nbseccmd -nbcaMigrate -hostsPendingRenewal
```

Ensure that the command returns zero (0) hosts as the output.

- 11 Restart the NetBackup Messaging Broker (`nbmqbroker`) service on this host.
- 12 Run the following command to complete the CA migration process:

```
nbseccmd -nbcaMigrate -completeMigration
```

- 13 After completing the NetBackup CA migration process and ensuring that the hosts use certificates that the new CA has issued, you can safely decommission the old NetBackup CA.

This clean-up task is optional.

See [“Decommissioning the inactive NetBackup CA”](#) on page 363.

Establishing communication with clients that do not have new CA certificates after CA migration

In certain scenarios, for example network issue, NetBackup clients may be unreachable during NetBackup CA migration. Such clients may not have new CA certificates and communication with such clients may fail.

To successfully communicate with NetBackup clients that were unreachable during CA migration

- 1 Run the following command on the client to get certificate:

```
nbcertcmd -getcacertificate -server master_server_name
```

- 2 Run the following command on the client to renew certificates:

```
nbcertcmd -renewcertificate -server master_server_name
```

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

Viewing a list of NetBackup CAs in the domain

You can view a list of NetBackup CAs that are available in your NetBackup domain.

To view list of NetBackup CAs in the domain

- ◆ Run the following command:

```
nbseccmd -nbcaList
```

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

If you want to view CAs with a specific state - for example, ABANDONED, ACTIVE, or DECOMMISSIONED - run the following command:

```
nbseccmd -nbcaList -state CA_state]
```

Viewing the CA migration summary

You can view the NetBackup CA migration summary at different stages. Information in the CA migration summary includes the current CA migration status and the fingerprint of the current certificate-issuing NetBackup CA.

To view the CA migration summary

- ◆ Run the following command:

```
nbseccmd -nbcaMigrate -summary
```

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

Decommissioning the inactive NetBackup CA

After completing the NetBackup CA migration process and ensuring that the hosts use certificates that the new CA has issued, you can safely decommission the old NetBackup CA.

To decommission the old NetBackup CA

- 1 Run the following command:

```
nbseccmd -nbcaMigrate -decommissionCA -fingerprint  
certificate_fingerprint
```

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

- 2 This step is mandatory if your NetBackup domain is enabled for NetBackup Access Control (NBAC):

Restart the NetBackup services on the primary server.

Configuring data-in-transit encryption (DTE)

This chapter includes the following topics:

- [About the data channel](#)
- [Data-in-transit encryption support](#)
- [Workflow to configure data-in-transit encryption](#)
- [Configure the global data-in-transit encryption setting](#)
- [Configure the DTE mode on a client](#)
- [View the DTE mode of a NetBackup job](#)
- [View the DTE-specific attributes of a NetBackup image and an image copy](#)
- [Configure the DTE mode on the media server](#)
- [Modify the DTE mode on a backup image](#)
- [Media device selection \(MDS\) and resource allocation](#)
- [How DTE configuration settings work in various NetBackup operations](#)

About the data channel

Data communication consists of the data that is backed up using NetBackup. The security policies require the Backup Administrators to ensure that the channel on which NetBackup clients send metadata and data to NetBackup servers be secure. In NetBackup 10.0 and later, the data and metadata are encrypted over the wire. This feature is referred to as data channel encryption or data in-transit encryption (DTE).

The following channels are classified as data channels:

- Tar stream - client to media server: Over this channel, the tar / data stream flows between the client and the media server. During a backup operation, the media server receives the data from the client and sends it to storage (for example, an OST plug-in). The direction is reversed during a restore.
- Tar stream - media server to media server: This channel is used during duplication.
- Catalog information - client to media server: Over this channel, the catalog information and control commands are transferred between the client and the media server. The amount of data that is transmitted over this channel is proportional to the number of files and directories that are part of the backup. The media server sends the catalog information that the client has sent to the primary server.
- Catalog information - media server to primary server: Over this channel, the catalog information is transferred from the media server to the primary server.

Note: In case of fresh NetBackup 10.3 installation, the data in-transit encryption is set to Preferred On by default. In case of upgrade, the previous setting is retained.

You can configure data in-transit encryption at various levels: global level (primary server-level) and client level.

Data-in-transit encryption support

Data-in-transit encryption is supported for the following NetBackup data and metadata operations:

- Data flow from a client to a media server
- Data flow from a media server to a client
- Metadata transfer from a media server to the primary server
- Data flow from one media server to another during duplication and synthetic backup

Data-in-transit encryption is not supported for the following NetBackup operations or communications:

- Communication between an OST plug-in and the underlying storage provider is not supported. It includes the following:
 - Communication between NetBackup and cloud storage

- Communication between NetBackup and the third-party OST providers such as DataDomain, NetApp, and so on
- Data-in-transit encryption is not supported for the following MSDP workflows:
 - Optimized Duplication
 - AIR replication

For these two operations, you need to explicitly configure the following option on both storage servers:

`OPTDUP_ENCRYPTION=1`

The DTE configuration in NetBackup does not control the data channel between two storage servers.

- Communication between NetBackup and workload applications such as VMware, Hyper-V, Microsoft Exchange, SharePoint, and Nutanix are not supported. Once the data is transferred from a workload application to NetBackup, it is then securely transferred over the TLS channel within the NetBackup boundary.
- NDMP communication
- SAN client communication
- Communication with the NBFSD process
 The process uses the standard NFS or CIFS protocol.

Workflow to configure data-in-transit encryption

This topic provides the steps to carry out data-in-transit encryption (DTE) in your NetBackup environment. The DTE configuration comprises the following two primary options:

- Global DTE mode
- Client DTE mode

Table 20-1 Workflow of DTE configuration

Step number	Step	Reference topic
Step 1	Review the configuration settings of the global DTE mode option and configure the option as per your DTE requirements	See “Configure the global data-in-transit encryption setting” on page 367.

Table 20-1 Workflow of DTE configuration (*continued*)

Step number	Step	Reference topic
Step 2	Review the configuration settings of the client DTE mode option and configure the option as per your DTE requirements	See “Configure the DTE mode on a client” on page 369.
Step 3	Review how the decision about data encryption is made based on the NetBackup operation that you want to perform and the DTE configuration settings.	See “How DTE configuration settings work in various NetBackup operations” on page 377. Note: If you plan to modify any existing DTE configuration settings, you must review this topic to understand the impact on the NetBackup operations.

Apart from the primary DTE configuration settings, the following settings are used in certain scenarios:

- Media server DTE mode
See [“Configure the DTE mode on the media server”](#) on page 372.
- Backup image DTE mode
See [“Modify the DTE mode on a backup image”](#) on page 373.
See [“DTE_IGNORE_IMAGE_MODE for NetBackup servers”](#) on page 374.

Configure the global data-in-transit encryption setting

To configure the data-in-transit encryption (DTE) in your NetBackup environment, you need to first set the global DTE configuration setting (or global DTE mode) and then the client DTE mode.

Data-in-transit encryption decision for various NetBackup operations is carried out based on the global DTE mode, the client DTE mode, and the image DTE mode.

The supported values for the global DTE mode are as follows:

- `Preferred Off`: Specifies that the data-in-transit encryption is disabled in the NetBackup domain. This setting can be overridden by the NetBackup client setting.
- `Preferred On`: Specifies that the data-in-transit encryption is enabled only for NetBackup 9.1 and later clients.

In case of fresh NetBackup installation, the global DTE mode is set to `Preferred On` by default.

In case of NetBackup upgrade, the previous setting is retained.

This setting can be overridden by the NetBackup client setting.

- **Enforced:** Specifies that the data-in-transit encryption is enforced if the NetBackup client setting is either 'Automatic' or 'On'. With this option selected, jobs fail for the NetBackup clients that have the data-in-transit encryption set to 'Off' and for the hosts earlier than 9.1.

Note: By default, the DTE mode for 9.1 clients is set to `Off` and for 10.0 and later clients, it is set to `Automatic`.

See [“DTE_CLIENT_MODE for clients”](#) on page 369.

RESTful API to be used for the global DTE configuration:

- GET - `/security/properties`
- POST - `/security/properties`

To set or view the global DTE mode using the NetBackup web UI

- 1 Sign in to the NetBackup web UI.
- 2 At the top right, select **Security > Global security**.
- 3 On the **Secure communication** tab, select one of the following global DTE settings:
 - Preferred Off
 - Preferred On
 - Enforced

To set and view the global DTE mode using the command-line interface

- 1 Run the following command to set the global DTE mode:

```
nbseccmd -setsecurityconfig -dteglobalmode 0|1|2
```

Where the value `0` represents `Preferred Off`, `1` represents `Preferred On`, and `2` represents `Enforced`.

- 2 Run the following command to view the value that is set for the global DTE mode:

```
nbseccmd -getsecurityconfig -dteglobalmode
```

Configure the DTE mode on a client

The `DTE_CLIENT_MODE` configuration option specifies the data-in-transit encryption (DTE) mode that is set on the NetBackup client.

See [“DTE_CLIENT_MODE for clients”](#) on page 369.

You can update and view the client DTE mode using the following commands:

`bpsetconfig/nbsetconfig` and `bpgetconfig/nbgetconfig`

DTE_CLIENT_MODE for clients

The `DTE_CLIENT_MODE` option specifies the data-in-transit encryption (DTE) mode that is set on the NetBackup client.

Table 20-2 `DTE_CLIENT_MODE` information

Usage	Description
Where to use	On NetBackup clients.
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: <pre>DTE_CLIENT_MODE = AUTOMATIC ON OFF</pre> By default, the DTE mode for 9.1 clients is set to <code>OFF</code> and for 10.0 and later clients, it is set to <code>AUTOMATIC</code>. ■ If the <code>DTE_CLIENT_MODE</code> option is set to <code>AUTOMATIC</code>, the client follows the DTE mode that is set at the global level: <code>Enforced</code>, <code>Preferred On</code>, or <code>Preferred Off</code>. ■ If the option is set to <code>ON</code>, data-in-transit encryption is enabled for the client. ■ If the option is set to <code>OFF</code>, data-in-transit encryption is disabled for the client. This setting can be used to exclude a client for encryption if the global DTE mode is set to <code>Preferred On</code>. Note: If the global DTE mode is set to <code>Enforced</code>, jobs fail for the NetBackup clients that have the <code>DTE_CLIENT_MODE</code> option set to <code>‘OFF’</code> and also for the hosts earlier than 9.1.

Table 20-2 DTE_CLIENT_MODE information (*continued*)

Usage	Description
Equivalent NetBackup web UI property	No equivalent exists. Global settings are configured in Settings > Global security > Secure communication > Data-in-transit encryption .

View the DTE mode of a NetBackup job

Primarily, the global DTE mode and the client DTE mode decide whether the data-in-transit encryption takes place or not for a NetBackup operation. If the data is encrypted when a NetBackup job runs, the 'DTE mode' attribute of the job is set to `On`.

If the data is not encrypted when a NetBackup job runs, the 'DTE mode' attribute of the job is set to `Off`.

RESTful API to view the DTE mode of a job:

- GET - `/admin/jobs`
- GET - `/admin/jobs/{jobId}`

To view the DTE mode of a job using the NetBackup web UI

- 1 Sign in to the NetBackup web UI.
- 2 On the left, select **Activity Monitor > Jobs**.

You can see the `Data-in-transit encryption` column that determines the DTE mode of the job.

To view the DTE mode of a job using the command-line interface

- ◆ Run the following command:

```
bpdbjobs -dtemode Off|On
```

The command lists the jobs according to the DTE mode that is set.

View the DTE-specific attributes of a NetBackup image and an image copy

Primarily, the global DTE mode and the client DTE mode decide whether the data-in-transit encryption takes place or not for a backup operation. If the data is

encrypted during a backup operation, the DTE mode attribute of the associated NetBackup image is set to `On`.

Based on the global DTE mode and the client DTE mode, if the data cannot be encrypted during a backup operation, the DTE mode attribute of the image is set to `Off`.

See [“Modify the DTE mode on a backup image”](#) on page 373.

An image copy has two DTE-specific attributes:

Copy DTE mode	Specifies whether the data is transferred over a secure channel when the current image copy is created.
Copy Hierarchical DTE mode	Specifies whether the data is transferred over a secure channel when the current image copy and all its parent copies in the hierarchy are created. If the data is transferred over an insecure channel when one of the parent copies in the hierarchy is created, the current copy's hierarchical DTE mode is set to <code>Off</code>. If the copy hierarchical DTE mode is <code>Off</code>, the copy is said to be insecure. It indicates that any parent copy in the hierarchy can be compromised and copying from a compromised copy is not secure even if the current copy is generated securely.

Note: The image DTE mode is always shown as `Off` if the media server that is involved in the data transfer is earlier than 9.1. Copy DTE and Copy Hierarchical DTE modes are always shown as `Off` if the media server that is involved in the data transfer is earlier than 10.0.

RESTful API to be used to view the image attributes:

- GET - `/catalog/images`
- GET - `/catalog/images/{backupId}`

To view the DTE attributes of an image and an image copy using the NetBackup web UI

- 1 Sign in to the NetBackup web UI.
- 2 On the left, select **Catalog**.

When you search for backup images, the image list displays at the bottom of the screen. The DTE-specific attributes of the image and the image copy - Image DTE mode, Copy DTE mode, and Copy Hierarchical DTE mode - are also displayed.

To view the DTE attributes of an image and an image copy using the command-line interface

- ◆ Use the following commands: `bpimagelist`, `bpclimagelist` and `bpimmedia`.
For more details on the commands, see the NetBackup Commands Reference Guide.

To view the DTE attributes of an image using the NetBackup BAR Console

- ◆ In the **NetBackup BAR Console**, see the following reports to verify the DTE mode (Data-in-transit encryption column) of the image:
 - **NetBackup Management > Reports > Images on Media**
 - **NetBackup Management > Reports > Tape Reports > Images on Tape**
 - **NetBackup Management > Reports > Disk Reports > Images on Disk**

Configure the DTE mode on the media server

The media server setting can be used only to turn off data-in-transit encryption (DTE) for NetBackup operations.

In a NetBackup configuration where a media server is slow because of the old hardware, you can turn off the media server DTE mode so that there is no performance issue. However, it is recommended that you upgrade the old media server hardware. This setting is available for media servers with NetBackup 10.0 and later.

RESTful API to be used for the global DTE configuration:

- GET - `/config/media-servers/{hostName}`
- PATCH - `/config/media-servers/{hostName}`

To set or view the media server DTE mode

- 1 Ensure that you have an RBAC role with the following permissions on the media server resource:

- View
- Update
- Manage access

See “[Default RBAC roles](#)” on page 135.

- 2 Run the following command to set the media server DTE mode:

```
nbseccmd -setsecurityconfig -dtemediamode off|on -mediaserver  
media_server_name
```

- 3 Run the following command to view the media server DTE mode:

```
nbseccmd -getsecurityconfig -dtemediamode -mediaserver  
media_server_name
```

Note: For 9.1 media servers, you can only view the DTE mode as `On`, but you cannot set it.

Modify the DTE mode on a backup image

The data-in-transit (DTE) feature of NetBackup introduces an additional image attribute (DTE mode) when a backup image is created.

Primarily, the global DTE mode and the client DTE mode decide whether the data-in-transit encryption takes place or not for a NetBackup operation. If the data is encrypted during backup, the DTE mode attribute of the associated NetBackup image is set to `On`.

If based on the global DTE mode and the client DTE mode, the data cannot be encrypted during backup, the DTE mode attribute of the image is set to `Off`.

The image DTE mode should be honored and retained for all subsequent operations on that image. For example, restore and secondary operations like duplication, replication, import and so on. If the image DTE mode is set to `On`, subsequent operations always encrypt the data for DTE supported hosts.

If the host does not support DTE, then the job fails. If the image DTE mode is set to `Off`, the DTE for subsequent operations is decided based on the global and client DTE modes at that point of time. This is the default behavior.

In certain cases, you may want to modify the image DTE mode that was set at the time of its creation.

RESTful API to be used to modify the image DTE mode:

- PATCH - /catalog/images/{backupId}

To modify the image DTE mode

- ◆ Run the following command:

```
bpimage -update -image_dtemode Off|On
```

You can also change the image DTE mode using the **NetBackup Web UI > Catalog** node.

See [“DTE_IGNORE_IMAGE_MODE for NetBackup servers”](#) on page 374.

See [“View the DTE-specific attributes of a NetBackup image and an image copy”](#) on page 370.

DTE_IGNORE_IMAGE_MODE for NetBackup servers

Use the `DTE_IGNORE_IMAGE_MODE` option if you do not want the data to be encrypted even if the data-in-transit encryption (DTE) mode of the backup image is enabled.

The `DTE_IGNORE_IMAGE_MODE` option is applicable for all backup images.

Table 20-3 DTE_IGNORE_IMAGE_MODE information

Usage	Description
Where to use	On NetBackup servers.

Table 20-3 DTE_IGNORE_IMAGE_MODE information (*continued*)

Usage	Description
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: <pre>DTE_IGNORE_IMAGE_MODE = NEVER ALWAYS WHERE_UNSUPPORTED</pre> The default value of the <code>DTE_IGNORE_IMAGE_MODE</code> option is <code>NEVER</code>. ■ <code>NEVER</code> - Use this option to specify that the data-in-transit encryption takes place based on the DTE mode of the image. ■ <code>ALWAYS</code> - Use this option to specify that the DTE mode of the image is always ignored during data-in-transit encryption irrespective of whether the NetBackup host supports the encryption or not. Data-in-transit encryption takes place based on the global DTE mode and client DTE mode. ■ <code>WHERE_UNSUPPORTED</code> - Use this option if you have NetBackup hosts earlier than 9.1 in your environment and you do not want the jobs to fail for these hosts when the DTE mode is enabled for the image. With this configuration, data-in-transit encryption happens based on the global and client DTE mode settings. The image DTE mode is ignored.
Equivalent NetBackup web UI property	No equivalent exists.

Media device selection (MDS) and resource allocation

Based on the global DTE mode, client DTE mode, media server DTE mode, and image DTE mode, the resources are allocated.

For dynamic storage units, like MSDP or Storage Unit Group, a media server with the DTE mode `On` is preferred if that is a requirement for the job.

Note: For Snapshot Manager backup and recovery work flows, if DTE is required to be `on`, you need to ensure that DTE is configured to be `on` for each media server that is configured for the respective storage unit.

If the job demands a media server with the DTE mode `on`, but such a media server is not available, NetBackup falls back on the original resource allocation decisions.

In such cases, it is possible that the job goes ahead and sees a failure later on during job execution (in `nbjm` or `bprd` or other such daemons and CLIs), where NetBackup the DTE is required by media server.

The following process describes how the media device selection and DTE validations take place:

- 1 In case of a backup operation, directly go to step 2. For any other operations such as restore, duplication, replication, import, verify, the source image DTE mode is taken into consideration:
 - If the DTE mode of an image is `ON`, the media server DTE media server is `ON`, irrespective of any other DTE configuration.
 - If DTE mode of an image is `OFF`, check for global, client and media server DTE modes.
- 2 If the global DTE setting is `ENFORCED`, then a DTE enabled media server is preferred.
- 3 If the global DTE setting is `PREFERRED ON` or `PREFERRED OFF`, a client DTE mode is taken into consideration.
 - If the client DTE mode is `ON` – DTE enabled media server is preferred.
 - If the client DTE mode is `OFF` – any available media server can be selected.
 - If the client DTE mode is `Automatic` – the decision is made based on the global DTE setting. It means if the global DTE setting is set to `PREFERRED OFF`, select any available media server, else select the DTE enabled media server.

During resource allocation, many parameters play an important role. Following are the special conditions:

- If the client name is blank, it signifies a secondary operation such as duplication, replication, import, verify and so on. The image DTE mode or global DTE mode are honored.
- If the client name is not blank, however it is not present in the host database as the client is earlier than 8.0, the client does not support DTE. Hence, any media server can be selected.

- After the global and client DTE settings, media server's version and its DTE setting are checked:
 - NetBackup 9.1 and later media servers are by default DTE capable and DTE enabled.
- `DTE_IGNORE_IMAGE_MODE` setting (for any secondary operations based on an image)
 - If the image DTE mode is `ON`, and if the `DTE_IGNORE_IMAGE_MODE` option is applied, the global, client, and media server settings are used for the media server selection.

How DTE configuration settings work in various NetBackup operations

This topic provides information on how you can change the DTE configuration settings to achieve the required data-in-transit encryption with respect to various NetBackup operations.

Review the following reference topics before you modify any DTE configuration settings.

The following tables show how DTE setting (unencrypted or encrypted) is decided for a certain NetBackup workflow under different NetBackup configurations along with DTE configuration settings.

Backup

In the backup workflow, data is transferred between a media server and a client as part of a backup job.

Figure 20-1 Backup workflow

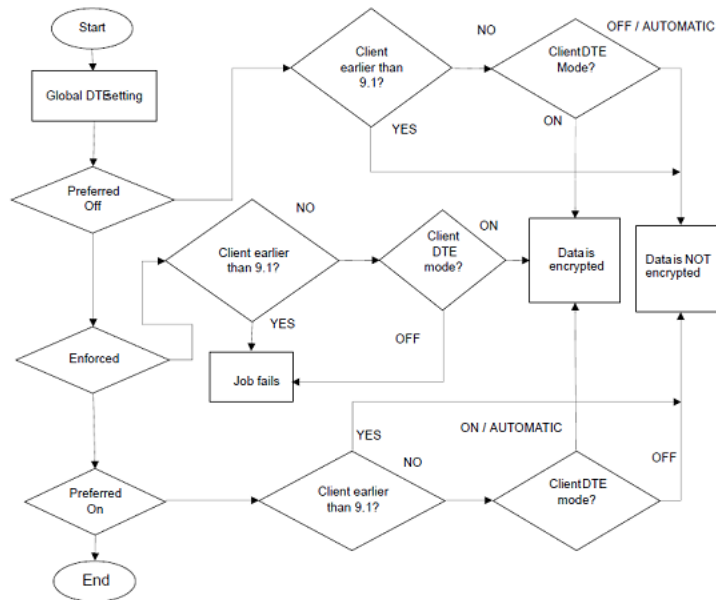


Table 20-4 The media server DTE mode is On (default)

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred Off	Data is encrypted	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Data is encrypted	Operation fails

Table 20-5 The media server DTE mode is Off (default)

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred Off	Operation fails	Data is not encrypted	Data is not encrypted	Data is not encrypted

Table 20-5 The media server DTE mode is Off (default) (*continued*)

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred On	Operation fails	Data is not encrypted	Data is not encrypted	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails	Operation fails

Restore

In the restore workflow, there can be two DTE scenarios:

- When the image DTE mode is Off
- When the image DTE mode is On

In either of the scenarios, there can be one or more media servers involved (if multiple images are selected) while restoring data on a client for single NetBackup job.

Image DTE mode is Off

Table 20-6 Media server DTE mode is On (default)

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred Off	Data is encrypted	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Data is encrypted	Operation fails

Table 20-7 Media server DTE mode is Off

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred Off	Operation fails	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Operation fails	Data is not encrypted	Data is not encrypted	Data is not encrypted

Table 20-7 Media server DTE mode is Off (*continued*)

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Enforced	Operation fails	Operation fails	Operation fails	Operation fails

Table 20-8 Mixed media servers (9.1 and 10.0 or later) - Media1: DTE mode On, Media2: DTE mode Off

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred Off	Media1 - Data is encrypted	Media1- Data is not encrypted	Media1- Data is not encrypted	Media1- Data is not encrypted
	Media2 - Operation fails	Media2 - Data is not encrypted	Media2 - Data is not encrypted	Media2 - Data is not encrypted
	Job state - Partial Success			
	Job DTE mode - On			
Preferred On	Media1- Data is encrypted	Media1- Data is not encrypted	Media1 - Data is encrypted	Media1- Data is not encrypted
	Media2- Operation fails	Media2 - Data is not encrypted	Media2 - Data is not encrypted	Media2 - Data is not encrypted
	Job state - Partial Success		Job DTE mode - Off	
	Job DTE mode - On			
Enforced	Media1 - Data is encrypted	Media1 - Operation fails	Media1 - Data is encrypted	Media1 - Operation fails
	Media2 - Operation fails	Media2 - Operation fails	Media2 - Operation fails	Media2 - Operation fails
	Job state - Partial Success	Job state - Fail	Job state - Partial Success	Job state - Operation fails
	Job DTE mode - On		Job DTE mode - On	

Image DTE mode is On

If the image DTE mode is On, the default behavior is to restore with data-in-transit encryption for 9.1 and later hosts and to fail the job if any DTE unsupported host

involves in the workflow . However, you can still restore by ignoring the image DTE mode.

Use the `DTE_IGNORE_IMAGE_MODE` configuration option that is to be set on the primary server. Possible values: `NEVER` (default) | `ALWAYS` | `WHERE_UNSUPPORTED`

Table 20-9 When the image DTE mode is On and the media server DTE mode is On

Global DTE mode	Host	Value of the <code>DTE_IGNORE_IMAGE_MODE</code> configuration option		
		<code>NEVER</code> (default)	<code>WHERE_UNSUPPORTED</code>	<code>ALWAYS</code>
Preferred Off	NetBackup client 9.1 or later with DTE mode ON	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Data is not encrypted
	NetBackup client 9.1 or later with DTE mode AUTOMATIC	Data is encrypted	Data is encrypted	Data is not encrypted
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Data is not encrypted	Data is not encrypted
Preferred On	NetBackup client 9.1 or later with DTE mode ON	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Data is not encrypted
	NetBackup client 9.1 or later with DTE mode AUTOMATIC	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Data is not encrypted	Data is not encrypted

Table 20-9 When the image DTE mode is On and the media server DTE mode is On (*continued*)

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Enforced	NetBackup client 9.1 or later with DTE mode ON	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Operation fails
	NetBackup client 9.1 or later with DTE mode AUTOMATIC	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Operation fails	Operation fails

Table 20-10 When the image DTE mode is On and the DTE setting on 10.0 and later media server is Off

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	NetBackup Client 9.1 or later with DTE mode ON	Operation fails	Operation fails	Operation fails
	NetBackup Client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Data is not encrypted
	NetBackup Client 9.1 or later with DTE mode AUTOMATIC	Operation fails	Operation fails	Data is not encrypted
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Data is not encrypted	Data is not encrypted

Table 20-10 When the image DTE mode is On and the DTE setting on 10.0 and later media server is Off (*continued*)

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred On	NetBackup Client 9.1 or later with DTE mode ON	Operation fails	Operation fails	Operation fails
	NetBackup Client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Data is not encrypted
	NetBackup Client 9.1 or later with DTE mode AUTOMATIC	Operation fails	Operation fails	Data is not encrypted
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Data is not encrypted	Data is not encrypted
Enforced	NetBackup Client 9.1 or later with DTE mode ON	Operation fails	Operation fails	Operation fails
	NetBackup Client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Operation fails
	NetBackup Client 9.1 or later with DTE mode AUTOMATIC	Operation fails	Operation fails	Operation fails
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Operation fails	Operation fails

Note: If the `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - [Table 20-7](#).

MSDP backup, restore, and optimized duplication

Data-in-transit encryption (DTE) feature is now integrated with MSDP storage server for backup and restore workflows.

For backup on MSDP disk pool, the encryption of data path from client to media server is controlled by the NetBackup DTE settings (global and client DTE modes).

If the MSDP storage server has multiple load balancing media servers attached to it and if the selected media server is 10.0.0.1 or later, the storage server must be

10.0.0.1 or later. Else, backup job fails. You must upgrade the 10.0 storage server to 10.0.0.1. If the load balancing media server is 10.0 or earlier, the data may be transferred in plain text and job is always successful, even if DTE was to be honored.

Ideally, you must have load balancing media servers and storage servers with 10.0.0.1 or later when DTE is enabled.

These given conditions are also valid for the optimized duplication workflow.

In case of mixed environment, where either storage server or one of the load balancing media servers is earlier than 10.0, the following configuration will be required in order to honor an end-to-end encryption:

- DTE should be enabled from NetBackup side based on DTE configurations i.e. Global/Media Server/Client Settings
- Encryption should be enabled from MSDP side using ENCRYPTION flag in `pd.conf`
See the *NetBackup Deduplication Guide* for details on enabling the encryption using MSDP.

Note: If data-in-transit encryption is enabled in NetBackup and the `ENCRYPTION` flag in `pd.conf` is also enabled, MSDP encryption takes the precedence over NetBackup DTE. It results into data-at-rest encryption and not in data-in-transit encryption.

Universal-Share policy backup

For Universal-Share policy type, client selection can either be storage server name where the Universal Share resides or the host name where the Universal Share is mounted. So the client for this policy type can be a host where the NetBackup client software is not installed.

Because of this limitation, NetBackup cannot check the client DTE mode. It checks for the global and media server DTE modes for Universal-Share policy backup and works as per the following table:

Table 20-11 DTE for Universal-Share policy backup

Global DTE mode	DTE mode of media server 9.1 or later		Media server earlier than 9.1
	On	Off	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is not encrypted

Table 20-11 DTE for Universal-Share policy backup (*continued*)

Global DTE mode	DTE mode of media server 9.1 or later		Media server earlier than 9.1
	On	Off	
Enforced	Data is encrypted	Operation fails	Operation fails

Catalog backup and recovery

Media server should be of the same NetBackup version as the primary server for catalog backup and recovery workflow.

Review the following points:

- DTE mode for catalog backup jobs is similar to the file system workflow and DTE decision is similar to the backup workflow described above.
- DTE mode in catalog backup jobs:
 - Parent catalog backup job does not have DTE mode set.
 - Database staging child job does not have DTE mode set.
 - Other child jobs have DTE mode set as per the configured DTE settings.
- DTE mode in catalog recovery jobs:
 - First 2 jobs have the DTE mode set as per the following tables depending on the image DTE mode.
 - The first two jobs replace the global DTE setting and primary server's bp.conf values, so the 3rd job DTE mode is set as per the recovered global DTE setting and primary server's bp.conf values.

The image DTE mode is Off

Table 20-12 When the image DTE mode is Off and the media server DTE setting is On

Global DTE mode	NetBackup Primary server 9.1 and later with DTE mode		
	On	Off	Automatic
Preferred Off	Data is encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is encrypted
Enforced	Data is encrypted	Data is encrypted	Data is encrypted

Note: When the global DTE setting is set to `ENFORCED` and the `DTE_CLIENT_MODE` is Off, DTE is preferred over failure in case of catalog recovery.

Table 20-13 When the image DTE mode is Off and the media server DTE setting is Off

Global DTE mode	NetBackup Primary server 9.1 and later with DTE mode		
	On	Off	Automatic
Preferred Off	Data is encrypted *	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted *	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted *	Data is encrypted *	Data is encrypted *

* signifies that DTE is preferred over failure during catalog recovery. It ignores the DTE setting on the media server, that is Off unless the client DTE mode is set to Automatic.

The image DTE mode is On

Table 20-14 When the image DTE mode is On and the media server DTE setting is On

Global DTE mode	Host	Value of the <code>DTE_IGNORE_IMAGE_MODE</code> configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Primary server with <code>DTE_CLIENT_MODE</code> as ON	Data is encrypted	Data is encrypted	Data is encrypted
	Primary server with <code>DTE_CLIENT_MODE</code> as OFF	Data is encrypted	Data is encrypted	Data is not encrypted
	Primary server with <code>DTE_CLIENT_MODE</code> as AUTOMATIC	Data is encrypted	Data is encrypted	Data is not encrypted

Table 20-14 When the image DTE mode is On and the media server DTE setting is On (*continued*)

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred On	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted	Data is encrypted	Data is encrypted
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted	Data is encrypted	Data is not encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted	Data is encrypted	Data is encrypted
Enforced	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted	Data is encrypted	Data is encrypted
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted	Data is encrypted	Data is encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted	Data is encrypted	Data is encrypted

Note: If DTE_IGNORE_IMAGE_MODE is set to ALWAYS, the DTE decision is as per the table - [Table 20-12](#).

Table 20-15 When the image DTE mode is On and the media server DTE setting is Off

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted *	Data is encrypted *	Data is encrypted *
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted *	Data is encrypted *	Data is not encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted *	Data is encrypted *	Data is not encrypted
Preferred On	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted *	Data is encrypted *	Data is encrypted *
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted *	Data is encrypted *	Data is not encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted *	Data is encrypted *	Data is not encrypted
Enforced	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted *	Data is encrypted *	Data is encrypted *
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted *	Data is encrypted *	Data is encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted *	Data is encrypted *	Data is encrypted *

* signifies that DTE is preferred over failure during catalog recovery. It ignores the DTE setting on the media server, that is Off unless the client DTE mode is set to Automatic.

Duplication

In the duplication workflow, a backup copy is copied from one storage unit to another storage unit, so there is no client that comes into picture. The hosts that participate are source media server and target media server from the same domain.

Table 20-16 The image DTE mode is Off

Global DTE mode	Both media servers are 9.1 or later with DTE mode		One of the media servers is earlier than 9.1
	On	Off	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Operation fails

Table 20-17 When the image DTE mode is On and the media server DTE setting is On

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Both NetBackup media servers 9.1 or later	Data is encrypted	Data is encrypted	Data is not encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Preferred On	Both NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Enforced	Both NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Operation fails	Operation fails

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - [Table 20-16](#).

Table 20-18 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Operation fails	Operation fails	Data is not encrypted
Preferred On	Operation fails	Operation fails	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails

Synthetic backup

A synthetic backup can be a synthetic full or a synthetic cumulative backup. The images that are used to create the synthetic image are known as component images. For instance, the component images in a synthetic full backup are the previous full image and the subsequent incremental images. A typical NetBackup backup process accesses the client to create a backup. A synthetic backup is a backup image created without using the client. Instead, a synthetic backup process creates a full or a cumulative incremental image by using previously created backup images called component images. In the synthetic backup workflow, images are fetched from different source storage units, synthesized, and copied to a target storage unit.

The hosts that come into the picture are source media servers and target media server from the same domain.

Table 20-19 DTE mode is OFF in the image

Global DTE mode	All NetBackup media server 9.1 and later with DTE mode		Any NetBackup media server earlier than 9.1
	On	Off	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Operation fails

Table 20-20 When DTE mode is On for any one of the images and media server DTE setting is On

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	All NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is not encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Preferred On	All NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Enforced	All NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Operation fails	Operation fails

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - [Table 20-19](#).

Table 20-21 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Operation fails	Operation fails	Data is not encrypted
Preferred On	Operation fails	Operation fails	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - [Table 20-19](#).

Note:

Verify

In the verification workflow, backup image header is read, and its integrity is checked with the catalog. Therefore, a client does not come into picture. The hosts that participate are media server and primary server from the same domain.

Table 20-22 The image DTE mode is Off

Global DTE mode	NetBackup media server 9.1 and later with DTE mode		NetBackup media server earlier than 9.1
	On	Off	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Operation fails

Table 20-23 When the image DTE mode is On and the media server DTE setting is On

Global DTE mode	DTE mode of NetBackup client 9.1 or later	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Media server 9.1 or later	Data is encrypted	Data is encrypted	Data is not encrypted
	Media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Preferred On	Media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Enforced	Media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Media server earlier than 9.1	Operation fails	Operation fails	Operation fails

Table 20-24 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Operation fails	Operation fails	Data is not encrypted
Preferred On	Operation fails	Operation fails	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails

Import

In the import workflow, backup image is read from the storage unit and the NetBackup catalog is created. Therefore, a client does not come into picture. The hosts that participate are the media server and the primary server from the same domain.

Note: If you want to retain the DTE controls based on the image, you must upgrade the media servers that are to be used for the import operations to NetBackup 10.0 before you perform the import operation.

The following table is applicable for all import workflows such as phase-1 import, phase-2 import and Storage Lifecycle Policy (SLP) import.

Table 20-25 DTE mode is OFF in the image

Global DTE mode	Media server 9.1 or later with DTE mode		Media server earlier than 9.1
	On	Off	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Operation fails

Table 20-26 When the image DTE mode is On and the media server DTE setting is On

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	NetBackup media server 9.1 and later	Data is encrypted	Data is encrypted	Data is not encrypted
	NetBackup media server earlier than 9.1	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	NetBackup media server 9.1 and later	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup media server earlier than 9.1	Data is not encrypted	Data is not encrypted	Data is not encrypted
Enforced	NetBackup media server 9.1 and later	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup media server earlier than 9.1	Operation fails	Operation fails	Operation fails

Note: For phase-1 import, you need to set `DTE_IGNORE_IMAGE_MODE` on the media server to ignore the DTE mode of the image for 9.1 and later media servers.

For phase-1 import scenario, NetBackup media server earlier than 9.1 is not aware of the DTE mode in the image. If the image was created with the DTE mode set to On, for phase-1 import, the job does not fail for media servers with version earlier than 9.1 and the image DTE mode is set to Off in the catalog.

Note: When `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, DTE decision is as per [Table 20-25](#).

Table 20-27 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Operation fails	Operation fails	Data is not encrypted
Preferred On	Operation fails	Operation fails	Data is not encrypted

Table 20-27 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off (*continued*)

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Enforced	Operation fails	Operation fails	Operation fails

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - [Table 20-25](#).

MSDP SLP import at target domain

In this case, the image is already replicated in the target disk pool and now the intention is to create a catalog out of that image through SLP import policy. As this operation happens in the target domain and no cross-domain operation happens, the target DTE global setting comes into the picture.

If the replicated image has the DTE mode On, then irrespective of other DTE configurations, the import operation is carried out with DTE mode On.

If the replicated image has the DTE mode Off, the DTE mode is derived based on the target domain global DTE setting and import is carried out based on the derived DTE mode.

Review the following MSDP limitations that need to be considered for this workflow:

- If the MSDP storage server has multiple load balancing media servers attached to it and if the selected media server is 10.0.0.1 or later, the storage server must be 10.0.0.1 or later. Else, backup job fails. You must upgrade the 10.0 storage server to 10.0.0.1.
If the load balancing media server is 10.0 or earlier, the data may be transferred in plain text and job is always successful, even if DTE was to be honored.
Ideally, you must have load balancing media servers and storage servers with 10.0.0.1 or later when DTE is enabled.
- In case of mixed environment, where either storage server or even one of the load balancing media servers is of version earlier than 10.0, the following configuration is required in order to honor end-to-end encryption:
 - DTE should be enabled from NetBackup side based on the DTE configuration settings - global / media server / client DTE mode
 - Encryption should be enabled from MSDP side using the `ENCRYPTION` flag in `pd.conf`

Refer to the NetBackup Deduplication Guide for details on enabling encryption using MSDP.

Note: If you set DTE On for NetBackup, but the ENCRYPTION flag in pd.conf is not enabled, the data path from the load balancing media server to the storage server is not encrypted. However, the job DTE mode and the image DTE mode may be On.

If DTE is enabled at the NetBackup side and encryption is enabled from MSDP side (ENCRYPTION flag in pd.conf), MSDP encryption takes the precedence over NetBackup DTE. It results in data-at-rest encryption and not data-in-transit encryption.

Replication

If the MSDP storage server is used for replication, the following considerations need to be reviewed:

- The Data-in-transit (DTE) encryption feature is not integrated with MSDP storage for replication workflows and it is controlled by the OPTDUP_ENCRYPTION flag in pd.conf.
- The job DTE mode depends on the image DTE mode or the global DTE setting of the source domain.
- The correct values must be set for the DTE configuration settings and the OPTDUP_ENCRYPTION flag for the source and target domains.

For details on enabling encryption using MSDP, see the *NetBackup Deduplication Guide*.

Table 20-28 The image DTE mode is Off

Global DTE mode	Media server 9.1 or later with DTE mode		Media server earlier than 9.1
	On	Off	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is encrypted
Enforced	Data is encrypted	Operation fails	Data is encrypted

Table 20-29 When the image DTE mode is On and media server DTE setting is On

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is not encrypted
	NetBackup media server earlier than 9.1	Data is encrypted	Data is encrypted	Data is not encrypted
Preferred On	NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup media server earlier than 9.1	Data is encrypted	Data is encrypted	Data is encrypted
Enforced	NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup media server earlier than 9.1	Data is encrypted	Data is encrypted	Data is encrypted

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - [Table 20-28](#).

Table 20-30 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Operation fails	Operation fails	Data is not encrypted
Preferred On	Operation fails	Operation fails	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - [Table 20-28](#).

External CA and external certificates

This chapter includes the following topics:

- [About external CA support in NetBackup](#)
- [Workflow to use external certificates for NetBackup host communication](#)
- [Configuration options for external CA-signed certificates](#)
- [Limitations of Windows Certificate Store support when NetBackup services are running in Local Service account context](#)
- [About certificate revocation lists for external CA](#)
- [About certificate enrollment](#)
- [About viewing enrollment status of primary servers](#)
- [Configure an external certificate for the NetBackup web server](#)
- [Configuring the primary server to use an external CA-signed certificate](#)
- [Configuring a NetBackup host \(media server, client, or cluster node\) to use an external CA-signed certificate after installation](#)
- [Enrolling an external certificate for a remote host](#)
- [Viewing the certificate authorities that your NetBackup domain supports](#)
- [Viewing external CA-signed certificates in the NetBackup web UI](#)
- [Renewing a file-based external certificate](#)
- [Configuring rotation of external CA-issued certificates for host communication](#)

- [Removing certificate enrollment](#)
- [Disabling the NetBackup CA in a NetBackup domain](#)
- [Enabling the NetBackup CA in a NetBackup domain](#)
- [Disabling an external CA in a NetBackup domain](#)
- [Changing the subject name of an enrolled external certificate](#)
- [About external certificate configuration for a clustered primary server](#)

About external CA support in NetBackup

You can now use X.509 certificates that your trusted certificate authority (CA) has issued.

NetBackup supports file-based certificates and Windows certificate store as sources for external certificates for NetBackup hosts. It supports certificates in PEM, DER, and P7B formats.

Note: NetBackup does not support Windows certificate store as source for the NetBackup web server certificate.

Note: The following API is used to configure an external certificate for WORM container on NetBackup Flex:

`/security/external-certificates/hosts/{hostUUID}.`

About the terminology used for certificates in NetBackup

The following terms that are specific to security certificates are used in NetBackup:

- A certificate authority (CA) other than the NetBackup CA is referred to as an external CA.
- Certificates that are issued by a CA other than the NetBackup CA are referred to as external CA-signed certificates or external certificates.
- Certificates that the NetBackup CA has issued are referred to as NetBackup CA-signed certificates or NetBackup certificates.
- A NetBackup certificate that is used for secure communications over control channel is also referred to as host ID-based certificate.

Important notes about host certificates

- A host ID-based certificate is deployed on the primary server during NetBackup installation. You need to manually configure an external certificate on the primary server after installation.
 See [“Configuring the primary server to use an external CA-signed certificate”](#) on page 426.
- You can configure an external certificate on a NetBackup host (media server or client) either during installation or after installation.
 See [“Configuring a NetBackup host \(media server, client, or cluster node\) to use an external CA-signed certificate after installation”](#) on page 429.
- Host ID-based certificates are required on all NetBackup 8.1 and higher hosts for enabling mutually authenticated secure communications. Starting 8.2, NetBackup CA-signed host ID-based certificates can be replaced by external CA-signed certificates.
 In addition to the host ID-based certificate, a host name-based certificate may need to be deployed on some hosts in domains that have NetBackup Access Control (NBAC) enabled. The host name-based certificates are issued by the NetBackup CA.
 See [“Overview of security certificates in NetBackup”](#) on page 273.

Requirements for external certificate configuration

- On Windows platform, if external certificates are used for host communication, the `NT AUTHORITY\SYSTEM` user must be able to access the certificates that are located at `ECA_CERT_PATH`. The `ECA_CERT_PATH` configuration option is available in the Windows registry.
- On Windows platform, Universal Naming Convention (UNC) paths (or network paths) are not supported for the following external CA parameters: Certificate chain, certificate's private key, trust store, passphrase file for certificate's private key, and CRL cache.
- The following requirement is applicable for the NetBackup web server certificate: If the subject alternative name (SAN) is not empty, the certificate should contain all host names that the primary server is known by (the host names that are listed in the `SERVER` configuration option entries of other hosts in the domain) in the SAN field of the certificate.
- Requirements for the subject name of the certificate:
 - Subject name should not be empty.
 - Common name of the subject name should not be empty.
 - Subject name should be unique for each host.

- Subject name should be fewer than 255 characters.
- Only ASCII 7 characters are supported for the certificate subject and the subject alternative name (SAN).
- Requirements for key usage purposes:

If the certificate has a X509v3 Key Usage extension present, it must include the following key usage purposes:

- For the web server certificate: At least one of the Digital Signature or Key Encipherment should be present.
- For a NetBackup host certificate: Digital Signature purpose should be present. Key Encipherment may or may not be present.
- For a certificate that is used for both web server and NetBackup host: Digital Signature purpose should be present. Key Encipherment may or may not be present.
- The certificate may have other key usage purposes listed in addition to the purposes specified here. These additional purposes are ignored.
- The X509v3 Key Usage extension may be either critical or non-critical.
- A certificate without a X509v3 Key Usage extension is also usable with NetBackup.

If the certificate has a X509v3 Extended Key Usage extension present, it must include the following key usage purposes:

- For the web server certificate: TLS Web Server Authentication.
- For a NetBackup host certificate: TLS Web Server Authentication and TLS Web Client Authentication.
- For a certificate that is used for both web server and NetBackup host: TLS Web Server Authentication and TLS Web Client Authentication.
- The certificate may have other key usage purposes listed in addition to the purposes specified here. These additional purposes are ignored.
- The X509v3 Extended Key Usage extension may be either critical or non-critical.
- A certificate without a X509v3 Extended Key Usage extension is also usable with NetBackup.
- If the certificate does not meet these requirements, contact your certificate provider to obtain a new certificate.

Command-line options used for external certificate configuration

Use the following command-line options are specific to external certificate configuration:

nbcertcmd	■ -cleanupCRLCache ■ -createECACertEntry ■ -deleteECACertEntry ■ -ecaHealthCheck ■ -enrollCertificate ■ -getExternalCertDetails ■ -listEnrollmentStatus ■ -removeEnrollment ■ -updateCRLCache
configureWebServerCerts	■ -addExternalCert ■ -removeExternalCert ■ -validateExternalCert

The following command-line options are used for both external and NetBackup certificate configurations:

nbcertcmd	■ -listCertDetails - This command option is by default applicable for NetBackup CA-signed certificate. When used with -ECA option, it is applicable for external CA-signed certificates. ■ -listCACertDetails - This command option is by default applicable for NetBackup CA-signed certificate. When used with -ECA option, it is applicable for external CA-signed certificates.
-----------	--

For more information about the commands, refer to the [NetBackup Commands Reference Guide](#).

Workflow to use external certificates for NetBackup host communication

To configure NetBackup to use external CA-signed certificates for secure communication, you should carry out the following steps in the given order:

Table 21-1 Workflow to use external certificates for NetBackup host communication

Step	Description
Step 1	Ensure the following: ■ The external certificates for the web server, primary server, and all hosts are placed at the appropriate locations. ■ In case of file-based certificates, the private key files for the external certificates are placed at the appropriate locations. See “ECA_PRIVATE_KEY_PATH for NetBackup servers and clients” on page 409. If the private keys are encrypted, passphrase files should be placed at the appropriate locations. See “ECA_KEY_PASSPHRASEFILE for NetBackup servers and clients” on page 410. ■ The CRLs are placed at the required locations on the hosts as per their CRL configuration options and they are accessible. See “About certificate revocation lists for external CA” on page 419.
Step 2	Install the NetBackup software on the primary server (or upgrade the primary server).
Step 3	Enable the NetBackup domain to use external certificates by configuring the NetBackup web server. See “Configure an external certificate for the NetBackup web server” on page 423.
Step 4	Configure an external certificate for the NetBackup primary server host. See “Configuring the primary server to use an external CA-signed certificate” on page 426.
Step 5	Install the NetBackup software on the media server and clients (or upgrade the media server and clients). If the primary server is configured to use external certificates, the Installer prompts you to provide external certificate information for the host.

Table 21-1 Workflow to use external certificates for NetBackup host communication (*continued*)

Step	Description
Step 6	Note: This step is required for the hosts (media server and clients) that have the current NetBackup software, but are not configured to use external certificate. NetBackup hosts may not have external certificate configuration because of the following reasons: ■ You did not provide the external certificate information during installation or upgrade of the host. ■ The NetBackup primary server was not configured to use external certificates during installation or upgrade of the host. Configure an external certificate for a NetBackup host (media server or client) after installation. See “Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate after installation” on page 429.

Configuration options for external CA-signed certificates

To configure a NetBackup primary server, media server, or client to use external CA-signed certificate for host communication, you must define certain configuration options in the NetBackup configuration file (`bp.conf` on UNIX platform or Windows registry).

About the mandatory and optional configuration options

- For external certificate configuration, for file-based certificates, the following configuration options are mandatory:
 - `ECA_CERT_PATH`
 - `ECA_TRUST_STORE_PATH`
 - `ECA_PRIVATE_KEY_PATH`

If the private key of the external certificate is encrypted, `ECA_KEY_PASSPHRASEFILE` is also mandatory:
- For Windows certificate store, the following configuration options are mandatory:
 - `ECA_CERT_PATH`
- The following options are optional:

- `ECA_CRL_CHECK`
 If the option is set to `DISABLE` (or 0) the `ECA_CRL_PATH` option is ignored and revocation status of a peer host's certificate is not verified.
 If the option is set to a value other than `DISABLE` and 0, revocation status of a peer host's certificate is verified based on `ECA_CRL_PATH`.
- `ECA_DR_BKUP_WIN_CERT_STORE`
 For Windows certificate store, specify this option if you want to backup the external certificates during catalog backup.
- `ECA_CRL_PATH_SYNC_HOURS`
 This option is used when `ECA_CRL_CHECK` is enabled and `ECA_CRL_PATH` is defined.
- `ECA_CRL_REFRESH_HOURS`
 This option is used when `ECA_CRL_CHECK` is enabled, but `ECA_CRL_PATH` is not defined (when CDP is used as a CRL source).
 See [“About certificate revocation lists for external CA”](#) on page 419.

ECA_CERT_PATH for NetBackup servers and clients

The `ECA_CERT_PATH` option specifies the path to the external CA-signed certificate of the host. This option is mandatory.

NetBackup supports the following certificate sources for host certificates:

- Windows certificate store

Note: The Windows certificate store is not supported for clustered primary servers.

- File-based certificates

Certificate order in the certificate file

A certificate file must have a certificate chain with certificates in the correct order. The chain starts with the server certificate (also known as the leaf certificate) and is followed by zero or more intermediate certificates. The chain must contain all intermediate certificates up to the Root CA certificate but should not contain the Root CA certificate itself. The chain is created such that each certificate in the chain signs the previous certificate in the chain.

The certificate file should be in one of the following formats:

- PKCS #7 or P7B file that is either DER or PEM encoded that has certificates in the specified order

- A file with the PEM certificates that are concatenated together in the specified order

Table 21-2 ECA_CERT_PATH information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. For file-based certificates, use the following format: <pre>ECA_CERT_PATH = Path to the external certificate of the host</pre> For example: <code>c:\server.pem</code> If you use this option on a Flex Appliance application instance, the path must be <code>/mnt/nbdata/hostcert/</code>. For Windows certificate store, use the following format: <pre>ECA_CERT_PATH = Certificate store name\Issuer name\Subject name</pre> You can specify multiple certificate selection queries in a comma-separated format. <pre>ECA_CERT_PATH = Store name1\Issuer name1\Subject name1,Store name2\Issuer name2\Subject name2</pre> See “Specifying Windows certificate store for ECA_CERT_PATH” on page 406.
Equivalent NetBackup web UI property	No equivalent exists.

Specifying Windows certificate store for ECA_CERT_PATH

NetBackup selects a certificate from any of the local machine certificate stores on a Windows host.

In case of Windows certificate store, `ECA_CERT_PATH` is a list of comma-separated clauses.

Each clause is of the form *Store name\Issue\Subject*. Each clause element contains a query.

`$hostname` is a keyword that is replaced with the fully qualified domain name of the host. Use double quotes when a `\` is present in the actual path. For example, `MY\Veritas\NetBackup\hostname`.

`$shorthostname` is a keyword that is replaced with the short name of the host. Use double quotes when a `\` is present in the actual path. For example, `MY\Veritas\NetBackup\shorthostname`.

The 'Store name' should be the exact name of the store where the certificate resides. For example: 'MY'

The 'Issuer' is optional. If this is provided, NetBackup picks the certificates for which the Issuer DN contains the provided substring.

The 'Subject' is mandatory. NetBackup picks the certificate for which the Subject DN contains the provided substring.

You must ensure to:

- Add the root certificate to Trusted Root Certification Authorities or Third-Party Root Certification Authorities in the Windows certificate store.
- If you have any intermediate CAs, add their certificates to the Intermediate Certification Authorities in the Windows certificate store.

Example - Certificate locations with WHERE CLAUSE:

- `MY\Veritas\hostname, My\ExampleCompany\hostname`
 Where (certificate store is MY, Issuer DN contains `Veritas`, Subject DN contains `hostname`) OR (certificate store name is MY, Issuer DN contains `ExampleCompany`, Subject DN contains `hostname`)
- `MY\Veritas\NetBackup\hostname`
 Where certificate store name is MY, Issuer DN contains `Veritas`, Subject DN contains `NetBackup\hostname`
- `MY\hostname`
 Where certificate store name is MY, any Issuer DN, Subject DN contains `hostname`
- `MY\shorthostname`
 Where certificate store name is MY, any Issuer DN, Subject DN contains `shorthostname`
- `MY\Veritas\NetBackup hostname`
 Where certificate store name is MY, Issuer DN contains `Veritas`, Subject DN contains `NetBackup hostname`

If you provide a space between words, it is considered as a valid character.

Example - Certificate locations with invalid data:

- `MY\`
The Subject DN should have some value.
- `My\$hostname`
The Subject DN should have some value.
- `\\$hostname`
The certificate store name should have exact value of the store in which the certificate resides.
- `MY\CN=Veritas\CN=$hostname`
The Subject DN and issuer DN cannot contain =, and also specific tags like CN=.

ECA_TRUST_STORE_PATH for NetBackup servers and clients

The `ECA_TRUST_STORE_PATH` option specifies the file path to the certificate bundle file that contains all trusted root CA certificates.

This certificate file should have one or more certificates in PEM format.

Do not specify the `ECA_TRUST_STORE_PATH` option if you use the Windows certificate store.

The trust store supports certificates in the following formats:

- PKCS #7 or P7B file having certificates of the trusted root certificate authorities that are bundled together. This file may either be PEM or DER encoded.
- A file containing the PEM encoded certificates of the trusted root certificate authorities that are concatenated together.

This option is mandatory for file-based certificates.

The root CA certificate in Cloudera distribution can be obtained from the Cloudera administrator. It may have a manual TLS configuration or an Auto-TLS enabled for the Hadoop cluster. For both cases, NetBackup needs a root CA certificate from the administrator.

The root CA certificate from the Hadoop cluster can validate the certificates for all nodes and allow NetBackup to run the backup and restore process in case of the secure (SSL) cluster. This root CA certificate is a bundle of certificates that has been issued to all such nodes.

Certificate from root CA must be configured under `ECA_TRUST_STORE_PATH` in case of self-signed, third party CA or Local/Intermediate CA environments. For example: In case of AUTO-TLS enabled Cloudera environments, you can typically find the root CA file named with `cm-auto-global_cacerts.pem` at path

`/var/lib/cloudera-scm-agent/agent-cert`. For more details, refer Cloudera documentation.

Table 21-3 ECA_TRUST_STORE_PATH information

Usage	Description
Where to use	On NetBackup servers or clients. If certificate validation is required for VMware, Red Hat Virtualization servers, or Nutanix AHV, this option must be set on the NetBackup primary server and respective access hosts, irrespective of the certificate authority that NetBackup uses for host communication (NetBackup CA or external CA).
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: <pre>ECA_TRUST_STORE_PATH = Path to the external CA certificate</pre> For example: <code>c:\rootCA.pem</code> If you use this option on a Flex Appliance application instance, the path must be <code>/mnt/nbdata/hostcert/</code>.
Equivalent UI property	No equivalent exists.

ECA_PRIVATE_KEY_PATH for NetBackup servers and clients

The `ECA_PRIVATE_KEY_PATH` option specifies the file path to the private key for the external CA-signed certificate of the host.

This option is mandatory for file-based certificates.

If the private key of the certificate is encrypted, you should specify the `ECA_KEY_PASSPHRASEFILE` option.

See “[ECA_KEY_PASSPHRASEFILE for NetBackup servers and clients](#)” on page 410.

NetBackup supports PKCS #1 and PKCS #8 formatted private keys that are either plain text or encrypted. These may either be PEM or DER encoded. However, if it is PKCS #1 encrypted, it must be PEM encoded.

For encrypted private keys, NetBackup supports the following encryption algorithms:

- DES, 3DES, and AES if the private key is in the PKCS #1 format

- DES, 3DES, AES, RC2, and RC4 if the private key is in the PKCS #8 format

Note: You should not specify the `ECA_PRIVATE_KEY_PATH` option if Windows certificate store is specified for the `ECA_CERT_PATH` option.

See [“ECA_CERT_PATH for NetBackup servers and clients”](#) on page 405.

Table 21-4 `ECA_PRIVATE_KEY_PATH` information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: <pre>ECA_PRIVATE_KEY_PATH = Path to the private key of the external certificate</pre> For example: <code>c:\key.pem</code> If you use this option on a Flex Appliance application instance, the path must be <code>/mnt/nbdata/hostcert/</code>.
Equivalent UI property	No equivalent exists.

ECA_KEY_PASSPHRASEFILE for NetBackup servers and clients

The `ECA_KEY_PASSPHRASEFILE` option specifies the path to the text file where the passphrase for the external certificate’s private key is stored.

You should specify the `ECA_KEY_PASSPHRASEFILE` option only if the certificate’s private key is encrypted.

See [“ECA_PRIVATE_KEY_PATH for NetBackup servers and clients”](#) on page 409.

Note: You should not specify the `ECA_KEY_PASSPHRASEFILE` option if you use Windows certificate store.

See [“ECA_CERT_PATH for NetBackup servers and clients”](#) on page 405.

Note: Do not use the ECA_KEY_PASSPHRASEFILE on the MSDP servers that are used for MSDP direct cloud tiering as it is not supported with MSDP direct cloud tiering.

Table 21-5 ECA_KEY_PASSPHRASEFILE information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: <pre>ECA_KEY_PASSPHRASEFILE = Path to the passphrase file</pre>
Equivalent UI property	No equivalent exists.

ECA_CRL_CHECK for NetBackup servers and clients

The `ECA_CRL_CHECK` option lets you specify the revocation check level for external certificates of the host. It also lets you disable the revocation check for the external certificates. Based on the check, revocation status of the certificate is validated against the Certificate Revocation List (CRL) during host communication.

You can choose to use the CRLs from the directory that is specified for the `ECA_CRL_PATH` configuration option in the configuration file (`bp.conf` on UNIX or Windows registry) or the CRL Distribution Point (CDP).

See [“ECA_CRL_PATH for NetBackup servers and clients”](#) on page 412.

Table 21-6 ECA_CRL_CHECK information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 21-6 ECA_CRL_CHECK information (*continued*)

Usage	Description
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: <pre>HADOOP_CRL_CHECK = CRL check</pre> You can specify one of the following: ■ DISABLE (or 0) - Revocation check is disabled. Revocation status of the certificate is not validated against the CRL during host communication. This is the default value. ■ LEAF (or 1) - Revocation status of the leaf certificate is validated against the CRL. ■ CHAIN (or 2) - Revocation status of all certificates from the certificate chain are validated against the CRL.
Equivalent web UI property	No equivalent exists.

ECA_CRL_PATH for NetBackup servers and clients

The `ECA_CRL_PATH` option specifies the path to the directory where the Certificate Revocation Lists (CRL) of the external certificate authority (ECA) are located.

These CRLs are copied to NetBackup CRL cache. Revocation status of the external certificate is validated against the CRLs from the CRL cache.

CRL in the CRL cache is periodically updated with the CRL on the location that is specified for `ECA_CRL_PATH` based on the `ECA_CRL_PATH_SYNC_HOURS` option.

If the `ECA_CRL_CHECK` or `HADOOP_CRL_CHECK` option is not set to **DISABLE** (or 0) and the `ECA_CRL_PATH` option is not specified, NetBackup downloads the CRLs from the URLs that are specified in the CRL distribution point (CDP) and uses them to verify revocation status of the peer host's certificate.

Note: For validating the revocation status of a virtualization server certificate, the `VIRTUALIZATION_CRL_CHECK` option is used.

For validating the revocation status of a Hadoop server certificate, the `HADOOP_CRL_CHECK` option is used.

Table 21-7 ECA_CRL_PATH information

Usage	Description
Where to use	On NetBackup servers or clients. If certificate validation is required for VMware, Red Hat Virtualization servers, Nutanix AHV, or Hadoop, this option must be set on the NetBackup primary server and respective access or backup hosts, irrespective of the certificate authority that NetBackup uses for host communication (NetBackup CA or external CA). If certificate validation is required for VMware, Red Hat Virtualization servers, or Hadoop, this option must be set on the NetBackup primary server and respective access or backup hosts, irrespective of the certificate authority that NetBackup uses for host communication (NetBackup CA or external CA).
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format to specify a path to the CRL directory: <pre>ECA_CRL_PATH = Path to the CRL directory</pre> For example: <pre>ECA_CRL_PATH = /usr/eca/crl/eca_crl_file.crl</pre> If you use this option on a Flex Appliance application instance, the path must be <code>/mnt/nbdata/hostcert/crl</code>.
Equivalent UI property	No equivalent exists.

ECA_CRL_PATH_SYNC_HOURS for NetBackup servers and clients

The `ECA_CRL_PATH_SYNC_HOURS` option specifies the time interval in hours to update the Certificate revocation lists (CRL) in the NetBackup CRL cache with the CRLs in the directory that is specified for the `ECA_CRL_PATH` configuration option.

See “[ECA_CRL_PATH for NetBackup servers and clients](#)” on page 412.

The `ECA_CRL_PATH_SYNC_HOURS` option is not applicable if CDP is used for CRLs.

By default, CRLs in the cache are updated every one hour.

During host communication, revocation status of the external certificate is validated against the CRLs from the CRL cache.

Table 21-8 ECA_CRL_PATH_SYNC_HOURS information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: <pre>ECA_CRL_PATH_SYNC_HOURS = Number of hours</pre> Minimum number of hours that you can specify - 1 hour Maximum number of hours that you can specify - 720 hour The default value is one hour.
Equivalent UI property	No equivalent exists.

ECA_CRL_REFRESH_HOURS for NetBackup servers and clients

The `ECA_CRL_REFRESH_HOURS` option specifies the time interval in hours to download the CRLs from the URLs that are specified in the peer host certificate's CRL distribution points (CDP).

The `ECA_CRL_REFRESH_HOURS` option is applicable when you use CDP for CRLs.

See [“ECA_CRL_PATH for NetBackup servers and clients”](#) on page 412.

After the specified time interval, CRLs of the certificate authority are downloaded from the URLs that are available in CDP.

By default, the CRLs are downloaded from the CDP after every 24 hours.

Table 21-9 ECA_CRL_REFRESH_HOURS information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 21-9 ECA_CRL_REFRESH_HOURS information (*continued*)

Usage	Description
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: <pre>ECA_CRL_REFRESH_HOURS = Number of hours</pre> Minimum number of hours that you can specify - 0 hour, which indicates that CRLs from the CDP are not periodically downloaded. Maximum number of hours that you can specify - 4380 hours The default value for the option is 24 hours. Note: CRLs are also downloaded from the CDP during host communication if they are expired or not available in the CRL cache, irrespective of the time interval set for the <code>ECA_CRL_REFRESH_HOURS</code> option.
Equivalent UI property	No equivalent exists.

ECA_DISABLE_AUTO_ENROLLMENT for NetBackup servers and clients

When NetBackup is configured to use the certificates that an external CA has signed, such certificates are automatically enrolled with the primary server during host communication. If you want to disable automatic enrollment of such certificates, set the `ECA_DISABLE_AUTO_ENROLLMENT` to '1'.

When automatic enrollment is disabled, you can enroll the external certificates manually using the `nbcertcmd -enrollCertificate` command.

A certificate must be enrolled with the primary server before it can be used for host communication.

By default, automatic certificate enrollment is enabled.

Table 21-10 ECA_DISABLE_AUTO_ENROLLMENT information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 21-10 ECA_DISABLE_AUTO_ENROLLMENT information (*continued*)

Usage	Description
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: <pre>ECA_DISABLE_AUTO_ENROLLMENT = 1</pre>
Equivalent UI property	No equivalent exists.

ECA_DR_BKUP_WIN_CERT_STORE for NetBackup servers and clients

The `ECA_DR_BKUP_WIN_CERT_STORE` option specifies whether you want to take a backup of the Windows certificate store information during catalog backup or not. By default, Windows certificate store information is backed up during catalog backup.

Note: If the Windows certificate store information is not exportable, it cannot be backed up during catalog backup.

Table 21-11 ECA_DR_BKUP_WIN_CERT_STORE information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. If you do not want the catalog backup operation to take a backup of the Windows certificate store information, use the following format: <pre>ECA_DR_BKUP_WIN_CERT_STORE = NO</pre>
Equivalent UI property	No equivalent exists.

MANAGE_WIN_CERT_STORE_PRIVATE_KEY option for NetBackup primary servers

The `MANAGE_WIN_CERT_STORE_PRIVATE_KEY` option lets you disable the automatic permission management of the private key of the certificate in Windows Certificate Store.

This option is applicable for Windows Certificate Store and only when the NetBackup services are running in the Local Service account context.

When NetBackup services are running in the Local Service account context, the services need to have permissions to read the private key for certificate in Windows Certificate Store.

When the `MANAGE_WIN_CERT_STORE_PRIVATE_KEY` option is set to `Automatic`, the NetBackup service that is running in the privileged user account context grants access to all other NetBackup services for reading the private key whenever required.

By default, permissions for the private key are automatically managed. When the `MANAGE_WIN_CERT_STORE_PRIVATE_KEY` option is set to `Disabled`, the permissions of the private key need to be managed manually.

Note: It is not recommended to set the `MANAGE_WIN_CERT_STORE_PRIVATE_KEY` option to `Disabled`.

To manually update the permissions when this option is `Disabled`, run the following command:

```
nbcertcmd -setWinCertPrivKeyPermissions -reason audit reason -force
```

Refer to the [NetBackup Commands Reference Guide](#) for more details on the command-line options.

Table 21-12 `MANAGE_WIN_CERT_STORE_PRIVATE_KEY` information

Usage	Description
Where to use	On NetBackup primary server.
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: <pre>MANAGE_WIN_CERT_STORE_PRIVATE_KEY = Automatic</pre>

Table 21-12 MANAGE_WIN_CERT_STORE_PRIVATE_KEY information
(continued)

Usage	Description
Equivalent NetBackup web UI property	No equivalent exists.

Limitations of Windows Certificate Store support when NetBackup services are running in Local Service account context

When NetBackup services are running in Local Service account context, the services need to have read access to the private key. NetBackup updates permissions of the private key during certificate enrollment so that NetBackup services have read access to the private key.

To set the permissions the Cryptographic Service Provider (CSP) or Key Storage Provider (KSP) of the certificate being used must support security descriptors.

To know if the security descriptors are supported by the provider, run the following command:

```
nbcertcmd -ecaHealthCheck -serviceUser LocalService
```

Refer to the [NetBackup Commands Reference Guide](#) for more details on the command-line options.

If security descriptors are not supported by the provider, you need to use a provider that supports security descriptors or use an administrator account to run NetBackup services.

To change your provider, you need to re-deploy your certificate. Provider cannot be changed once the certificate is deployed. Providers that support security descriptors: Microsoft Software Key Storage Provider, Microsoft Enhanced Cryptographic Provider v1.0, Microsoft Enhanced RSA and AES Cryptographic Provider, Microsoft Strong Cryptographic Provider and so on.

If you have PFX file, you can re-import it to change your provider.

- 1 Remove certificate and private key from Windows Certificate Store.
- 2 Import the `pfx` file using `certutil` command:

```
C:\Windows\System32\certutil.exe -importPfx -csp provider name  
pfxfile
```

For an ADCS deployed certificate, the provider can be changed from the certificate template and then deploying the certificate again.

You can also select a provider while requesting a new certificate depending on the configuration.

To use administrator account to run NetBackup services, run the following command:

```
nbseviceusercmd.exe -changeUser
```

Refer to the [NetBackup Commands Reference Guide](#) for more details on the command-line options.

About certificate revocation lists for external CA

Certificate revocation list (CRL) for an external certificate authority (CA) contains a list of digital certificates that the external CA has revoked before the scheduled expiration date and should no longer be trusted.

NetBackup supports PEM and DER formats for CRLs for external CA.

CRLs for all CRL issuers or external CAs are stored in the NetBackup CRL cache that resides on each host.

During secure communication, each NetBackup host verifies the revocation status of the peer host's external certificate with the CRL that is available in the NetBackup CRL cache, based on the `ECA_CRL_CHECK` configuration option.

See [“ECA_CRL_CHECK for NetBackup servers and clients”](#) on page 411.

The NetBackup CRL cache is updated with the required CRLs using one of the following CRL sources:

<code>ECA_CRL_PATH</code> configuration option	A NetBackup configuration option (from <code>bp.conf</code> file on UNIX or Windows registry) that specifies the path where the CRL exists. See “ECA_CRL_PATH_SYNC_HOURS for NetBackup servers and clients” on page 413. See “How CRLs from ECA_CRL_PATH are used” on page 420.
CRL distribution point (CDP)	If you have not specified <code>ECA_CRL_PATH</code>, NetBackup downloads the CRLs from the URLs that are specified in the peer host certificate's CDP and caches them in the NetBackup CRL cache. See “How CRLs from CDP URLs are used” on page 421. NetBackup supports downloading CRLs from HTTP and HTTPS URLs that are specified in CDP.

The NetBackup CRL cache contains only the latest copy of a CRL for each CA (including root and intermediate CAs).

The `bpcintcmd -crl_download` service updates the CRL cache during host communication in the following scenarios irrespective of the time interval set for the `ECA_CRL_PATH_SYNC_HOURS` or `ECA_CRL_REFRESH_HOURS` options:

- When CRLs in the CRL cache are expired
- If CRLs are available in the CRL source (`ECA_CRL_PATH` or CDP), but they are missing from the CRL cache

Note: Once the `bpcintcmd -crl_download` service updates the CRLs in the CRL cache, it does not download the CRLs for the same CA for the next 15 min even though a valid download scenario has occurred. If you want to update the CRL within 15 min, terminate the `bpcintcmd -crl_download` service.

How CRLs from `ECA_CRL_PATH` are used

Use this section if you want to use `ECA_CRL_PATH` as the CRL source for the NetBackup CRL cache.

To use CRLs from `ECA_CRL_PATH`

- 1 Ensure that the CRLs for external CAs are stored in a directory and the directory path is accessible by the host.

If you have a Flex Appliance application instance, the files must be stored in the following directory on the instance: `/mnt/nbdata/hostcert/crl`

You can specify the CRL details that are required for external CA configuration during NetBackup installation or upgrade on the host.

Select one of the following certificate revocation list (CRL) options during installation or upgrade:

- **Use the CRL defined in the certificate** - No additional information is required.
- **Use the CRL at the following path** - You are prompted to provide a path to the CRL.

If you choose to use the **Do not use a CRL** option, peer host's certificate is not verified with the CRL during host communication.

For more information, refer to the [NetBackup Installation Guide](#).

- 2 Specify the CRL directory path for the `ECA_CRL_PATH` configuration option.
- 3 Ensure that the `ECA_CRL_CHECK` configuration option is set to a value other than `DISABLE`.

During host communication, the revocation status of the external certificate is verified with the CRL in the NetBackup CRL cache that contains the CRLs from `ECA_CRL_PATH`.

By default, CRLs from the cache are updated every one hour. To change the time interval, set the `ECA_CRL_PATH_SYNC_HOURS` option to a different value.

To manually update the CRL cache with the `ECA_CRL_PATH` CRLs, run the `nbcertcmd -updateCRLCache` command.

To manually delete the CRLs from the CRL cache, run the `nbcertcmd -cleanupCRLCache` command.

How CRLs from CDP URLs are used

Use this section if you want to use CRL Distribution Point (CDP) as the CRL source for the NetBackup CRL cache.

To use CRLs from CDP

- 1 Ensure that the `ECA_CRL_PATH` configuration option is not specified.
- 2 Ensure that the host can access the URLs that are specified in the peer host's CDP.
- 3 Ensure that the `ECA_CRL_CHECK` configuration option is set to a value other than `DISABLE`.

During host communication, the revocation status of the external certificate is verified with the CRL in the NetBackup CRL cache that contains the CRLs from CDP URLs.

By default, CRLs are downloaded from the CDP after every 24 hours and updated in the CRL cache. To change the time interval, set the `ECA_CRL_REFRESH_HOURS` configuration option to a different value.

To manually delete the CRLs from the CRL cache, run the `nbcertcmd -cleanupCRLCache` command.

About certificate enrollment

In case of NetBackup CA, certificates are automatically enrolled with the primary server during certificate deployment.

In case of external CA, certificates are automatically enrolled with the primary server during host communication if the `ECA_DISABLE_AUTO_ENROLLMENT` option is enabled. You can enroll the certificate manually using the `nbcertcmd -enrollCertificate` command.

The enrolled certificates are used for host communication.

See [“Removing certificate enrollment”](#) on page 437.

About automatic enrollment of an external certificate

An external certificate of a host is automatically enrolled with a primary server when communication takes place for the first time. You can disable the automatic certificate enrollment process and enroll the certificates manually as and when required using the `nbcertcmd -enrollCertificate` command.

See [“ECA_DISABLE_AUTO_ENROLLMENT for NetBackup servers and clients”](#) on page 415.

If automatic enrollment is enabled for communicating hosts and both hosts have external certificates configured, NetBackup tries to enroll the external certificates.

The external certificates are enrolled with the associated primary server. During any subsequent communications between the hosts associated with this primary server, the enrolled external certificates are used.

External certificates are not automatically enrolled in the following scenarios:

- Communication with NAT clients
For more information about NAT client support in NetBackup, refer to the [NetBackup Administrator's Guide Volume I](#).
- Communication between media servers as part of media server deduplication (MSDP) image replication
- Communication with the **NetBackup BAR Console**

About viewing enrollment status of primary servers

To configure a NetBackup host to use an external certificate, you need to define the required configuration options and then enroll a certificate for the host. The

enrolled certificate is used for communication between the host and the primary server domain that exists in the `SERVER` option.

See [“Configuring the primary server to use an external CA-signed certificate”](#) on page 426.

See [“Configuring a NetBackup host \(media server, client, or cluster node\) to use an external CA-signed certificate after installation”](#) on page 429.

You can view the enrollment status by running the `nbcertcmd -listEnrollmentStatus` command. The command lists only those records where the subject name matches that of the certificate that is configured for the `ECA_CERT_PATH` option.

The following enrollment statuses are displayed:

- Not enrolled - The external certificate is not enrolled with this primary server domain. The primary server is present in primary server list in the `SERVER` option.
- To be updated - The external certificate is required to be enrolled again with this primary server domain.
- Enrolled - The external certificate is enrolled with the primary server.

See [“Enrolling an external certificate for a remote host”](#) on page 431.

Configure an external certificate for the NetBackup web server

Note: Before enrolling the certificate for the primary server, ensure that you complete the prerequisite steps as described in the following topic.

See [“Workflow to use external certificates for NetBackup host communication”](#) on page 402.

By default, NetBackup uses the security certificates that the NetBackup CA has issued. If you have a certificate that an external CA has issued, you can configure the NetBackup web server to use it for secure communication.

Note: Windows certificate store is not supported as certificate source for the NetBackup web server.

The API that you can use to configure the external certificate for the NetBackup web server: `POST security/web-certificates/{certificate_id}`.

If external certificate for the web server is configured using the API, the configuration process is audited.

To configure an external certificate for the web server

- 1 Ensure that you have valid certificate, private key of the certificate, and trusted CA bundle.
- 2 Ensure that the NetBackup Web Management Console service is up and running.
- 3 Run the following command:

```
configureWebServerCerts -addExternalCert -webUI -certPath
certificate path -privateKeyPath private key path -trustStorePath
CA bundle path [-passphrasePath passphrase file path]
```

The `configureWebServerCerts` command does not support use of Windows certificate store paths.

Refer to the [NetBackup Commands Reference Guide](#) for more details on the command-line options.

- In a clustered setup, to avoid a failover run the following command on the active node:

```
install_path/netbackup/bin/bpclusterutil -freeze
```

- If the FIPS mode is enabled on the primary server, you can use only the PEM-formatted files for the `configureWebServerCerts` command.

- 4 Restart the NetBackup Web Management Console service to reflect the changes.

On UNIX, run the following commands:

- `install_path/netbackup/bin/nbwmc -terminate`
- `install_path/netbackup/bin/nbwmc start`

On Windows, use the **Services** application in the **Windows Control Panel**.

Location of the commands:

Windows `install_path\NetBackup\wmc\bin\install\`

UNIX `install_path/wmc/bin/install`

- In a clustered setup, unfreeze the cluster using the following command on the active node:

```
install_path/netbackup/bin/bpclusterutil -unfreeze
```

- 5 Restart the NetBackup Messaging Queue Broker (`nbmqbroker`) service as follows:
 On Windows:
 Go to the **Services** application in the **Windows Control Panel** and manually restart the NetBackup Messaging Queue Broker service.
 On UNIX:
 Run the following command:

```
nbmqbroker stop; nbmqbroker start
```
- 6 Verify that you can access the NetBackup web user interface using a browser, without a certificate warning message.

Update or renew the external certificate for the web server

You can update or renew the external certificate that you configured for the web server.

To update or renew the external certificate for the web server

- 1 Ensure that you have the latest external certificate, the matching private key, and the CA bundle file.
- 2 Run the following command (in a clustered setup, run the command on the active node):

```
configureWebServerCerts -addExternalCert -webUI -certPath
certificate path -privateKeyPath private key path -trustStorePath
CA bundle path
```

Remove the external certificate configured for the web server

You can remove the external certificate that is configured for the NetBackup web server. NetBackup then uses the NetBackup CA-signed certificate for secure communication.

The API that you can use to remove the external certificate for the NetBackup web server: `DELETE security/web-certificates/{certificate_id}`.

To remove the external certificate configured for the web server

- 1 Ensure that the NetBackup Web Management Console service is up and running.
- 2 Run the following command (in a clustered primary server setup, run this command on the active node):

```
configureWebServerCerts -removeExternalCert -webUI
```

Refer to the [NetBackup Commands Reference Guide](#) for more details on the command-line options.

- In a clustered primary server setup, run the following command on the active node to freeze the cluster to avoid a failover:

```
install_path/netbackup/bin/bpclusterutil -freeze
```

3 Restart the NetBackup Web Management Console service.

- In a clustered primary server setup, run the following command on the active node to unfreeze the cluster:

```
install_path/netbackup/bin/bpclusterutil -unfreeze
```

4 Restart the NetBackup Messaging Queue Broker (nbmqbroker) service as follows:

On Windows:

Go to the **Services** application in the **Windows Control Panel** and manually restart the NetBackup Messaging Queue Broker service.

On UNIX:

Run the following command:

```
nbmqbroker stop; nbmqbroker start
```

Configuring the primary server to use an external CA-signed certificate

A NetBackup host ID-based certificate is deployed on the primary server during installation or upgrade. You can configure the primary server to use an external CA-signed certificate after installation. It includes:

- Defining the external certificate configuration options
See [“Configuration options for external CA-signed certificates”](#) on page 404.
- Enrolling the external certificate for the primary server host
The enrolled certificate is used for communication between the host and the primary server domain that is listed in the `SERVER` configuration option on the host.

See [“Viewing external CA-signed certificates in the NetBackup web UI”](#) on page 432.

See [“Configuring an external certificate for a clustered primary server”](#) on page 445.

Important notes

- Ensure that the NetBackup domain is enabled to use external CA-signed certificates by configuring the NetBackup web server.
See [“Configure an external certificate for the NetBackup web server”](#) on page 423.
- External certificates for the NetBackup web server and the primary server must be issued by the same root certificate authority.
If the two certificate authorities do not match, communication between the **NetBackup BAR Console** and the NetBackup Web Management Console service (`nbwmc` service) fails.
- Ensure that the certificate revocation lists (CRLs) for the external CA are stored at the required location.
If CRL distribution point (CDP) is used, ensure that the URLs that are specified in the CDP are accessible.
See [“About certificate revocation lists for external CA”](#) on page 419.
- When NetBackup primary server is configured to use the service user (non-privileged user on UNIX and Local Service on Windows) to start most of the daemons or services, you must ensure that the following ECA paths are accessible to the service user:
 - `ECA_CERT_PATH`
 - `ECA_PRIVATE_KEY_PATH`
 - `ECA_TRUST_STORE_PATH`
 - `ECA_KEY_PASSPHRASEFILE` (optional)
 - `ECA_CRL_PATH` (optional)

See [“About a NetBackup service user account”](#) on page 589.

To grant access to the service user, do the following:

On Unix, use the `chmod` or the `chown` command.

On Windows run the following command:

```
install_path\NetBackup\bin\goodies\nbserviceusercmd.exe -addAcl
ECA path -reason reason
```

To configure the primary server to use an external certificate

- 1 Update the NetBackup configuration file (`bp.conf` file on UNIX or Windows registry) on the primary server with the external certificate-specific parameters.
See [“Configuration options for external CA-signed certificates”](#) on page 404.

For Windows certificate store Use the `nbsetconfig` command to configure the following parameters:

- `ECA_CERT_PATH`
- `ECA_CRL_CHECK` (optional)
- `ECA_CRL_PATH` (optional)
- `ECA_CRL_PATH_SYNC_HOURS` (optional)
- `ECA_CRL_REFRESH_HOURS` (optional)
- `ECA_DR_BKUP_WIN_CERT_STORE` (optional)

For file-based certificates Use the `nbsetconfig` command to configure the following parameters:

- `ECA_CERT_PATH`
- `ECA_PRIVATE_KEY_PATH`
- `ECA_TRUST_STORE_PATH`
- `ECA_KEY_PASSPHRASEFILE` (optional)
- `ECA_CRL_CHECK` (optional)
- `ECA_CRL_PATH` (optional)
- `ECA_CRL_PATH_SYNC_HOURS` (optional)
- `ECA_CRL_REFRESH_HOURS` (optional)

Note: If you have a Flex Appliance application instance, the certificate files must be stored in the following directories on the instance:

`ECA_CERT_PATH`, `ECA_PRIVATE_KEY_PATH`, and
`ECA_TRUST_STORE_PATH`: `/mnt/nbdata/hostcert/`
`ECA_CRL_PATH`: `/mnt/nbdata/hostcert/crl`

- 2 Run the following command on the primary server to enroll an external certificate with the primary server domain that is defined in the `SERVER` option:

```
nbcertcmd -enrollCertificate
```

For more details on the command, refer to the [NetBackup Commands Reference Guide](#).

Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate after installation

A NetBackup host (media server or client) is configured to use an external certificate during installation or upgrade. You may choose to do the configuration after installation.

Use this section to configure a host to use an external certificate.

You can use this section to configure an external certificate for a cluster node.

See [“About external certificate configuration for a clustered primary server”](#) on page 440.

The configuration steps include:

- Defining the external certificate configuration options
See [“Configuration options for external CA-signed certificates”](#) on page 404.
- Ensuring that automatic enrollment is enabled - `ECA_DISABLE_AUTO_ENROLLMENT` is set to `TRUE` - or enrolling the external certificate manually for the host
See [“Enrolling an external certificate for a remote host”](#) on page 431.
The enrolled certificate is used for communication between the host and the primary server domain that is listed in the `SERVER` configuration option on the host.

The enrolled certificate is used for host communication.

See [“Viewing external CA-signed certificates in the NetBackup web UI”](#) on page 432.

Important notes

- Ensure that the NetBackup domain is enabled to use external CA-signed certificates by configuring the NetBackup web server.
See [“Configure an external certificate for the NetBackup web server”](#) on page 423.
- It is recommended that you enroll an external certificate for the primary server host before you enroll one for other hosts.
See [“Configuring the primary server to use an external CA-signed certificate”](#) on page 426.
- Ensure that the certificate revocation lists (CRLs) for the external CA are stored at the required location.
If CRL distribution point (CDP) is used, ensure that the URLs that are specified in the CDP are accessible.
See [“About certificate revocation lists for external CA”](#) on page 419.

To configure a host (media server or client) to use an external certificate

- 1 Update the configuration file (`bp.conf` file or Windows registry) with the required external certificate-specific parameters on the host:

See [“Configuration options for external CA-signed certificates”](#) on page 404.

For Windows certificate store	Use the <code>nbsetconfig</code> command to configure the following parameters:
----------------------------------	--

- `ECA_CERT_PATH`
- `ECA_CRL_CHECK` (optional)
- `ECA_CRL_PATH` (optional)
- `ECA_CRL_PATH_SYNC_HOURS` (optional)
- `ECA_CRL_REFRESH_HOURS` (optional)
- `ECA_DR_BKUP_WIN_CERT_STORE` (optional)

For file-based certificates

Use the `nbsetconfig` command to configure the following parameters:

- `ECA_CERT_PATH`
- `ECA_PRIVATE_KEY_PATH`
- `ECA_TRUST_STORE_PATH`
- `ECA_KEY_PASSPHRASEFILE` (optional)
- `ECA_CRL_CHECK_LEVEL` (optional)
- `ECA_CRL_PATH` (optional)
- `ECA_CRL_PATH_SYNC_HOURS` (optional)
- `ECA_CRL_REFRESH_HOURS` (optional)

Note: If you have a Flex Appliance application instance, the certificate files must be stored in the following directories on the instance:

`ECA_CERT_PATH`, `ECA_PRIVATE_KEY_PATH`, and
`ECA_TRUST_STORE_PATH`: `/mnt/nbdata/hostcert/`
`ECA_CRL_PATH`: `/mnt/nbdata/hostcert/crl`

- 2 Ensure that the `ECA_DISABLE_AUTO_ENROLLMENT` option is set to `TRUE` using the `nbgetconfig` command. This ensures that automatic enrollment is enabled.

If the option is disabled and you want to manually enroll the certificate, run the following command on the host to enroll an external certificate with the primary server domain that is defined in the `SERVER` configuration option on the host:

```
nbcertcmd -enrollCertificate
```

See [“About viewing enrollment status of primary servers”](#) on page 422.

For more details on the command, refer to the *NetBackup Commands Reference Guide*.

Enrolling an external certificate for a remote host

Use this section to enroll an external certificate for a NetBackup host remotely. This lets the security administrator to enroll external certificate for multiple remote hosts from the same host.

To enroll an external certificate for a remote host (or to perform an enrollment sync operation on a remote host), ensure that the server from which you want to enroll the certificate is listed in the `SERVER` configuration option on the remote host.

To enroll certificate for a remote host

- ◆ Run the following command on the local host:

```
nbcertcmd -enrollCertificate -remoteHost remote_host_name -server
primary_server_name
```

An external certificate is enrolled for the specified remote host with the primary server that you provide with the `-server` option. This primary server must be available in the remote host's `SERVER` configuration option.

See [“Configuration options for external CA-signed certificates”](#) on page 404.

For more details on the commands, refer to the *NetBackup Commands Reference Guide*.

Viewing the certificate authorities that your NetBackup domain supports

The **Master server certificate configuration** option in the **NetBackup BAR Console** and on the **NetBackup Web UI** displays the certificate authorities - NetBackup CA, external CA, or both - that your NetBackup domain supports.

- In the **NetBackup BAR Console**, expand **Security Management > Global Security Settings** and click the **Secure Communication** tab to view the supported certificate authorities.
- On the **NetBackup Web UI**, click the **Global Security Settings** option to view the supported certificate authorities.

Viewing external CA-signed certificates in the NetBackup web UI

You can view a list of external certificates that are issued to hosts in your domain using the **NetBackup web UI > Security > Certificates** screen.

For more information, refer to the *NetBackup Web UI Administrator's Guide*.

Renewing a file-based external certificate

Use this section to renew a file-based external certificate.

While you replace the certificate, private key, and passphrase files one by one with all the services up, communication may fail because of mismatch in the certificate

- private key pair. To avoid any communication failure, create copies of the files that NetBackup can use if there is a mismatch in the files.

To renew a file-based external certificate

- 1 Make a copy of the certificate file and rename it with `.old` extension.
For example, if the certificate file name is `cert.pem`, rename it as `cert.pem.old`.
- 2 Make a copy of the private key file and rename it with `.old` extension.
- 3 Carry out the following step if the certificate's private key is encrypted.
Make a copy of the passphrase file and rename it with `.old` extension.
- 4 Replace the original certificate, private key, and passphrase files with the renewed certificate, private key, and passphrase files.
- 5 Restart the NetBackup services.
- 6 Ensure that the host communication is successful with the renewed certificate and then delete the old certificate files.

Configuring rotation of external CA-issued certificates for host communication

Rotation of external CA-signed certificates can now be configured using the NetBackup web UI and APIs.

This operation can be performed by a security administrator or a user with appropriate RBAC permissions. It is used to rotate external CA-issued certificates for BYO, Flex (including WORM containers), NetBackup Appliance, NetBackup Snapshot Manager hosts, and clustered primary server setups.

The operation is audited.

Terminology

- ECA - External certificate authority
- Certificate artifacts - refers to a set of certificates and associated information that is required for secure communication. Certificate artifacts include:
 - Certificate chain
 - Private key
 - Trust store
 - Passphrase

- CRL check level (default : LEAF)

Important notes

- External CA-issued certificate rotation is not supported for NetBackup Cloud Scale and NetBackup Flex Scale.
- If a host is configured to use Windows Certificate Store, it starts using file-based certificates after certificate renewal.
- It is advised that certificate rotation should be performed only under maintenance mode. Else, backup or restore jobs may fail.
- Migration from NetBackup CA to external CA is not supported using these APIs.

Prerequisites

- You should ensure that external certificates are already enrolled on the host before you configure certificate rotation.
See [“Configuring a NetBackup host \(media server, client, or cluster node\) to use an external CA-signed certificate after installation”](#) on page 429.
- To rotate external certificates using web UI or APIs for a particular host, it must have already enrolled valid external certificate.
- The new certificate should have the same subject name as that of what is configured on the host. Except, when the setting `externalCertificateIdentityField` is enabled, in which case the subject name can be different but common name has to be the same.
- Only CDP is supported as a CRL check for the certificate.
If CRL check level is not DISABLE, upload of external certificate artifacts will fail in case CRL is not accessible from the primary server.
- In case the CRLs are not accessible on the host, the host might not be able to connect to the primary after upload of external certificate artifacts , and the rotation of certificates might get stuck in an intermediate state.
- CRL check level should be disabled if the certificate does not have a valid CDP URL, or it is not accessible by the host or the primary server.
- The certificate chain size should be less than 40 KB. Else, the rotation process may fail during validation.

Workflow for external CA-signed certificate rotation process

Using the NetBackup web UI, you can upload certificate artifacts for a host. The rotation process is triggered when the client host uses the `loginwithcert` function every 24 hours. This triggers a chain of processes on the host as follows:

- Downloading the certificate artifacts by the client
- Performing validation of artifacts in a dry run with the primary server
- Moving the files to the final location
- Updating the configuration

As for the server, it retains these artifacts for 30 days. They are deleted earlier than 30 days if they are successfully downloaded and applied on the client host.

When the renewal process is complete, the certificates are automatically cleaned up. If a host does not connect to the primary server for 30 days, the artifacts for such host are cleaned up from the primary server.

You can check the current state of the certificate rotation process that is available in the **External certificates** tab, as part of the new **Renewal status** column.

See [“View certificate renewal status for a host”](#) on page 436.

Restrictions for uploading the certificate artifacts for rotation

- Flex deployments only support certificate artifacts in PEM X509 format.
- The upload option is not allowed for back-level hosts, and hosts that don't have ECA configured.
- If the domain is in FIPS mode, ensure that the FIPS compliance is in place, for example certificate formats and key sizes are compliant.

Location of the certificates

The certificate artifacts are stored in the CMS on the server. After they are downloaded, they are stored at the following location:

For a clustered primary server host (virtual):

CA certificate path - *Install_Path/var/global/vxss/*

Certificate chain, private key, passphrase path -

Install_Path/var/global/vxss/credentials/ecaartifacts/

For other hosts (including nodes of clustered primary server):

CA certificate path - *Install_Path/var/vxss/*

Certificate chain, private key, passphrase path -

Install_Path/var/vxss/credentials/ecaartifacts/

Configure rotation of external certificates for a host

To configure rotation of external certificate of a host

- 1 Sign into the NetBackup web UI using the security administrator account.
- 2 In the left pane, click **Security > Certificates > External certificates** tab.
The tab lists all the hosts and their external certificates.
- 3 Select the host for which you want to configure rotation of external certificates and click **Actions > Upload**.

Provide the following certificate artifacts:

- Certificate
- Private key
- Passphrase
- Trust store
- CRL check level: leaf, chain, or none

- 4 Click **Upload**.

View certificate renewal status for a host

You can view certificate renewal status for a host.

To view certificate renewal status

- 1 Sign into the NetBackup web UI using the security administrator account.
- 2 In the left pane, click **Security > Certificates > External certificates** tab.
- 3 Select a host to view the associated certificate renewal status.

An external certificate can have one of the following renewal statuses:

- N/A: Specifies that no active certificate renewal for this host is in progress or the renewal completed in the last 7 days.
- Failed: Specifies that the certificate renewal for this host has failed.
- In progress: Specifies that the certificate renewal for this host is in progress.
- Completed: Represents that the certificate renewal for this host completed in the past 7 days.

Delete uploaded certificate artifacts for a host

You can delete uploaded certificate artifacts from the CMS database.

Note: Uploaded certificate artifacts cannot be deleted if the artifacts are downloaded by a host and the renewal process is started but not yet complete or has failed.

To delete uploaded certificate artifacts

- 1 Sign into the NetBackup web UI using the security administrator account.
- 2 In the left pane, click **Security > Certificates > External certificates** tab.
- 3 Select the host for which you want to delete certificate artifacts and click **Actions > Delete renewal artifacts**.

Removing certificate enrollment

You can remove the external certificate enrollment with a certain primary server if you do not want to use the certificate for host communication.

To remove certificate enrollment

- ◆ Run the following command:

```
nbcertcmd -removeEnrollment -server primary_server_name
```

Disabling the NetBackup CA in a NetBackup domain

Use this section to disable the existing NetBackup CA support from your domain when all the hosts in your domain are configured to use external certificates for host communication.

Note: If you have NAT clients in your environment and the NetBackup Messaging Broker (`nbmqbroker`) service is enabled, you may need to restart the service after you disable the NetBackup CA to use external certificates only.

For more information about NAT support in NetBackup, refer to the [NetBackup Administrator's Guide, Volume I](#).

If you have hosts that can communicate securely but cannot be configured to use external certificates (NetBackup 8.1, 8.1.1, or 8.1.2), you should not disable NetBackup CA configuration to avoid communication failure.

To disable NetBackup CA support in your domain

- 1 Ensure that all the hosts in your domain are configured to use external certificates.

 See [“Configure an external certificate for the NetBackup web server”](#) on page 423.

 See [“Configuring the primary server to use an external CA-signed certificate”](#) on page 426.

 See [“Configuring a NetBackup host \(media server, client, or cluster node\) to use an external CA-signed certificate after installation”](#) on page 429.
- 2 After each host in the domain is configured to use external certificates, remove the NetBackup CA support from each host (media servers and clients) in the domain.

 Run the following commands on each host in the given order:
 - `nbcertcmd -removeCACertificate -fingerPrint NetBackup CA certificate fingerprint`
 - `nbcertcmd -deleteCertificate -hostid host ID of the host`
- 3 Remove the NetBackup CA support from the primary server.

 Run the following commands on the primary server in the given order:
 - `nbcertcmd -removeCACertificate -fingerPrint NetBackup CA certificate fingerprint`
 - `nbcertcmd -deleteCertificate -hostid host ID of the primary server`
- 4 Revoke all host ID-based certificates in the domain. This is an optional step.

 See [“Revoking a host ID-based certificate”](#) on page 339.
- 5 Remove the NetBackup CA support from the web server. Ensure that you do not need the NetBackup certificates for host communication.

 Run the following command on the web server:


```
configureWebServerCerts -removeNBCert
```

For more information about the commands, refer to the [NetBackup Commands Reference Guide](#).
- 6 Restart the NetBackup Web Management Console (`nbwmc`) service.

Enabling the NetBackup CA in a NetBackup domain

Use this section to enable a NetBackup domain to use NetBackup CA-signed certificates (or host ID-based certificates) for host communication.

To enable a NetBackup domain to support NetBackup CA configuration

- 1 Configure the NetBackup web server to use NetBackup (host ID-based) certificates.
 - Run the following command:

```
configureWebServerCerts -addNBCert
```

 See [“Configure an external certificate for the NetBackup web server”](#) on page 423.
 - Restart the NetBackup Web Management Console (`nbwmc`) service.
- 2 Deploy a NetBackup host ID-based certificate on the primary server:
 See [“Deploying host ID-based certificates”](#) on page 312.
- 3 Deploy a NetBackup host ID-based certificate on each host.
 See [“Deploying host ID-based certificates”](#) on page 312.

Disabling an external CA in a NetBackup domain

Use this section to disable an external CA in a NetBackup domain.

To disable an external CA

- 1 Ensure that each host in the domain is configured to use NetBackup host ID-based certificates.
- 2 Remove all the external certificate configuration options from the configuration file (`bp.conf` on UNIX or Windows registry), which exists on the host.
 For example, `ECA_CERT_PATH`.
 See [“Configuration options for external CA-signed certificates for a virtual name”](#) on page 442.
- 3 Remove the external CA support from the primary server.
 - Remove all the external certificate configuration options from the configuration file (`bp.conf` on UNIX or Windows registry), which exists on the primary server.
 For example, `ECA_CERT_PATH`.

See [“Configuration options for external CA-signed certificates for a virtual name”](#) on page 442.

- 4 Delete all external certificate entries from the NetBackup database.

Run the following command:

```
nbcertcmd -deleteECACertEntry -subject subject name of the certificate
```

- 5 Remove the external CA support from the web server.

```
configureWebServerCerts -removeExternalCert
```

For more information about the commands, refer to the [NetBackup Commands Reference Guide](#).

- 6 Remove the certificate enrollment using the following command:

```
nbcertcmd -removeEnrollment
```

Changing the subject name of an enrolled external certificate

Use this section if you want to change the subject name of an already enrolled external certificate of a host.

To change the subject name of an enrolled external certificate

- 1 Change the subject name of the certificate.
- 2 If the host is part of multiple primary server domains, you need to carry out this step for all primary servers.

Do one of the following:

- Run the following command to manually enroll the certificate:

```
Install_Path/bin/nbcertcmd -enrollCertificate
```

- Run following command to remove the existing enrollment:

```
Install_Path/bin/nbcertcmd -removeEnrollment
```

About external certificate configuration for a clustered primary server

You can now use X.509 certificates that your trusted certificate authority (CA) has issued, for a clustered primary server.

You should first enable your NetBackup domain to use external CA-signed certificates by configuring the NetBackup web server.

You can then configure the NetBackup clustered primary server to use external CA-signed certificates for secure host communication.

See [“Workflow to use external certificates for a clustered primary server”](#) on page 441.

Important notes

Review the following notes before you configure NetBackup to use external certificates:

- NetBackup certificate or host ID-based certificate is deployed on the primary server during NetBackup installation. You need to manually configure an external certificate on the clustered primary server after installation.
- In a clustered primary server setup, you require to configure one external certificate for each cluster node, which resides on the local disk of each node. Additionally, you need to configure one certificate for the virtual name, which resides on the shared disk of the cluster.
- The NetBackup configuration options (for example, `CLUSTER_ECA_CERT_PATH`) that are required for external certificate enrollment for the virtual name are stored in the `nbc1.conf` file. This file resides on the shared disk and external certificate configuration options for each cluster node are stored in the `bp.conf` file or Windows registry.
- Windows certificate store is not supported as an external certificate source for virtual name. It can be used as a source for certificates for cluster nodes.
- There is no separate CRL configuration option for the virtual name. Based on the `ECA_CRL_CHECK` configuration option on the node, certificate revocation lists (CRLs) - `ECA_CRL_PATH` or CDP - of the cluster nodes are used to verify the revocation status of the peer host's certificate during communication. Therefore, the CRL configuration options should be set before using an external certificate for the primary server virtual name.

See [“About certificate revocation lists for external CA”](#) on page 419.

Workflow to use external certificates for a clustered primary server

To configure NetBackup to use external CA-signed certificates for secure communication, you should carry out the following steps in the given order:

Table 21-13 Workflow to use external certificates in a cluster setup

Step	Process
1	Ensure the following: ■ The certificate for the virtual name is placed at the appropriate location on the shared disk. ■ The external certificates for cluster nodes are placed at the appropriate locations on the nodes. ■ The CRLs are placed at the required locations on the nodes as per their CRL configuration options and are accessible. See “About certificate revocation lists for external CA” on page 419.
2	Install NetBackup software or upgrade the existing software on each cluster node.
3	Enable the NetBackup domain to use external certificates by configuring the NetBackup web server. See “Configure an external certificate for the NetBackup web server” on page 423.
4	Configure an external certificate for the virtual name and for each cluster node. See “Configuring an external certificate for a clustered primary server” on page 445.

Configuration options for external CA-signed certificates for a virtual name

To configure a clustered NetBackup primary server to use external CA-signed certificate for host communication, you must define certain configuration options in the `nbcl.conf` file.

CLUSTER_ECA_CERT_PATH for clustered primary server

The `CLUSTER_ECA_CERT_PATH` option is specific to clustered primary server. It specifies the path to the external CA-signed certificate of the virtual name.

Table 21-14 `CLUSTER_ECA_CERT_PATH` information

Usage	Description
Where to use	On clustered primary server.

Table 21-14 CLUSTER_ECA_CERT_PATH information (*continued*)

Usage	Description
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: <pre>CLUSTER_ECA_CERT_PATH = Path to the certificate of the virtual identity</pre>
Equivalent NetBackup web UI property	No equivalent exists in the host properties.

CLUSTER_ECA_TRUST_STORE_PATH for clustered primary server

The `CLUSTER_ECA_TRUST_STORE_PATH` option is specific to clustered primary server. It specifies the path to the certificate bundle file that contains all trusted root CA certificates in PEM format.

Table 21-15 CLUSTER_ECA_TRUST_STORE_PATH information

Usage	Description
Where to use	On clustered primary server.
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: <pre>CLUSTER_ECA_TRUST_STORE_PATH = Path to the external CA certificate</pre>
Equivalent NetBackup web UI property	No equivalent exists in the host properties.

CLUSTER_ECA_PRIVATE_KEY_PATH for clustered primary server

The `CLUSTER_ECA_PRIVATE_KEY_PATH` option is specific to clustered primary server. It specifies the path to the private key for the external CA-signed certificate of the virtual name.

If the virtual name certificate's private key is encrypted, you should define the `CLUSTER_ECA_KEY_PASSPHRASEFILE` option.

See [“CLUSTER_ECA_KEY_PASSPHRASEFILE for clustered primary server”](#) on page 444.

Table 21-16 `CLUSTER_ECA_PRIVATE_KEY_PATH` information

Usage	Description
Where to use	On clustered primary server.
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: <pre>CLUSTER_ECA_PRIVATE_KEY_PATH = Path to the private key of the external certificate</pre>
Equivalent NetBackup web UI property	No equivalent exists in the host properties.

CLUSTER_ECA_KEY_PASSPHRASEFILE for clustered primary server

The `CLUSTER_ECA_KEY_PASSPHRASEFILE` option is specific to clustered primary server. It specifies the path to the text file where the passphrase for the virtual name certificate's private key is stored.

`CLUSTER_ECA_KEY_PASSPHRASEFILE` is optional. You should define this option if the virtual name certificate's private key is encrypted.

See [“CLUSTER_ECA_PRIVATE_KEY_PATH for clustered primary server”](#) on page 444.

Table 21-17 CLUSTER_ECA_KEY_PASSPHRASEFILE information

Usage	Description
Where to use	On clustered primary server.
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: <pre>CLUSTER_ECA_KEY_PASSPHRASE_FILE = Path to the passphrase file</pre>
Equivalent NetBackup web UI property	No equivalent exists in the host properties.

Configuring an external certificate for a clustered primary server

Use this section to configure an external CA-signed certificate for a clustered primary server. The enrolled certificate is used for host communication.

Requirements

- Ensure that the NetBackup domain is enabled to use external CA-signed certificates by configuring the NetBackup web server.
See [“Configure an external certificate for the NetBackup web server”](#) on page 423.
- Ensure that external certificates for the NetBackup web server and the virtual name are issued by the same certificate authority.
If the two certificate authorities do not match, communication between the **NetBackup BAR Console** and the NetBackup Web Management Console service (`nbwmc` service) fails.

To enroll an external certificate for a clustered primary server

- 1 Update the NetBackup configuration file that is present on the shared disk (`nbcl.conf`) with the external certificate configuration options.

See [“Configuration options for external CA-signed certificates for a virtual name”](#) on page 442.

Use the `nbsetconfig` command to configure the following options:

- `CLUSTER_ECA_CERT_PATH`
- `CLUSTER_ECA_TRUST_STORE_PATH`

- `CLUSTER_ECA_PRIVATE_KEY_PATH`
- `CLUSTER_ECA_KEY_PASSPHRASEFILE` (optional)

You need to configure the certificate revocation list (CRL) configuration options for each node.

See [“About certificate revocation lists for external CA”](#) on page 419.

- 2** Run the following command on the primary server:

```
nbcertcmd -enrollCertificate -cluster
```

The enrolled certificate is used for communication between the active node and the primary server domain that is listed in the `SERVER` configuration option on the host.

For more details on the command, refer to the *NetBackup Commands Reference Guide*.

- 3** Configure an external certificate on each cluster node.

See [“Configuring a NetBackup host \(media server, client, or cluster node\) to use an external CA-signed certificate after installation”](#) on page 429.

Regenerating keys and certificates

This chapter includes the following topics:

- [About regenerating keys and certificates](#)
- [Regenerating NetBackup authentication broker keys and certificates](#)
- [Regenerating host identity keys and certificates](#)
- [Regenerating web service keys and certificates](#)
- [Regenerating nbcertservice keys and certificates](#)
- [Regenerating web server keys and certificates](#)
- [Regenerating JWT keys](#)
- [Regenerating NetBackup gateway certificates](#)
- [Regenerating web trust store certificates](#)
- [Regenerating VMware vCenter plug-in certificates](#)
- [Regenerating NetBackup Administrator Console session certificates](#)
- [Regenerating NetBackup encryption key file](#)

About regenerating keys and certificates

Some of the keys and certificates can be recreated by simply restarting the NetBackup services. If you encounter any error related to keys or certificates, as a best practice, restart the NetBackup services and verify if the keys or the certificate

is recreated. If the key or certificate is not created proceed with the procedures mentioned in the following sections.

Regenerating NetBackup authentication broker keys and certificates

Follow the steps to regenerate NetBackup Authentication Brokers:

- Public and private keys on primary server and media server.
- Certificates on the media server and clients.

To regenerate NetBackup authentication broker keys and certificates

- 1 Restart the NetBackup Authentication service. Ensure that the service is up and running.
- 2 Run the following command:

```
bpbaz -ConfigureAuth
```

Answer **y** when prompted.

For information on the command, see *NetBackup Commands Reference Guide*.

- 3 Restart all the NetBackup services. Before you restart the services, ensure that no jobs are running.

For information on how to restart the services, see the *NetBackup Administrator's Guide, Volume I*.

Regenerating host identity keys and certificates

To regenerate host identity public keys, private keys, and certificates on the primary server, media server, and clients:

- Change the key pair for a host.
Changing a key pair results in both a new host ID-based certificate and a new host name-based certificate.
See [“Changing the key pair for a host”](#) on page 329.

Regenerating web service keys and certificates

Follow the steps to regenerate web service public key and certificate on the primary server.

To regenerate web service keys and certificates

- 1 Generate the security certificate. Run the following command:
 - Windows


```
set WEBSVC_PASSWORD=<Password of User>
nbcertconfig -t -user <User Name>
```
 - UNIX


```
export WEBSVC_PASSWORD=<Password of User>
nbcertconfig -t -user <User Name>
```
- 2 Configure NetBackup Authentication service for the web service user and web service. Run the following command:


```
nbcertconfig -u -user <username>
nbcertconfig -m -user <username>
```
- 3 Restart the NetBackup Authentication service.

Regenerating nbcertservice keys and certificates

Follow the steps to regenerate nbcertservice keys and certificates on the primary server.

To regenerate nbcertservice keys and certificates

- 1 Remove the old folder with user name.
- 2 Generate the security certificate. Run the following command:
 - Windows


```
set WEBSVC_PASSWORD=<Password of User>
nbcertconfig -u -user <User Name>
```
 - UNIX


```
export WEBSVC_PASSWORD=<Password of User>
nbcertconfig -u -user <User Name>
```

Regenerating web server keys and certificates

Follow the steps to regenerate Tomcat web server public key, private key, and certificates on the primary server.

Note: The jkskey is a key to decrypt the keystore used by tomcat and is backed up as part of the catalog backup. There is no need to regenerate it.

To regenerate tomcat keys and certificates

- 1 Generate the security certificate. Run the following command:
 - Windows

```
set WEBSVC_PASSWORD=<Password of User>
nbcertconfig -t -user <User Name>
```
 - UNIX

```
export WEBSVC_PASSWORD=<Password of User>
nbcertconfig -t -user <User Name>
```
- 2 Regenerate other files in `tomcatcreds` folder apart from the `keystore` and the `credentials` file. Run the following command:
 - Windows

```
Install_Path\NetBackup\wmc\bin\install>configurecerts.bat
```
 - UNIX

```
/usr/openv/wmc/bin/install/configurecerts
```

Regenerating JWT keys

Use this topic to regenerate JWT public and private keys on the primary server:

To regenerate JWT public and private keys

- 1 Stop NetBackup services.
- 2 Delete `/usr/openv/var/global/vxss/jwtkeys/jwtPublicKey`
- 3 Delete `/usr/openv/var/global/vxss/jwtkeys/private/jwtPrivateKey`
- 4 Start NetBackup services. This creates a new public and private key pair.

For information on how to stop and start the services, see *NetBackup Administrator's Guide, Volume I*.

Regenerating NetBackup gateway certificates

To regenerate nbgateway certificates on the primary server:

- Restart all the NetBackup service.
For information on how to restart the services, see *NetBackup Administrator's Guide, Volume I*.

Regenerating web trust store certificates

To regenerate web trust store certificates on the primary and media server, run the following command:

```
nbcertcmd -getCACertificate
```

Answer **y** when prompted.

For information on the nbcertcmd command, see *NetBackup Commands Reference Guide*.

Regenerating VMware vCenter plug-in certificates

Follow the steps to regenerate vCenter plug-in certificates on the primary server.

To regenerate VMware vCenter plug-in certificates

- 1 List the existing certificates and identify the existing entry for invalid certificates. Run the following command:

- Windows

```
Install_Path\NetBackup\wmc\bin\install\manageClientCerts.bat  
-list
```

- UNIX

```
/usr/opensv/wmc/bin/install/manageClientCerts -list
```

- 2 Delete the invalid certificate. Run the following command:

- Windows

```
Install_Path\NetBackup\wmc\bin\install\manageClientCerts.bat  
-delete
```

- UNIX

```
/usr/opensv/wmc/bin/install/manageClientCerts -delete
```

- 3 Generate a new certificate. Run the following command:

- Windows

```
Install_Path\NetBackup\wmc\bin\install\manageClientCerts.bat  
-create <master_server_name>
```

- UNIX

```
/usr/opensv/wmc/bin/install/manageClientCerts -create  
<master_server_name>
```

- 4 Register the newly created certificate with the vCenter plug-in.

For more information, see *NetBackup Plug-in for VMware vCenter Guide*.

Regenerating NetBackup Administrator Console session certificates

To regenerate session certificates on the primary server:

- Close the NetBackup Administrator Console and restart all the NetBackup services.

For information on how to restart the services, see *NetBackup Administrator's Guide, Volume I*.

Regenerating NetBackup encryption key file

To regenerate NetBackup encryption key file, run the following command:

```
bpkeyutil -clients client_name1,client_name2,...,client_namen
```

When you are prompted to enter the passphrase, enter the passphrase you had saved originally.

For more information about key files, see See [“About creating encryption key files on the clients”](#) on page 466.

To perform this task using the `bpkeyutil`, see *NetBackup Commands Reference Guide*.

Encryption of data at rest

- [Chapter 23. Data at rest encryption security](#)
- [Chapter 24. NetBackup key management service configuration](#)
- [Chapter 25. External key management service configuration in NetBackup](#)
- [Chapter 26. Cloud key management service configuration in NetBackup](#)
- [Chapter 27. Hardware Security Module \(HSM\) support in NetBackup](#)

Data at rest encryption security

This chapter includes the following topics:

- [Data at rest encryption terminology](#)
- [Data at rest encryption considerations](#)
- [Destination types for encryption of data at rest](#)
- [Encryption security questions to consider](#)
- [Comparison of encryption options](#)
- [About NetBackup client encryption](#)
- [Configuring standard encryption on clients](#)
- [Configuring legacy encryption on clients](#)

Data at rest encryption terminology

The following table describes the data at rest encryption terminology.

Table 23-1 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 23-1 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 23-2 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 23-2 Data at rest encryption limitations (*continued*)

Limitation	Description
FIPS certification for my encryption solution	While FIPS certification may be required for use by the US government, it should not be the only criteria that is used to evaluate an encryption solution. Other considerations should be part of any decision-making process as follows: ■ FIPS certificates only apply to the named version of a product. And then only when the product is used in conformance with the "FIPS security policy" the document that is submitted when the product was validated. Future product versions and non-standard uses would be subject to questioned validation. ■ The security of algorithms like AES is not in the obscurity of how they work. Rather the security is in the difficulty to deduce an unknown encryption key. The years of scrutiny and peer review for AES, have lead to mature implementations. In fact, tests exist for AES where specific keys and data sets are input, and verified against the expected output. ■ Data encryption is much like automobile security. Most problems are related to lost or misplaced keys and not related to malfunctioning locks. ■ Since misuse is more likely to lead to problems, the usability of an encryption product should be part of the consideration. Usability considerations include the following: ■ Encryption integration with the product ■ Encryption integration with business processes. ■ Appropriate encryption key granularity ■ Recoverability
Appropriate encryption key granularity	The appropriate encryption key granularity is best explained with the example of home security. A single house key is convenient. You can enter the garage, front door, or backdoor all using the same key. This security is good until the key is compromised (for example, if the key is stolen). Then you need to change all the locks that used the key. An extreme example is to have a key for every drawer and cupboard in a house. Then, a lost key would require the changing of on a single lock. The correct solution is somewhere in between. You must understand your tolerance for a compromised or lost key from your business process perspective. A lost key implies all the data that is encrypted with that key is destroyed. A compromised key implies all the data that is encrypted with that key must be decrypted and reencrypted to become secure.

Destination types for encryption of data at rest

The following destination types for encryption of data at rest are available:

- Client-side encryption
See “[About NetBackup client encryption](#)” on page 458.
- MSDP encryption
See the 'About MSDP encryption' topic from the [NetBackup Deduplication Guide](#).
- Tape drive encryption - The volume pool name must have ENCR_ as a prefix for NetBackup to enable encryption for tapes.
- Cloud encryption
See the 'About data encryption for cloud storage' topic from the [NetBackup Cloud Administrator's Guide](#).
- AdvancedDisk

Encryption security questions to consider

Before considering encryption security, the following questions should be asked.

The answers depend upon your particular encryption needs as follows:

- How do I choose the best encryption?
- Why would I use encryption security?
- What protection do I need from possible inside attacks?
- What protection do I need from possible outside attacks?
- What are the specific areas of NetBackup that encryption security protects?
- Do I need to create drawings of NetBackup architecture showing encryption security at work?
- What are my deployment use cases for encryption security?

Comparison of encryption options

The following NetBackup options exist for data at rest encryption:

- NetBackup client encryption, with standard encryption
- NetBackup client encryption, with legacy encryption
- Third-party encryption appliances and hardware devices

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

Table 23-3 Encryption options comparison

Encryption option	Potential advantages	Potential disadvantages
Client encryption, standard encryption See “Configuring standard encryption on clients” on page 463.	■ The encryption key is on the client computer and not controlled by the NetBackup administrator ■ Can be deployed without affecting the NetBackup primary and media servers ■ Can be deployed on a per client basis	■ The encryption key on the client does not scale well to environments where each client must have a unique encryption key and individual encryption key ■ Encryption and compression taking place on the client can affect client performance
Client encryption, legacy encryption See “Configuring legacy encryption on clients” on page 469.	Same advantages as client encryption with standard encryption.	Same disadvantages as client encryption with standard encryption.
Third-party encryption appliances and hardware devices	■ Little or no performance effect due to added hardware. ■ Generally NIST FIPS 140 certified.	■ The NetBackup Compatibility lab tests some of these solutions. This testing is neither an endorsement or rejection or a particular solution. This effort verifies that basic functionality was verified when used with a specific version of NetBackup. ■ No integration with NetBackup configuration, operation, or diagnostics. ■ The Disaster recovery scenario is provided by the appliance or device.

About NetBackup client encryption

The NetBackup client encryption option is best for the following:

- Clients that can handle the CPU burden for compression / encryption
- Clients that want to retain control of the data encryption keys
- Situations where the tightest integration of NetBackup and encryption is desired
- Situations where encryption is needed in terms of a per client basis

Installation prerequisites for encryption security

Encrypted backups require the NetBackup encryption software, which is included in NetBackup server and client installations. To use encryption, you must have a

valid license. Refer to the [NetBackup Administrator's Guide, Volume I](#) for details on how to administer NetBackup licenses.

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

For a list of the platforms on which you can configure NetBackup Encryption, see the [NetBackup Release Notes](#).

About running an encryption backup

You can run an encryption backup as follows:

- Choosing encryption for a backup
See [“About choosing encryption for a backup”](#) on page 459.
- Standard encryption backup process
See [“Standard encryption backup process”](#) on page 460.
- Legacy encryption backup process
See [“Legacy encryption backup process”](#) on page 461.

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 23-4 Type of backup performed

CRYPT_OPTION	Encryption policy attribute with CRYPT_OPTION	Encryption policy attribute without CRYPT_OPTION
REQUIRED	Encrypted	None

Table 23-4 Type of backup performed (*continued*)

CRYPT_OPTION	Encryption policy attribute with CRYPT_OPTION	Encryption policy attribute without CRYPT_OPTION
ALLOWED	Encrypted	Non-encrypted
DENIED	None	Non-encrypted

See [“Standard encryption backup process”](#) on page 460.

See [“NetBackup standard encryption restore process”](#) on page 461.

See [“Legacy encryption backup process”](#) on page 461.

See [“NetBackup legacy encryption restore process”](#) on page 462.

Standard encryption backup process

The prerequisites for encrypting a standard backup are as follows:

- The encryption software is automatically installed with the NetBackup UNIX or Linux server and client installations.
- A key file must exist. The key file is created when you run the `bpkeyutil` command from the server or from the client.
- The **Encryption** attribute must be selected on the NetBackup policy that includes the client.

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

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

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

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

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

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

Legacy encryption backup process

The prerequisites for encrypting a legacy backup are as follows:

- The encryption software must include the appropriate DES library, as follows:
 - For 40-bit DES encryption, `libvdes40.suffix`; the suffix is `so`, `sl`, or `dll`, depending on the client platform.
 - For 56-bit DES encryption, `libvdes56.suffix`; the suffix is `so`, `sl`, or `dll`, depending on the client platform.

Note: The encryption software is automatically installed with the NetBackup UNIX server and client installations.

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

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

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

For each backed-up file, the following occurs:

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

NetBackup standard encryption restore process

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

- The encryption software must be loaded onto the client.

Note: The encryption software is automatically installed with the NetBackup UNIX server and client installations.

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

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

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

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

NetBackup legacy encryption restore process

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

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

Note: The encryption software is automatically installed with the NetBackup UNIX server and client installations.

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

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

If the prerequisites are met, the following occurs:

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

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

Configuring standard encryption on clients

This topic describes how to configure standard NetBackup encryption.

The following configuration options are in the `bp.conf` file on UNIX clients, and in the registry on Windows clients.

The configuration options are as follows:

- `CRYPT_OPTION`
- `CRYPT_KIND`
- `CRYPT_CIPHER`

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 23-5 Three encryption-related configuration options

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

About creating encryption key files on the clients

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

- If the server is in a cluster and is also an encryption client, all nodes in the cluster must have the same key file.
- The `bpkeyutil` command sets the cipher-based encryption key file and pass phrase on each NetBackup Encryption client.
 - For a Windows server, the full path to the command is as follows:

```
install_path\NetBackup\bin\bpkeyutil
```

- For a UNIX server, the full path to the command is as follows:

```
/usr/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 include the key file in the back up to a client, add the key file's path name to the client's include list.

Redirected restores require special configuration changes to allow a restore.

Restoring an encrypted backup file to another client

Redirected restores are described in the following procedure.

To restore an encrypted backup to another client

- 1 The server must allow redirected restores, and you (the user) must be authorized to perform such restores.

See the [NetBackup Administrator's Guide, Volume I](#) for details on redirected restores.
- 2 Obtain the pass phrase that was used on the other client when the encrypted backup was made. Without that pass phrase, you cannot restore the files.

Note if the pass phrase is the same on both clients, skip to step 5.
- 3 To preserve your own (current) key file, move or rename it.
- 4 Use the `bpkeyutil` command to create a key file that matches the other client's. When the `bpkeyutil` process prompts you for the pass phrase, specify the other client's pass phrase.
- 5 Restore the files to the other client.

After you restore the encrypted files from the client, rename or delete the key file that you created in step 4.

Next, you move or rename the original key file to its original location or name. If you do not re-establish your key file to its original location and name, you may not be able to restore your own encrypted backups.

About configuring standard encryption directly on clients

You can also configure NetBackup encryption directly on clients as explained in the following topics:

- Setting standard encryption attribute in policies
See [“Setting standard encryption attribute in policies”](#) on page 469.
- Changing client encryption settings from the server
See [“Changing the client encryption settings from the NetBackup server”](#) on page 469.

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 BAR Console** to set or clear the **Encryption** attribute for a policy.

Changing the client encryption settings from the NetBackup server

You can change the encryption settings for a NetBackup client in the **Encryption** host properties for the client on the NetBackup server.

To change the client encryption settings from the NetBackup server

- 1 On the left pane, select **Host > Host properties**.
- 2 Select the name of the client you want to change. Click **Connect** and then **Edit client**.
- 3 Click **Encryption**.

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 463.

For additional explanations of the settings, 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 web UI** 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 23-6 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.
	required REQUIRED	Specifies that the client requires encrypted backups. If the server requests an unencrypted backup, it is considered an error.
CRYPT_KIND = <i>kind</i>		Defines the encryption type on NetBackup clients. The possible values for <i>kind</i> follow:

Table 23-6 Legacy encryption configuration options (*continued*)

Option	Value	Description
	NONE	Neither standard encryption nor legacy encryption is configured on the client.
	LEGACY	Specifies the legacy encryption type, either 40-bit DES or 56-bit DES. This option is the default if the legacy encryption type is configured on the client, and the standard encryption type is not configured.
	STANDARD	Specifies the cipher encryption type, which can be either 128-bit encryption or 256-bit encryption.
CRYPT_STRENGTH = <i>strength</i>		Defines the encryption strength on NetBackup clients. The possible values for <i>strength</i> follow:
	des_40 DES_40	(The default value) Specifies 40-bit DES encryption.
	des_56 DES_56	Specifies the 56-bit DES encryption.
CRYPT_LIBPATH = <i>directory_path</i>		Defines the directory that contains the encryption libraries on NetBackup clients. The <i>install_path</i> is the directory where NetBackup is installed and by default is C:\VERITAS.
	/usr/opensv/lib/	The default value on UNIX systems.
	<i>install_path</i> \NetBackup\bin\	The default value on Windows systems
CRYPT_KEYFILE = <i>file_path</i>		Defines the file that contains the encryption keys on NetBackup clients.
	/usr/opensv/var/keyfile	The default value on UNIX systems.
	<i>install_path</i> \NetBackup\var\keyfile.dat	The default value on Windows systems.

Managing legacy encryption key files

This topic describes managing legacy encryption key files.

Note: The key file must be the same on all nodes in a cluster.

Each NetBackup client that does encrypted backups and restores needs a key file. The key file contains the data that the client uses to generate DES keys to encrypt backups.

You can use the `bpkeyfile` command on the client to manage the key file. Check the `bpkeyfile` command description in the [NetBackup Commands Reference Guide](#) for a detailed description.

The first thing that you need to do is to create a key file if it does not already exist. The key file exists if you set a pass phrase from the `bpinst -LEGACY_CRYPT` command from the server to this client name.

The file name should be the same as the file name that you specified with the `CRYPT_KEYFILE` configuration option as follows:

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

```
install_path\NetBackup\var\keyfile.dat
```

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

```
/usr/opensv/var/keyfile
```

NetBackup uses a key file pass phrase to generate a DES key, and it uses the DES key to encrypt a key file.

Generally, you use the key file pass phrase that is hard-coded into NetBackup applications. However, for added security you may want to use your own key file pass phrase.

See [“Additional legacy key file security for UNIX clients”](#) on page 478.

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/var/keyfile
Enter new keyfile pass phrase: (standard keyfile pass phrase)
Re-enter new keyfile pass phrase: (standard keyfile pass phrase)
```

```
Enter new NetBackup pass phrase: *****  
Re-enter new NetBackup pass phrase: *****
```

You may enter new NetBackup pass phrases fairly often. Information about old pass phrases is kept in the key file. This method lets you restore any data that was encrypted with DES keys generated from old pass phrases. You can use the `-change_netbackup_pass_phrase` (or `-cnpp`) option on the `bpkeyfile` command to enter a new NetBackup pass phrase.

If you want to enter a new NetBackup pass phrase on a Windows client, enter a command similar to the following example:

```
bpkeyfile.exe -cnpp install_path\NetBackup\var\keyfile.dat  
Enter old keyfile pass phrase: (standard keyfile pass phrase)  
Enter new NetBackup pass phrase: *****  
Re-enter new NetBackup pass phrase: *****
```

Caution: You must ensure that pass phrases, whether they are new or were in use previously, are secure and retrievable. If a client's key file is damaged or lost, you need all of the previous pass phrases to recreate the key file. Without the key file, you cannot restore the files that were encrypted with the pass phrases.

The key file must only be accessible to the administrator of the client machine.

For a UNIX client, you must ensure the following:

- The owner is root.
- The mode bits are 600.
- The file is not on a file system that can be NFS mounted.

You must consider whether to back up your key file. For encrypted backups, such a backup has little value, because the key file can only be restored if the key file is already on the client. Instead, you can set up a NetBackup policy that does non-encrypted backups of the key files of the clients. This policy is useful you require an emergency restore of the key file. However, this method also means that a client's key file can be restored on a different client.

If you want to prevent the key file from being backed up, add the key file's path name to the client's exclude list.

About configuring legacy encryption from the server

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

Prerequisites for this method include the following:

- The NetBackup client software must be running on a platform that supports NetBackup encryption.
Refer to the *NetBackup Release Notes* for details on supported platforms.
- The NetBackup clients must be running the required NetBackup version.
- If a clustered server is a client for NetBackup encryption, ensure that all nodes in the cluster have the same key file.

The `bpinst` command is loaded into the NetBackup bin directory on the server as follows:

- For a Windows server, the bin directory is as follows

```
install_path\NetBackup\bin
```

- For a UNIX server, the bin directory is as follows

```
/usr/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 474.

See [“About pushing the legacy encryption pass phrases to clients”](#) on page 475.

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 primary server `USE_VXSS` setting in `bp.conf` should be set to `AUTOMATIC`. Use this setting when pushing from an NBAC enabled primary to a host that does not have NetBackup previously installed. Also use this setting when NBAC has not enabled the primary server's `USE_VXSS` setting in `bp.conf`.

About pushing the legacy encryption pass phrases to clients

To send a pass phrase to a NetBackup client, you can use the `bpinst` options `-passphrase_prompt` or `-passphrase_stdin`. The NetBackup client uses the pass phrase to create or update data in its key file.

The key file contains the data that the client uses to generate DES keys to encrypt backups as follows:

- If you use the `-passphrase_prompt` option, you are prompted at your terminal for a zero to 62 character pass phrase. The characters are hidden while you type the pass phrase. You are prompted again to retype the pass phrase to make sure that is the one you intended to enter.
- If you use the `-passphrase_stdin` option, you must enter the zero to 62 character pass phrase twice through standard input. Generally, the `-passphrase_prompt` option is more secure than the `-passphrase_stdin` option, but `-passphrase_stdin` is more convenient if you use `bpinst` in a shell script.

To enter a pass phrase for the client named `client1` from a NetBackup server through standard input, you would enter commands like the following:

```
bpinst -LEGACY_CRYPT -passphrase_stdin client1 <<EOF  
This pass phrase is not very secure
```

```
This pass phase is not very secure
EOF
```

To enter a pass phrase for the client named client2 from a NetBackup server, you would enter commands like the following:

```
bpinst -LEGACY_CRYPT -passphrase_prompt client2
Enter new NetBackup pass phrase: *****
Re-enter new NetBackup pass phrase: *****
```

You may enter new pass phrases fairly often. The NetBackup client keeps information about old pass phrases in its key file. It can restore the data that was encrypted with DES keys generated from old pass phrases.

Caution: You must ensure that pass phrases, whether they are new or were in use previously, are secure and retrievable. If a client's key file is damaged or lost, you need all of the previous pass phrases to recreate the key file. Without the key file, you cannot restore the files that were encrypted with the pass phrases.

You must decide whether to use the same pass phrase for many clients. Using the same pass phrase is convenient because you can use a single `bpinst` command to specify a pass phrase for each client. You can also do redirected restores between clients when they use the same pass phrase.

Note: If you want to prevent redirected restores, you should specify different pass phrases by entering a separate `bpinst` command for each client.

For clustered environments you can do the following:

- Push the configuration to the client only from the active node.
- Specify the host names of the individual nodes (not the virtual names) in the list of clients.

Note: The primary server `USE_VXSS` setting in `bp.conf` should be set to `AUTOMATIC`. Use this setting when pushing from an NBAC enabled primary server to a host that does not have NetBackup previously installed. Also use this setting when NBAC has not enabled the primary 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 about 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 BAR Console** to set or clear the **Encryption** attribute for a policy.

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 On the left pane, select **Host > Host properties**.
- 2 Select the name of the client you want to change and click **Edit client**.
- 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: It is not recommended to use 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 479.

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/var/keyfile
Enter old keyfile pass phrase: (standard keyfile pass phrase)
Enter new keyfile pass phrase: (standard keyfile pass phrase)
*****
Re-enter new keyfile pass phrase: (standard keyfile pass
phrase) *****
```

If you type a carriage return at the prompt, NetBackup uses the standard key file pass phrase.

- 2 Stop the existing `bpcd` by issuing the `bpcd -terminate` command.
- 3 Initiate the `bpcd` command with the `-keyfile` option. Enter the new key file pass phrase when prompted.

```
bpcd -keyfile
Please enter keyfile pass phrase: *****
```

`bpcd` now runs in the background, and waits for requests from the NetBackup server.

You can change the key file pass phrase at any time with the `bpkeyfile` command and the `-ckfpp` option. The new key file pass phrase does not take effect until the next time you start `bpcd`.

You can also change the NetBackup pass phrase that is used to generate the DES keys to encrypt backups. Change this phrase at any time with the `bpkeyfile` command and the `-cnpp` option. Note, however, that the new NetBackup pass phrase does not take effect until you kill the current `bpcd` process and restart `bpcd`.

Terminating `bpcd` on UNIX clients

To terminate `bpcd` on UNIX clients, use the `bpcd -terminate` command.

NetBackup key management service configuration

This chapter includes the following topics:

- [About FIPS enabled KMS](#)
- [Installing KMS](#)
- [Configuring KMS](#)
- [About using KMS for encryption](#)
- [KMS database constituents](#)
- [KMS operations using command-line interface \(CLI\)](#)
- [Troubleshooting KMS](#)

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.

See [“About Federal Information Processing Standards \(FIPS\)”](#) on page 483.

When you create a new key, a salt is always generated with the new key. Providing the salt value is mandatory when you want to recover a key.

Consider the following example; `hrs09to12hrs` is a key created using an older version of NetBackup:

Key Group Name : ENCR_Monday

Supported Cipher : AES_256

Number of Keys : 8

Has Active Key : Yes

Creation Time : Wed Feb 25 22:46:32 2015

Last Modification Time: Wed Feb 25 22:46:32 2015

Description : -

Key Tag :

5e16a6ea988fc8ec7cc9bdbbc230811b65583cdc0437748db4521278f9c1bbdf9

Key Name : hrs09to12hrs

Current State : ACTIVE

Creation Time : Wed Feb 25 22:50:01 2015

Last Modification Time: Wed Feb 25 23:14:18 2015

Description : active

The key hrs09to12hrs is moved from key group ENCR_Monday to a new key group ENCR_77.

```
Install_Path\NetBackup\bin\admincmd>nbkmsutil -modifykey -keyname
hrs09to12hrs -kgname ENCR_Monday -move_to_kgname ENCR_77
```

Key details are updated successfully

Now list all the keys of the ENCR_77 key group. Note that the new key Fips77 would be FIPS approved, but not hrs09to12hrs that was created using an older version of NetBackup.

```
Install_Path\NetBackup\bin\admincmd>nbkmsutil -listkeys -kgname NCR_77
```

Key Group Name : ENCR_77 Supported

Cipher : AES_256

Number of Keys : 2

Has Active Key : Yes

Creation Time : Thu Feb 26 04:44:12 2015

Last Modification Time: Thu Feb 26 04:44:12 2015

Description : -

```

Key Tag :
5e16a6ea988fc8ec7cc9bdbbc230811b65583cdc0437748db4521278f9c1bbdf9

Key Name : hrs09to12hrs

Current State : ACTIVE

Creation Time : Wed Feb 25 22:50:01 2015

Last Modification Time: Thu Feb 26 04:48:17 2015

Description : active

FIPS Approved Key : No

Key Tag :
4590e304aa53da036a961cd198de97f24be43b212b2a1091f896e2ce3f4269a6

Key Name : Fips77

Current State : INACTIVE

Creation Time : Thu Feb 26 04:44:58 2015

Last Modification Time: Thu Feb 26 04:48:17 2015

Description : active

FIPS Approved Key : Yes

Salt : 53025d5710ab36ac1099194fb97bad318da596e27fdfe1f2

Number of Keys: 2

```

The new key `Fips77` is FIPS approved and also has a Salt value.

KMS with FIPS compliance is supported on the following platforms:

- MS Windows Server 2012
- Linux.2.6.16 x86-64 Suse-10
- Linux.2.6.18 x86-64 RHEL-5

About 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 481.

Installing KMS

The following procedure describes how to install KMS.

Note: For more information about 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 KMS service as follows:

On UNIX, run the following command:

```
/usr/opensv/netbackup/bin/nbkms
```

On Windows, do the following:

```
Start > Run > Services.msc > Start the NetBackup Key Management Service
```

- 7 Use the `grep` command to ensure that the service has started, as follows: `ps -ef | grep nbkms`

- 8 Run the following command to register the `nbkms` service with NetBackup web services:

```
nbkmscmd -discovernbkms
```

- 9 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 and PureDisk, the `ENCR_` prefix is not required for the key group name.

To create a (non-Cloud storage) key group use the following command syntax.

```
nbkmsutil -createkg -kgname ENCR_volumepoolname
```

The `ENCR_` prefix is essential. When BPTM receives a volume pool request that includes the `ENCR_` prefix, it provides that volume pool name to KMS. KMS identifies it as an exact match of the volume pool and then picks the active key record for backups out of that group.

To create a Cloud storage key group use the following command syntax.

```
nbkmsutil -createkg -kgname storage_server_name:volume_name
```

- 10 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.

- 11 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"
```

- 12** 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.

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

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

Note: You need the passphrase, salt (if applicable), key group name, and key tag to recover this key if it is lost. You must store all this information at a secure place. Salt, key group name, and key tag can be found in the output of the `nbkmsutil -listkeys` command execution.

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 487.

See [“Using KMS with NBAC”](#) on page 487.

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 24-1](#) shows the default KMS permissions for each of the NetBackup user groups.

Table 24-1 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. In this section, we document the manual steps that set up KMS to get cluster monitored.

Enabling the monitoring of the KMS service

You can enable the monitoring of the KMS service and failover NetBackup when the service fails.

To enable monitoring of the KMS service and failover NetBackup if it fails

- 1 Open a command prompt on the active node of the cluster.
- 2 Change the directory, as follows:
On Windows: `<NetBackup_install_path>\NetBackup\bin`
On UNIX: `/usr/opensv/netbackup/bin`
- 3 Run the following command.
On Windows: `bpclusterutil -enableSvc "NetBackup Key Management Service"`
On UNIX: `bpclusterutil -enableSvc nbkms`

Disabling the monitoring of the KMS service

You can disable monitoring of the KMS service.

To disable monitoring of the KMS service

- 1 Open a command prompt on the active node of the cluster.
- 2 Change the directory, as follows:
On Windows: `<NetBackup_install_path>\NetBackup\bin`
On UNIX: `/usr/opensv/netbackup/bin`
- 3 Run the following command:
On Windows: `bpclusterutil -disableSvc "NetBackup Key Management Service"`
On UNIX: `bpclusterutil -disableSvc nbkms`

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:

```
NetBackup_install_path\kms\db\KMS_DATA.dat
NetBackup_install_path\kms\key\KMS_HMKF.dat
NetBackup_install_path\kms\key\KMS_HKPKF.dat
```

On a UNIX system, they can be found in the following files:

```
/usr/opensv/kms/db/KMS_DATA
/usr/opensv/kms/key/KMS_HMKF
/usr/opensv/kms/key/KMS_HKPKF
```

To create the key database

- 1 Run the following command:

```
nbkms -createemptydb.
```

- 2 Enter a pass phrase for the Host Master Key, or press Enter to use a randomly generated key. Re-enter the pass phrase at the following prompt.

- 3 Enter an HMK ID. This ID is associated with the HMK; you can use it to find this particular key in the future.
- 4 Enter a pass phrase for the Key Protection Key, or press Enter to use a randomly generated key. Re-enter the pass phrase at the following prompt.
- 5 Enter a KPK ID. The ID can be anything descriptive that you want to use to identify the KPK.

About key groups and key records

A key group is a logical collection of key records where no more than one record is in the active state.

A key group definition consists of the following:

- Name
Given to a key group. Should be unique within the keystore. Renaming of the key group is supported if the new name is unique within the keystore.
- Tag
Unique key group identifier (not mutable).
- Cipher
Supported cipher. All keys belonging to this key group are created with this cipher in mind (not mutable).
- Description
Any description (mutable).
- Creation Time
Time of creation of this key group (not mutable).
- Last Modification Time
Time of last modification to any of the mutable attributes (not mutable).

About creating key groups

The first step for setting up encryption is to create a key group.

In the following example, the key group `ENCR_mygroup` is created:

```
nbkmsutil -createkg -kgname ENCR_mygroup
```

Note: For AdvancedDisk and tape storage, 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

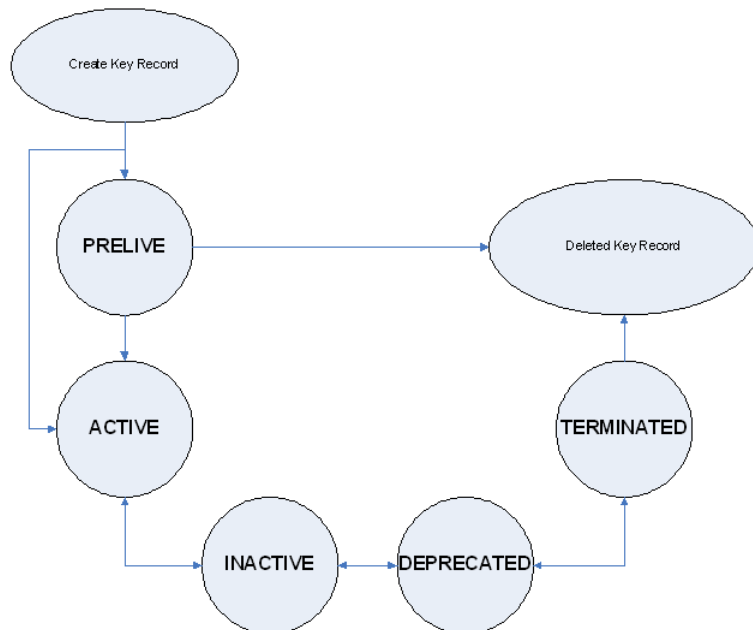
entered the active state (that is set up for encryption), the key must progress in proper order through the lifecycle. The proper order includes passing from one state to its adjacent state. A key cannot bypass any of the states.

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 24-1 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 the 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`, `KMS_HMKF`, and `KMS_KPKF` 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`, `KMS_HMKF`, and `KMS_KPKF` 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`, `KMS_HMKF`, and `KMS_KPKF` 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` by regenerating the `KMS_HMKF` and `KMS_KPKF` 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.

Note: A randomly-generated key cannot be recovered if it is lost.

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 passphrase (and salt) at the prompt. It must be an exact match with the original passphrase you previously provided.

Salt (if applicable) must match the salt corresponding to the key that you want to recover.

Note: If the tag you enter already exists in the KMS database, you cannot recreate the key.

- 4 If the recovered key is the key that you want to use for backups, run the following command to make the key active:

```
nbkmsutil -modifykey -kgname ENCR_pool1 -keyname Q1_2008_key  
-state active
```

The `-recoverkey` option places the key record in the inactive state, and it is brought into the KMS database in the inactive state.

- 5 If this is a key record that is to be deprecated, run the following command:

```
nbkmsutil -modifykey -kgname ENCR_pool1 -keyname Q1_2008_key  
-state deprecated
```

Problems backing up the KMS data files

There can be problems backing up the KMS data files with the normal NetBackup tapes or with the catalog backup.

Caution: The KMS data files are not included in the NetBackup catalog backups.

If the KPK, HMK, and key files were included in a catalog backup, and the catalog backup tape is lost, the keystore is compromised because the tape contains everything needed to gain access to the keys.

Significant problems can exist if both the catalog backup and data tapes are lost together on the same transport truck, for example. If both tapes are lost together then that situation is not be any better than not ever encrypting the tape in the first place.

Encrypting the catalog is not a good solution either. If the KPK, HMK, and key file were included in a catalog backup, and the catalog backup itself is encrypted, you have done the equivalent of locking the keys in the car. To protect from this problem is why KMS has been established as a separate service for NetBackup and why the KMS files are in a separate directory from the NetBackup directories. However, there are solutions for backing up the KMS data files.

Solutions for backing up the KMS data files

The best solution for backing up KMS data files is to do so outside of the normal NetBackup process, or rely on pass phrase generated encryption keys to manually rebuild KMS. All of the keys can be generated by pass phrases. So if you have recorded all of the pass phrases, then you can recreate the KMS manually from

the information you have written down. One way to back up KMS is to place the KMS information on a separate CD, DVD, or USB drive.

Creating a key record

The following procedure shows how to create a key record using a pass phrase and bypassing the prelive state and creating an active key.

Note: If an attempt is made to add a key to a group that already has an active key, the existing key is automatically moved to the inactive state.

To create a key record and create an active key

- 1 To create a key record enter the following command:

```
nbkmsutil -createkey -usepphrase -kgname ENCR_mygroup -keyname  
my_latest_key -activate -desc "key for Jan, Feb, March data"
```

- 2 Enter a pass phrase.

Listing keys from a key group

Use the following procedure to list all or selected keys that you created in a particular key group.

To list the keys in a key group

- ◆ To list the keys in a key group enter the following command:

```
nbkmsutil -listkeys -kgname ENCR_mygroup
```

The `nbkmsutil` outputs the list in the verbose format by default. Following is a non-verbose listing output.

```
KGR ENCR_mygroup AES_256 1 Yes 134220503860000000  
  
134220503860000000 -  
KR my_latest_key Active 134220507320000000 134220507320000000  
key for Jan, Feb, March data  
Number of keys: 1
```

The following options helps to list all keys from a specific key group or a specific key from a particular key group:

```
nbkmsutil -listkeys -all | -kgname <key_group_name> [ -keyname  
<key_name> | -activekey ]
```

```
[ -noverbose | -export ]
```

The `-all` option lists down all the keys from all the key groups. The keys are listed in a verbose format.

The `-kgname` option lists the keys from the specified key group.

The `-keyname` option lists a specific key from the specified key group. It must however be used with the option `-kgname`.

The `-activekey` option lists an active key from the specified key group name. It must however be used with the `-kgname` option.

Note: The `-activekey` and `-keyname` options are mutually exclusive.

The `-noverbose` option lists the details of the keys and key groups in a formatted form (non-readable). The default is a verbose list.

The `-export` option generates an output that the `key_file` requires. (The `key_file` is used in `nbkmsutil -export -path <key_container_path> -key_file file`. You can use the output for another `key_file`.

Run the following command to list all the keys from a specific key group:

```
nbkmsutil -listkeys -kgname <key_group_name>
```

Run the following command to list specific keys from a specific key group:

```
nbkmsutil -listkeys -kgname <key_group_name> -keyname <key_name>
```

Run the following command to list all keys from all groups:

```
nbkmsutil -listkeys -all
```

Run the following command to list all keys from a specific key group:

```
nbkmsutil -listkeys -kgname <key_group_name>
```

Run the following command to list the active keys from a specific key group:

```
nbkmsutil -listkeys -kgname <key_group_name> -activekey
```

Configuring NetBackup to work with KMS

Configuring NetBackup to work with KMS involves the following topics:

- NetBackup getting key records from KMS
See [“NetBackup and key records from KMS”](#) on page 500.
- Setting up NetBackup to use encryption
See [“Example of setting up NetBackup to use tape encryption”](#) on page 500.

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: For AdvancedDisk and tape storage, the Key Management feature requires the key group name and NetBackup volume pool name match identically and both be prefixed with `ENCR_`. For Cloud Storage and PureDisk key group name should be `storage_server_name:volume_name`. 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 BAR Console** with two volume pools with the correct naming convention to use KMS.

Figure 24-2 NetBackup BAR Console with two volume pools set up to use KMS

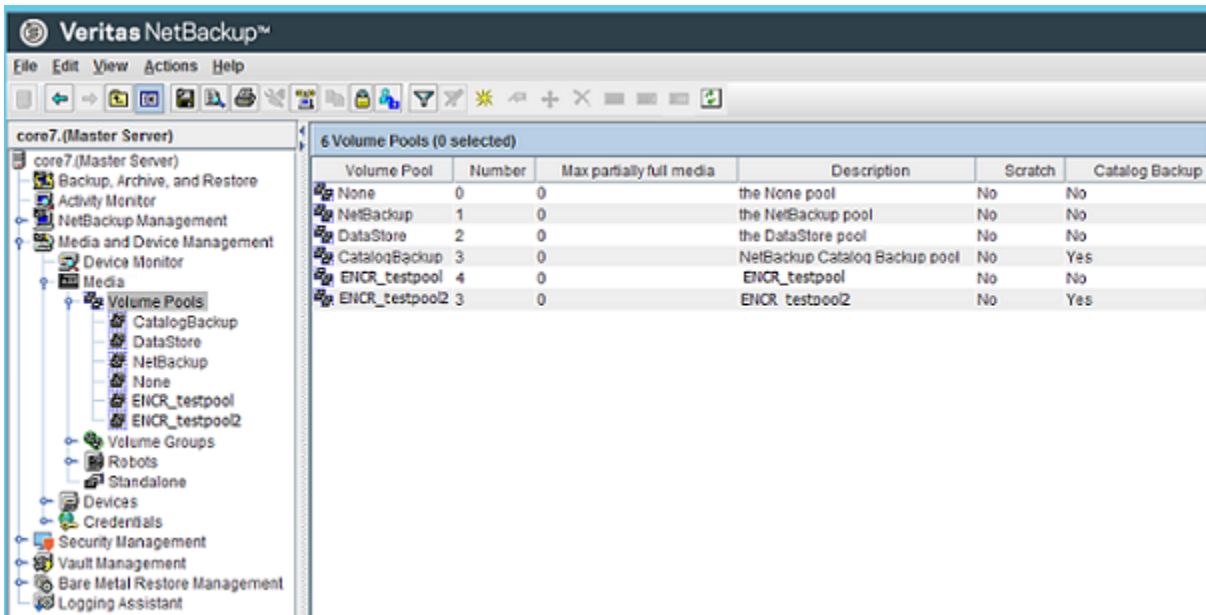
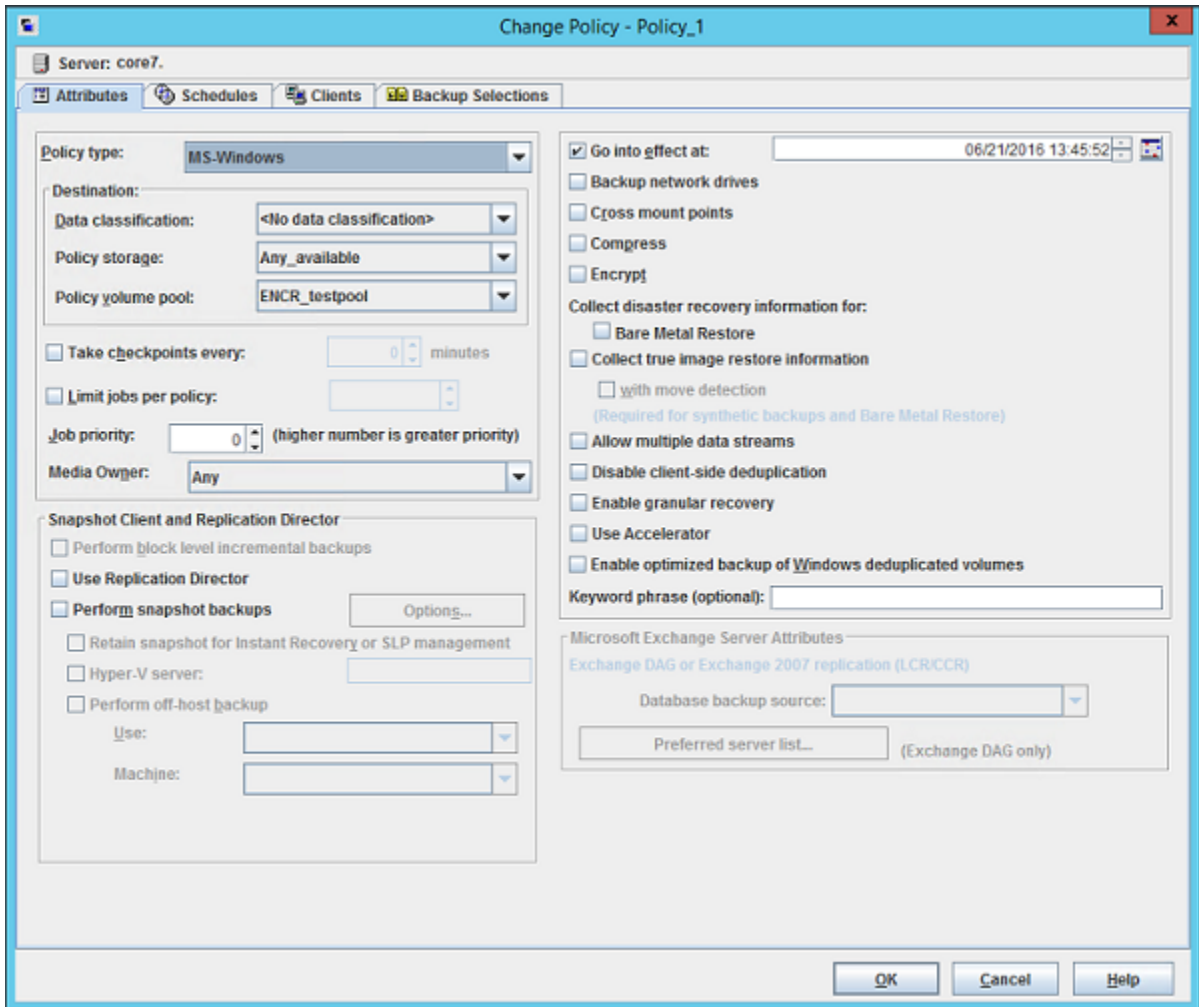


Figure 24-3 shows a NetBackup Policy that is configured to use the volume pool ENCR_testpool, which is the same name as the key group that you configured earlier.

Figure 24-3 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.

Configuring NetBackup KMS using the KMS web application

If you configure NetBackup KMS (NBKMS), NetBackup does not use it for key operations. To activate the KMS server, run the following command:

```
nbkmscmd -configureKMS -type NBKMS
```

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 503.
- Example of verifying an encryption backup
See [“Example of verifying an encryption backup”](#) on page 504.
- About importing KMS encrypted images
See [“About importing KMS encrypted images”](#) on page 503.

About importing KMS encrypted images

Importing KMS encrypted images is a two-phase operation. In phase one, the media header and each fragment backup header is read. This data is never encrypted. However, the backup headers indicate if the fragments file data is encrypted with KMS or not. In summary, phase one does not require a key.

Phase two rebuilds the catalog .f file, which requires it to read the encrypted data. The `key-tag` (KAD in SCSI terms) is stored on the tape by the hardware. The NBU/BPTM reads the `key-tag` from the drive, and sends it to KMS for a key lookup. If KMS has a key, then the phase two processes continues to read the encrypted data. If KMS has no key, the data is not readable until the KMS has the key recreated. This is when the pass phrase is important.

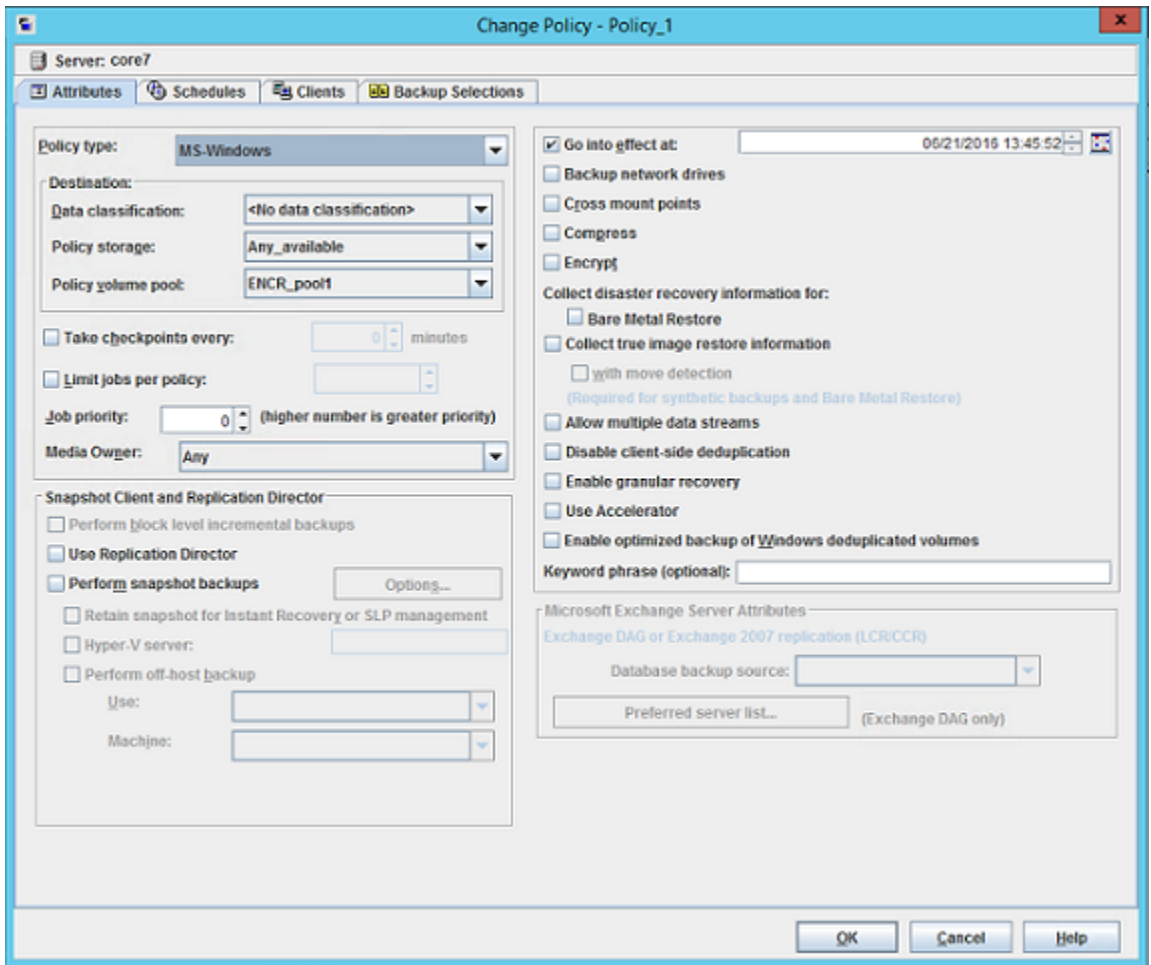
If you do not destroy keys, then KMS contains all the keys ever used and you can import any encrypted tape. Move the keystore to your DR site and you do not need to recreate it.

Example of running an encrypted tape backup

To run an encrypted tape backup, you must have a policy that is configured to draw from a volume pool with the same name as your key group.

[Figure 24-4](#) shows a NetBackup Policy that you have configured to use the volume pool `ENCR_pool1`.

Figure 24-4 NetBackup Change Policy dialog box with KMS volume pool ENCR_pool1



Example of verifying an encryption backup

When NetBackup runs a tape-encrypted backup, and you view the Images on Media, you see the encryption key tag that is registered with the record. This key tag is your indication that what was written to tape was encrypted. The encryption key tag uniquely identifies which key was used to encrypt the data. You can run a report and read down the policy column to determine whether everything on a particular tape was encrypted.

KMS database constituents

The KMS database consists of three files:

- The keystore file (`KMS_DATA`) contains all the key group and key records along with some metadata.
- The KPK file (`KMS_KPKF`) 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`) 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/HMK 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 `-nophrase` 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`, the Host Master Key `KMS_HMKF`, and the Key Protection Key `KMS_HKPKF`.

On Windows these files are as follows:

```
NetBackup_install_path\kms\kms\db\KMS_DATA.dat
NetBackup_install_path\Veritas\kms\key\KMS_HMKF.dat
NetBackup_install_path\Veritas\kms\key\KMS_KPKF.dat
```

On UNIX these files are at this location:

```
/usr/opensv/kms/db/KMS_DATA
/usr/opensv/kms/key/KMS_HMKF
/usr/opensv/kms/key/KMS_KPKF
```

KMS operations using command-line interface (CLI)

The following topics describe the KMS operations that can be performed using command-line interface (CLI):

- CLI usage help
See [“CLI usage help”](#) on page 509.
- Create a new key group

See [“Create a new key group”](#) on page 509.

- Create a new key
See [“Create a new key”](#) on page 510.
- Modify key group attributes
See [“Modify key group attributes”](#) on page 510.
- Modify key attributes
See [“Modify key attributes”](#) on page 511.
- Get details of key groups
See [“Get details of key groups”](#) on page 511.
- Get details of keys
See [“Get details of keys”](#) on page 512.
- Delete a key group
See [“Delete a key group”](#) on page 512.
- Delete a key
See [“Delete a key”](#) on page 513.
- Recover a key
See [“Recover a key”](#) on page 513.
- Modify host master key (HMK)
See [“Modify host master key \(HMK\)”](#) on page 518.
- Get host master key (HMK) ID
See [“Get host master key \(HMK\) ID”](#) on page 518.
- Modify key protection key (KPK)
See [“Modify key protection key \(KPK\)”](#) on page 518.
- Get key protection key (KPK) ID
See [“Get key protection key \(KPK\) ID”](#) on page 518.
- Get keystore statistics
See [“Get keystore statistics”](#) on page 519.
- Quiesce KMS database
See [“Quiesce KMS database”](#) on page 519.
- Unquiesce KMS database
See [“Unquiesce KMS database”](#) on page 519.

KMS operations with multiperson authorization

The following KMS operations support multiperson authorization:

Starting with NetBackup 10.5, if multiperson authorization is enabled for a key management operation, `bpbat -login` is required for this operation. A multiperson authorization ticket is generated and after the ticket is approved, an empty key database is created. For NetBackup releases earlier than 10.5, if multiperson authorization is enabled, you cannot perform the `-createemptydb` operation.

`nbkms`

- `-createemptydb`

Starting with NetBackup 10.5, if multiperson authorization is enabled for a key management operation, a ticket is generated. After the multiperson authorization ticket is approved, KMS is configured. For NetBackup releases earlier than 10.5, if multiperson authorization is enabled, you cannot perform `nbkmsutil` operations.

`nbkmsutil`

- `-createkg`
- `-createkey`
- `-modifykg`
- `-modifykey`
- `-deletekg`
- `-deletekey`
- `-modifyhmk`
- `-modifykpk`
- `-export`
- `-import`
- `-recoverkey`

Starting with NetBackup 10.5, if multiperson authorization is enabled for a key management operation, `bpbat -login` is required for all the `nbkmscmd` operations. A multiperson authorization ticket is generated and after the ticket is approved, the KMS operation is performed. For NetBackup releases earlier than 10.5, if multiperson authorization is enabled, you cannot perform `nbkmscmd` operations.

`bpbat -login` is required for the `nbkmscmd` operations that modify or delete the KMS configuration.

`nbkmscmd`

- `-configureKMS`
- `-deleteKMSConfig`

- `-updateKMSConfig`
- `-deleteCredential`
- `-updateCredential`
- `-createKey`

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 ]
[ -export ]
[ -import ]
[ -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: 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.

<code>-name</code>	Specifies the new name of the key group (should be unique within the keystore).
--------------------	---

Modify key attributes

To modify the key attributes use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

```
# nbkmsutil -help -modifykey
nbkmsutil -modifykey -keyname <key_name>
-kgroup <key_group_name>
[ -state <new_state> | -activate ]
[ -name <new_name_for_the_key> ]
[ -desc <new_description> ]
[ -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.

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 -all | -kgname <key_group_name>
[ -keyname <key_name> | -activekey ]
[ -noverbose | -export ]
```

<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.
<code>-export</code>	Generates an output that the <code>key_file</code> requires. The <code>key_file</code> is used in the <code>nbkmsutil -export -path <key_container_path> -key_file file</code> . The output can be used for another <code>key_file</code> .

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> -force
```

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

-force All the keys from the key group are 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, passphrase, and salt).

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

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

Note: 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 key 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 498.

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 511.

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 1000 key groups. Each key group has a limit of 16000 keys. The operation fails if more than 1000 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  
kms/key/KMS_HMKF  
kms/key/KMS_KPKF
```

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 24-5](#) 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 24-5 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 24-6 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 24-6 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 24-7 shows the BPTM log output. It logs the message within the 1227 error code in the BPTM log.

Figure 24-7 Output from `bptm` command

```
14:29:16.381 [19978] <2> manage_drive_attributes: MediaPool [ENCR_mygroup], MediaLabel [MEDIA=JRO111;]
14:29:16.384 [19978] <2> manage_drive_attributes: encryption status: nexus scope 0, key scope 0
14:29:16.384 [19978] <2> manage_drive_attributes: encryp mode 0x0, decryp mode 0x0, algorithm index 0, key instance 0
14:29:16.384 [19978] <2> KMCLIB::kmsGetKeyAndKad: Entering function... (KMCLib.cpp:583)
14:29:16.384 [19978] <2> KMCLIB::GetQueryableFacetInstance: Entering function... (KMCLib.cpp:207)
14:29:16.384 [19978] <2> KMCLIB::InitOrb: Entering function... (KMCLib.cpp:158)
14:29:16.385 [19978] <2> Orb::init: Created anon service name: NB 19978 1536015948517350 (Orb.cpp:600)
14:29:16.385 [19978] <2> Orb::init: endpointvalue is : pbxiop://1556:NB 19978 1536015948517350 (Orb.cpp:618)
14:29:16.385 [19978] <2> Orb::init: initializing ORB kmslib with: kmslib -ORBSvcConfDirective "-ORB DottedDecimalAddresses 0" -ORBSvcConfDirective "static PBXIOP_Factory" -ORBSvcConfDirective "static EndpointSelectorFactory" -ORBSvcConfDirective "static Resource_Factory -ORBPProtocolFactory PBXIOP_Factory" -ORBSvcConfDirective "static Resource_Factory -ORBPProtocolFactory IIOP_Factory" -ORBSvcConfDirective "static PBXIOP_Evaluator_Factory -orb kmslib" -ORBSvcConfDirective "static Resource_Factory -ORBConnectionCacheMax 1024" -ORBEndpoint pbxiop://1556:NB 19978 1536015948517350 -ORBSvcConf /dev/null -ORBSvcConfDirective "static Server Strategy Factory -ORBMaxRecvGIOPPayloadSize 268435456" (Orb.cpp:725)
14:29:16.406 [19978] <2> vnet_cached_gethostbyname: vnet hosts.c.307: found host in cache: felix.min.veritas.com
14:29:16.406 [19978] <2> vnet_cached_gethostbyaddr_rnl: vnet hosts.c.506: found IP in cache: 127.0.0.1
14:29:16.460 [19978] <2> db_error_add_to_file: dberror.c:midnite = 1205730000
14:29:16.461 [19978] <16> get_encryption_key: NBKMS failed with error status: Key group does not have an active key (1227)
14:29:16.462 [19978] <2> send_MDS_msg: MEDIADB 1 42 JRO111 4000007 *NULL* 6 1205781805 1205782033 1206991633 0 64 2 2 1 4 0 8193 1024 0 8 0
```

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 24-8 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 24-8 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 24-9 shows the `bptm` log output with the 1242 error returned.

Figure 24-9 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)

```

External key management service configuration in NetBackup

This chapter includes the following topics:

- [About external KMS](#)
- [Certificate configuration and authorization](#)
- [Workflow for external KMS configuration](#)
- [Validating KMS credentials](#)
- [Configuring KMS credentials](#)
- [Configuring KMS](#)
- [Configuring keys in an external KMS for NetBackup consumption](#)
- [Creating keys in an external KMS](#)
- [Determining a key group name during storage configuration](#)
- [Working with multiple KMS servers](#)
- [Working with external KMS during backup and restore](#)
- [Checking the compatibility of KMS vendor with NetBackup](#)
- [Key rotation](#)
- [Disaster recovery when catalog backup is encrypted using an external KMS server](#)

- [Alerts for expiration of KMS credentials](#)

About external KMS

The external KMS support offers an alternative to the NetBackup key management service (KMS) for data-at-rest encryption keys.

Backup images that are stored on storage configurations like tape, cloud, MSDP, and AdvancedDisk can be encrypted using the keys that the external KMS server maintains.

NetBackup supports the communication with external KMS using Key Management Interoperability Protocol (KMIP).

See the [NetBackup Compatibility List](#) for the KMIP versions that NetBackup supports.

NetBackup supports the authentication with external KMS server using security certificates. During each operation, NetBackup presents the certificate to the external KMS and requests to perform the required operation. External KMS validates the certificate and performs that operation if the user has the required permissions.

See the video *External KMS support in NetBackup* for details.

[Video link](#)

Certificate configuration and authorization

Before configuring any certificate to be used with NetBackup, you should do certain configurations on the external KMS server to ensure that NetBackup has the required permissions to perform key-specific operations. Configuration steps may vary for different external KMS solutions.

Ensure the following:

- An entity (user) is created in the external KMS that represents NetBackup primary server.
- The primary server host has a certificate that the external KMS server trusts.
- The certificate common name (CN) is associated with the entity that represents the primary server.

Workflow for external KMS configuration

For external KMS integration, centralized configuration on the NetBackup primary server is used. The primary server should establish an outbound connection with the KMIP port on the external KMS server. Configure the communication channel

with external KMS on the primary server with certificate credentials. The primary server then sends all the requests to the external KMS servers on behalf of other servers such as media servers.

Table 25-1 Workflow to configure a KMS

Step number	Step	Reference topic
Step 1	Validate KMS credentials	See “Validating KMS credentials” on page 528.
Step 2	Configure KMS credentials	See “Configuring KMS credentials” on page 529.
Step 3	Configure KMS	See “Configuring KMS” on page 531.
Step 4	Create keys	See “Creating keys in an external KMS” on page 534.
Step 5	Configure storage	Refer to the NetBackup Administrator's Guide, Volume I .
Step 6	Configure policy	Refer to the NetBackup Administrator's Guide, Volume I .

Validating KMS credentials

If incorrect credentials are configured in NetBackup, communication with external KMS server may fail. To avoid such failures, you can carry out certain validations before a credential can be configured for the KMS use. If a validation check is not passed, the credential cannot be configured.

See [“Configuring KMS credentials”](#) on page 529.

See [“Checking the compatibility of KMS vendor with NetBackup”](#) on page 540.

The `-validate` command option is useful when the KMS vendor is listed as a supported KMS vendor in the NetBackup hardware compatibility list.

The following validations are carried out while you configure a new credential or update an existing one.

It is not recommended to configure credentials if one or more checks fail:

- The certificate path is valid
- The truststore path is valid
- The private key path is valid
- The certificates in certificate chain are readable

- The certificates in a truststore are readable
- The private key is readable
- The Common Name field is not empty
- The certificate is not expired
- The certificate is currently valid
- The private key matches the certificate
- The certificates are in the appropriate order
- The following CRL validation checks are performed, if the `ECA_CRL_PATH` is configured and the CRL check level is other than DISABLE:
 - The CRL directory consists of CRL files
 - The CRL check level is valid
 - The CRL path is valid
 - The available CRLs are readable

To validate KMS credentials and KMS functionality

- 1 Run the following command:

```
nbkmiputil -validate -kmsServer kms_server_name -port port  
-certPath cert_path -privateKeyPath private_key_path  
-trustStorePath trust_store_path
```

The `nbkmiputil` command validates the KMS functionality including connection to the KMS server.

It also tests operations like list keys, fetch keys, set attributes, and fetch attributes. For set attributes, you must have the 'write' permission for the KMS server. The `nbkmiputil` command also validates CA fingerprint on the server certificate that is exchanged through TLS handshake. `nbkmiputil` uses TLS 1.2 or later protocol for secure communication with external KMS server.

- 2 If the check fails, contact Cohesity Technical Support.

Configuring KMS credentials

To configure external KMS in NetBackup, you need to first configure the credentials that NetBackup uses to authenticate with the external KMS server. As part of this step, you need to specify the path for public key Infrastructure (PKI) artifacts that are required for certificate-based authentication. The following information is required:

- Certificate file path
- Keystore file path
- Trust store file path
- Passphrase or passphrase file path

Note: After external KMS configuration or keys are updated, NetBackup may take several minutes to consume appropriate key in backup or restore workflow. This is because NetBackup caches the key for 10 minutes (for external KMS). To immediately consume a key, cache can be cleared by executing the following command on the respective media server:

```
bpcintcmd -clear_host_cache
```

To configure KMS credentials

- ◆ Run the `nbkmscmd -configureCredential` command:

This command creates a copy of files that are provided on the command-line interface and stores them into the credentials database. When the command is successfully executed, you can delete these files if you do not need them. NetBackup does not track any updates to these files. If the certificate needs to be updated, typically in case of renewal, you need to run the `nbkmscmd -updateCredential` command again with new certificate files.

```
nbkmscmd -configureCredential -credName credential_name -certPath  
certificate_file_path -privateKeyPath private_key_file_path  
-trustStorePath CA_certificate_file_path [-passphrasePath  
private_key_passphrase_file_path] [-crlCheckLevel LEAF | CHAIN |  
DISABLE] [-server master_server_name] [-description description]
```

Listing KMS credentials

To list all credential details

- ◆ Run the following command:

```
nbkmscmd -listCredential
```

To list specific credential details

- ◆ Run the following command:

```
nbkmscmd -listCredential -credName credential_name
```

Updating KMS credentials

To update credential details

- ◆ Run the following command:

```
nbkmscmd -updateCredential -credName credential_name -certPath  
certificate_file_path -privatekeyPath private_key_file_path  
-trustStorePath CA_certificate_file_path -crlCheckLevel DISABLE
```

Deleting KMS credentials

To delete credential details

- ◆ Run the following command:

```
nbkmscmd -deleteCredential -credName credential_name
```

Configuring KMS

To configure NetBackup KMS (NBKMS)

- ◆ Run the following command:

```
nbkmscmd -configureKMS -name configuration_name -type NBKMS -hmkId  
host_master_key_ID_to_identify_HMK_passphrase -kpkId  
key_protection_key_ID_to_identify_KPK_passphrase  
[-useRandomPassphrase 0 | 1] [-enabledForBackup 0 | 1] [-priority  
priority_of_KMS_server] [-server master_server_name] [-description  
description]
```

To configure external KMS

- ◆ Run the following command:

```
nbkmscmd -configureKMS -name configuration_name -type KMIP -port  
port_to_connect_to_external_KMS_server -kmsServerName  
network_name_of_external_KMS_server -credId credential_ID |  
-credName credential_name [-enabledForBackup 0 | 1] [-priority  
priority_of_KMS_server] [-server master_server_name] [-description  
description]
```

Listing KMS configurations

To list configuration details for all KMS servers

- ◆ Run the following command:

```
nbkmscmd -listKMSConfig
```

To list configuration details for a specific KMS server

- ◆ Run the following command:

```
nbkmscmd -listKMSConfig -name configuration_name
```

Updating KMS configuration

Update priority of a KMS

To update priority of KMS, run the following command: `nbkmscmd -updateKMSConfig -name configuration_name -priority priority`

Disable a KMS configuration for backup

To disable keys from specified KMS to be used for backup, run the following command: `nbkmscmd -updateKMSConfig -name configuration_name -enabledForBackup 0`

Disable a KMS configuration temporarily for all operations

To disable a configured KMS for all operations, run the following command:

```
nbkmscmd -updateKMSConfig -name configuration_name -status 0
```

Note: After any update in external KMS configuration or keys, NetBackup may take several minutes to consume appropriate key in backup or restore workflow. This is because NetBackup caches the key for 10 minutes (for external KMS). To immediately consume a key, cache can be cleared by executing the following command on the respective media server:

```
bpcintcmd -clear_host_cache
```

Deleting KMS configuration

To delete KMS configuration, run the following command: `nbkmscmd`

```
-deleteKMSConfig -name configuration_name
```

Configuring keys in an external KMS for NetBackup consumption

NetBackup can use the keys that are already created in an external KMS or you can create keys in an external KMS using NetBackup, for which the NetBackup primary server needs to be authorized to create keys.

NetBackup can discover the keys that are created in an external KMS for the NetBackup use. Specify custom attributes `x-application` and `x-keygroup` while generating keys or associate these attributes to the existing keys, so NetBackup can determine the keys to be used. NetBackup uses any key that has these attributes for encryption purpose.

Key group name for tape volume pool must have `ENCR_` as a prefix.

Consider the following example: You have configured a tape volume pool with name `ENCR_P1`. The volume pool name suggests that the backup images in this volume pool are encrypted.

`x-keygroup` is case-sensitive and it should exactly match the volume pool name.

To configure keys

- 1 Create a key in an external KMS with the custom attribute `x-keygroup` and its value as `ENCR_P1`.
- 2 Set the custom attribute `x-application` with its value as `NetBackup` to indicate that this key belongs to NetBackup.
- 3 For the keys that are already created and are to be used for encryption for this volume pool, you can create the custom attributes.
- 4 To set these attributes, you can use the user interface that the respective KMS vendor has specified.

If the user interface of the KMS vendor does not support adding and setting custom attributes, you can use the `nbkmiutil` command to set the attributes for the keys.

```
nbkmiutil -kmsServer kms_server_name -port 5696 -certPath  
cert_path -privateKeyPath private_key_path -trustStorePath  
caCertificatePath -setAttribute -attributeName attributeName  
-attributeValue attributeVal
```

See the [NetBackup Commands Reference Guide](#) for more information on the command.

Creating keys in an external KMS

You can use NetBackup to create keys in an external KMS. NetBackup must have the required permissions to create keys in the external KMS.

To create keys in an external KMS

- ◆ Run the following command:

```
nbkmscmd -createkey -name configuration_name -keyGroupName  
keygroup_name -keyName key_name -comment comments
```

The `createKey` command creates a key in active state. For external KMS, you can have multiple active keys in a key group. NetBackup uses the latest active key. The command also sets all the required attributes for the key.

Note: After any update in external KMS configuration or key related changes, NetBackup may take some time to consume appropriate key in backup or restore workflow. This is because NetBackup caches the key for 10 min (for external KMS). To consume the key immediately, run the following command on the respective media server to clear the cache:

```
bpcintcmd -clear_host_cache.
```

Listing keys

Use the given procedure to list key IDs from the specified KMS.

To list key IDs

- ◆ `nbkmscmd -listKeys -name configuration_name`

Determining a key group name during storage configuration

NetBackup uses the preconfigured keys from an external KMS during storage configuration.

Ensure that the keys are created in an external KMS server with an attribute `x-keygroup` and are assigned to a key group name.

For every storage configuration, NetBackup determines the key group name as follows:

MSDP

Specify the key group name

Cloud	The key group name is <i>Name_of_storage_server.Name_of_disk_volume</i>
Tapes	The volume pool name is used as a key group name For tapes, the volume pool should have <code>ENCR</code> as a prefix.
AdvancedDisk	For UNIX: <i>Name_of_storage_server.Name_of_disk_volume</i> For Windows: <i>Name_of_storage_server</i>

Working with multiple KMS servers

NetBackup supports multiple KMS servers. You can use multiple KMS servers and migrate from one KMS server to another. You can also use a separate KMS server for each storage configuration like tape, cloud, and MSDP.

See [“Migrating one KMS server to another KMS server”](#) on page 536.

See [“Using a separate KMS server for each storage configuration”](#) on page 536.

To use multiple KMS servers effectively, you need to define the following KMS configuration attributes:

enableForBackup	Specifies whether keys from this KMS should be used for backup or not. The default value is 1. Provide 0 if the keys from this KMS server should not be used for backup. This attribute does not affect restores. If there is backup image, that was encrypted using the key from this KMS, during restore NetBackup uses this KMS server and fetches the keys to restore the data. These KMS servers can still be used for restoring an image. So, if you want to delete the KMS configuration, ensure that there are no images that are encrypted with keys of this KMS server. If the key is lost, the data cannot be restored from that image and it will be lost. During KMS server migration, at least one KMS configuration should have this property set to 1 else all the backups will fail.
priority	Specifies the KMS server to be used when NetBackup checks for keys during encryption or decryption. By default, the KMS server priority is set to 0. A KMS server with the highest value gets the first priority to be used during encryption or decryption. During backup or restore, NetBackup uses the ordered list of KMS servers, based on their priority to fetch keys. So, KMS with highest priority is used first to fetch keys. If multiple KMS servers have the same priority, one of them is used.

While configuring a KMS (using CLI or API) in NetBackup you can choose a value for these attributes. The options to set these attributes are available in the `configureKMS` and `updateKMSConfig` options in the `nbkmscmd` CLI operation.

See [“Configuring KMS”](#) on page 531.

See [“Updating KMS configuration”](#) on page 532.

Migrating one KMS server to another KMS server

If you have a KMS server configured in your environment (for example NetBackup KMS - KMS1) and you want to migrate to another KMS server (for example external KMS - KMS2), use the following procedure:

To migrate from one KMS server (KMS1) to another KMS server (KMS2)

- 1 Create required keys in KMS2 to ensure all storage pools in the domain that are enabled for encryption have keys in KMS2.
- 2 Run the following command to add the KMS2 configuration in NetBackup:

```
nbkmscmd -configureKMS -name KMS2 -type KMIP -port  
port_to_connect_to_external_KMS_server -kmsServerName  
network_name_of_external_KMS_server -credId credential_ID  
-credNamecredential_name -enabledForBackup 1 -priority  
priority_of_KMS_server -server master_server_name -description  
description
```

- 3 Run the following command to update the `enabledForBackup` flag for KMS1:

```
nbkmscmd -updatekmsconfig -name KMS1 -enabledForBackup 0
```

So hence forth, none of the backups will be encrypted using keys from KMS1. If a key is required and is not found in KMS2, NetBackup does not fall back to KMS1.

- 4 Ensure that none of the existing backup images are encrypted using KMS1.
- 5 Delete the KMS1 configuration from NetBackup configuration.

If you have the images that were encrypted using the deleted KMS server (KMS1), you cannot restore the data from such images. Reconfigure the KMS server (KMS1) and ensure that the respective keys are available in that KMS server before restoring the data.

Using a separate KMS server for each storage configuration

You may want to use separate KMS servers for different storage configurations. For example, you can use one KMS server for tape storage and another for cloud

storage. You can also use separate KMS servers for different tape volumes or for different MSDP storage servers.

NetBackup looks for keys from key groups. Each key group is associated with one storage. For example, every encryption-enabled tape volume has a corresponding key group.

To use separate KMS servers for tape and cloud storage

- 1 Add the first KMS configuration in NetBackup, say KMS1. The default value of the `enableForBackup` attribute for KMS1 is 1.
- 2 Add the second KMS configuration in NetBackup, say KMS2. The default value of the `enableForBackup` attribute for KMS2 is 1.

See [“Configuring KMS”](#) on page 531.

- 3 Create all the required key groups and keys for tapes in KMS1. Ensure that none of the key groups correspond to cloud storage.
- 4 Create all the required key groups and keys for cloud storage in KMS2. Ensure that none of the key groups correspond to tape.

See [“Configuring keys in an external KMS for NetBackup consumption”](#) on page 533.

See [“Creating keys in an external KMS”](#) on page 534.

- 5 To verify the configuration, run backups using tape and cloud storage.

Encryption-enabled storage servers of type tape and cloud use different KMS servers. During backup, NetBackup fetches the ordered KMS list and looks for the key group in the first KMS server and then the other one.

So, if KMS1 has higher priority than KMS2, KMS1 is first searched for the required key. Even for backups going on cloud storage, the key request first goes to KMS1 and then KMS2. Therefore, you need to ensure that KMS1 does not have any key group that corresponds to cloud storage.

During restores as well, the keys are searched in the available KMS servers based on the priority.

Working with external KMS during backup and restore

Backup

KMS workflow during backup

- 1 When you run a backup job, the media server sends the key request based on the key group name or disk pool name to the KMS web service.
- 2 Keys in an external KMS server are created with an attribute `x-keygroup`.
Key group names for tape volume pools must have `ENCR_` as a prefix.
- 3 The KMS web service connects with the external KMS server and validates if an active key with custom attribute `x-keyGroup` is present. If the key is present, the key is retrieved and returned to the media server.
- 4 If the external KMS is not configured or no such key is available in the external KMS, the web service falls back to `nbkms` for the key lookup.

Restore

KMS workflow during restore

- 1 During restore, the media server sends Key ID or KAD (key associated data) to the KMS web service to retrieve the key.
- 2 The KMS web service connects to all the KMS servers and retrieves all the possible keys that match KAD.
- 3 The media server uses all the keys to find the matching key and uses that key to decrypt the image.
- 4 If the KMS is configured and used for backup and restore, you can see the KMS configuration details in the job details for tape, AdvancedDisk, and cloud storage types.

Note: The KMS configuration details do not appear in the job details in case of MSDP.

Additional security considerations for MSDP media servers

This information is applicable only for MSDP storage servers.

Starting with NetBackup 11.1, the KMIP Encrypt/Decrypt operations are preferably used to communicate with an external KMS server. If the KMS server does not

support the Encrypt/Decrypt operations, NetBackup automatically starts using the GetKey operation to communicate with the KMS server.

With the GetKey operation, the key is transferred from KMS server to NetBackup primary server and this may cause security issues.

For enhanced security, you can configure NetBackup to disable the transfer of the key from the KMS server to the NetBackup primary server. The KMIP server must support the Encrypt/Decrypt operations for encryption and decryption to function as required.

See [“FETCH_MSDP_EKMS_KEY for NetBackup servers and clients”](#) on page 539.

FETCH_MSDP_EKMS_KEY for NetBackup servers and clients

Starting with NetBackup 11.1, the KMIP Encrypt/Decrypt operations are preferably used to communicate with an external KMS server. If the KMS server does not support the Encrypt/Decrypt operations, NetBackup automatically starts using the GetKey operation to communicate with the KMS server.

With the GetKey operation, the key is transferred from KMS server to NetBackup primary server and this may cause security issues.

Set the `FETCH_MSDP_EKMS_KEY` configuration option to '0' or 'False' to disable the transfer of the key from the KMS server to the NetBackup primary server.

Table 25-2

Usage	Description
Where to use	On NetBackup primary servers.
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. To disable the transfer of a key from KMS server to NetBackup primary server., use the following format: <pre>FETCH_MSDP_EKMS_KEY = 0</pre>
Equivalent NetBackup web UI property	No equivalent property in the web UI.

Checking the compatibility of KMS vendor with NetBackup

Check the compatibility of the KMS vendor with NetBackup for successful configuration of KMS in your environment.

See [“Configuring KMS credentials”](#) on page 529.

See [“Configuring KMS”](#) on page 531.

To check the compatibility of KMS vendor with NetBackup

- 1 Ensure that you to have the administrative privileges or the permissions from the KMS administrator to perform KMIP compatibility operations on the KMS.
- 2 Run the following command:

```
nbkmiutil -ekmsCheckCompat|-ecc -extended -kmsServer  
kms_server_name -port port -certPath cert_path -privateKeyPath  
private_key_path -truststorepath trust_store_path
```

The `-ekmsCheckCompat` command option is useful when the KMS vendor is not listed as a supported KMS vendor in the NetBackup hardware compatibility list and you want to verify the compatibility of the vendor with NetBackup.

The command checks for issues related to execution of the KMIP operation on the given KMS sever and the supported KMIP protocol versions.

The following validations and tasks are carried out when you run the command:

- Checking KMIP version compatibility
- Fetching server details
- Validating KMIP operation
- Creating keys
- Deactivating keys
- Compromising keys
- Fetching active keys by key groups
- Fetching NetBackup keys by key IDs
- Setting key attributes
- Fetching NetBackup keys based on attributes
- Retrieving attributes that are set for a key from the server and verifying them
- Destroying keys that were created by this command option

- 3 If a check fails, contact Cohesity Technical Support.
- 4 If the check passes, contact Cohesity Technical Support to add this KMS vendor in the NetBackup hardware compatibility list.

Key rotation

With external KMS, you can have one or more keys in a key group that are in active state. NetBackup always picks up the most recent key from the active keys for data encryption. If you want to change key for encryption (rotate key), create a new active key under a specific key group. The most recently created key is used for subsequent encryption request for that key group.

Note: After any update in external KMS configuration or keys, NetBackup may take some time to consume appropriate key in backup or restore workflow. This is because NetBackup caches the key for 10 minutes (for external KMS).

To immediately consume a key, cache can be cleared by executing the following command on the respective media server:

```
bpcintcmd -clear_host_cache
```

Disaster recovery when catalog backup is encrypted using an external KMS server

As part of a catalog backup, an email notification is sent that contains the disaster recovery (DR) package information. If the catalog backup image is encrypted, the email also contains KMS information. You need to configure the KMS servers that are listed in the email before the catalog restore.

To restore a catalog when the catalog backup is encrypted using an external KMS server

- 1 Install NetBackup using the appropriate DR package.
- 2 The disaster recovery email contains KMS-specific information as follows:

The primary server *ms1.example.veritas.com* is configured to use the following Key Management Servers.

KMS Server Name = *kms1.example.veritas.com*, KMS Server Type = KMIP

KMS Server Name = *kms2.example.veritas.com*, KMS Server Type = KMIP

KMS Server Name = *ms1.example.veritas.com*, KMS Server Type = NBKMS

Configure the KMS servers that are listed in the email.

- 3 Perform catalog restore.

Refer to the [NetBackup Troubleshooting Guide](#).

Alerts for expiration of KMS credentials

NetBackup uses the certificates that are stored in credential manager service to connect to KMS server. If this certificate is expired, jobs fail. To avoid job failures, you can configure the notifications that you can receive when the credential certificate is about to expire.

Refer to the [NetBackup Administrator's Guide, Volume I](#) to configure notifications.

Cloud key management service configuration in NetBackup

This chapter includes the following topics:

- [About cloud KMS](#)
- [Workflow to configure cloud KMS in NetBackup](#)
- [Creating credentials in the cloud with permissions to access the created key](#)
- [Add a credential for cloud KMS](#)
- [Configuring proxy server credentials to use with cloud KMS](#)
- [Configure cloud KMS](#)
- [Configuring a key in NetBackup to use the cloud KMS](#)
- [Examples of cloud KMS configuration using nbkmscmd command](#)

About cloud KMS

Along with NetBackup KMS and external KMS, NetBackup now supports cloud KMS to manage data-at-rest encryption keys.

The following cloud providers are supported for cloud KMS configuration in NetBackup:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

- Microsoft Azure

Backup images stored on MSDP storage servers can be encrypted using keys that are maintained in the respective Cloud KMS. NetBackup authenticates with the Cloud KMS using credentials configured in the NetBackup Credential Management System.

Optionally, you can configure an HTTP or HTTPS proxy server to communicate with cloud KMS. Proxy server credentials are managed through the NetBackup Credential Management System using the NetBackup web UI.

Support information for cloud KMS configuration

Cloud KMS is supported only on MSDP storage servers. Tapes, advanced disks, or cloud storage servers are not supported.

- Amazon Web Services (AWS)

- Both symmetric and asymmetric RSA keys are supported.
- For asymmetric RSA keys, RSA_OAEP and RSA_OAEP_256 algorithms are supported.
- For symmetric keys, the AWS-managed symmetric encryption algorithm is used.

- Google Cloud Platform (GCP)

- Only symmetric keys are supported.
- For symmetric keys, the Google-managed symmetric encryption algorithm is used.

- Microsoft Azure

- Only Key Vaults are supported.
- Only asymmetric RSA keys are supported.
- RSA_OAEP and RSA_OAEP_256 algorithms are supported.
- Hardware Security Module (HSM)-backed keys are not supported.

Workflow to configure cloud KMS in NetBackup

Table 26-1

Step	Description
Step 1	Create a cloud key in the required cloud service provider. Review the respective cloud service provider documentation.

Table 26-1 (continued)

Step	Description
Step 2	Create credentials in the cloud with permissions to access the created key. See “Creating credentials in the cloud with permissions to access the created key” on page 545.
Step 3	Add the cloud KMS credentials using NetBackup web UI. See “Add a credential for cloud KMS” on page 546.
Step 4	(Optional step) Add proxy server credentials using NetBackup web UI > Credential Management System . See “Configuring proxy server credentials to use with cloud KMS” on page 547.
Step 5	Configure a cloud KMS server in NetBackup using the credentials that you have added. See “Configure cloud KMS” on page 548.
Step 6	Create a key in NetBackup that maps to the cloud key. See “Configuring a key in NetBackup to use the cloud KMS” on page 549.
Step 7	Configure an MSDP storage server to use the NetBackup key that you have created. Refer to the <i>NetBackup Deduplication Guide</i> .

Creating credentials in the cloud with permissions to access the created key

NetBackup supports the following credential types with respect to the supported cloud providers:

- Amazon Web Services (AWS)
 - Access key – requires access key ID and secret access key.
 - IAM role – assign the role to the EC2 instance that runs the NetBackup primary server. The role must have KMS permissions (kms:Encrypt, kms:Decrypt) for the key you want to use.
- Google Cloud Platform (GCP)
 - Service account – requires client email address, private key, project ID, private key ID, and client ID. The service account must be granted the cloud

KMS CryptoKey Encrypter/Decrypter role
(roles/cloudkms.cryptoKeyEncrypterDecrypter).

- Application default credentials – attach a service account to the VM that runs the NetBackup primary server. This service account must have the roles/cloudkms.cryptoKeyEncrypterDecrypter role for the cloud KMS key.
- Microsoft Azure
 - Service principal – requires client ID, tenant ID, and secret key. The service principal must be granted Cryptographic Operations (encrypt, decrypt) permissions on the key in Azure key vault.
 - Managed identity – assign the managed identity to the Azure VM that runs the NetBackup primary server, and ensure that it has encrypt and decrypt permissions on the key vault key.

Add a credential for cloud KMS

This type of credential allows you to access a cloud KMS server that you have configured using the web UI.

To add a credential for a cloud KMS

- 1 On the left, click **Credential management**.
- 2 On the **Named credentials** tab, click **Add**.
- 3 Select **NetBackup** as credential store and click **Start..**
- 4 Provide the following properties:
 - Credential name
 - Tag
 - Description (for example: This credential is used to access cloud KMS server)
- 5 Click **Next**.
- 6 Select **Cloud KMS** as category.
- 7 Select one of the following access details options: Amazon Web Services, Google Cloud Platform, or Microsoft Azure
- 8 The authentication method to be selected changes as per the access details that are selected.
- 9 Click **Next**.
- 10 Add a role that you want to have access to the credential.

- Click **Add**.
 - Select the role.
 - Select the credential permissions that you want the role to have.
- 11 Click **Next** and follow the prompts to complete the wizard.

Configuring proxy server credentials to use with cloud KMS

Using a proxy server with cloud KMS is optional.

NetBackup can use a proxy server to communicate with the cloud KMS endpoints.

- HTTP and HTTPS proxy servers are supported.
If you are using HTTPS proxy server, ensure the following:
 - The proxy server certificate includes all hostnames of the proxy server in the Subject Alternative Names (SAN) field of the server certificate.
 - The certificate contains valid CRL distribution point (CDP) endpoints, so that NetBackup can check certificate revocation status.
- Only basic authentication is supported. Authentication methods such as Kerberos or NTLM are not supported.

You can use NetBackup web UI or `nbkmscmd` command to create proxy server credentials.

Refer to the [NetBackup Commands Reference Guide](#) to learn more about the `nbkmscmd` command.

Add a credential for proxy server

This type of credential allows you to access a proxy server that you have configured using the web UI.

To add a credential for a proxy server

- 1 On the left, click **Credential management**.
- 2 On the **Named credentials** tab, click **Add**.
- 3 Select **NetBackup** as credential store and click **Start**.
- 4 Provide the following properties:
 - Credential name
 - Tag

- Description (for example: This credential is used to access the proxy server)
- 5** Click **Next**.
- 6** Select **Proxy server** as category.
- 7** Select one of the following authentication options for the proxy server:
 - Authenticated proxy server (requires username and password)
 - Unauthenticated proxy server
- 8** Enter the following proxy server details:
 - Proxy username
 - Proxy password
 - Proxy server
 - Proxy port
 - CA certificate
- 9** Click **Next**.
- 10** Add a role that you want to have access to the credential.
- 11** Select the role and the credential permissions that you want the role to have.
- 12** Click **Next** and follow the prompts to complete the wizard.

Configure cloud KMS

Use this procedure to configure cloud KMS server in NetBackup using web UI.

See [“Add a key in NetBackup to use the cloud KMS server”](#) on page 549.

To configure cloud KMS server

- 1** On the left, click **Security > KMS**.
- 2** Click **Configure**.
- 3** On the **Configure key management server** dialog box, click the **Cloud KMS** option.
- 4** Specify the following KMS server attributes:
 - Enable for backup - Enable the option to use the keys from this KMS configuration for backup.
 - Name - Enter name of the KMS configuration. For example: Google Cloud KMS

- Credentials - Select the credentials for the cloud KMS that you have already added.
See [“Add a credential for cloud KMS”](#) on page 546.
- Priority - A higher value gives the server a higher priority during encryption or decryption.
- Description - Enter the description of the configuration.
- Proxy server - Select the credentials of the proxy server that you have already added and that you want to use for this cloud KMS configuration.
See [“Add a credential for proxy server”](#) on page 547.

5 Click **Configure**.

Configuring a key in NetBackup to use the cloud KMS

In addition to creating a KMS server in NetBackup, you need to create a key in that KMS server to use the key you created in the cloud. You can create the key by using the `nbkmscmd` command.

Refer to the [NetBackup Commands Reference Guide](#) to learn more about commands.

Add a key in NetBackup to use the cloud KMS server

Use this procedure to add a key to use the cloud KMS server using web UI.

After a KMS server is configured in NetBackup, you need to add a key in that KMS server to use the key you have created in the cloud.

See [“Configure cloud KMS”](#) on page 548.

To add a key to use the cloud KMS server

- 1 On the left, click **Security > KMS**.
- 2 Select the cloud KMS for which you want to create a key. On the **KMS details** page, in the **Key groups and keys** section, click **Add**.
- 3 On the **Add key** dialog box, specify the following details:
 - Key group name
 - Algorithm
 - Cloud KMS key ID

- Description

4 Click **Add**.

Examples of cloud KMS configuration using nbkmscmd command

The `-keyname` parameter of the `nbkmscmd` command specifies the unique identifier of the cloud KMS key:

- For AWS: KMS Key ARN (for example: `arn:aws:kms:ap-south-1:123456789012:key/abcd1234-56ef-78gh-90ij-klmnopqrstuv`)
- For GCP: Resource Name (for example: `projects/demo-project/locations/useast1/keyRings/demo-ring/cryptoKeys/demo-key`)
- For Azure: Key URI (for example: `https://demo-keyvault.vault.azure.net/keys/demokey/abcd1234567890`)

The `-keyGroupName` parameter can be a name that you can use in NetBackup for easier identification and management. This is the name that you can use to create MSDP storage server.

Amazon Web Services (AWS)

```
nbkmscmd -createKey \  
-name aws-kms-server-name \  
-keyname arn:aws:kms:region:account-id:key/key-id \  
-keyGroupName aws-key-group-name \  
-algorithm AWS_SYMMETRIC_DEFAULT  
  
nbkmscmd -createKey \  
-name aws-kms-server-name \  
-keyname arn:aws:kms:region:account-id:key/key-id \  
-keyGroupName aws-key-group-name \  
-algorithm RSA_OAEP_256
```

Google Cloud Platform (GCP)

```
nbkmscmd -createKey \  
-name gcp-kms-server-name \  
-keyname projects/demo-project/locations/useast1/keyRings/demo-ring/cryptoKeys/demo-key \  
-keyGroupName aws-key-group-name \  
-algorithm RSA_OAEP_256
```

```
-keyname projects/project-id/locations/<location>/keyRings/<key-ringname>/  
cryptoKeys/crypto-key-name \  
-keyGroupName gcp-key-group-name \  
-algorithm GOOGLE_SYMMETRIC_ENCRYPTION
```

Microsoft Azure

```
nbkmscmd -createKey \  
-name azure-kms-server-name \  
-keyname https://keyvault-name.vault.azure.net/keys/key-name \  
-keyGroupName azure-key-group-name \  
-algorithm RSA_OAEP_256
```

Hardware Security Module (HSM) support in NetBackup

This chapter includes the following topics:

- [Overview of Hardware Security Modules \(HSM\)](#)
- [Configuring Hardware Security Module on a NetBackup host](#)
- [Protecting host ID artefacts in NetBackup using HSM](#)
- [Moving back to file store-based encryption](#)
- [Migrating from one HSM to another HSM](#)

Overview of Hardware Security Modules (HSM)

A Hardware Security Module (HSM) is a physical device designed to generate, store, and manage cryptographic keys securely. HSMs are tamper-resistant and provide a robust mechanism for safeguarding sensitive cryptographic data, including private keys, digital certificates, and authentication tokens.

Some of the key features of an HSM include:

- **Tamper resistance:** HSMs are built to prevent unauthorized access and to wipe keys in case of physical tampering attempts.
- **Secure key generation and storage:** Keys are generated within the HSM ensuring that they never leave the device in unencrypted form.
- **High-performance encryption:** HSMs are optimized for performing cryptographic operations at high speed without compromising security.

To start with HSM usage in NetBackup, security artefacts of host ID credentials can be protected by HSM.

NetBackup leverages PKCS#11 version 2.40 to communicate with the HSM. This abstracts NetBackup from the HSM type that is being used and its hardware bindings (Software based HSM, USB, PCIe or networked) as long as the module (HSM) supports PKCS#11 version 2.40 for communication needs. NetBackup expects an HSM vendor to provide a dynamic library that provides PKCS#11 interface for interacting with HSM.

NetBackup leverages symmetric encryption algorithm that is exposed by HSM. Provisioning of such symmetry key in HSM module should be performed using methods and tools as recommended by HSM vendor.

Configuring Hardware Security Module on a NetBackup host

The NetBackup command `nbhsmcmd` can be used to configure NetBackup to leverage HSM. The `nbhsmcmd -configure` command initiates configuration workflow that requires you to provide the following information about properties of HSM, key to be used, and algorithm.

- Filesystem path to a shared object (with extensions `.so` or `.dll`) that implements PKCS#11 interface as provided by HSM vendor.
- HSM device (token) - configure a human-friendly name for this field.
- User PIN to access HSM. NetBackup never mutates HSM, therefore security officer (SO) PIN is not required.
- A pseudo identifier for the HSM key in NetBackup.
- Label of key that is configured in HSM. This label must exist in HSM for NetBackup to use.
- The key algorithm name. Possible values are as follows:

Note: Not all algorithms are supported by all HSM modules and vendors.

NetBackup supports the following algorithms for HSM usage: AES-GCM, AEC-CBC, AES-CBC-PAD and AES-CTR

- AES-GCM
- AEC-CBC
- AES-CBC-PAD

- AES-CTR

If HSM key, token pin, or PKCS#11 library path needs to be changed after the configuration, use the `nbhsmcmd -update` command to update the parameters.

The `nbhsmcmd -list` command lists the HSM configuration on a NetBackup host in JSON format.

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

Protecting host ID artefacts in NetBackup using HSM

After HSM is configured on NetBackup host using `nbhsmcmd` command, the private key of host ID certificate on NetBackup host can be encrypted using HSM by following steps:

To protect host ID artefacts in NetBackup using HSM

- 1 Use the `nbsetconfig` command to set the required configuration parameter as follows:.

```
NB_CIPHER_KEYSTORE_TYPE = HSM
```

- 2 Use the `nbcertcmd -rotatepassphrasekey` command to rotate passphrase key.
- 3 Use `nbcertcmd -listcertdetails` option to list host ID certificate details.

Check 'Private Key Encryption State' to ensure that the passphrase of the host ID certificate's private key is encrypted using HSM.

Moving back to file store-based encryption

After private key of host ID certificate is encrypted using HSM and if it is required to move out of HSM, the private key can be encrypted using keys that are stored on file systems. Note that the file store-based encryption is the default option.

To move back to file store-based encryption

- 1 Run the following command to change the NetBackup configuration parameter:

```
'nb_cipher_keystore_type' #nbsetconfig nbsetconfig >  
NB_CIPHER_KEYSTORE_TYPE = nbsetconfig >
```

- 2 Run the following command to rotate the passphrase key:

```
nbcertcmd -rotatepassphrasekey
```

- 3 Use the `nbcertcmd -listcertdetails` command to list the host ID certificate details.

Check the 'Private Key Encryption State' to ensure that the passphrase of the host ID certificate's private key is encrypted using file store.

Migrating from one HSM to another HSM

If you want to migrate from one HSM to another, use the following procedure:

To migrate from one HSM to another

- 1 Move to file store-based encryption by rotating passphrase key.
See [“Moving back to file store-based encryption”](#) on page 554.
- 2 Configure new HSM using the `nbhsmcmd` command.
See [“Configuring Hardware Security Module on a NetBackup host”](#) on page 553.
- 3 Encrypt private key of host ID certificate using new HSM.
See [“Protecting host ID artefacts in NetBackup using HSM”](#) on page 554.

Ciphers used in NetBackup for secure communication

This chapter includes the following topics:

- [Ciphers used in NetBackup](#)

Ciphers used in NetBackup

This section lists the ciphers that are used in NetBackup.

Ciphers used for local account password encryption

NetBackup typically does not use local accounts. Instead, accounts that are defined on the local OS or an external identity provider (SAML, AD, or LDAP) are used.

Ciphers used in NetBackup for web API and web UI access (port 443 and 1556)

Table 28-1 Ciphers used in NetBackup for web API and web UI access (port 443 and 1556)

Product version	TLS version	Enabled ciphers
NetBackup 10.0 to 10.3	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384

Table 28-1 Ciphers used in NetBackup for web API and web UI access (port 443 and 1556) (*continued*)

Product version	TLS version	Enabled ciphers
NetBackup 10.4 and later	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384
	TLSv1.3	TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384

Ciphers used in NetBackup for MQbroker (port 13781)

Table 28-2 Ciphers used in NetBackup for MQbroker (port 13781)

Product version	TLS version	Enabled ciphers
NetBackup 10.0 to 10.5	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384
NetBackup 10.5.0.1 and 11.0 (when FIPS mode is disabled)	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384
	TLSv1.3	TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256 TLS_CHACHA20_POLY1305_SHA256
NetBackup 10.5.0.1 and 11.0 (when FIPS mode is enabled)	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384
	TLSv1.3	TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256

Ciphers used for communication between NetBackup hosts

Table 28-3 Ciphers used for communication between NetBackup hosts

Product version	TLS version	Enabled ciphers
NetBackup 10.0 to 10.4	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384

Table 28-3 Ciphers used for communication between NetBackup hosts
(continued)

Product version	TLS version	Enabled ciphers
NetBackup 10.5 and 11.0 (when FIPS mode is disabled)	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384
	TLSv1.3	TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256
NetBackup 10.5 and 11.0 (when FIPS mode is enabled)	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384
	TLSv1.3	TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256

Ciphers used in NetBackup for communication with AD/LDAP servers

If configured, NetBackup uses Openldap to connect directly to LDAP or AD servers. Both LDAP and LDAPS (LDAP over TLS) are supported. The ciphers supported are listed in the following table. The actual cipher chosen for the connection is determined by the configuration of the AD/LDAP server.

Table 28-4 Ciphers used in NetBackup for communication with AD/LDAP servers

Product version	TLS version	Enabled ciphers
NetBackup 10.4	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA

Table 28-4 Ciphers used in NetBackup for communication with AD/LDAP servers *(continued)*

Product version	TLS version	Enabled ciphers
NetBackup 10.5 and later (when FIPS mode is disabled)	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA
	TLSv1.3	TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256
NetBackup 10.5 and later (when FIPS mode is enabled)	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA
	TLSv1.3	TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256

Ciphers used in NetBackup for data at rest encryption

Table 28-5 Ciphers used in NetBackup for data at rest encryption

Product version	Hardware or software-based encryption	Ciphers
NetBackup 10.x and 11.0	Software based except for tape drive encryption	MSDP: AES-256-CTR
		Legacy cloud connector and Advanced Disk Crypt: AES-256-CFB
		Client encryption (selected by customer): AES-128-CFB (default) AES-256-CFB
		Tape drive encryption (hardware-based): AES-256

FIPS compliance in NetBackup

This chapter includes the following topics:

- [About FIPS](#)
- [About FIPS support in NetBackup](#)
- [Prerequisites](#)
- [Specify entropy randomness in NetBackup](#)
- [Configure FIPS mode in your NetBackup domain](#)
- [Enable FIPS mode on NetBackup during installation](#)
- [Enable FIPS mode on a NetBackup host after installation](#)
- [Enable FIPS mode for the NetBackup Authentication Broker service](#)
- [Enable FIPS mode for the NetBackup BAR Console](#)
- [Disable FIPS mode for NetBackup](#)
- [NB_FIPS_MODE option for NetBackup servers and clients](#)
- [USE_URANDOM for NetBackup servers and clients](#)

About 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 the following location:

<http://csrc.nist.gov/groups/STM/cmvp>

About FIPS support in NetBackup

By default, FIPS mode is disabled in NetBackup.

The following workloads are supported in FIPS-compliant mode:

- Oracle, MS-SQL, SAP HANA, DB2, VMware, Hyper-V, RHV, Nutanix, DynamicNAS, MongoDB, Hadoop, HBase, MySQL, PostgreSQL, SQLite, MariaDB, SharePoint
- Cassandra, Sybase, Informix, MS-Exchange, Enterprise Vault, BMR, Universal Shares, OpenStack (cloud-based solution)

The following operating system-level support is available in FIPS mode:

- Once you enable FIPS mode on RHEL 8, the operating system requires that each RPM package has a SHA-256 digest. RPMs that do not have this digest will fail to install. The RPMs that are built using the native toolchain present on RHEL 6 or RHEL 7 platforms do not include a SHA-256 digest and therefore can fail to install on RHEL 8 when FIPS mode is enabled. This issue affects NetBackup 9.1 and earlier setups as packages for these versions are built using the OS native toolchain on RHEL 7 or earlier.
Starting with NetBackup 10.0, the packages are built using a toolchain that adds the SHA-256 digest and these can be installed on RHEL 8 with FIPS mode enabled.

The following components, configurations, or operations are not supported in FIPS mode:

- Client-side encryption

Note: To perform a backup with client-side encryption, you need to disable FIPS mode on the client host.

- NDMP backups
- Scripts (Perl, batch, shell, python) that are executed within NetBackup

- **Binaries or utilities:** `restore_spec_utility`, `nbcallhomeproxyconfig`, `nbbsdtar`, `nbrepo`
- **NetBackup domain with NBAC enabled**
If NBAC is configured in the NetBackup domain, it is recommended that you do not enable FIPS mode.
- The MQBROKER processes do not support NetBackup-level FIPS configuration on Windows.
- MIT Kerberos used by Hadoop and HBase does not operate with a FIPS-enabled OpenSSL. To perform backup with Kerberos authentication, you need to disable FIPS on the backup host.
- NetBackup CloudPoint does not support the CloudPoint host that is configured in FIPS mode.
- SharePoint internally uses encryption algorithms that do not comply with FIPS standards. The Windows FIPS policy blocks the MD5 hashing algorithms that SharePoint uses. Therefore, the OS-level FIPS policy should be disabled for the SharePoint restores for successful operation.
Note that NetBackup-FIPS is supported for protecting SharePoint.
See the following articles for more details:
[FIPS and SharePoint Server](#)
[SharePoint 2016 and FIPS](#)

Prerequisites

Review the given prerequisites before you configure FIPS in your NetBackup environment.

- Ensure the following before FIPS mode is enabled in the NetBackup domain and on the NetBackup clients.
 - The NetBackup primary server and media servers are 10.0 or later.
 - NetBackup clients are 8.1 or later.
 - You have reviewed FIPS support information.
See [“About FIPS support in NetBackup”](#) on page 562.

Note: If FIPS mode is enabled and the backups are targeted to the media server deduplication pool (MSDP), the CPU consumption of your system may increase.

- For seamless SSL communication among the NetBackup processes while FIPS mode is enabled, ensure the following:

- The NetBackup CA private key is in a FIPS-compliant encryption format that is PKCS 8.
- The private key is generated with a FIPS-compliant algorithm for example, RSA.
- The private key strength of the NetBackup CA is set to 2048 or 3072 bits. If the private key strength does not match the supported value, migrate the CA.
See [“Migrating NetBackup CA”](#) on page 357.
If you have configured external CA, contact the concerned security administrator.
See [“About external CA support in NetBackup”](#) on page 399.
- The ongoing NetBackup CA migration process is complete.

Warning: If the prerequisites are not met, some of the NetBackup functions may not work.

Specify entropy randomness in NetBackup

In computing, entropy is the randomness collected by an operating system or application for use in cryptography or other uses that require random data.

This requirement is only for Linux platforms and with Java programs or processes.

You need to specify which randomness to use with JVM arguments. If not specified, it uses `dev/random` by default.

The following is specified as JVM arguments to the Java program:

```
-DjavaDjava.security.egd=file:/dev/./random
```

Enable the `use_urandom` configuration option to make use of `dev/urandom` and restart the services or re-launch the NetBackup BAR Console.

See [“USE_URANDOM for NetBackup servers and clients”](#) on page 574.

Configure FIPS mode in your NetBackup domain

This section provides steps to enable FIPS mode in your NetBackup domain. Before proceeding with the steps, ensure that the prerequisites are met in your environment.

See [“Prerequisites”](#) on page 563.

See [“About FIPS support in NetBackup”](#) on page 562.

Configure FIPS mode on NetBackup during installation

You can configure FIPS mode on NetBackup during installation. Refer to the following topics:

1. See [“Enable FIPS mode on NetBackup during installation”](#) on page 565.
1. See [“Enable FIPS mode for the NetBackup BAR Console”](#) on page 568.

Configure FIPS mode on NetBackup after installation

You can configure FIPS mode on NetBackup after installation. Refer to the following topics:

Note: Ensure that the required configuration steps are carried out on every NetBackup host as applicable.

1. Enable FIPS mode for each host in the NetBackup domain.
See [“Enable FIPS mode on a NetBackup host after installation”](#) on page 566.
 - You must carry out the following step if the host is a primary server:
You must enable FIPS mode for the NetBackup Authentication Broker (AT) by updating the `VRTSatlocal.conf` configuration file on the primary server.
See [“Enable FIPS mode for the NetBackup Authentication Broker service”](#) on page 567.
2. Enable FIPS mode for the **NetBackup BAR Console**.
See [“Enable FIPS mode for the NetBackup BAR Console”](#) on page 568.

Enable FIPS mode on NetBackup during installation

NetBackup lets you enable FIPS mode during installation. For more information, refer to the [NetBackup Installation Guide](#).

After you enable FIPS mode on NetBackup during installation, enable FIPS mode for the **NetBackup BAR Console**.

See [“Enable FIPS mode for the NetBackup BAR Console”](#) on page 568.

Enable FIPS mode on a NetBackup host after installation

This section provides steps to enable FIPS mode on a primary server, a media server, or a client in a NetBackup domain. You should do the following configurations on each host to enable FIPS.

If the host is a primary server, enable FIPS mode for the NetBackup Authentication Broker (AT) by updating the `VRTSatlocal.conf` configuration file on the primary server.

See [“Enable FIPS mode for the NetBackup Authentication Broker service”](#) on page 567.

To enable FIPS mode on a NetBackup host

- 1 Enable the `NB_FIPS_MODE` flag in the NetBackup configuration file.

See [“NB_FIPS_MODE option for NetBackup servers and clients”](#) on page 573.

- 2 Restart the NetBackup services.

To verify if a certain daemon or a command runs in FIPS mode, check the respective logs. The log lines are available only for the daemons and commands that use cryptography.

Example 1: To verify if the `nbcertcmd` command runs in FIPS mode

- 1 Run the following command:

```
nbcertcmd -ping
```

Location of the command:

Windows: `install_path\NetBackup\bin\nbcertcmd`

UNIX: `/usr/opensv/netbackup/bin/nbcertcmd`

- 2 Check the `nbcertcmd` logs.

Location of the log directory:

Windows: `install_path\NetBackup\logs\nbcert`

UNIX: `/usr/opensv/netbackup/logs/nbcert`

The following log lines should be present:

```
<2> nbcertcmd: ./nbcertcmd -ping ProcessContext: ProcessName:[nbcertcmd],  
FipsMode:[ENABLED], Username:[root], IsServiceAdmin:[0], UserID:[0], GroupID:[0]
```

Example 2: To verify if the NetBackup Web Management Console runs in FIPS mode

- ◆ By default, FIPS mode is disabled when the **NetBackup Web Management Console** (`nbwmc`) service runs. FIPS mode is enabled for the `nbwmc` service after you enable it for the NetBackup host.

Check the `catalina` log file on the NetBackup primary server host to verify if the `nbwmc` service runs in FIPS mode.

Location of the log file:

Windows:

```
install_path\NetBackup\wmc\webserver\logs\catalina-date.log
```

UNIX: `/usr/opensv/wmc/webserver/logs/catalina-date.log`

The following log lines should be present:

```
The nbwmc service is running in FIPS approved mode
```

Enable FIPS mode for the NetBackup Authentication Broker service

The NetBackup Authentication Broker (`nbatd`) service runs only on the NetBackup primary server, therefore you need to enable FIPS mode on the primary server to enable it for the `nbatd` service.

FIPS mode is disabled by default.

Note: From version 10.5 and later, for Cloud Scale deployment, the `nbatd` containerized service is running in a separate Kubernetes Pod cluster server rather than the NetBackup primary server Pod. To enable the FIPS mode for the NetBackup Authentication Broker service, execute the same steps on the `nbatd` containerized service mentioned in the section *Enable FIPS mode for the NetBackup Authentication Broker service*.

To enable FIPS mode for the `nbatd` service or the `nbatd` containerized service

- 1 Open the following directory on the primary server:

On UNIX: `/usr/opensv/netbackup/sec/at/bin/`

On Windows: `install_path\NetBackup\sec\at\bin\`

- 2 Run the following command:

On UNIX: `run vssregctl -s -f`

`/usr/opensv/var/global/vxss/eab/data/root/.VRTSat/profile/VRTSatlocal.conf`
`-b "Security\Authentication\Client" -k FipsMode -t int -v 1`

On Windows: `run vssregctl -s -f`

`"install_path\NetBackup\var\global\vxss\eab\data\systemprofile\VRTSatlocal.conf"`
`-b "Security\Authentication\Client" -k FipsMode -t int -v 1`

For example:

Run the following command on Windows:

```
vssregctl -s -f
"Install_Path\NetBackup\var\global\vxss\eab\data\systemprofile\VRTSatlocal.conf"
-b "Security\Authentication\Client" -k FipsMode -t int -v 1 3
```

Check the `nbatd` logs.

Location of the `nbatd` logs:

On UNIX:

`/usr/opensv/logs/nbatd`

On Windows:

`install_path\NetBackup\logs\nbatd`

The following log lines should be present:

```
*** Trying to start Broker In FIPS mode ***
```

```
*** Broker In FIPS mode already ***
```

- 3 Restart the NetBackup services.

Enable FIPS mode for the NetBackup BAR Console

By default, FIPS mode for the **NetBackup BAR Console** is disabled.

To enable FIPS mode for the NetBackup BAR Console (on local or remote host)

- 1 Open the **NetBackup BAR Console** configuration file.
 - On Windows computers, the file containing configuration options for the **NetBackup BAR Console** is: `install_path\java\nbj.conf`
 - On UNIX computers, the file containing configuration options for the **NetBackup BAR Console** is: `/usr/opensv/java/nbj.conf`
- 2 In the configuration file, enable the `NB_FIPS_MODE` option. Use the following format:

```
NB_FIPS_MODE = true
```

- 3 Save the changes.
- 4 Restart the **NetBackup BAR Console**.

To verify if the NetBackup BAR Console runs in FIPS mode

- ◆ Check the **NetBackup BAR Console** logs.

Log location:

On Windows:

```
install_path\logs\user_ops\nbjlogs\jbp.root.jnbSA.pid.log
```

On UNIX: `/usr/opensv/netbackup/logs/user_ops/nbjlogs/jbp.root.jnbSA.pid.log`

On a standalone console, create a directory structure and check the logs.

If the log file contains the following log lines, it means the console runs in FIPS mode:

```
com.safelogic.cryptocomply.fips.approved_only: true
```

It should have the following log lines:

```
JavaPresentationLayer- FIPS mode enforced. Reconfiguring SunJSSE.  
JavaPresentationLayer- BAR console is running in FIPS approved mode
```

Note: This FIPS mode configuration does not affect the NetBackup KMS FIPS mode. NetBackup KMS continues to run in FIPS mode by default.

Disable FIPS mode for NetBackup

The following configurations are required to disable FIPS mode in your NetBackup domain:

- Disable FIPS mode for each NetBackup host.
See [“Disable FIPS mode for a NetBackup host”](#) on page 570.
- Disable FIPS mode for the NetBackup Authentication Broker (`nbatd`) service.
See [“Disable FIPS mode for NetBackup Authentication broker \(`nbatd`\)”](#) on page 571.
- Disable FIPS mode for the **NetBackup BAR Console**.
See [“Disable FIPS mode for the NetBackup BAR Console”](#) on page 572.

Disable FIPS mode for a NetBackup host

Carry out the following steps on each NetBackup host to disable FIPS mode.

To disable FIPS mode for a host

- 1 Disable the `NB_FIPS_MODE` flag in the NetBackup configuration file.
See [“NB_FIPS_MODE option for NetBackup servers and clients”](#) on page 573.
- 2 Restart the NetBackup services.

To verify if FIPS mode is disabled for a certain daemon or a command, check the respective logs. The log lines are available only for the daemons and commands that use cryptography.

Example 1: To verify if FIPS mode is disabled for the `nbcertcmd` command

- 1 Go to the following directory:
UNIX: `/usr/opensv/netbackup/bin`
Windows: `install_path\NetBackup\bin`
- 2 Run the following command: `nbcertcmd -ping`
- 3 Go to the `nbcertcmd` logs at the following directory:

UNIX: `/usr/opensv/netbackup/logs/nbcert`

Windows: `install_path\NetBackup\logs\nbcert`

- 4 Check the logs. The log file should contain the following log lines:

```
ProcessContext: ProcessName:[nbcertcmd], FipsMode:[DISABLED], Username:[r  
IsServiceAdmin:[0], UserID:[0], GroupID:[0]
```

Example 2: To verify if FIPS mode is disabled for the NetBackup Web Management Console (nbwmc) service

- 1 Disabling FIPS mode for NetBackup services also disable FIPS mode for `nbwmc` service running on the primary server host.

Open the following log file on the NetBackup primary server host:

UNIX: `/usr/opensv/wmc/webserver/logs/catalina-date.log`

Windows:

`install_path\NetBackup\wmc\webserver\logs\catalina-date.log`

- 2 Check if the log file contains the following log line:

`The nbwmc service is running in non-FIPS mode`

Disable FIPS mode for NetBackup Authentication broker (`nbatd`)

Carry out the following steps to disable FIPS mode for `nbatd` that runs on NetBackup primary server host.

To disable FIPS mode for `nbatd`

- 1 Open the following directory on the primary server.

On UNIX:

```
/usr/opensv/netbackup/sec/at/bin/
```

On Windows:

```
install_path\NetBackup\sec\at\bin\
```

- 2 Run the following command:

On UNIX:

```
run vssregctl -s -f  
/usr/opensv/var/global/vxss/eab/data/root/.VRTSat/profile/VRTSatlocal.conf  
-b "Security\Authentication\Client" -k FipsMode -t int -v 0
```

On Windows

```
run vssregctl -s -f  
"install_path\NetBackup\var\global\vxss\eab\data\systemprofile\VRTSatlocal.conf"  
-b "Security\Authentication\Client" -k FipsMode -t int -v 0
```

Run the following command on Windows:

```
vssregctl -s -f  
"Install_Path\NetBackup\var\global\vxss\eab\data\systemprofile\VRTSatlocal.conf"  
-b "Security\Authentication\Client" -k FipsMode -t int -v 0
```

- 3 Restart the NetBackup services.

To verify if FIPS mode is disabled for the `nbatd` service

- 1 Go to the `nbatd` logs at:

UNIX:

```
/usr/opensv/logs/nbatd/
```

Windows:

```
install_path\NetBackup\logs\nbatd\
```

- 2 Check if the log file has the following log line:

```
Broker Not In FIPS mode
```

Disable FIPS mode for the NetBackup BAR Console

Carry out the following steps on each NetBackup host to disable FIPS mode.

To disable FIPS mode for the NetBackup BAR Console (on a local or a remote host)

- 1 Open the **NetBackup BAR Console** configuration file.

On Windows computers, the file containing configuration options for the **NetBackup BAR Console** is: `install_path\java\nbj.conf`

On UNIX computers, the file containing configuration options for the **NetBackup BAR Console** is: `/usr/opensv/java/nbj.conf`

- 2 In the configuration file, disable the `NB_FIPS_MODE` option. Use the following format:

`NB_FIPS_MODE = false`

- 3 Save the changes.

- 4 Restart the **NetBackup BAR Console**.

To verify if FIPS mode is disabled for the NetBackup BAR Console

- ◆ Check the **NetBackup BAR Console** logs.

Log location:

On UNIX: `/usr/opensv/netbackup/logs/user_ops/nbjlogs/jbp.root.jnbSA.pid.log`

On Windows:

`install_path\logs\user_ops\nbjlogs\jbp.root.jnbSA.pid.log`

On a standalone console, create a directory structure (for example, `Install_Path\NetBackup\logs\user_ops\nbjlogs`) and check the logs.

If the log file contains the following log lines, it means FIPS mode is disabled for the console:

```
JavaPresentationLayer- Fips approved mode system property is - false
JavaPresentationLayer- BAR console is running in non-FIPS mode
```

NB_FIPS_MODE option for NetBackup servers and clients

Use the `NB_FIPS_MODE` option to enable the FIPS mode in your NetBackup domain.

Table 29-1 NB_FIPS_MODE information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. By default, the <code>NB_FIPS_MODE</code> option is disabled. To enable the option, use the following format: <pre>NB_FIPS_MODE = ENABLE</pre> To disable the option, use the following format: <pre>NB_FIPS_MODE = DISABLE</pre>
Equivalent NetBackup web UI property	No equivalent exists in the host properties.

USE_URANDOM for NetBackup servers and clients

In computing, entropy is the randomness collected by an operating system or application for use in cryptography or other uses that require random data.

Enable the `USE_URANDOM` option to specify `/dev/urandom` as the character device to provide cryptographically secure random output in your NetBackup environment.

Table 29-2 USE_URANDOM information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 29-2 USE_URANDOM information (*continued*)

Usage	Description
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. The default value of the <code>USE_URANDOM</code> option is 0. When the <code>USE_URANDOM</code> option is set to default, the character device to be used is based on the value of the <code>NB_FIPS_MODE</code> option. If <code>NB_FIPS_MODE</code> is enabled, <code>dev/random</code> is used. If <code>NB_FIPS_MODE</code> is disabled, <code>dev/urandom</code> is used. See “NB_FIPS_MODE option for NetBackup servers and clients” on page 573. To enable the <code>USE_URANDOM</code> option, use the following format: <pre>USE_URANDOM = 1</pre> If <code>USE_URANDOM</code> is set to 2 (or is disabled), the <code>dev/random</code> character device is used to provide cryptographically secure random output.
Equivalent NetBackup web UI property	No equivalent exists in the host properties.

Post-Quantum Cryptography (PQC) support in NetBackup

This chapter includes the following topics:

- [About Post-Quantum Cryptography \(PQC\)](#)
- [PQC support for TLS communication](#)
- [Configuring PQC in NetBackup](#)
- [Configuring PQC for deduplication](#)

About Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography (PQC) aims to construct public key cryptosystems that are believed to be secure even against quantum computers. While traditional public-key cryptographic systems like RSA, ECC, and DH rely on the computational difficulty of problems like integer factorization and discrete logarithms, quantum computers that leverage Shor's algorithm can solve these problems efficiently. PQC focuses on algorithms based on mathematical problems that are resistant to quantum computing attacks, such as lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography, and hash-based cryptography. PQC is crucial for securing communications in a future where quantum computers become practical.

Adversaries can now intercept and store encrypted communications with the intent to decrypt them in the future when quantum computers are capable of breaking current cryptographic systems.

The transition to quantum-safe cryptography is a proactive measure to ensure long-term confidentiality and security of your data and domain.

PQC support for TLS communication

NetBackup supports Post-Quantum Cryptography (PQC) for TLS 1.3 communication using the Open Quantum Safe (OQS) provider. While the OQS provider prepares you for a quantum-safe future, it is currently widely used in experimental and research environments.

Note: It is recommended that you thoroughly assess all associated risks and ensure that the use of the OQS provider aligns with your organization's security policies and compliance requirements before enabling PQC in NetBackup.

- PQC is supported for TLS 1.3 communication using hybrid KEMs. By default, NetBackup uses x25519_kyber768 TLS group.
- NetBackup does not support PQC in FIPS mode.
- NetBackup 11.0 or later hosts support PQC. Communication with NetBackup hosts earlier than 11.0 is in a traditional way.
- In NetBackup 11.0, PQC is supported only for RHEL and Windows platforms.
- PQC is currently supported for communication with the following NetBackup components:
 - Secure comms proxies (vnetd proxies)
 - Data In-Transit Encryption (DTE)
 - KMIP
 - cURL clients (libnbcurl, CRL downloader, ckms, cloud plugins, shelteredharbor)
 - MSDP (except deduplication to cloud communication)

Configuring PQC in NetBackup

The `NB_PQC_MODE` option enables the use of Post Quantum Cryptography (PQC) algorithm in TLS 1.3 Hybrid Key Exchange.

See “[About Post-Quantum Cryptography \(PQC\)](#)” on page 576.

Caution: NetBackup leverages the Open Quantum Safe (OQS) provider to support PQC for secure communications. While the provider is a significant step towards preparing for a quantum-safe future, it is widely used in experimental and research environments. It is recommended that you thoroughly assess all the associated risks and ensure that its usage aligns with your organization's security policies and compliance requirements before you enable the `NB_PQC_MODE` option.

Note: The PQC mode is supported only if the FIPS mode is disabled.

Table 30-1 `NB_PQC_MODE`

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the <i>NetBackup Commands Reference Guide</i>. By default, the <code>NB_PQC_MODE</code> option is disabled. To enable the option, use the following format: <pre>NB_PQC_MODE = ENABLE</pre> To disable the option, use the following format: <pre>NB_PQC_MODE = DISABLE</pre> After you enable or disable PQC in NetBackup, restart the NetBackup service on the server and the client using the following commands: For UNIX, run the following commands: <pre>/usr/opensv/netbackup/bin/bp.kill_all /usr/opensv/netbackup/bin/bp.start_all</pre> For Windows: <pre>install_path\NetBackup\bin\bpdown install_path\NetBackup\bin\bpup</pre>
Equivalent NetBackup web UI property	No equivalent exists in the host properties.

The cluster failover or restarting services through cluster console does not restart the `vnetd` or `bpcd` service that is already running on cluster nodes.

Restart the `vnetd` service manually on each cluster node to reflect the changes in the PQC mode.

On UNIX, do the following:

To stop `vnetd` service on UNIX, run the following command:

```
/usr/opensv/netbackup/bin/vnetd -terminate
```

To start `vnetd` service on UNIX, run the following command:

```
/usr/opensv/netbackup/bin/vnetd -standalone
```

On Windows, restart 'NetBackup Legacy Network Service' using the Service Control Manager (SCM).

Configuring PQC for deduplication

Ensure that you have configured the storage server before you enable PQC for media server deduplication (MSDP).

Note: The PQC mode is not supported for Open Cloud Storage Daemon (OCSD).

For more information on deduplication, see the [NetBackup Deduplication Guide](#).

Enabling PQC for MSDP

To enable PQC for MSDP

- 1 Run the following commands to set the PQC mode:

On UNIX:

```
/usr/opensv/pdde/pdag/scripts/set_pqc_mode.sh 1
```

On Windows:

```
install_path\Veritas\pdde\set_pqc_mode.bat 1
```

- 2 Restart the NetBackup service on the server and the client using the following commands.

On UNIX:

```
/usr/opensv/netbackup/bin/bp.kill_all
```

```
/usr/opensv/netbackup/bin/bp.start_all
```

On Windows:

```
install_path\NetBackup\bin\bpdown
```

```
install_path\NetBackup\bin\bpup
```

Disabling PQC for MSDP

To disable PQC for MSDP

- 1 Run the following commands to disable PQC:

On UNIX:

```
/usr/opensv/pdde/pdag/scripts/set_pqc_mode.sh 0
```

On Windows:

```
install_path\Veritas\pdde\set_pqc_mode.bat 0
```

- 2 Restart the NetBackup service on the server and the client using the following commands.

On UNIX:

```
/usr/opensv/netbackup/bin/bp.kill_all
```

```
/usr/opensv/netbackup/bin/bp.start_all
```

On Windows:

```
install_path\NetBackup\bin\bpdown
```

```
install_path\NetBackup\bin\bpup
```

Viewing the PQC status for MSDP

To view status of the MSDP PQC mode, use the following commands:

On UNIX:

```
/usr/opensv/pdde/pdcr/bin/crcontrol --getmode
```

On Windows:

```
install_path\Veritas\pdde\crcontrol.exe --getmode
```

STIG compliance support in NetBackup

This chapter includes the following topics:

- [About STIG compliance support](#)
- [NBFP_CHECK option for NetBackup servers and clients](#)
- [Verifying and correcting file permissions using nbfp command](#)

About STIG compliance support

Starting with 11.1, NetBackup supports STIG compliance through RPM verification of packaged files.

Workflow to enable STIG compliance support in NetBackup

Table 31-1

Step	Description
Step 1	Set the <code>NBFP_CHECK</code> configuration option to the appropriate value. See “NBFP_CHECK option for NetBackup servers and clients” on page 583.
Step 2	Use the <code>nbfp</code> command to perform various operations that are related to STIG compliance support. See “Verifying and correcting file permissions using nbfp command” on page 583. See the NetBackup Commands Guide for more details on the <code>nbfp</code> command.

NBFP_CHECK option for NetBackup servers and clients

Use the `NBFP_CHECK` option to control whether permissions and ownership of NetBackup files should be verified, corrected, and reported to the web UI or not.

Table 31-2

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. The <code>NBFP_CHECK</code> configuration option can have the following values: <code>FIX</code> – Corrects permissions and ownership of the files. <code>FIX_NOTIFY</code> – Corrects permissions and ownership of the files, and posts the results on to the NetBackup web UI. <code>VERIFY</code> – Verifies permissions and ownership of the files. <code>VERIFY_NOTIFY</code> – Verifies permissions and ownership, and posts the results on to the NetBackup web UI. To disable the option, use the following format: <pre>NBFP_CHECK = OFF</pre>
Equivalent NetBackup web UI property	No equivalent exists in the NetBackup web UI.

Verifying and correcting file permissions using `nbfp` command

Use the `nbfp` command to verify and correct file permissions required for STIG compliance.

The `nbfp` command resets the file permissions of the NetBackup installation directory to the default values.

To verify and correct file permissions

- 1 Run the following command to verify file permissions:

```
nbfp--verify [--path=path1 [path2...pathn]] [--exclude_path=path1  
[path2...pathn]] [--exclude_large_dirs] [--silent] [--verbose]  
[--json]
```

- 2 Run the following command to fix the file permissions:

```
nbfp --fix [--path=path1 [path2...pathn]] [--exclude_path=path1  
[path2...pathn]] [--exclude_large_dirs] [--silent] [--verbose]  
[--json]
```

NetBackup web services account

This chapter includes the following topics:

- [About the NetBackup web services account](#)
- [Changing the web service user account](#)

About the NetBackup web services account

Beginning with NetBackup 8.0, the NetBackup primary server includes a configured web server to support critical backup operations. This web server operates under user account elements with limited privileges. These user account elements must be available on each primary server (or each node of a clustered primary server).

NetBackup requires account information for web services as part of the NetBackup primary server installation.

More information is available on configuring this account prior to installation and on how to change the account after installation.

See the *NetBackup Installation Guide* for information on how to create the web server user and group.

See [“Changing the web service user account”](#) on page 586.

Note: For security purposes, do not allow the web server users or groups to have administrator or superuser privileges.

Changing the web service user account

To support changing web service user accounts, use the utility script `wmcUtils`. This utility script does not validate if a web service user and group exist. Before you use this utility, you must ensure that the web service user and the group exist and the user is part of the group. Consider the following when changing the web service user account:

- If your environment uses Windows domain users, use the `DOMAIN\USER` format.
- If you use a clustered environment on a Windows platform, the NetBackup web services user account must be a `DOMAIN` user. (Example: AD user)
- If you use non-clustered environments, the NetBackup web service user can be a local or a domain user.
- If you use a clustered environment on Linux or UNIX platforms, the NetBackup web service user can be a local user. Additionally, the group can be a local group. The NetBackup web service user must have the same name and UID on all nodes of the cluster. Also, the group must have the same name and GID on all nodes of the cluster. It is recommended to use domain users (Example: NIS) for clustered environments.

Note: Do not use the logged on user to run the `wmcUtils` utility script. If you are logged into an environment as `my_domain\my_user`, you cannot use this account to run the NetBackup Web Management Console service. NetBackup does not support this scenario.

Correcting file permissions

To correct file permissions, run the following command:

```
wmcUtils -fixPerms/-forceFixPerms
```

Refer to the *NetBackup Commands Reference Guide* for more details.

To change the web service user account on Windows

- 1 Open command prompt.
- 2 Change the directory to: `install_path\wmc\bin\install`

- 3 Run `wmcUtils.bat -changeUser` to change the web service user.

Example: (`nbwebsvc1` is the web service user and `nbwebgrp1` is the user group that `nbwebsvc1` is a member of)

```
wmcUtils.bat -changeUser nbwebsvc1 nbwebgrp1
```

For more information about the `wmcUtils.bat` utility script, use the `wmcUtils.bat -help` option.

- 4 (Conditional) If using a clustered environment, run `wmcUtils.bat -changeUser` on the active and the inactive nodes.
- 5 Enter the web service user password (example: `nbwebsvc1`) when prompted by the script.

The NetBackup Web Management Console service is restarted when the correct password is entered. If you enter an incorrect password, a **Logon failure** error is displayed before the NetBackup Web Management Console service starts.

- 6 To verify that the web service user is changed, ensure that `install_path\bin\NBCertCmd.exe -ping` works.

Note: The output of `wmcUtils.bat` utility script is captured in the `nbwmc_support.log`. The log is located here:
`install_path\wmc\webserver\logs\nbwmc_support.log`

To change the web service user account on Linux or UNIX

- 1 Open a shell.
- 2 Change the directory to: `/usr/opensv/wmc/bin/install`
- 3 Run `wmcUtils -changeUser` to change the web service user.

Example: (`nbwebsvc1` is the web service user and `nbwebgrp1` is the user group that `nbwebsvc1` is a member of)

```
usr/opensv/wmc/bin/install/wmcUtils -changeUser nbwebsvc1 nbwebgrp1
```

For more information about the `wmcUtils` utility script, use the `wmcUtils -help` option.

- 4 (Conditional) If using a clustered environment, run `wmcUtils.bat -changeUser` on the active and the inactive nodes.

- 5 Enter the web service user password (example: `nbwebsvc1`) when prompted by the script.

The NetBackup Web Management Console service is restarted when the correct password is entered. If you enter an incorrect password, a **Logon failure** error is displayed before the NetBackup Web Management Console service starts.

- 6 To verify that the web service user is changed, ensure that `/usr/opensv/netbackup/bin/nbcertcmd -ping` works.

Note: The output of `wmcUtils` utility script is captured in the `nbwmc_support.log`. The log is located here: `/usr/opensv/wmc/webserver/logs/nbwmc_support.log`

Note: On UNIX/Linux primary servers where `/usr/opensv` is a symlink to a non-default installation directory, changing the service user can sometimes prevent the NetBackup Web Management Console from starting, even though the command completes successfully. If this issue occurs, log on as the root user and run `wmcUtils -fixPerms` to correct the file permissions. Then verify that the NetBackup Web Management Console is running. For more information, see [Troubleshooting issues with the non-privileged user \(service user\) account](#).

Running NetBackup services with non-privileged user (service user) account

This chapter includes the following topics:

- [About a NetBackup service user account](#)
- [Configuring a service user account](#)
- [Changing a service user account after installation or upgrade](#)
- [Giving access permissions to service user account on external paths](#)
- [NetBackup services that run with the service user account](#)

About a NetBackup service user account

Starting with NetBackup 9.1, most of the primary server services can be run with a non-privileged user, which is highly recommended. The non-privileged user is referred to as `service user` and is intended only to run NetBackup services.

Important considerations for using a service user account

Review the following to run NetBackup services with the service user account.

- Do not use the service user account to perform any NetBackup operations. The service user account is intended only to run NetBackup services.

- It is recommended that the primary group of the service user must only be for the service user.
- It is not recommended to use the root user as the service user.
- The `nbwebsvc` user should not be used as the service user.
- `nbwebgrp` must be a secondary group of the service user.
- Number of processes that can be run with the service user must be same as the processes that run with the root user.
Use `ulimit -u` to find the maximum number of user processes that can run with the service user.
- Number of files that can be opened with the service user must be same as the files that are opened with the root user.
Use the `ulimit -Hn` command to view the maximum number of files that can be open with the service user.
- Using a service user account other than the root user account involves a one-time conversion that may significantly increase the upgrade time based on your catalog size.
- Other than the installation directory, all external paths must be accessible by the service user.
See [“Giving access permissions to service user account on external paths”](#) on page 592.
- Environment variable paths must be accessible by the service user.
- The service user must have access to the OS temporary directory that is usually `/tmp` or `/var/tmp`. This may be dictated by `P_tmpdir` macro.
- Service user account can be a password-less account.
- If a service user is configured, legacy log files (`/user/openssl/netbackup/logs` on UNIX or `C:\Program Files\Veritas\NetBackup\logs` on Windows) have a prefix as `SERVICE_USER`.
For example: `SERVICE_USER.040921_00001.log`
- The service user name must contain less than 32 characters and must have English characters only.
- If the `bpcd` and `vneta` processes run under an application account such as Oracle Admin, you must not change that account to the service user account.

Configuring a service user account

The service user must be created in advance and must have `nbwebgrp` as the secondary group.

Configuring a service user account on UNIX

During installation or upgrade of the primary server on UNIX, you can see a new prompt to specify a new user - preferably a non-root user - that can be used as a service user. Most daemons on the primary server now run with the new service user.

To create the local user account on UNIX, run the following command:

```
useradd -c 'NetBackup Services account' -d /usr/opensv/  
service_user_name
```

To add the service user to the `nbwebgrp` secondary group, run the following command:

```
usermod -a -G nbwebgrp service_user_name
```

Review the following:

- In a clustered environment, ensure that local accounts are defined consistently on all cluster nodes. If you use a clustered environment on Linux or UNIX platforms, the NetBackup service user can be a local user. The NetBackup service user must have the same name and UID on all nodes of the cluster.
- It is recommended to use domain users (for example: NIS) in a clustered environment. LDAP accounts are supported and can be used on UNIX.
- The NetBackup service account must use a POSIX compliant shell.

Configuring a service user account on Windows

On Windows, fresh installation uses the Local Service built-in account. There is no change in the upgrade process.

Changing a service user account after installation or upgrade

On UNIX, you can change service user account to any other user account using the `nbSERVICEUSERCMD` command.

On Windows, you can change service user account to Administrator, Local System or Local Service using `nbSERVICEUSERCMD` command.

Use the following command to correct file permissions:

```
nbserveusercmd --fixPerms/--forceFixPerms
```

Refer to the [NetBackup Commands Reference Guide](#) for more details.

Giving access permissions to service user account on external paths

NetBackup operations fail if the service user account does not have access permissions on directory paths that are external to NetBackup and their contents. Other than the installation directory, all external paths must be accessible by the service user account, for example:

- Disaster recovery (DR) path
- External CA certificate paths
- External paths that are used as parameters to the following commands:
 - `nbdb_admin`
 - `create_nbdb`
 - `nbdb_move`
 - `nbdb_backup`
 - `nbdb_restore`
 - `nbdb_unload`
 - `cat_export`
 - `cat_import`

To give access permissions to service user account on external paths

- 1 Ensure that the paths that are specific to NetBackup operations are not shared across multiple users on the host.
 - On UNIX, ensure that the paths are not as follows:
`/tmp`, `/root`, or home directory of any other non-root user
 - On Windows, ensure that the paths are not directories of a different user account that resides in `C:\users`.
- 2 Run the following command to give access to the service user account on external paths and their contents:
 - On UNIX: `chown -R service_user_name path`
After the `chown` command is run, verify if the service user can write to the specified path using the following command:

```
su service_user_name -c "touch path/test.txt"
```

- On Windows:

```
netbackup_install_path\NetBackup\bin\goodies\nbserviceusercmd.exe  
-addacl path -reason reason
```

NetBackup services that run with the service user account

Windows

UNIX

NetBackup Request Daemon	bprd
NetBackup Database Manager	bpdbm
-	bpjobd
NetBackup Compatibility Service	bpcompatd
NetBackup Audit Manager	nbaudit
NetBackup Event Manager	nbevtmgr
NetBackup Enterprise Media Manager	nbemm
NetBackup Resource Broker	nbrb
NetBackup Job Manager	nbjm
NetBackup Policy Execution Manager	nbpem
NetBackup Service Layer	nbsl
NetBackup Storage Lifecycle Manager	nbstserv
NetBackup Proxy Service	nbproxy
NetBackup Indexing Manager	nbim
NetBackup Agent Request Server	nbars
NetBackup Key Management Service	nbkms
NetBackup Vault Manager	nbvault
Anomaly Detection Management Service	nbanomalygmt

Windows

`vnetd-child-proxies`

- `vnetd -proxy inbound_proxy -number 0`
- `vnetd -proxy outbound_proxy -number 0`
- `vnetd -proxy http_api_tunnel -number 0`
- `vnetd -proxy http_pbx_tunnel -number 0`

Note: If you have selected Administrator account as a privileged service account (the user account that the `vnetd` standalone service uses) then the `vnetd` child proxies run with the same Administrator account.

UNIX

`vnetd-child-proxies`

- `vnetd -proxy inbound_proxy -number 0`
- `vnetd -proxy outbound_proxy -number 0`
- `vnetd -proxy http_api_tunnel -number 0`
- `vnetd -proxy http_pbx_tunnel -number 0`

Running NetBackup commands with non-privileged user account

This chapter includes the following topics:

- [Running NetBackup commands using the `nbcmdrun` wrapper command](#)

Running NetBackup commands using the `nbcmdrun` wrapper command

`nbcmdrun` is a wrapper command that is used to run other NetBackup commands on a NetBackup host. The NetBackup host can be a primary server, a media server, or a client.

Certain NetBackup commands can be run only by the Operating System (OS) Administrator if run without the `nbcmdrun` wrapper. However with the `nbcmdrun` wrapper, a non-privileged OS user with the required RBAC permissions can also run these commands.

For consistency in the use of NetBackup commands, it is recommended that you run all commands using the `nbcmdrun` wrapper command.

See the [NetBackup Commands Reference Guide](#) for more information on the NetBackup commands.

Who can run NetBackup commands

Users with the following roles can run the NetBackup commands:

- OS Administrator (root in Linux and Administrator Group members in Windows)
- RBAC Administrator
- RBAC CLI-Administrators

For example, OS Administrator, RBAC Administrator, and RBAC CLI-Administrator can run the following commands:

- `nbcmdrun bppllist [arguments]`
- `nbcmdrun bpstuadd [arguments]`
- `nbcmdrun nbdb_move [arguments]`
- `nbcmdrun mklogdir [arguments]`
- `nbcmdrun tpconfig [arguments]`

Users with specific RBAC permissions can run NetBackup policy-specific commands (such as `bpolicynew`, `bpplsched`).

See the following examples:

- User with the 'Policy > Delete' permission can run the `nbcmdrun bppldelete` command.
- User with the 'Policy > Update' permission can run the `nbcmdrun bpplinfo -set | -modify` command.

To see the entire list of RBAC-supported commands that can be run with `nbcmdrun`, run the following command:

```
nbcmdrun -listRbacCommands
```

How does `nbcmdrun` function

To run the `nbcmdrun` command, you must authenticate yourself by performing one of the following tasks:

- Do a web login in the current NetBackup domain using the `bpnbat -login -loginType WEB` command.
- Use the following command to present the file with JWT or API-Key as an environment variable:

```
set FILE_LOGIN_CONTEXT=jwt or api-key file
```

Alternatively use the following command:

```
export FILE_LOGIN_CONTEXT=jwt or api-key file
```

`nbcmdrun` retrieves this authentication token (JWT or API-Key) of the user and presents it to the server for the user's authentication, authorization, and auditing.

`nbcmdrun` has multiple connection points based on the command that is run with `nbcmdrun`.

- `nbcmdrun` can run a command (for example: `nbcmdrun bpstulist`) in the same user context, wherein the command itself connects to the domain services like `bpdbm` or `nbemm`.
- `nbcmdrun` can run a command (for example: `nbcmdrun nbdb_move`) as is under the service account (`vnetd`).
- `nbcmdrun` can run a command (for example: `nbcmdrun tpconfig`) as is under the privileged account (NBPAS).
- `nbcmdrun` can run a command (for example: `nbcmdrun bppolicynew`) as is via web services (`nbwebservice`).

Immutability and indelibility of data in NetBackup

This chapter includes the following topics:

- [About immutable and indelible data](#)
- [Workflow to configure immutable and indelible data](#)
- [Deleting an immutable image from storage using the bpexpdate command](#)
- [Removing an immutable image from the catalog using the bpexpdate command](#)

About immutable and indelible data

NetBackup protects your data from being encrypted, modified, and deleted using WORM properties.

WORM is the acronym for Write Once Read Many.

WORM properties provide two additional levels of security for backup images:

- **Immutability** - this protection ensures that the backup image is read-only and cannot be modified, corrupted, or encrypted after backup.
- **Indelibility** - this property protects the backup image from being deleted before it expires. The data is protected from malicious deletion.

Configuring these WORM properties protects your data from certain malware attacks to some extent, for example ransomware.

NetBackup provides the ability to write backups to WORM storage devices so their data cannot be corrupted. Additionally, it lets you take advantage of advanced options available from your storage vendors to ensure backups are retained unaltered on storage platforms to meet regulatory and compliance requirements.

All NetBackup image copies have an Expiration Time. This time is calculated by using the configured retention level in the schedule and the start time of the backup job.

When a NetBackup image is written to a WORM-enabled storage unit, the data cannot be altered or deleted until the WORM Unlock Time for that image has elapsed. Unlike the Copy Expiration time that is calculated from the start time of the backup job, the WORM Unlock Time is associated with the WORM storage. The WORM Unlock Time value is calculated using the configured retention level and the write completion timestamp for the backup image onto WORM storage.

When you use `bpimagelist` to view an image that is written to WORM storage, the timestamp that is associated with the Copy Expiration time precedes the WORM Unlock Time for that copy of the backup image. For longer-running backups or duplication jobs, the difference is greater between Copy Expiration Time and WORM Unlock Time.

As part of normal operations, copies of backup images on WORM storage are not removed from the catalog and storage until both Copy Expiration Time and Worm Unlock Time timestamps have elapsed. The WORM Unlock Time of a copy that is written to WORM storage can only be extended and cannot be shortened. To extend the expiration date, use the `bpexptime -extend_worm_locks` command.

In special circumstances, the `bpexptime -try_expire_worm_copy` option can be used to force an attempted removal of a WORM indelible image from the NetBackup catalog. This option is only recommended to be used after removing WORM locks directly on the storage device. Only use this option with assistance from Cohesity technical support.

When duplicating an image onto WORM storage, the WORM Unlock Time can be configured to match the Copy Expiration Time by running the `bpduplicate` command using the `-worm_unlock_match_expiration` option that was introduced in NetBackup 10.1.

If older backup images are duplicated to WORM storage without using this command option, the WORM Unlock Time for the duplicated copy is calculated using the configured retention level, and the timestamp when the duplication job was complete.

The `bpduplicate -worm_unlock_match_expiration` command option is not used for SLP driven duplications. For SLP driven duplications, the retention period is applied from the end of the duplication job to calculate WORM Unlock Time of the new copy. The Copy Expiration Time for the new copy is calculated from the retention period that is applied to the backup time (for copy 1).

For A.I.R. jobs, the retention period is applied from the end of the import job to calculate the WORM Unlock Time of the imported copy. The Copy Expiration Time

is calculated as the retention period that is applied from the beginning of the import job.

more information about the `bpduplicate` command and the `bpexpdate` command, see the [NetBackup Commands Reference Guide](#).

Note: When you use the `bpduplicate -worm_unlock_match_expiration` and `bpexpdate -extend_worm_locks` command options, they rely on the accuracy of the NetBackup primary server clock. That is because the WORM Unlock Time mirrors the Image Expiration timestamp for that copy.

For more information about how to base the WORM Unlock Time on the original backup time, see the following knowledge base article:

[Images duplicated to WORM storage have unlock time calculated from duplication date not backup date](#)

Workflow to configure immutable and indelible data

Carry out the following steps in the given order to protect your data by configuring immutability and indelibility.

Table 35-1 Workflow to configure immutable and indelible data

Step	Description
1	Configure the following WORM settings on the storage server. The storage administrator configures these settings outside of NetBackup. ■ WORM capable - If the storage unit and the associated disk pool are enabled to use the WORM property at the time of backup image creation, the backup images are set to be immutable and indelible. ■ Lock Minimum Duration - Specifies the minimum allowed duration for which the data for a backup image is indelible. The storage administrator sets this duration on the Logical Storage Unit (LSU) or the Domain Volume (DV), which NetBackup discovers. ■ Lock Maximum Duration - Specifies the maximum allowed duration for which the data for a backup image is indelible. The storage administrator sets this duration on the Logical Storage Unit (LSU) or the Domain Volume, which NetBackup discovers. Refer to the OST vendor plug-in documentation.
2	Configure a disk pool using WORM-capable volumes.
3	Configure a storage unit with the Use WORM option enabled.

Table 35-1 Workflow to configure immutable and indelible data (continued)

Step	Description
4	Configure a backup policy using the WORM-enabled storage unit.

Note: In case of storage changes or third-party OST vendor software upgrades, you need to manually update the storage servers and the disk pools. See the 'Completing your system update after an upgrade' section from the [NetBackup Upgrade Guide](#).

Deleting an immutable image from storage using the `bpexpdate` command

Deletion of an immutable image can only happen when storage is used that allows for lock deletion. The lock deletion can be done using the Enterprise mode on Flex Appliance, Flex Scale Appliance, Access Appliance, or a third-party storage device that supports lock deletion. When an immutable image is deleted, the storage that you use is responsible for the lock deletion and NetBackup is responsible for the image deletion.

When you use Flex Appliance, Flex Scale Appliance, or Access Appliance, you must use the command line or an SSH session to remove the lock on the image. If you use a third-party storage device, refer to that vendor’s documentation for steps on removing locked images.

To delete the immutable image on the appliance

- 1 Verify that the appliance is in Enterprise mode.
- 2 From the NetBackup Command Line, use `bpimagelist` command to find the image ID.

This procedure uses the following example image ID:

Backup ID: `server123.veritas.com_1234567890`

- 3 Delete the image lock on storage using the command line option or the SSH session option.
 - For Flex Appliance: You must use the default `msdpadm` user to run the following options.
 - For Flex Scale Appliance and Access Appliance: You must use an appliance user with the appliance administrator role.

Command line option:

- Open the `/usr/openv/pdde/pdcr/bin/` directory.
- Use the following command to query and modify the catalog database for the given backup ID (Example: `server123.veritas.com_1234567890`). The `-worm disable` option disables the retention lock for an image using the backup ID.

```
sudo -u msdpvc /usr/openv/pdde/pdcr/bin/catdbutil -worm
disable -backupid
```

SSH session option:

- Open an SSH session to the WORM storage server instance.
- Use the `retention policy disable` command to query and modify the catalog database for the given policy. The `policydisable` arguments disable the retention lock for an image using the policy ID used for the image retention that has a retention lock.

For more information about the command options in this step, see the [NetBackup Deduplication Guide](#).

- 4 Add the image ID to `bpexpdate` with the `-try_expire_worm_copy` option.

```
bpexpdate -d 0 backupid server123.veritas.com_1234567890
-try_expire_worm_copy -copy 1
```

- 5 Use `y` or `n` to confirm deletion.

If the storage lock is not removed, NetBackup returns an error indicating that there is a WORM lock error.

Note: Disabling the retention lock on an image does not update the NetBackup UI. The UI may continue to display the previous retention lock status for that image even after the lock has been disabled. Users can safely run the `bpexpdate` command to expire the image.

See [“Removing an immutable image from the catalog using the `bpexpdate` command”](#) on page 603.

See [“About immutable and indelible data”](#) on page 598.

Removing an immutable image from the catalog using the `bpexpdate` command

You can remove an immutable image from the NetBackup catalog and have that image remain on storage.

To remove an immutable image from the catalog

- 1** Open the NetBackup Command Line Interface (CLI).
- 2** Delete the image from the catalog using the `bpexpdate` command with the `-try_expire_worm_copy` and the `-nodelete` options.

```
bpexpdate -d 0 -backupid server123.veritas.com_1234567890
        -copy 1 -try_expire_worm_copy -nodelete
```

Using the `-try_expire-worm_copy` and `-nodelete` options together removes the image from the catalog only and does not affect storage.

- 3** Use `y` or `n` to confirm deletion.

See [“Deleting an immutable image from storage using the `bpexpdate` command”](#) on page 601.

See [“About immutable and indelible data”](#) on page 598.

Anomaly detection

This chapter includes the following topics:

- [About backup anomaly detection](#)
- [About system anomaly detection](#)
- [Anomaly configuration to enable automatic scanning](#)
- [Computation of entropy and file attributes in NetBackup](#)

About backup anomaly detection

NetBackup can now detect anomalies in backup metadata. It can detect any unusual job data in the data backup flow. For example, it can detect a file count or a file size that is different than the usual count or size.

Note: By default, the anomaly detection algorithm runs on the NetBackup primary server. If you see any impact on the primary server because of the anomaly detection process, you can configure a media server to detect anomalies.

The following backup job metadata, attributes, or features are verified during backup anomaly detection:

- Backup image size
- Number of backup files
- Data that is transferred in KB
- Deduplication rate
- Backup job completion time

Any unusual deviation in these backup job attributes is considered to be an anomaly and is notified using the NetBackup web UI.

NetBackup can detect anomalies for Oracle workload only for the image size attribute. If an Oracle workload job fails multiple times with status code 5407, NetBackup flags it as an anomaly.

Workflow of backup anomaly detection and notification

The workflow of the backup anomaly detection and notification is as follows:

Table 36-1 Workflow

Step	Description
Step 1	Install or upgrade NetBackup software on the primary server and the media server. See the NetBackup Installation or Upgrade Guide .
Step 2	Enable the primary server to detect backup anomalies. See “ Detecting backup anomalies on the primary server ” on page 609. By default, the anomaly detection algorithm runs on the NetBackup primary server. If you see any impact on the primary server because of the anomaly detection process, you can configure a media server to detect anomalies. See “ Detecting backup anomalies on the media server ” on page 609.
Step 3	Configure anomaly detection settings using the NetBackup web UI. See “ Configure backup anomaly detection settings ” on page 606.
Step 4	View the anomalies using the NetBackup web UI. See “ View backup anomalies ” on page 610.

How NetBackup detects backup anomalies

Example scenario

An organization usually backs up about 1 GB of data each day for a specific client and using a backup policy. If the backup size increases to 10 GB on a given day, NetBackup identifies and reports it as an image size anomaly because the current image size is much larger than the typical 1 GB size.

How the anomaly score is calculated

The anomaly score is calculated by comparing the current data with a cluster of similar historical observations. In this example, the cluster consists of backups that are about 1 GB. Higher anomaly scores indicate greater severity.

Significant deviation in the metadata is termed as an anomaly based on its anomaly score.

An anomaly score is calculated based on how far the current data is from the cluster of similar observations of the data in the past. In this example, a cluster is of 1 GB of data backups. You can determine the severity of anomalies based on their scores.

For example:

Anomaly score of Anomaly A = 7

Anomaly score of Anomaly B = 2

Anomaly A has a higher anomaly score than Anomaly B. Showing a more significant deviation from prior backups.

NetBackup considers the configured anomaly detection settings, including default and advanced settings when available, during anomaly detection.

Configure backup anomaly detection settings

After you enable anomaly detection, anomaly data gathering, detection service, and events are enabled. Basic and advanced backup anomaly detection settings are available to be configured.

See [“About backup anomaly detection”](#) on page 604.

See [“View backup anomalies”](#) on page 610.

To configure backup anomaly detection settings

- 1 Sign in to the NetBackup web UI.
- 2 On the left, click **Detection and reporting > Anomaly detection**.
- 3 On the top right, click **Anomaly detection settings > Backup anomaly detection settings**.
- 4 Click **Edit** on the right to configure the following **Anomaly detection > Enable anomaly detection activities** settings:
 - **Enable only for unstructured data** - Enables anomaly detection for the following policy types: Standard, MS-Windows, NAS-Data-Protection, and Universal share.

Note: This is the default configuration for fresh NetBackup 10.4 installation.

- **Enable** - Enables anomaly detection for all policy types except for the ones that are excluded in the **Advanced settings > Disable policy type or specific features for machine learning**.

- **Disable** - Disables anomaly detection in NetBackup for all workload types.
- Click **Save**.

In the case of NetBackup 10.4 upgrade, the value of the **Anomaly detection** option is set based on the previous setting.

- If the option was set to **Enable anomaly data collection, detection service, and events** in the previous version, the option is set to **Enable** after the upgrade.
- If the option was set to a value other than **Enable anomaly data collection, detection service, and events** in the previous version, the option is set to **Disable** after the upgrade.

5 Click **Edit** on the right to configure the **Anomaly detection > Enable automatic scan for imported copy** setting.

- On the **Enable automatic scan for imported copy** pop-up screen, select the **Turn on automatic scan for imported copy** check box.

After enabling the scan for imported copy from the web UI, you must do the following configurations in the `anomaly_config.conf` file:

```
[AUTOMATED_MALWARE_SCAN_SETTINGS]
SCAN_HOST_POOL_NAME=ScanHostPoolName
ENABLE_ALL_CLIENTS=1
TRIGGER_SCAN_FOR_LOW_SEVERITY=1
TRIGGER_SCAN_FOR_MEDIUM_SEVERITY=1
```

- Click **Save**.

6 Select **Edit** to modify the following **Basic Settings**:

- **Anomaly detection sensitivity**
Use this setting to increase or decrease the sensitivity with which anomalies are detected. If the sensitivity is low, anomalies are detected based on less number of anomalous events.
If the sensitivity is high, anomalies are detected based on a large number of anomalous events.
- **Data retention settings**
Use this setting to specify how long you want to retain the anomaly data (in months).
- **Data gathering settings**
Use this setting to specify the time interval (in minutes) after which the anomaly data is gathered for analysis.
- **Anomaly proxy server settings**

Use this setting to specify the NetBackup media server where the anomalies are going to be processed. If not specified, the processing takes place on the primary server.

- Click **Save**.

7 Expand the **Advanced settings** section to configure the following settings:

- Click **Edit** on the right to configure the **Disable anomaly settings for clients** settings.
 See [“Disable backup anomaly detection and computation of entropy and file attributes for a client”](#) on page 624.
 Click **Save**.
- Click **Edit** on the right to configure the **Disable policy type or specific features for machine learning** settings.
 On the pop-up screen, all the policies are listed.
 Use the action menus to disable one or all of the following anomaly features for machine learning for the given policy: Backup files count, Data transferred, Deduplication ratio, Image size, and Total time.
 - **Disable all** - Use this option to disable all of the anomaly features for machine learning for the given policy.
 - **Disable specific features** - Use this option to select specific anomaly features that you want to disable for machine learning.
 - Click **Save**.
- Click **Edit** on the right to configure the **Suspicious file extension settings**.
 - Select the **Turn on suspicious file extension detection** to enable NetBackup to detect files with suspicious file extensions.
 A malware such as ransomware attacks the data and encrypts it. After the file encryption, the ransomware renames the files with a specific extension such as `.lockbit`. NetBackup detects such known suspicious file extensions during backups and generates an anomaly.
 - **Files with suspicious extensions (in %)**
 Select the percentage (1 to 50) of files with suspicious extensions from the **Percent** drop-down list, which is acceptable in your environment.
 When the percentage of the files with suspicious extensions exceeds this threshold, an anomaly is generated.
- You can add or remove the suspicious file extensions from the list.
- Click **Save**.

Client offline anomaly type

As part of backup anomaly detection, clients that are offline under suspicious circumstances (with error code 7647) are detected and anomalies are generated.

Detecting backup anomalies on the primary server

This topic provides the procedure to enable the primary server to detect backup anomalies.

To enable the primary server to detect backup anomalies

- 1 Install the NetBackup primary server software on your system (or upgrade the primary server software).

After the installation, the following configurations are automatically done on the primary server:

- The NetBackup Anomaly Detection Management service (nbanomalygmt) is started on the primary server.
The anomaly detection and alert services do not run by default.

Note: The NetBackup Anomaly Detection Management service stops if the proxy server takes more than 45 minutes to connect to the primary server.

- 2 Configure the backup anomaly settings using the NetBackup web UI. NetBackup takes these settings into account during anomaly detection.

See [“Configure backup anomaly detection settings”](#) on page 606.

See [“How NetBackup detects backup anomalies”](#) on page 605.

If any anomalies are detected, they are notified through the NetBackup web UI.

See [“View backup anomalies”](#) on page 610.

Detecting backup anomalies on the media server

This topic provides the workflow and the procedure that enable the media server to detect backup anomalies.

Note: By default, the anomaly detection algorithm runs on the NetBackup primary server. If you see any impact on the primary server because of the anomaly detection process, you can configure a media server to detect anomalies.

To enable the media server to detect backup anomalies

- 1 Install the NetBackup media server software on your system (or upgrade the media server software).
- 2 On the primary server, add anomaly proxy server details. The proxy server should be the media server where you want the anomaly algorithms to be run.
See [“Configure backup anomaly detection settings”](#) on page 606.
- 3 (Optional) If you want to preserve the data that the primary server has gathered earlier, do the following:
 - Ensure that the `nbanomalygmt` service is disabled using the web UI.
 - Ensure that the `nbanomalygmt` service on the media server is stopped.
 - Go to the following directory:
On Windows: `Install_Path\NetBackup\var\global`
On UNIX: `/usr/opensv/var/global`
The directory resides on the shared disk on a clustered primary server.
 - Copy the `NB_Anomaly.db`, `NB_Anomaly.db-shm`, and `NB_Anomaly-wal` files from the `anomaly_detection` folder on the primary server to the `anomaly_detection` folder on the media server.
You can copy the `anomaly_config.conf` file to preserve the automatic malware scan settings.
 - Start the `nbanomalygmt` service on the media server.
- 4 On the media server, start the `nbanomalygmt` service manually. Use the following script:

```
nbanomalygmt -start
```
- 5 Configure the backup anomaly settings in the NetBackup web UI. NetBackup takes these settings into account during anomaly detection.
See [“Configure backup anomaly detection settings”](#) on page 606.
See [“How NetBackup detects backup anomalies”](#) on page 605.
If any anomalies are detected, they are notified using the NetBackup web UI.
See [“View backup anomalies”](#) on page 610.

View backup anomalies

NetBackup can now detect anomalies in backup metadata. It can detect any unusual job data in the data backup flow. For example, it can detect a file count or a file size that is different than the usual count or size.

Consider the following example:

An anomaly of the image size type is displayed as 100MB (Usual 350MB, 450MB). This information implies that the current image size that is reported as anomaly is 100 MB. However, the usual image size range is 350 MB - 450 MB that is derived from the analysis of past data. Because of the significant difference between the current image size and usual image size range, NetBackup notifies it as an anomaly.

See [“About backup anomaly detection”](#) on page 604.

Note: Anomaly count of 0 indicates that there are no anomalies generated or that the anomaly detection services are not running.

To view backup anomalies

- 1 Sign in to the NetBackup web UI.
- 2 In the NetBackup web UI, select **Detection and reporting > Anomaly detection > Backup anomalies**.

The following columns are displayed:

- Job ID - ID of the job for which the anomaly is detected
All child jobs and the associated anomaly details are also shown when you expand the parent job.
- Severity - Severity of the anomalies that are notified for this job
- Asset name - Name of the NetBackup client where the anomaly is detected
- Summary - For the parent job, details like types of anomalies, number of anomalies, and increase or decrease in the number of anomalies are shown. For child jobs, types of anomalies are shown, such as Database corruption.
- Anomaly type - Type of the anomaly such as Image entropy, Job metadata, Suspicious file extension, Client offline
- Backup selection - The backup selection (client or file to be backed up) that is specified in the policy
- Policy name - The policy name of the associated backup job
- Policy type - The policy type of the associated backup job
- Schedule type - The schedule type of the associated backup job
- Impacted number of jobs - The number jobs for which anomalies are detected

- Review status - The anomaly status that indicates whether the detected anomaly is reported as a false positive or an actual anomaly, or it can be ignored.
 - Last updated - The date and time when the anomaly status is updated
- 3** Select the job ID to see the job details in the Activity monitor. Expand a parent job to see the details of each child job.
- 4** You can perform the following actions on the anomaly record:
- Select **Report as false positive** if the anomaly is a false positive. Similar anomalies are not shown in the future.
 The **Review status** of the anomaly record appears as `False positive`.
 - Select **Confirm as anomaly** when you want to take some action on the anomaly condition.
 The **Review status** of the anomaly record appears as `Anomaly`.
 - Select **Mark as ignore** when you can ignore the anomaly condition.
 The **Review status** of the anomaly record appears as `Ignore`.
 - Select **View modified files** to view the files that changed in an anomalous backup job. You can view the files that changed relative to the anomalous backup date, filtered by a selected time frame. You can download the results as a CSV for deeper analysis in your security tools.

Note: The **View modified files** option is available only for entropy-based anomalies on Standard or MS-Windows policies, and only if the backup image has not expired.

About system anomaly detection

NetBackup can detect system anomalies during critical operations as follows:

- Risk engine-based system anomaly
 See [“Configure risk engine-based anomaly detection”](#) on page 615.
- Monitor database corruption in workloads during job failures - This anomaly monitors database corruption in workloads like MS SQL Server and Oracle during backup job failures.
- Rule-based system anomaly
 See [“Configure rules-based anomaly detection”](#) on page 614.

See [“View system anomalies”](#) on page 618.

Configure system anomaly detection settings

After you enable anomaly detection, anomaly data gathering, detection service, and events are enabled. You can configure specific settings to detect system anomalies in your domain.

See [“About system anomaly detection”](#) on page 612.

To configure system anomaly detection settings

- 1 Sign in to the NetBackup web UI.
- 2 On the left, click **Detection and reporting > Anomaly detection**.
- 3 On the top right, click **Anomaly detection settings > System anomaly detection configuration**.
- 4 On the **System anomaly detection configuration** screen, configure the following settings:
 - **Risk engine-based anomaly detection**
See [“Configure risk engine-based anomaly detection”](#) on page 615.
 - **System anomaly detection > Monitor database corruption in workloads during job failures**
This anomaly monitors database corruption in workloads like Microsoft SQL Server and Oracle during backup job failures.
Select the checkbox to generate an anomaly alert when NetBackup detects backup job failures because of database corruption in workloads like Microsoft SQL Server and Oracle.
If database corruption in a workload is detected, status code 5464 is attributed to the parent job that is displayed in the **Activity monitor > Jobs** tab.
Click the status code number to view information about this status code in the Cohesity Knowledge Base.
See the [NetBackup Status Codes Reference Guide](#).

Note: For detecting database corruption in Microsoft SQL Server, the 'Microsoft SQL Server checksum' option must be set to 'Fail on Error' during MS SQL Server policy configuration.

See [“View backup anomalies”](#) on page 610.

- **Rules-based anomaly detection**
See [“Configure rules-based anomaly detection”](#) on page 614.

Configure rules-based anomaly detection

Rules engine-based anomaly detection allows you to define certain rules. If the threshold values that are defined in the rule are exceeded, anomalies are generated. For example, an anomaly is generated if a certain number of failed login attempts occur in a specified time period.

For each rule, you can configure the following parameters: execution frequency, query period, and threshold.

To modify the rule parameters, use the `/security/anomaly/rules/{ruleId}` API.

To configure rules-based anomaly detection

- 1 Sign in to the NetBackup web UI.
- 2 On the left, click **Detection and reporting > Anomaly detection**.
- 3 On the top right, click **Anomaly detection settings > System anomaly detection configuration**.
- 4 On the **System anomaly detection configuration** screen, expand **Rules-based anomaly detection** and select the **Detect anomalies using NetBackup anomaly detection rules** check box.

The following details for each of the predefined rules are displayed:

- Rule name
- Description
- Severity
- Version
- Enabled

For the latest rules file, go to the Cohesity Download Center and download the rules file (.zip) for which you want to generate anomalies.

Select **Upload rules** to select the rules file that you have downloaded. All the latest rules are listed in the **Rules-based anomaly detection** section.

- 5 Select the rules that you want to enable and for which you want to generate anomalies.

Select **Enable**.

NetBackup generates anomalies for the conditions that meet the rule criteria.

Configure risk engine-based anomaly detection

The NetBackup risk engine detects certain system anomalies in a proactive manner and sends appropriate alerts. It helps you take corrective action before you face any security threat in your environment.

You can configure the following options that the risk engine uses to detect anomalies for the given operations:

Detect suspicious image expiration

Use this option to detect when images are expired in an unusual or a suspicious manner.

By default, a system anomaly is generated when the risk engine detects an unusual or a suspicious image expiration attempt and allows the operation to proceed.

However, for additional security, you can configure multiperson authorization for such image expiration attempts, where an MPA approver needs to approve the operation.

Important notes on the Detect suspicious image expiration option

- If the audit retention period is set to less than 3 months, this option accumulates data of 3 months and then becomes active.
- This option supports full backup schedules. Other types of schedule are not considered. The retention level of an image is also not considered for this rule.
- Images are expired by media ID, server name, or by recalculating the retention period.

Select **Edit** and select the **Generate multiperson authorization ticket if images are deleted in a suspicious manner** option.

Note: To successfully review the multiperson authorization tickets, ensure that one or more MPA approvers are available in your environment.

See [“About multiperson authorization”](#) on page 248.

See [“RBAC roles and permissions for multiperson authorization”](#) on page 252.

Detect unusual user sign in

Use this option to detect when a user attempts to sign in to the NetBackup web UI at an unusual time. NetBackup identifies deviations in user sign-in patterns, and flags them.

A notification is generated when an unusual user login is detected.

For additional security, you can configure multiperson authorization for such unusual login attempts, where an MPA approver needs to approve the operation.

See [“Configure multiperson authorization”](#) on page 257.

- If an unusual login attempt is detected on a NetBackup host earlier than 11.0, the request is rejected. Carry out the operation on a NetBackup 11.0 host.
- If none of the users can login and they are placed on hold because of unusual login pattern, the NetBackup administrator can disable the unusual login detection to allow the users to sign in to the NetBackup web UI using the following command:

```
NBU_INSTALL_PATH/netbackup/bin/admincmd/nbseccmd  
-disableLoginAnomalyDetection
```

- User logins that are based on the authentication types such as SAML, smart card, and API keys do not support login anomaly detection.

Click **Edit** and use the **Place user's sign in on hold and generate multiperson authorization ticket if a user signs in at an unusual time** option to enable multiperson authentication.

- To successfully review the multiperson authorization tickets, ensure that one or more MPA approvers are available in your environment.
- If multiperson authorization is enabled and an unusual user login is detected, the user's login is placed on hold.
- A ticket is generated and requires approval for the user to proceed. Until the ticket is approved, the user shall not be able to login from the device.
- If the ticket is approved, the user is allowed login and granted a free pass for the next 24 hours. During the free pass period, the user is not subjected to further scrutiny for unusual login attempts.
- If the ticket is rejected, the user cannot log in for the current session but can try again with their credentials.
- The user can choose to cancel their login request.

Detect unusual updates to policies

By default, a system anomaly is generated when the risk engine detects an unusual deletion or update of a policy. An alert is generated and the operation proceeds.

For additional security, you can configure multiperson authorization for such unusual policy update or deletion attempts, where an MPA approver needs to approve the operation.

See [“Configure multiperson authorization”](#) on page 257.

Click **Edit** and use the **Generate multiperson authorization ticket if policy is being modified or deleted in an unusual manner** option to enable multiperson authorization for the **Detect unusual updates to policies** type of anomaly.

- To successfully review the multiperson authorization tickets, ensure that one or more MPA approvers are available in your environment.
- Two alerts are generated for unusual updates to a policy for the next 48 hours. After the second alert, no alert is generated for the next 48 hours even if the policy is modified.
- If multiperson authorization is enabled, a ticket is generated for modification of a policy.
- Approving two consecutive tickets for the same policy does not generate new tickets for the next 48 hours for the same policy.
- If multiperson authorization is enabled for the policy operations on the global level, the **Detect unusual updates to policies** option is disabled.

Note: If multiperson authorization is enabled for the **Detect unusual updates to policies** option, you cannot update or delete policies using the command-line interface.

Alternatively, use the `nbcmdrun` command to update or delete policies. For more information on the commands, see the [NetBackup Commands Reference Guide](#).

Secure critical operations

Use this option to protect critical operations such as modifying global security settings and creating API key. When you select this option, you are required to reauthenticate yourself by entering the one-time password that you see in the authenticator application on your smart device before you perform the given critical operations.

Ensure that you have configured multifactor authentication for your user account. If multifactor authentication is not configured, you are not prompted to reauthenticate.

Note: It is strongly recommended that you configure multifactor authentication in your environment to prevent security threats by malicious sources.

See [“Configure multifactor authentication for your user account”](#) on page 244.

Detect possible session hijack

Use this option to detect if there is a possible user session hijack by a malicious source.

The risk engine detects if the same user session token is used by another IP address, and sends a maximum of 10 alerts per day.

Select **Edit** and select the check box to terminate the user session when the risk engine detects that there is a possible session hijack.

View system anomalies

NetBackup can detect system anomalies. This anomaly detection is enabled by default for all policy types.

To view system anomalies

- 1 Sign in to the NetBackup web UI.
- 2 On the left, select **Detection and reporting > Anomaly detection > System anomalies**.

The following columns are displayed:

- Detected on - The date when the anomaly is detected
- Review status - Anomaly status that indicates whether the detected anomaly is reported as a false positive or an actual anomaly, or it can be ignored.
- Anomaly type - Type of the anomaly
- Severity - Severity of the anomaly
- Description - Additional information about the anomaly
- Anomaly ID - ID of the anomaly record

- 3 Expand a row to see the details of the selected anomaly.
- 4 You can perform the following actions on the anomaly record:
 - Select **Report as false positive** if the anomaly is a false positive. Similar anomaly conditions are not reported in the future.
 - Select **Confirm as anomaly** when you want to take some action on the anomaly condition.
 - Select **Mark as ignore** when you can ignore the anomaly condition.

Anomaly configuration to enable automatic scanning

Starting with NetBackup 11.0, the automatic scan is available for the images with high anomaly severity.

Use the configuration file on the primary server to do the required settings.

In NetBackup 10.1 and later, the anomaly detection process can trigger automatic malware scan for all anomalies based on the configuration file settings.

Use the configuration file on the anomaly proxy server to do the required settings.

You need to modify the anomaly configuration file to specify values for the scan host and trigger parameters.

See [“About malware scanning”](#) on page 630.

See [“Prerequisites for a scan host”](#) on page 671.

You can enable automatic malware scan on secondary domain for anomalous imported images using the **Enable automatic scan for imported copy** option on the web UI.

See [“Configure backup anomaly detection settings”](#) on page 606.

To enable automatic malware scan for the images on which an anomaly was detected

- 1 Create the `anomaly_config.conf` configuration file on the primary server on the given location:

On Windows : `Install_Path\NetBackup\var\global\anomaly_detection`

On UNIX : `/usr/opensv/var/global/anomaly_detection`

- 2 Add the following contents in the `anomaly_config.conf` configuration file:

```
#Use this setting to start malware scan on anomaly detected image
automatically.
```

```
[AUTOMATED_MALWARE_SCAN_SETTINGS]
```

```
#1 = Enable 0 = Disable
```

```
ENABLE_AUTOMATED_SCAN=1
```

```
# Enable all clients. In this case pool mentioned
SCAN_HOST_POOL_NAME will be used for clients not mentioned
```

```
# under batch
```

```
ENABLE_ALL_CLIENTS=1 (for primary copy)
```

```
SCAN_HOST_POOL_NAME=<scan_host_pool_name> # Default pool name
```

```
#Use specific pool for mentioned clients
```

```
NUM_CLIENTS_BATCH_SPECIFIED=2
```

```
ENABLE_SCAN_ON_SPECIFIC_CLIENT_1=client1,client2
```

```
SCAN_HOST_POOL_NAME_1=<scan_host_pool_for_batch_1>
```

```
ENABLE_SCAN_ON_SPECIFIC_CLIENT_2=client3,client4
```

```
SCAN_HOST_POOL_NAME_2=<scan_host_pool_for_batch_2>
```

- 3 Note that `SCAN_HOST_POOL_NAME` is a mandatory field.

For the `ENABLE_SCAN_ON_SPECIFIC_CLIENT_n` option, you should specify complete client names.

- 4 Ensure that all settings are under `[AUTOMATED_MALWARE_SCAN_SETTINGS]`. Review the following descriptions of the settings:

`ENABLE_AUTOMATED_SCAN=1`

Starts malware scan for images with high anomaly severity.

`ENABLE_ALL_CLIENTS=1`

Enable all clients for scan. If this value is 0, scanning happens only on the clients that are mentioned for the following option:

`ENABLE_SCAN_ON_SPECIFIC_CLIENT_<Batch_Number>`

`NUM_CLIENTS_BATCH_SPECIFIED=<batches>` - This option specifies the number of batches for different scan host pool. For example, if you want to use a specific scan host pool for a set of clients, use this setting.

- 5 Do the following to automatically trigger malware scan for various severity levels of anomalies:
 - For low severity anomaly, set the `TRIGGER_SCAN_FOR_LOW_SEVERITY` option as follows:
`TRIGGER_SCAN_FOR_LOW_SEVERITY=1`
 - For medium severity anomaly, set the `TRIGGER_SCAN_FOR_MEDIUM_SEVERITY` option as follows:
`TRIGGER_SCAN_FOR_MEDIUM_SEVERITY=1`
 - To automatically trigger malware scan for the anomaly severity of the image that is greater than or equal to the given value, set the `TRIGGER_SCAN_FOR_SCORE_GREATER_THAN` option to a positive value.
 For example:
`TRIGGER_SCAN_FOR_SCORE_GREATER_THAN=2.5`

Computation of entropy and file attributes in NetBackup

NetBackup 10.3 and later clients compute an additional risk signal in-line, called entropy. It improves the quality of detected anomalies. Entropy is a measure of randomness of file contents. Threat vectors that encrypt files tend to abruptly change the entropy. The entropy metric is used with the anomaly detection in Cohesity Alta View to help you detect such potential malicious activity. When this indicates anomaly activities, it is recommended to check the system for potential malicious actors and not to use those images as a recovery point if suspicious activities are found.

NetBackup 10.4 and later servers run a real-time, in-line ransomware detection process (`nbinlinerwdetect`) that analyzes the entropy and the following file attributes, and detects anomalies:

- File size
- File extension
- File permission
- File access time
- File modified time
- File change time

Note: Inline Entropy Analysis is not supported when dynamic multi-streaming is enabled for a Standard policy.

Enable computation of entropy and file attributes in NetBackup

Use the `COMPUTE_IMAGE_ENTROPY` option in NetBackup to enable computation of entropy and file attributes in NetBackup that enhances cyber resiliency in the NetBackup - Cohesity Alta™ View environment.

See [“COMPUTE_IMAGE_ENTROPY for NetBackup primary servers”](#) on page 623.

See the [Cohesity Alta View Help](#) to learn more about entropy score and how to view it in the Cohesity Alta View UI. Entropy score helps you identify potential anomalies in your NetBackup - Cohesity Alta View environment.

Disable computation of entropy and file attributes for a NetBackup client

Computation of entropy and file attributes can be disabled for specific NetBackup clients.

See [“Disable backup anomaly detection and computation of entropy and file attributes for a client”](#) on page 624.

Support information for computation of entropy and file attributes

To use the computation of entropy and file attributes feature, NetBackup primary server, and media server must be 10.4 or later, and NetBackup clients must be 10.3 or later.

Job types that the computation of entropy and file attributes feature supports

- Backup
- Backup from Snapshot

Policy types that the computation of entropy and file attributes feature supports

- Cloud (virtual machines only - excluding PaaS)

Note: The **Enable granular recovery for files or folders** option must be selected.

- Cloud-Object-Store
- FlashBackup
- FlashBackup-Windows
- MS-Windows
- Standard
- VMware (excluding Continuous Data Protection plan)

Protection plans that the computation of entropy and file attributes feature supports

- Cloud (virtual machines only - excluding PaaS)

Note: The **Enable granular recovery for files or folders** option must be selected.

- VMware (excluding Continuous Data Protection)

Note: The computation of entropy and file attributes feature does not support Ushare policy type.

COMPUTE_IMAGE_ENTROPY for NetBackup primary servers

Use the `COMPUTE_IMAGE_ENTROPY` option to enable computation of entropy and file attributes in NetBackup that enhances cyber resiliency in a NetBackup - Alta View environment.

The entropy metric is used with the anomaly detection in Alta View to help you detect potential malicious activity.

Table 36-2 COMPUTE_IMAGE_ENTROPY information

Usage	Description
Where to use	On NetBackup primary servers.
How to use	Use the <code>nbgetconfig</code> and the <code>nbsetconfig</code> commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: <pre>COMPUTE_IMAGE_ENTROPY = Value</pre> You can specify one of the following values for the <code>COMPUTE_IMAGE_ENTROPY</code> option: ■ ALWAYS - Computation of entropy and file attributes is always enabled. This is the default value. ■ NEVER - Computation of entropy and file attributes is always disabled. ■ IF_MANAGED_BY_ALTA - Computation of entropy and file attributes is enabled if Alta View manages the associated NetBackup primary server. If Alta View does not manage the primary server, computation is disabled. Note: After the NetBackup primary server is registered with the Alta View server, computation of entropy and file attributes starts within the next 24 hours with the new backup jobs.
Equivalent NetBackup web UI property	No equivalent exists.

Disable backup anomaly detection and computation of entropy and file attributes for a client

You can disable backup anomaly detection and computation of entropy and file attributes for certain NetBackup clients.

To disable backup anomaly detection and computation of entropy and file attributes

- 1 Sign in to the NetBackup web UI.
- 2 On the left, click **Detection and reporting > Anomaly detection**.

- 3 On the top right, click **Anomaly detection settings > Backup anomaly detection settings**.
- 4 Expand the **Advanced settings** section.
- 5 Select the respective **Edit** option to modify **Disable anomaly settings for clients**.
- 6 On the **Disable anomaly settings for clients** pop-up screen, specify the NetBackup client for which you do not want to generate anomalies and compute entropy.
- 7 In the search results, click the **Add to list** option next to the required client.
- 8 Select **Save**.

The selected clients are added in the excluded clients' list.

Note: After the client is excluded or included again, the computation of entropy and file attributes stops or starts within the next 24 hours with the new backup jobs.

Compute host

This chapter includes the following topics:

- [About compute hosts](#)
- [Add a compute host](#)
- [Activate a compute host](#)
- [Deactivate a compute host](#)
- [Edit a compute host](#)
- [Delete a compute host](#)
- [Configure compute host settings](#)

About compute hosts

A compute host is used to perform YARA scanning on NetBackup backup images.

See [“About YARA scanning”](#) on page 740.

Prerequisites

Ensure that the following prerequisites are met before you start using a compute host for YARA scanning:

- NetBackup client binaries are installed and configured on the host.
- YARA scanning tools are configured on the host.

Add a compute host

You must add and configure a compute host before you perform YARA scanning on backup images.

To add a compute host

- 1 On the left, click **Detection and reporting > Compute host**.
- 2 Click **Add**.
- 3 Select a NetBackup client host with the required scanning tool configuration.
- 4 Select the operations that the compute host can perform, for example: YARA scanner.
- 5 Select the scanner type, for example: YARA scanner.
 See ["About YARA scanning"](#) on page 740.
- 6 Select one of the following options for a storage server to associate with the compute host:
 - Allow any storage server to use this compute host
 - Select storage servers.
- 7 Click **Add**.

Activate a compute host

After you add a compute host, you need to activate it for scanning.

To activate a compute host

- 1 On the left, click **Detection and reporting > Compute host**.
- 2 Select the compute host that you want to activate.
- 3 Click **Activate**.

Deactivate a compute host

You deactivate a compute host if you do not want it to be used for scanning.

To deactivate a compute host

- 1 On the left, click **Detection and reporting > Compute host**.
- 2 Select the activated compute host that you want to now deactivate.
- 3 Click **Deactivate**.

Edit a compute host

You can edit configurations of an existing compute host.

To edit a compute host

- 1 On the left, click **Detection and reporting > Compute host**.
- 2 Select the compute host that you want to edit.
- 3 Click **Edit**.
- 4 On the **Edit compute host** dialog box, update the configurations such as operations, scanner type, or storage server.
- 5 Click **Update**.

Delete a compute host

You can delete a compute host if you no longer need it for scanning.

To delete a compute host

- 1 On the left, click **Detection and reporting > Compute host**.
- 2 Select the compute host that you want to delete.
- 3 Click **Delete**.

Configure compute host settings

You can configure compute host settings such as resource limit.

To configure compute host settings

- 1 On the left, click **Detection and reporting > Compute host**.
- 2 At the top right, click **Compute host settings > Resource limits**.

Configure the following resource limits:

- Number of jobs per scan host
- Number of jobs per storage server

Malware scanning

- [Chapter 38. Introduction](#)
- [Chapter 39. How to setup Malware scanning](#)
- [Chapter 40. Instant Access configurations](#)
- [Chapter 41. Malware tools configurations](#)
- [Chapter 42. Scan host configurations](#)
- [Chapter 43. Performing malware scan](#)
- [Chapter 44. Managing scan tasks for malware and YARA scanning](#)
- [Chapter 45. Malware scan configuration parameters](#)
- [Chapter 46. Troubleshooting](#)

Introduction

This chapter includes the following topics:

- [About malware scanning](#)
- [About dynamic scan](#)
- [About file hash search with malware hash](#)
- [Limitations](#)

About malware scanning

NetBackup finds malware in supported backup images and finds the last good-known image that is malware free. This feature is supported for Standard, MS-Windows, NAS-Data-Protection, Cloud, Cloud-Object-Store, Universal shares, Kubernetes, VMware and Nutanix AHV workload.

NetBackup can scan images that are stored on MSDP, MSDP cloud, DirectIO, AdvancedDisk or OST by using one of the the following **Search by** options:

- **Backup images**
This option is used for scanning policy of client backup images for malware.
- **Assets by policy type**
NetBackup supports Standard, MS-Windows, Nutanix AHV, Hypervisor (Nutanix AHV), Hyper-V, Universal-Share, Cloud object store, VMware or Cloud policy types for malware scan. The following section describes the procedure for scanning NAS-Data-Protection backup images for malware.

NAS-Data-Protection

Each NAS volume or share is read over NFS or SMB, and backed up using a configured number of backup streams. The maximum number of streams per volume determines the number of backup streams that are created to back up each volume. For example, consider a policy that contains 10 volumes and the

maximum number of streams is 4. The backup of the policy creates 4 backup streams for each volume, with a total of 40 child backup streams and 10 parent backup streams.

Note: The number of scans depends on the number of batches that were created to perform the scan. Only the parent stream backup image is visible on the UI.

For more information on multi stream backups, refer to *NetBackup NAS Administrator's Guide*.

■ **Assets by workload type**

This option of malware scanning is used for scanning VMware, Universal shares, Kubernetes, Cloud VM and Nutanix AHV assets for malware.

Note: NetBackup supports VMware assets for malware scan of backup images with MSDP and DirectIO.

Ensure that the following prerequisites are met:

- The backups were performed with a storage server at NetBackup 10.1 or later.
- Backup images are stored on MSDP storage only with instant access capability, for the supported policy type only.

Note: For DirectIO backup images, a media server with instant access capability is required.

- The last backup must be successful.
- You must have an RBAC role with permissions to perform malware scans.

Note: According to selection criterion, scan gets initiated to maximum of 100 images.

Benefits of malware scanning

Malware scanning provides the following benefits:

- You can select one or more backup images of the supported policy-types for an on-demand scan. You can use a predefined list of scan hosts.
- If malware is detected during the scanning, a notification is generated in the Web UI.

- If a file hash server is configured to a NetBackup domain that is not managed by Alta View, an automatic file hash search job of the malware hash is triggered periodically (interval configurable) to entire image catalog after a malware is detected.

For more information on file hash search, refer to the “About the file hash search in NetBackup” section in the *NetBackup Web UI Administrator's Guide*.

- In case files are skipped due to not being accessible to scanner or failure from malware scanner, then following respective notifications are generated with information about number and list of skipped files:
 - Critical severity: In case malware is found in the backup image and some of the files were skipped during scan.
 - Warning severity: In case no malware found in the backup image but some of the files were skipped during scan.

This information can be obtained by clicking on **Actions > Export unscannable files list**.

Note: The malware scan job in **Activity monitor** takes few minutes to reflect the final state of the scan operation running for multiple backup images.

For example, if scan operation runs for 5 backup images in a single request, then the malware scan job in **Activity monitor** would take 5 minutes to reflect the final state which is after completing the last (fifth) backup image scan job.

Note: During recovery if user starts recovery from a malware-affected backup image, a warning message is shown and confirmation is required for proceeding with recovery. Only users with permission to restore from malware-affected images can proceed with recovery.

For more information on best practices for malware scanning, refer to [Smart use of Malware Scanning in NetBackup](#).

Malware scanning before recovery

- User can trigger malware scan of the selected files/folders for recovery as part of recovery flow from Web UI and decide the recovery actions based on malware scan results.
- Catalog entry for the backup image is not updated after recovery time scan as only subset of files are scanned in the backup. Notification would be generated if malware is found as part of recovery time scan.
- During recovery time scan all the images in the start and end date are scanned for malware. Malware scanning of backup image may take long time depending

on the number of files selected for recovery. It is recommended to set the Start /End date to include only images which are intended to be used for recovery.

- User can trigger multiple recovery time scan for same backup image.
- Malware scan as part of recovery may take minimum 15-20 minutes for small size backup based on availability of scan host and number of scan jobs in progress. User can track the progress using **Activity monitor > Jobs**. Scan results would be displayed incrementally in the malware detection page. List of backup images in start and end date would be picked up for malware scan incrementally in batches.
- Supported policy types for recovery time scan: Standard, MS-Windows, Cloud-Object-Store, Universal Share, and NAS-Data-Protection.

Note: For successful recovery time malware scan operation, the media server version must be 10.4 or later.

Workflow for malware scanning

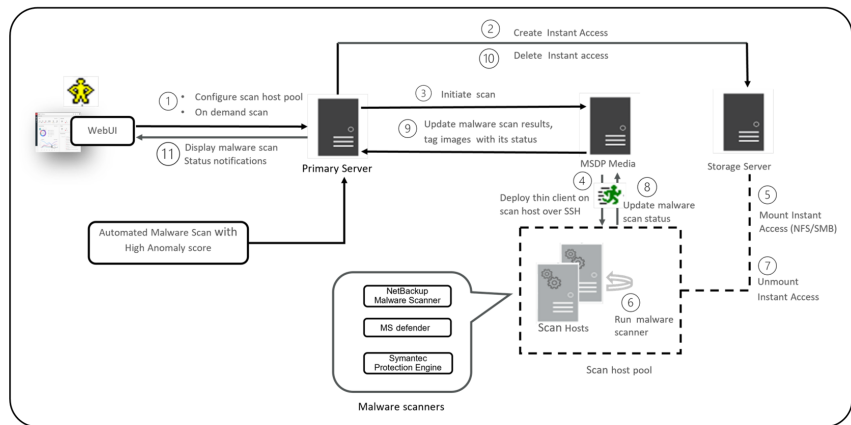
This section describes the workflow for malware scanning for the following:

- MSDP and DirectIO backup images using Agentless host as the scan host: The **Agentless host** requires SSH credentials to connect and perform the scan through thin client.
- MSDP and DirectIO backup images using NetBackup client as the scan host: The **NetBackup client** uses the client secure communication and performs the scan on the NetBackup client.
- OST and AdvancedDisk: For a complete list of supported OpenStorage servers, see the 'OST Storage Servers' section in *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.

Malware scanning workflow for MSDP backup images using Agentless host as the scan host

NetBackup provides support for **Agentless host** as the scan host to perform the malware scan. The **Agentless host** requires SSH credentials to connect and perform the scan through thin client.

The following figure displays the workflow of malware scanning for MSDP backup images:



The following steps depict the workflow for malware scanning for MSDP backup images:

1. After triggering **On Demand Scan**, primary server will validate backup images and create scan jobs for each eligible backup image and identify available scan host for them. Following are few of the criteria's on which the backup images are validated:
 - Backup image must be supported for malware detection.
 - Backup image must have a valid Instant Access copy.
 - For an on-demand scan, no existing scan must be running for same backup image. For DNAS the related streams are also considered.
 - Malware detection does not support media server associated with storage.
 - Unable to get information for backup image from catalog.
2. After the backup images are queued for an on-demand scan, the primary server identifies the storage server. An instant access mount is created on the storage server of the configured share type that is specified in scan host pool.

Note: Currently the primary server starts 50 scan threads at a time. After the thread is available it processes the next job in the queue. Until then the queued jobs are in the pending state.

For NetBackup version 10.3 and later, large backups are scanned in batches of 500K files. Each batch is scanned by a separate scan thread.

In addition to the Standard workloads, batch operations are supported for VMware workload backups also if backup policy has **Enable file recovery from VM backup** option enabled.

For recovery time scan, scan in batches feature is not supported.

3. Primary server identifies available and supported MSDP media server and instructs the media server to initiate the malware scan.

If the scan host connectivity type is **Agentless host**, then it instructs the media server to initiate the malware scan.
4. MSDP media server deploys the thin client on the scan host over SSH.
5. Thin client mounts the instant access mount on the scan host.
6. Scan is initiated using the malware tool that is configured in the scan host pool.

Media server fetches the progress of scan from scan host and update the primary server.
7. After the scan is completed, the scan host unmounts the instant access mount from the scan host.
8. Malware scan status is updated to the media server over SSH. Scan logs are copied to the media server log directory.
9. Media server updates the scan status and the infected file list along with skipped file list (if any infected files) to the primary server.
10. Primary server updates the scan results and deletes instant access.
11. Malware scan status notification is generated.
12. Malware scan will timeout in case there is no update on scan. Default timeout period is 48 hours.

Malware detection performs an automated cleanup of eligible scan jobs that are older than 30 days.

Note: The infected scan jobs would be cleaned automatically.

See [“MALWARE_DETECTION_CLEANUP_PERIOD”](#) on page 719.

Note: You can download a malware scanner from the Microsoft Azure Marketplace and the AWS Marketplace. Follow the instructions on how to install, configure, and use the malware scanner for AWS and Azure.

Refer to the following for more information:

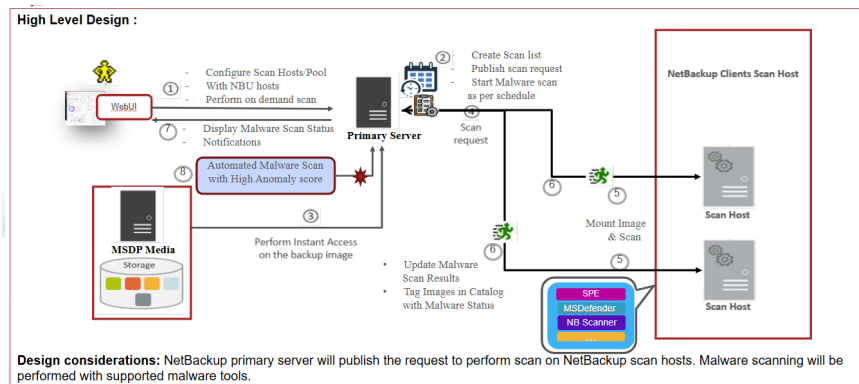
AWS: [AWS Marketplace](#) and [NetBackup Marketplace Deployment on AWS Cloud](#)

Microsoft Azure: [Microsoft Azure Marketplace](#) and [Microsoft Azure Marketplace](#)

Malware scanning workflow for the MSDP backup images that use the NetBackup client as the scan host

NetBackup version 11.0 and later provides support for **NetBackup client** as the scan host to perform the malware scan. The **NetBackup client** uses the client secure communication and performs the scan on the NetBackup client.

The following figure displays the workflow of malware scanning for MSDP backup images:



The following steps depict the workflow for malware scanning for MSDP backup images:

- 1 After you start the **On Demand Scan**, the primary server validates the backup images and creates the scan jobs for each eligible backup image and identifies the available scan host for them. The following are a few of the criteria by which the backup images are validated:
 - Backup image must be supported for malware detection.
 - Backup image must have a valid Instant Access copy.
 - For an on-demand scan, no scans must be running for the same backup image. For DNAS the related streams are also considered.

- Malware detection does not support a media server that is associated with storage.
 - Catalog must have details of the backup image.
- 2 After the backup images are queued for an on-demand scan, the primary server identifies the storage server. An instant access mount is created on the storage server of the configured share type that is specified in scan host pool.

Note: Currently the primary server starts 50 scan threads at a time. After the thread is available it processes the next job in the queue. Until then the queued jobs are in the pending state.

For NetBackup version 10.3 and later, large backups are scanned in batches of 500KB files. NetBackup scans each batch with a separate scan thread.

In addition to the Standard workloads, batch operations are supported for VMware workload backups also if backup policy has **Enable file recovery from VM backup** option enabled.

For recovery time scan, scan in batches feature is not supported.

To configure the NetBackup client as the scan host, see the steps in the following section:

See [“Configuring NetBackup client as the scan host”](#) on page 688.

- 3 The primary server identifies the available and the supported MSDP media server and instructs the media server to initiate the malware scan.
- If the scan host connectivity type is **NetBackup client**, then the primary server identifies the available NetBackup client scan host from the scan host pool. It then instructs the NetBackup client scan host to initiate the malware scan.
- 4 **NetBackup client** as the scan host:
- The NetBackup client mounts the instant access mount on the scan host.
 - Scan is initiated using the malware tool that is configured in the scan host pool.
 - The NetBackup client performs the scan operation and updates the progress of the scan from scan host to the primary server.
- 5 After the scan is completed, the scan host unmounts the instant access mount from the scan host.
- NetBackup client** as the scan host:
- Malware scan status is updated to the primary server. The scan logs are copied to the NetBackup client scan host log directory (`nbmalwarescanner`).

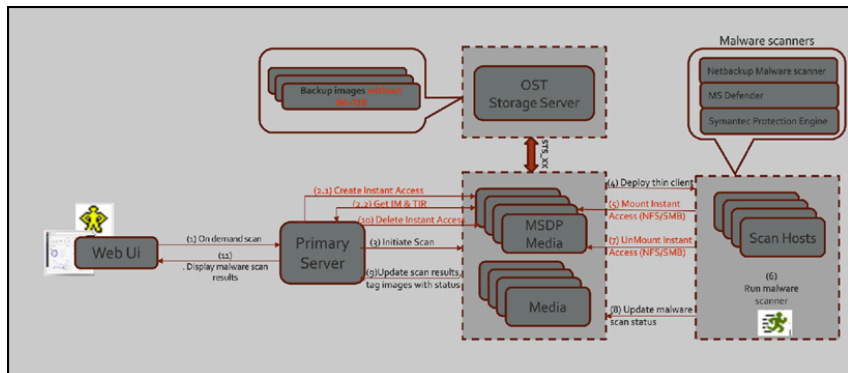
- The NetBackup client scan host updates the scan status and the infected file list along with the skipped file list (if any infected files) to the primary server.
- 6 The primary server updates the scan results and deletes instant access.
 - 7 A malware scan status notification is generated.
 - 8 The malware scan times out if there is no update on the scan. Default time out period is 48 hours.

Malware detection performs an automated cleanup of eligible scan jobs that are older than 30 days.

Malware scanning workflow for OST and AdvancedDisk

For a complete list of supported OpenStorage servers, see the 'OST Storage Servers' section in *NetBackup Hardware and Cloud Storage Compatibility List (HCL)*.

The following figure displays the workflow of malware scanning for DirectIO, OST and AdvancedDisk.



The following prerequisites exist for malware scanning of DirectIO, OST and AdvancedDisk:

- MSDP component for example, SPWS, VPFSD are required for an instant access mount. Hence for OST and AdvancedDisk storage, any one of the media servers must be configured as MSDP storage server so that it can serve the instant access API.
- Primary servers and media servers must be upgraded to NetBackup version 10.4 or later.
- Media servers must be accessible to the OST or AdvancedDisk storage server.

- OST plug-in must be deployed on instant access (host with MSDP components) hosts. For more information on the supported versions of OST plug-ins, refer to the *NetBackup Hardware Compatibility List*.
- Compatible instant access host (RHEL).
- The throttling limit on concurrent instant access from OST and AdvancedDisk STU is same as instant access from MSDP.

The following steps depict the workflow for malware scanning for OST and AdvancedDisk.

1. Using the **On Demand Scan** APIs, the backup image is added to the worklist table on Primary server.

Primary server identifies the available scan host from the specified scan host pool.

2. As part of processing the work list:

(2.1) Create media server for instant access:

- From the backup images, it finds out the storage server.
- From the storage server it finds out the eligible media server.
Media server with instant access capability.
Media server with NetBackup version 10.3 or later.
- Sends the instant access API request to the selected media server.
- If multiple media servers are eligible for an instant access mount request, it selects the media server with minimum number of ongoing instant access requests. This way it can distribute the instant access requests and achieve the load balance.

(2.2) Get IM & TIR

- On the selected media server, in the context of instant access API, it fetches the IM and TIR information from the primary server. It stores the information in the same format that the OS requires for mounting the backup image by VPFSD.
- After instant access mount, for IO file, VPFSD uses OST API to read backup image from storage server.
- Update worklist with images for which instant access was performed with `mountId`, `exportPath`, `storageServer`, and `status`.

3. The primary server identifies the available MSDP media server and instructs the media server to initiate the malware scan.

Note: The media server that is selected for the instant access mount and the server that is selected for communication with the scan host can be the same server or a different server.

4. When it receives the **scan** request, the scan manager from the media server initiates the malware scan on the scan host using thin client (`nbmalwareutil`) through remote communication using SSH.

Note: In NetBackup 10.5 or later, the hash values (SHA-256) of infected files are computed when infected files are found by the NetBackup Malware Scanner. The values can be viewed when exported through **Export infected files list**.

5. Depending on the configuration of scan host, from the scan host it mounts the export using either NFS or SMB from the media server. This media server is where the backup image is mounted using instant access API.
6. Scan is initiated using the malware tool that is configured in the scan host pool.

Note: VPFSD on the media server, uses STS_XXX APIs to open and read the backup images from the OST or AdvancedDisk storage server.

7. After the scan is completed, the scan host unmounts the export path from the media server where backup image is mounted using instant access API.
8. Malware scan status is updated to the media server over SSH. Scan logs are copied to the media server log directory.
9. Media server updates the scan status and the infected file list (if there are any infected files) to the primary server.
10. Primary server updates the scan results and deletes instant access request to the selected media.

Note: In NetBackup 10.5.0.1 or later, the hash values (SHA-256) of infected files are maintained in the Enterprise Media Manager (EMM) database. The hash values are submitted to the triggered file hash search job request.

11. Malware scan status notification is generated.

About dynamic scan

For malware scanning on Standard, MS-Windows, NAS-Data-Protection, Cloud, Cloud-Object-Store, Universal shares, Kubernetes, VMware and Nutanix AHV workloads, NetBackup 10.3 or later provides support for **dynamic scan** feature.

This feature provisions all files in the backup images on demand unless the file is accessed and read or there is no overhead on the file's provisioning.

In comparison to malware scan using Instant Access mount points in NetBackup versions prior to 10.3, dynamic scan optimizes instant access and scan performance for MSDP (for large number of files in the backup). This improves the instant access time as well as the scan performance.

NetBackup Media/Storage server 10.3 or later supports Instant Access on OST target volumes backup for malware scanning, and support malware scanning for big ADS information.

- *For MSDP storage*, dynamic scan feature is applied on platform BYO, NBA, Flex, Flex-worm, FlexScale, Azure Kubernetes Services Cluster / Amazon Elastic Kubernetes Cluster.
- *For DirectIO, OST and Advanced Disk storage*, dynamic scan feature is applied only on platform BYO, NBA and Flex appliance.

About file hash search with malware hash

For a NetBackup domain that is not managed by Alta View and with a configured file hash server, NetBackup version 10.5.0.1 or later provides the feature of file hash search with malware hash.

This feature complements the existing malware scanning service and provides the capabilities of identifying malware from backup images. When malware scan reports an infected status, an automated file hash search job navigates through the NetBackup images to identify an IOC (indicator of compromise).

When a malware is found by malware scanning, the file hash value (SHA-256) of the malware is stored in Enterprise Media Manager (EMM) database if no matching record exists in the database.

Every 8 hours, the most recent malware hash values (max 10,000 records) from the database are submitted to the triggered file hash search job request with **MALWARE** as the search tag. The result of the file hash search job is available in the Activity monitor of NetBackup Web UI. An audit message that contains the file hash search job ID and file hash search request ID is also generated. The message can be found under the **Audit Events** tab of Security events menu in the Security

pane of NetBackup Web UI. Use the **FILE_HASH_SEARCH_INTERVAL_SECONDS** option to configure the interval between search jobs that are triggered.

Every 24 hours, the records stored in NetBackup database that have not been updated for the past 30 days are removed for maintenance purpose. Use the **MALWARE_HASH_RETENTION_DAYS** option to configure the number of days when a malware hash is treated as outdated.

See [“Malware hash configuration parameters”](#) on page 721.

Note the following:

The file hash search computation is supported for the following types of backup policies:

- NAS-Data-Protection
- Windows
- Standard

The file hash search job may report a matching malware if there is any for the backup images of the above types of backup policies.

Limitations

- Client-side encryption and client-based compressed backups are unavailable for scanning using Instant Access mount points. MSDP KMS-based encryption techniques are recommended and can be configured (See the *NetBackup Security and Encryption Guide*.)
- User archive backups and synthetic backups are unavailable for scanning using Instant Access mount points.
- For VMware and Hyper-V: Incremental backup images without accelerator feature enabled are not supported for VMware workload.
- Windows EFS files/folders are unavailable for scanning using Instant Access mount points.
- (For OST and AdvancedDisk) Supports malware scan for unstructured data only. For more information, see the *NetBackup Software Compatibility List*.
- NetBackup does not support SMB share type on AKS/EKS Active Directory platform. For more information, see the *NetBackup Deduplication Guide*.
- NetBackup images replicated to different NetBackup domain must be scanned in the target domain again. Malware scan detailed status (for example, infected file list, malware scanner used, signature information) of the backup images in the source domain is not preserved during replication.

- Back-level compatibility for media servers and old backup images on upgraded media servers is only supported from NetBackup version 10.3 onwards. This support is applicable to workload type support provided in NetBackup version 10.4 or later.
- During the clean file recovery for the selected time range, NetBackup would provide a list of infected files to be excluded and to include clean copy of the file if found in the previous backup. Clean file recovery is not triggered if the list of files to be included/excluded exceeds the maximum limit of 4000 files and fails with an error message.
- Clean file recovery is not supported for **True image backups** type of restore.
- Starting with NetBackup 10.3, if malware scan is run for a client-side encrypted backup, all the files are skipped. A notification is generated for the skipped file and displayed in the NetBackup Web UI.
- Malware scan result of the AIR replicated image may appear as **Not scanned** if replication appears before the malware scan is completed. Malware scan can take longer time to complete depending on the number of files in the backup and other malware scans which are in progress.
- (For Flex application as the scan host)
 - In the event that the scan host pool is accidentally deleted, the user must manually add the new pool using the `POST API /malware/scan-host-pools` with the **scanHostType** set to **FLEX_SCAN_HOST**. The existing scan host must then be added to the new pool.
 - When a Flex configuration is configured for High Availability (HA), the application is deactivated when it is stopped. However, the host is automatically activated as a result of fail over operation. The intention was not to send the scan requests to this host; however, the users must ensure that this scan host is available to conduct fresh scans due to the availability of another instance.
- (For VxMS based Instant Access scan)
 - The VxMS based Instant Access scan is supported only for BYO, NetBackup Appliances, and Flex Appliance.
 - When a VM contains a filesystem unsupported by VxMS, and a backup is created using the **Enable file recovery from VM backup** option, VxMS will fail to create a catalog for this backup. As a result, any malware scan carried out on such a backup will not scan the files associated with the unsupported filesystem. Do not enable the **Enable file recovery from VM backup** option in the backup policy for these VMs.

- When the recovery time scan option **If any files are infected with malware, recover all files, including infected files** is selected, infected files are skipped if the backup images selected for malware scan and recovery have already been scanned and marked as infected. To recover these files, select the **Allow the selection of images that are malware-affected** option.

How to setup Malware scanning

This chapter includes the following topics:

- [How to set up malware scanning](#)

How to set up malware scanning

[Table 39-1](#) describes a high level process for setting up malware scanning.

Table 39-1 Process for setting up malware scanning

Steps	Description
Step 1	Install or upgrade NetBackup software on the primary server, the media server, and MSDP storage server to version 10.0 or later. NetBackup Installation or Upgrade Guide
Step 2	For BYO setup, Instant access must be configured on MSDP storage server. See “MSDP build-your-own (BYO) server prerequisites and hardware requirements to configure Instant Access” on page 648.

Table 39-1 Process for setting up malware scanning (*continued*)

Steps	Description
Step 3	On the scan host, configure any of the following malware tool: ■ NetBackup Malware Scanner (Avira) Note: (<i>Applicable only for Avira</i>) Avira is configured automatically when using the automated scripts as described in Step 4 below. ■ Symantec Protection Engine ■ Microsoft Defender Antivirus ■ Trend Micro Malware Scanner ■ NetBackup NextGen Malware Scanner Note: Ensure that the host user has required permission to scan with configured malware tool and is able to access the mount on the storage server. See “Supported malware tools” on page 652.
Step 4	Malware scanning feature requires additional configurations on scan host. The scan host configuration can be performed through automated scripts or manually. ■ Automated scripts: See “Automated scan host configuration” on page 678. ■ Manual configuration: See “Manual scan host configuration” on page 682. Scenario based scan host configuration: ■ For Agentless host See “Configure malware scan host for Windows NFS share type and Microsoft Defender” on page 684. See “Configure malware scan host for Linux NFS share type and Avira” on page 686. ■ For NetBackup client as the scan host See “Configuring NetBackup client as the scan host” on page 688.
Step 5	On the NetBackup Web UI, configure the malware detection settings. See “Configuring a scan host pool” on page 689.

Instant Access configurations

This chapter includes the following topics:

- [About Instant Access configurations](#)
- [MSDP build-your-own \(BYO\) server prerequisites and hardware requirements to configure Instant Access](#)
- [Instant Access tuning parameters for malware scanning \(BYO\)](#)
- [Configuration for scan instances](#)

About Instant Access configurations

Perform the steps provided in the following sections for configuring the Instant Access for malware scanning:

- [MSDP build-your-own \(BYO\) server prerequisites and hardware requirements to configure Instant Access](#)
- [Instant Access tuning parameters for malware scanning \(BYO\)](#)
- [Configuration for scan instances](#)

The procedures mentioned in the above three sections are also applicable for Media server of OST storage server which is configured as a MSDP storage (for Instant Access capability) which is described in the following section:

See [“Malware scanning workflow for OST and AdvancedDisk”](#) on page 638.

MSDP build-your-own (BYO) server prerequisites and hardware requirements to configure Instant Access

The following are prerequisites for using the Instant Access MSDP build-your-own (BYO) server feature:

- The Instant Access feature is supported on an MSDP BYO storage server with Red Hat Enterprise Linux 7.6 or later.
- The Instant Access feature is not supported on SUSE Linux.
- *(For SMB)* You must set up Active Directory-based user authentication for the Instant Access.

For more information, see *Active Directory-based authentication* section in the [NetBackup Deduplication Guide](#).

(For NFS) Instant Access works without Active Directory-based user authentication.

- NFS services must be installed and running if you want to use the instant access over NFS.
- Samba services must be installed and running if you want to use instant access over CIFS/SMB.
You must configure Samba users on the corresponding storage server and enter the credentials on the client.
For more information, see *Active Directory-based authentication* section in the [NetBackup Deduplication Guide](#).

- *(For NFS)* Ensure that the `nfs-utils` is installed using the following command:

```
yum install nfs-utils -y
```

- *(For SMB)*

- Ensure that the Linux `samba` and `samba winbind` packages are installed using the following command:

```
yum install samba samba-common samba-winbind  
samba-winbind-clients samba-winbind-modules -y
```

- Ensure that the following commands are run to grant permissions to the SMB shares:

```
setsebool -P samba_export_all_rw on  
setsebool -P samba_export_all_ro on
```

- NGINX is installed and running.
 - Installing NGINX from Red Hat Software Collections:

Refer to <https://www.softwarecollections.org/en/scls/rhscl/rh-nginx114/> for instructions.

Because the package name depends on the NGINX version, run `yum search rh-nginx` to check if a new version is available. (For NetBackup 8.3, an EEB is required if NGINX is installed from Red Hat Software Collections.)

- Installing NGINX from the EPEL repository:

Refer to <https://fedoraproject.org/wiki/EPEL> for installation instructions of the repository and further information.

The EPEL repository is a volunteer-based community effort and not commercially supported by Red Hat.

- Before you start the storage configuration, ensure that the new BYO NGINX configuration entry `/etc/nginx/conf.d/byo.conf` is included as part of the HTTP section of the original `/etc/nginx/nginx.conf` file.

- If SE Linux has been configured, ensure that the `polycoreutils` and `polycoreutils-python` packages are installed from the same RHEL yum source (RHEL server), and then run the following commands:

```
semanage port -a -t http_port_t -p tcp 10087
setsebool -P httpd_can_network_connect 1
```

Enable the `logrotate` permission in SE Linux using the following command:

```
semanage permissive -a logrotate_t
```

- After NGINX is installed, the HTTP web service at port 80 is enabled by default. Remove `/etc/nginx/conf.d/default.conf` or edit the file to disable the HTTP web service if it is not needed.
- Ensure that the `/mnt` folder on the storage server is not directly mounted by any mount points. Mount points should be mounted to its subfolders.
- If you configure the Instant Access feature on BYO after storage is configured or upgraded without the NGINX service installed, run the command:
`/usr/opensv/pdde/vpfs/bin/vpfs_config.sh --configure_byo`
- (For Hyper-V backup images) For mounting Instant Access, following libraries are required on media server:

- `libguestfs`
- `python3-libguestfs`
- `libguestfs-winsupport`
- `libguestfs-tools`
- `libguestfs-xfs`
- `libguestfs-tools`

- `libguestfs-tools-c`
- Ensure that the required network ports are open.
See "NetBackup media server ports" in the *NetBackup Network Ports Reference Guide*.

CPU	Memory	Disk
■ Minimum 2.2-GHz clock rate. ■ 64-bit processor. ■ Minimum 4 cores; 8 cores recommended. For 64 TBs of storage, the Intel x86-64 architecture requires eight cores. ■ Enable the VT-X option in the CPU configuration.	■ 16 GB (For 8 TBs to 32 TBs of storage - 1GB RAM for 1TB of storage). ■ 32 GBs of RAM for more than 32 TBs of storage. ■ An additional 500MB of RAM for each live mount.	■ Disk size depends on the size of your backup. Refer to the hardware requirements for NetBackup and Media Server Deduplication Pool (MSDP). ■ If a system has multiple data partitions, all the partitions must be the same size. Example: If a BYO server has a first partition at 4TB, all additional data partitions must be at 4TB in size.

Instant Access tuning parameters for malware scanning (BYO)

- Perform the following to update the Linux kernel **vm.max_map_count** parameter:
 - Add the following to parameter with value to the `/etc/sysctl.conf` file:
`vm.max_map_count=262144`
 - Reload the configuration file using the following command:
`root: sysctl -p`
 - Verify the updated new value of **vm.max_map_count** parameter using the following command:
`cat /proc/sys/vm/max_map_count`

Configuration for scan instances

The traditional malware scan using Instant Access is based on `vpfsd` instance. NetBackup 10.3 and later uses a separate `vpfsd` instance for malware scanning which is configurable. This configuration is done using the **numOfScanInstance**

parameter. By default, malware scan uses one instance. In most cases, scan instance is adequate but increasing the number of scan instances improves scan performance, although it also requires more CPU and memory. You can increase the number of scan instances from 1 to 4 and distribute the malware scan shares cross all the scan instances.

To change the number of scan instances

- 1 Stop NetBackup on the media server using the following command:

```
systemctl stop netbackup
```

Or

```
/usr/opensv/netbackup/bin/goodies/netbackup stop
```

- 2 Modify the number of scan instances as follows:

Change the value of **numOfScanInstance** parameter in the `vpfsd_config.json` file. The value must be an integer between 1 and 4.

For example:

```
# grep numOfInstance /msdp/vol1/etc/puredisk/vpfsd_config.json
```

BYO (build-your-own): <storage path>/etc/puredisk/vpfsd_config.json

NetBackup Appliance and NetBackup Flex Scale:

```
/msdp/data/dp1/pdvol/etc/puredisk/vpfsd_config.json
```

NetBackup Flex: /mnt/msdp/vol0/etc/puredisk/vpfsd_config.json

- 3 Modify the number of vpfsd instances (**numOfInstance**), the value must be an integer between 2 and 16. Ensure that the value of **numOfInstance** is greater than **numOfScanInstance**.

- 4 Start NetBackup on the media server using the following command:

```
systemctl start netbackup
```

Or

```
/usr/opensv/netbackup/bin/goodies/netbackup start
```

Note: Malware scan instances are part of vpfsd instances, which are reserved only for malware scanning.

Malware tools configurations

This chapter includes the following topics:

- [Supported malware tools](#)
- [Configuring NetBackup Malware Scanner \(Avira\)](#)
- [Configuring Symantec Protection Engine](#)
- [Configuring Microsoft Defender Antivirus](#)
- [Configuring Trend Micro Malware Scanner](#)
- [Configuring NetBackup NextGen Malware Scanner](#)

Supported malware tools

Note: Ensure that scan jobs are cancelled before upgrading any malware scanner tool or restarting the master server.

NetBackup provides support for the following malware detection tools:

- NetBackup Malware Scanner (Avira)
See [“Configure the NetBackup Malware Scanner on scan host”](#) on page 659.

Note: The malware signature gets updated before every scan. If scan host does not have access to internet, then user must first configure the mirror server or a proxy server. For more information, refer to the following section:

See [“Configuration of mirror server for Signature update”](#) on page 654.

- Symantec Protection Engine
 See [“Configuring Symantec Protection Engine”](#) on page 664.
- Microsoft Defender Antivirus
 See [“Configuring Microsoft Defender Antivirus”](#) on page 665.
- Trend Micro Malware Scanner
 See [“Configuring Trend Micro Malware Scanner”](#) on page 666.

Note: NetBackup 11.0 and later now provides support for malware scanning using the Trend Micro Malware Scanner only for Linux.

- NetBackup NextGen Malware Scanner
 See [“Configuring NetBackup NextGen Malware Scanner”](#) on page 666.

Note: When using any other malware scanner tool on Windows scan host, user must disable the **Real time protection** option of the Windows Defender while malware scan is in progress.

Configuring NetBackup Malware Scanner (Avira)

This section includes the following:

- Mirror server configuration for signature update of malware scanner tool (Avira) when internet connectivity is not there on scan host.
- Proxy server configuration for malware scanner tool (Avira) when no direct internet connectivity.
- NetBackup malware scanner configuration on scan host.

NetBackup Malware Scanner configuration can also be performed using automated scripts. For more information, refer to the following section:

See [“Automated scan host configuration”](#) on page 678.

Note: Automated scripts do not include mirror server and proxy server configuration. If required, then manually perform the steps in the following:

[Configuration of mirror server for Signature update](#)

[Configure a proxy server on Windows or Linux](#)

Note: Ensure that you have the latest version of NetBackup Malware Scanner (Avira) downloaded.

Configuration of mirror server for Signature update

NetBackup Malware Scanner (Avira) mirror server must be configured for signature update only when scan host does not have access to internet.

Creating local mirror server

- 1 A designated host with NetBackup Malware Scanner must be installed.
- 2 Login with the same user credentials used to install the NetBackup Malware scanner and run the following command:

```
cd $NB_MALWARE_SCANNER_PATH

./avupdate.bin --mirror --config=avupdate-savapilib-product.conf
--install-dir=<update_path>
```

- 3 Publish the <update_path> over HTTP.

For example, **https://<local_mirror_server>/<update_path>**.

Note: Periodically run `./avupdate.bin --mirror` command to keep the signature data up-to-date on the mirror server.

Using local mirror server during signature update

- 1 The `update.sh` script refers to `avupdate-savapilib-product.conf` file which is at the same location as that of `update.sh`, that is `$NB_MALWARE_SCANNER_PATH`.
- 2 Update the `internet-srvs` entry in `.conf` file to point to the URL served by the local mirror server mentioned above.

```
~/savapi-sdk-linux64/bin> cat avupdate-savapilib-product.conf
#This configuration updates the entire SAVAPI Library (binaries,
  engine, signatures)
#internet-srvs=https://oem.avira-update.com/update
internet-srvs=https://<local_mirror_server>/<update_path>
master-file=/idx/master.idx
product-file=/idx/savapi4lib-linux64-en.info.gz
install-dir=./
temp-dir=./tmp
check-product
```

3 In the `update.sh` file, comment and uncomment the sentences marked in bold:

Old file:

```
#!/usr/bin/env bash
#
# Copyright (c) Avira Operations GmbH
#
# VERSION=1.0.0.8
# Description: Contains the basic update commands for SAVAPI
Server and Library
#
#
# SAVAPI Server update
#
# product update (all modules)
./avupdate.bin --config=avupdate-savapi-product.conf
--check-product
# engine update (engine binaries and virus definition modules)
# ./avupdate.bin --config=avupdate-savapi-engine.conf
--check-product
#
# SAVAPI Library update
#
# product update (all modules)
#!/avupdate.bin --config=avupdate-savapilib-product.conf
--check-product
# engine update (engine binaries and virus definition modules)
# ./avupdate.bin --config=avupdate-savapilib-engine.conf
--check-product
```

New file (After commenting and uncommenting the sentences in bold above):

```
#!/usr/bin/env bash
#
# Copyright (c) Avira Operations GmbH
#
# VERSION=1.0.0.8
# Description: Contains the basic update commands for SAVAPI
Server and Library
#
#
# SAVAPI Server update
#
```

```
# product update (all modules)
# ./avupdate.bin --config=avupdate-savapi-product.conf
--check-product
# engine update (engine binaries and virus definition modules)
# ./avupdate.bin --config=avupdate-savapi-engine.conf
--check-product
#
# SAVAPI Library update
#
# product update (all modules)
# ./avupdate.bin --config=avupdate-savapilib-product.conf
--check-product
# engine update (engine binaries and virus definition modules)
```

```
#./avupdate.bin --config=avupdate-savapilib-engine.conf
--check-product
```

4 Run the `update.sh` script to ensure that the update is working correctly.

The `avupdate.log` file displays the following entries:

```
~/savapi-sdk-linux64/bin> head avupdate.log
18/09/2022 23:31:47 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:
  Avupdate Version: 2.6.10.36
18/09/2022 23:31:47 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:
  Operating System: LINUX X86_64 5.3.18-22-DEFAULT
18/09/2022 23:31:47 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:
  Installation Directory: .
18/09/2022 23:31:47 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:
  Backup Directory: ./avupdate_backup
18/09/2022 23:31:47 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:
  Temp Directory: ./tmp/avupdate_tmp_njoOb5
18/09/2022 23:31:47 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:
  Cache Modules Directory: ./idx
18/09/2022 23:31:47 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:
  Proxy settings: Direct connection
18/09/2022 23:31:47 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:

Downloading
https://local_mirror_server/<update_path>/idx/master.idx
to ./tmp/avupdate_tmp_njoOb5/idx/master.idx
18/09/2022 23:31:48 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:

Downloading
https://<local_mirror_server>/<update_path>/idx/savapi4lib-linux64-en.info.gz

to ./tmp/avupdate_tmp_njoOb5/idx/savapi4lib-linux64-en.info.gz
18/09/2022 23:31:49 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:

Downloading
https://<local_mirror_server>/<update_path>/idx/xvdf.info.gz
to ./tmp/avupdate_tmp_njoOb5/idx/xvdf.info.gz
```

Manually updating local mirror server during no internet connectivity

- 1 On system with internet connectivity, download the signature database.

Note: The `NBAntiMalwareClient` must be installed on the system with internet connectivity.

```
./avupdate.bin --config=avupdate-savapilib-product.conf --mirror
--install-dir=<mirror_dir>
```

- 2 Copy the contents of `<mirror_dir>` from above to the mirror server:

```
./avupdate.bin --config=avupdate-savapilib-product.conf
--internet-srvs=<local_copy_of_mirror_dir>
```

Configure a proxy server on Windows or Linux

To configure a proxy server on Windows

- 1 Add the proxy server entry in the environment variable with the `http_proxy` name and the `<proxy_server>` value.

For example:

```
http_proxy=http://<username>:<password>@proxy_server_ip:<port>
```

- 2 Add the proxy server details in the `avupdate-savapilib-product.conf` file which is available at NetBackup malware scanner installed path.

For example:

```
proxy-username=<username>
proxy-password=<password_paintext>
proxy-host=<proxy_server_ip>
proxy-port=<proxy_server_port>
update-auth-type=any
receive-timeout=600000
connect-timeout=600000
```

To configure a proxy server on Linux

- 1 Add proxy server entry in the environment variable with **http_proxy** name.

For example:

```
http_proxy=http://<username>:<password>@proxy_server_ip:<port>
```

This variable should be added in the `.bashrc` file of the scan host.

- 2 Add the proxy server details in the `avupdate-savapilib-product.conf` file.

For example:

```
proxy-username=<username>
proxy-password=<password_paintext>
proxy-host=<proxy_server_ip>
proxy-port=<proxy_server_port>
update-auth-type=any
receive-timeout=600000
connect-timeout=600000
```

- 3 In the `savapi` logs, verify if the correct proxy settings are used for malware scanning.

Configure the NetBackup Malware Scanner on scan host

Recommendation for Avira

It is recommended not to change the name of the EICAR test file downloaded from [EICAR](#) website.

Avira does not detect files with `.txt` extension. Avira considers these as simple text files and skips malware scan of such files.

The description and purpose of the EICAR test file is as follows:

The EICAR Anti-Virus test file, also known as the EICAR test file, is a computer file developed by the European Institute for Computer Antivirus Research (EICAR) and the Computer Antivirus Research Organization (CARO). Its purpose is to test the response of computer antivirus (AV) programs without using real malware that could cause actual damage. Instead of using harmful viruses, the EICAR test file allows people to safely evaluate their antivirus software.

Configure the NetBackup Malware Scanner for Windows

To configure the NetBackup Malware Scanner for Windows

- 1 Download the **NetBackup Malware Scanner** from [Veritas Download Center](#).
- 2 Extract the downloaded zip files. Extracted files must have the following structure:

```
NBAntiMalwareClient_version number
  Readme.txt

  NBAntiMalwareClient_version number_AMD64
    savapi-sdk-win64.zip
    setup.bat
    cleanup.bat
```

- 3 Refer to the `Readme.txt` file for install, upgrade, or uninstall processes.

To install or upgrade the NetBackup Malware scanner on a Windows computer:

- Navigate to `NBAntiMalwareClient_version number_AMD64` folder and run the `setup.bat` file.
- Enter the target location to install the NetBackup Malware scanner.

Note: If NetBackup Malware Scanner is already installed, then `setup.bat/setup.sh` overwrites the existing binary files.

To uninstall NetBackup Malware scanner from Windows computer:

- Run the `cleanup.bat` file.

- 4 An optional setting can be used to increase number of threads in scanning.

Update the `aviraconf.txt` file. Add the following entry:

```
NumThreads = Number of threads
```

Where *Number of threads* is the number of threads for the scanning. The default value is the number of CPU cores. (Minimum value is 1. Maximum value is 300).

Note: If the number of CPUs on the scan host is less than 16, then number of threads defaults to the number of CPUs. If greater than 16, then the number of threads defaults to 16 threads. If `NumThreads` is configured, that value determines the number of threads for scanning.

- 5 To validate that the scan works with NetBackup Malware Scanner on a Windows setup, perform the following:
 - Run the `./update.bat` command to get the latest signature update.
 - Navigate to the NetBackup Malware Scanner installed path and run the `avira_lib_dir_scan.exe` file with the required `scan_path` and `conf_path` parameters.

- 6 Configuration file must be present in NetBackup Malware Scanner installed path.

For example:

```
avira_lib_dir_scan.exe "c:\malwaresample" -log_path
"C:\NBMalwareScanner.log" -conf_path
"C:\NBMalwareScannerInstallPath\savapi-sdk-win64\bin\aviraconf.txt
```

Ensure that the output of the command is successful. For the existing sample malware files, the output must be a list of infected files. Else the output must be empty.

- 7 (Optional) The **MALWARE_LOG** environment variable can be used to increase the logging level.

For example, the setting `MALWARE_LOG=2` sets the logging level to `WARNING`.

```
0 DEBUG
1 INFO
2 WARNING
3 ALERT
4 ERROR
```

Configure a NetBackup Malware Scanner Linux

To configure a NetBackup Malware Scanner for Linux

- 1 Download **NetBackup Malware Scanner** from [Veritas Download Center](#).
- 2 Extract the downloaded zip file. Files must contain the following structure;

```
NBAntiMalwareClient_version number_LinuxR_x86
    savapi-sdk-linux64.zip
    setup.sh
    cleanup.sh

NBAntiMalwareClient_version number_LinuxS_x86 ->
NBAntiMalwareClient_version number_LinuxR_x86
    savapi-sdk-linux64.zip
    setup.sh
    cleanup.sh
```

Warning: The `setup.sh` script modifies the `bashrc` file on Linux.

- 3 Refer to the `Readme.txt` file for install, upgrade, or uninstall processes.

To install or upgrade NetBackup Malware Scanner on Linux RHEL computer.

- Navigate to `NBAntiMalwareClient_version number_LinuxR_x86` folder and run the `setup.sh` script using `scanuser`.
- Enter the target location to install the NetBackup Malware Scanner.

To install or upgrade NetBackup Malware Scanner on Linux SUSE computer:

- Navigate to `NBAntiMalwareClient_version number_LinuxS_x86` folder and run the `setup.sh` script using `scanuser`.
- Enter the target location to install the NetBackup Malware Scanner.

Note: For Linux SUSE computer, if `.bashrc` file is not present then create an empty `.bashrc` file in users home directory.

Note: The path of the scanner directory (/bin) is added in the `.bashrc` file of the Linux user which is installing the NetBackup Malware Scanner.

If you are using NetBackup client as the scan host, then it is recommended to add the same entry in `/usr/opensv/netbackup/bp.conf` configuration file so that any Linux user (to be used for malware scanning) knows the scanner directory (/bin) path. For example,

```
NB_MALWARE_SCANNER_PATH=/root/Avira/savapi-sdk-linux64/bin
```

To uninstall NetBackup Malware Scanner from Linux computer:

- Run the `cleanup.sh` script.

4 To validate that the scan works with the NetBackup Malware Scanner on a Linux setup, perform the following:

- Run the `./update.sh` script to get the latest signature update.
- Navigate to NetBackup Malware Scanner installed path and run the `avira_lib_dir_scan` binary with the required scan path and `conf_path` parameters.
- Configuration file must be present in NetBackup Malware Scanner installed path.

For example,

```
avira_lib_dir_scan "/root/malwareSample" -log_path
"/root/NBMalwareScanner.log" -conf_path
"/root/NBMalwareScannerInstalledPath/savapi-sdk-linux64/bin/
aviraconf.txt
```

Ensure that the output of the command is successful. For existing sample malware files, the output must be a list of infected files. Else the output must be empty.

Configuring Symantec Protection Engine

Windows

Configuring Symantec Protection Engine for Windows

- 1 Set Command-line executable path in PATH environment variable.

For example: `C:\Program Files\Symantec\Scan Engine\CmdLineScanner\C`

- 2 Run the following command on command prompt and verify the output:

```
sseccls -mode scan -scantype S C:\
```

Note: For license error, apply the updated licenses.

- 3 (Optional) Set the **SCAN_FILE_BUCKET_SIZE** environment variable.

For example:

```
SCAN_FILE_BUCKET_SIZE = 40
```

If `SCAN_FILE_BUCKET_SIZE` not set then default
`SCAN_FILE_BUCKET_SIZE` is 20.

Note: The `sseccls` scanner CLI supports multiple files to be scanned at a time which are specified on command line. The **SCAN_FILE_BUCKET_SIZE** environment variable can be updated to change the default value which is 20.

Linux

Configuring Symantec Protection Engine for Linux

- 1 Set executable path in `bashrc` file.

For example: `export PATH="/opt/SYMCScan/ssecls/C"`
`LD_LIBRARY_PATH= $LD_LIBRARY_PATH:/opt/SYMCScan`

- 2 Run the following command on command prompt and verify the output:

```
ssecls -mode scan -scantype F /
```

Note: For license error, apply the updated licenses.

- 3 (Optional) Set the **SCAN_FILE_BUCKET_SIZE** environment variable.

For example:

```
SCAN_FILE_BUCKET_SIZE = 40
```

If `SCAN_FILE_BUCKET_SIZE` not set then default
`SCAN_FILE_BUCKET_SIZE` is 20.

Configuring Microsoft Defender Antivirus

Configuring Microsoft Windows Defender Antivirus

- 1 Navigate to **Control Panel > System and Security > System**. Select **Advanced System** and set executable path in **PATH** environment variable.

For example: `C:\Program Files\Windows Defender`

- 2 Run the following command in command prompt:

```
MpCmdRun -Scan -ScanType 3 -DisableRemediation -File <filepath>  
check if result is proper
```

For example:

```
C:\Program Files\Windows Defender>MpCmdRun -Scan -ScanType 3  
-DisableRemediation -File "C:\Program Files\Windows Defender"  
Scan starting...  
Scan finished.  
Scanning C:\Program Files\Windows Defender found no threats.
```

Configuring Trend Micro Malware Scanner

NetBackup 11.0 and later provides support for malware scanning using the Trend Micro Malware Scanner.

Note: The Trend Micro Malware Scanner is currently only supported for Linux.

To configure Trend Micro Malware Scanner for Linux

- 1 Install Trend Micro Deep Security Manager and Agent from [Trend Business Software Download Center](#).

Note the following:

- Deep Security Manager can be installed on another setup other than the scan host.
- Deep Security Agent must be installed on the scan host.
The minimum required version of Deep Security Agent is 20.0.1-690.

- 2 The Trend Micro Malware Scanner supports malware scanning only through the root user. This requirement is due to the following support of the `dsa_scan` command in Trend Micro:

If you have root access rights on Linux, you can use the `dsa_scan` command to run a scan task with specified files or directories, including the subdirectories.

- 3 Set the environment variable `TREND_MICRO_AGENT_PATH` in `.bashrc` file as follows:

For example: `export TREND_MICRO_AGENT_PATH=/opt/ds_agent`

Note: If you use the NetBackup client as the scan host, then it is recommended to add the same entry in `/usr/openv/netbackup/bp.conf` configuration file.

For example, `TREND_MICRO_AGENT_PATH=/opt/ds_agent`

- 4 Run the following command on the command prompt and verify the output:

```
/opt/ds_agent/dsa_scan --action pass --target <path to scan>
```

Configuring NetBackup NextGen Malware Scanner

NetBackup 11.1 and later now provides support for malware scanning using the NetBackup NextGen Malware Scanner.

Prerequisites

Ensure that **wget** is installed and available in the system PATH.

For Windows systems, you can download the **wget** utility from the following link:

<https://eternallybored.org/misc/wget/>

Windows

Configuring NetBackup NextGen Malware Scanner for Windows

- 1 Download the NetBackup NextGen Malware Scanner from [Veritas Download Center](#).
- 2 Extract the downloaded zip files. Extracted files must have the following structure:

```
NBNextGenMalwareScanner_version_number
    Readme.txt
    NBNextGenMalwareScanner_version_number_AMD64
        savapi-sdk-win64.zip
        setup.bat
```

- 3 Refer to the `Readme.txt` file for install, upgrade or uninstall processes.

To install or upgrade the NetBackup NextGen Malware Scanner on a Windows computer:

- Navigate to the `NBNextGenMalwareScanner_version_number_AMD64` folder and run the `setup.bat` file as an administrator user, this is required to register DLL.
- Enter the target location to install the NetBackup NextGen Malware Scanner.

Note: If NetBackup NextGen Malware Scanner is already installed, then `setup.bat` overwrites the existing binary files.

To uninstall the NetBackup Malware Scanner from a Windows computer:

- Run the `cleanup.bat` file.
- 4 To validate that the scan works with NetBackup NextGen Malware Scanner on a Windows setup, perform the following:
 - Navigate to the NetBackup NextGen Malware Scanner installed path and run `sophos_update` to get the latest signature update.
 - Run `sophos_scan_cmd.exe` command with the required parameters.
 For example, `sophos_scan_cmd.exe -i ./ide -d ./vdl <sample file path>`

Ensure that the output of the command is successful:

- For existing sample malware files, the output must be a list of infected files.
- Otherwise, the output must be empty.

Linux

Configuring NetBackup NextGen Malware Scanner for Linux

- 1 Download the NetBackup NextGen Malware Scanner from [Veritas Download Center](#).
- 2 Extract the downloaded zip files. Extracted files must have the following structure:

```
NBNextGenMalwareScanner_version_number_LinuxR_x86
    savapi-sdk-linux64.zip
    setup.sh
    cleanup.sh
    NBNextGenMalwareScanner_version_number_LinuxS_x86
        savapi-sdk-linux64.zip
        setup.sh
        cleanup.sh
```

Warning: The `setup.sh` script modifies the `.bashrc` file on Linux.

- 3 Refer to the `Readme.txt` file for install, upgrade, or uninstall processes.

To install or upgrade NetBackup NextGen Malware Scanner on a Linux *RHEL* computer:

- Navigate to the `NBNextGenMalwareScanner_version_number_LinuxR_x86` folder and run the `setup.sh` script using the **scanuser** (name of the user used for scanning).
- Enter the target location to install the NetBackup NextGen Malware Scanner.

To install or upgrade NetBackup NextGen Malware Scanner on a Linux *SUSE* computer:

- Navigate to the `NBNextGenMalwareScanner_version_number_LinuxS_x86` folder and run the `setup.sh` script using **scanuser** (name of the user used for scanning).
- Enter the target location to install the NetBackup NextGen Malware Scanner.

Note: For Linux SUSE computers, if the `.bashrc` file is not present, create an empty `.bashrc` file in the user's home directory.

The path of the scanner directory (`/bin`) is added to the `.bashrc` file of the Linux user installing the NetBackup NextGen Malware Scanner.

To uninstall NetBackup NextGen Malware Scanner from a Linux computer:

- Run the `cleanup.sh` script.
- 4 To validate that the scan works with the NetBackup NextGen Malware Scanner on a Linux setup, perform the following:
- Navigate to the NetBackup NextGen Malware Scanner installed path and run `sophos_update` to get the latest signature update.
 - Run `sophos_scan_cmd.exe` command with the required parameters.
For example, `./sophos_scan_cmd -i ./ide -d ./vdl <sample file path>`
Ensure that the output of the command is successful:
 - For existing sample malware files, the output must be a list of infected files.
 - Otherwise, the output must be empty.

Note: When using a NetBackup Client as the scan host, configure the **NB_NEXTGEN_MALWARE_SCANNER_PATH** environment variable for the NetBackup Client processes. One option is to add the following entry to the `bp.conf` file:

```
NB_NEXTGEN_MALWARE_SCANNER_PATH = <sophos installed
path>/sophos-sdk-linux64/bin
```

Although this is a supported method, it is not mandatory for malware scan execution.

Ensure that the environment variable is configured persistently so that it remains available after an operating system reboot. If the setting is not persistent, malware scanning operations may fail following a restart.

After updating the environment variable, restart the NetBackup Client services on the scan host for the changes to take effect.

Scan host configurations

This chapter includes the following topics:

- [NetBackup malware scan host capabilities](#)
- [Prerequisites for a scan host](#)
- [Limitations and considerations for scan host using NFS share](#)
- [Configuring scan host](#)
- [Configuring a scan host pool](#)
- [Managing a scan host](#)
- [Configure resource limits for malware detection](#)

NetBackup malware scan host capabilities

The NetBackup malware scan host that is configured on stand-alone Windows vs Linux operating system will differ slightly in its capabilities and behavior. Windows and Linux hosts can be used as a stand-alone scan host for on-demand malware scan. The prerequisites for a scan host, for Windows and Linux operating system hosts are mentioned in the following section:

See [“Prerequisites for a scan host”](#) on page 671.

Note: For faster scans, better resource utilizations (including support for multiple parallel scans), and consistent scan performance, it is recommended to use a Linux scan host configured with the NFS share type, together with either the NetBackup Malware Scanner (Avira) or the NetBackup NextGen Malware Scanner.

Windows and Linux scan host will not be able to scan the following file types (these will be skipped):

- Password protected files
- Encrypted files
- Compressed and password protected file archives (zip, tar, gzip)
- Corrupted files

Windows and Linux scan host will skip a file if the scanner is unable to determine the file type.

Prerequisites for a scan host

A scan host is a host machine that has the required malware tool configured. Once it is integrated with NetBackup, NetBackup initiates scanning on the scan host.

Ensure that you meet the following prerequisites:

- The minimum required configuration for the scan host is 8 CPU and 32-GB RAM.
- The malware tool must be installed and configured.
- For the supported operating systems of the scan host, refer to the [Software Compatibility List](#).
- The scan host must have a share type configured, that is, an NFS or an SMB client.
- If the scan host connectivity type is **Agentless host**:
 - NetBackup footprint is not required on the scan host. The existing systems with the NetBackup client or media server can be used as scan host, too.
 - The scan host must be reachable from the media server over SSH.

Note: The SSH connection to the scan host from the media server must be successful. You can verify this connection by running the following command from the media server:

```
ssh scanuser@scanhost
```

If the scan host connectivity type is **NetBackup client**:

- NetBackup footprint is required on the scan host.
- The NetBackup primary server and the media server providing the Instant Access mounts must be reachable from the NetBackup client.

- By default, the NetBackup client scan host would be in a deactivate state. After adding NetBackup client scan host to scan host pool you must activate the scan host.
See [“Activate or deactivate the scan host”](#) on page 693.
- The malware tool uses the temporary location to store the files that are created during the malware scan. The path of the temporary location is configured in the web UI in the **Malware global settings**. Ensure that the user has write permissions to this path.
For archive scanning purposes, it is recommended to have the free disk space of 10 GB on the scan host.

Note: (*Applicable for NetBackup version 10.0 and later*) Any other malware scanner tools that are installed on the scan host with on-access/real time protection enabled can interfere with backup scanning. Disable or add NFS/SMB mounts on the scan host to the exclusion list of the scanner.

For example, on a Windows scan host, the user must disable the **Real time protection** option of the Windows Defender while the malware scan is in progress.

- Depending on the platform, ensure that the following additional prerequisites are met:
Windows: See [“Prerequisites for Windows scan host”](#) on page 672.
Linux: See [“Prerequisites for Linux scan host”](#) on page 675.

Note: It is recommended to keep only the required ports open for malware scanning.

Allow NFS/SMB read from the NetBackup storage server. Refer to *NetBackup Network Ports Reference Guide*.

Allow SSH from the NetBackup media server (used for connecting to scan host).

Allow Malware signature updates. The updates that are needed depend on the malware scanner that is used. For NetBackup Malware Scanner, the update happens over HTTPS (<https://oem.avira-update.com/update>).

Prerequisites for Windows scan host

In addition to the prerequisites listed in [Prerequisites for a scan host](#), ensure that you meet the following requirements for Windows platform:

- For a non-administrator user on Windows: A non-administrator user of a Windows scan host must be added to the administrators group.

- For supporting non-English characters on the Windows scan host, enable multibyte characters support.
For more information on enabling multibyte characters support in Microsoft Windows Server 2019, refer to the article [Retrieve Data in UTF-8 on Windows](#).
- For supporting long paths on the Windows scan host, enable long path support. For more information on enabling maximum path length support, refer to [Maximum Path Length Limitation](#).
- If the scan host connectivity type is **Agentless host**, then `OpenSSH` must be configured on windows scan host. Create the firewall rule for `OpenSSH` so that scan host is accessible from the media server.
If the scan host connectivity type is **NetBackup client**, then `OpenSSH` is not required.

Note the following:

- For Windows 2016, get `OpenSSH` from the GIT hub repository and for Windows 2019, enable the `OpenSSH` server feature. For more details, refer to the [Microsoft documentation](#).
- Microsoft Visual C/C++ Redistributable is an additional dependency if the media server is updated to 10.1.1 or later.
The Visual C/C++ run-time library DLL is required to run the `nbmalwareutil` utility on a windows scan host. The run-time DLL can be obtained from the [Microsoft Visual C++ Redistributable latest supported downloads](#).

Prerequisites for Windows scan host for NFS share type

Note: Run the scan host credential validation again from the Web UI if changes are done to ID mapping.

For VMware and Cloud workload policy scanning, UID and GID mapping must be set to 0. This requires a separate scan host pool having separate scan host.

Perform the following

1 Enable local `passwd` file mapping using PowerShell:

```
C:\Users\Administrator> Set-NfsMappingStore -EnableUNMLookup  
$True -UNMServer localhost  
C:\Users\Administrator> nfsadmin mapping
```

The following are the settings on localhost

```
Mapping Server Lookup      : Enabled  
Mapping Server             : localhost  
AD Lookup                  : Disabled  
AD Domain                  :
```

2 Install NFS client by running the following command on PowerShell:

```
Install-WindowsFeature -Name NFS-Client
```

3 The entry must be as follows in the respective files (in file type format):

Note: Ensure that the **scanuser** and **scangroup** are created. The **scanuser** must be part of the **scangroup** and **Administrators** group.

In `C:\Windows\System32\drivers\etc\passwd` file:

```
scanuser:x:1001:1001:Description:C:\Users\scanuser
```

In `C:\Windows\System32\drivers\etc\group` file:

```
scangroup:x:1001:1001
```

4 Restart `nfsadmin` client as follows:

```
nfsadmin client stop  
  
nfsadmin client start
```

5 Verify the ID (UID/GID) mapping for user by running the following command using PowerShell:

```
Get-NfsMappedIdentity -AccountName scanuser -AccountType User  
  
UserIdentifier      : 1001  
GroupIdentifier     : 1001  
UserName           : scanuser  
PrimaryGroup       :  
SupplementaryGroups :
```

Prerequisites for Linux scan host

In addition to the prerequisites listed in [Prerequisites for a scan host](#), ensure that you meet the following requirements for Linux platform:

- For a Linux scan host the default login shell must be bash.
- For RHEL 9 (and above) scan host, ensure that the SCP Linux command is not disabled.
- Install the following:
For NFS share type: `nfs-utils`
For SMB share type: `cifs-utils`
- For NetBackup malware detection utility to run on scan host, install `libnsl.so.1` library on scan host. If the latest version of `libnsl` library file is present (for example, `/usr/lib64/libnsl.so.2`), then create a soft link file `/usr/lib64/libnsl.so.1` which points to `/usr/lib64/libnsl.so.2` file.
Example to create a soft link file:

```
# cd /usr/lib64 # ln -sf libnsl.so.2 libnsl.so.1
```

Note: For assistance on installing the `libnsl*` library file, contact operating system administrator.

- (Optional) A new variable entry (`$TMPDIR`) having a value equal to the desired location can be added for malware scan temp directory in the scan user's `bashrc` file.

For example, `$TMPDIR=/mytempdirectory/malware` to overwrite the default `/tmp/malware` temporary location. If user specifies `$TMPDIR=/home/scanuser` as the temporary directory, then `/home/scanuser/tmp/malware` directory would be used as the temporary directory for all the malware related files.

Note: Ensure that the scanuser has the required permissions to `$TMPDIR` folder for performing the malware scan successfully.

- **For a non-root user on Linux:**

- Allow the `ssh` connection with a non-root user.
For example: Add the `Allow Users root scanuser` entry in the `/etc/ssh/sshd_config` file.

Note: A scan user is a non-root user that is created in the system.

- Provide user permission to mount and umount. Add the user permission entry in `sudoers` file.
For example: In the `/etc/sudoers` file add one of the following:
 - **scanuser ALL=(ALL) NOPASSWD:ALL**
 - **scanuser ALL=(ALL) NOPASSWD:/bin/umount, /bin/mount**
- Configure the malware tool with a non-root user on the scan host.

Note: If scanning is done using the root user, then change the permission of the `/tmp/malware` folder to provide write permissions to the non-root user.

For example: `chmod a+rwX /tmp/malware`

Note: For VMware and Cloud workload policy scanning, UID and GID mapping must be set to 0.

(If scan host is created in Azure or AWS from marketplace images) Enable root access for scan host as follows:

- Change the root password using the following command:
`- sudo -i passwd`
- Change `/etc/ssh/sshd_config` file to provide the permit for root login as follows:

```
"PermitRootLogin yes"
"PasswordAuthentication yes"
```

- Restart the service with the following command:

```
- service sshd reload
```
- Change `/etc/cloud/cloud.cfg` file as follows to enable root user:

```
disable_root 0
```

Limitations and considerations for scan host using NFS share

Limitations specific to a Windows scan host using NFS share

Following is a limitation for Windows operating system and NetBackup Malware Scanner (Avira) version 2.3:

A Windows scan host with Windows Defender malware tool, file paths having non-English characters will not get scanned. These are skipped during a scan. Thus, the number of files scanned reported on Web UI could be less than the total files in that image.

If the malware scan encountered files could not be scanned for any reason, then the following message is displayed:

```
Malware scan encountered <number of files> files which could not be scanned.
```

A report of files that were skipped can be obtained by clicking on **Actions > Export unscannable files list**.

Considerations specific to a Windows scan host using NFS share

- The built-in administrator account can be used as the scan user and would be able to scan all types of images. This account would be disabled on production servers for security consideration.
 Hence a non-administrator local user (for example, name: scan-user) must be created and added to the **Administrators** group. To enhance the security, map the account identity to secure the interactions with NFS shares. Active Directory integration is not required when using the local **passwd** and **group** files located at the following location:

```
C:\windows\system32\drivers\etc\passwd  
C:\windows\system32\drivers\etc\group
```

- When scanning images of Standard and MS-Windows policy type, the local scan-user account must have UserIdentifier (UID) permissions set to non-zero value.

For example, UID 1001 is added to the **passwd** and **group** file:

passwd file: scan-user:x:1001:1001:Description:C:\Users\scan-user

group file: scangroup:x:1001:1001

- When scanning images of VMware and cloud workloads, the scan-user account must have UserIdentifier (UID) permissions set to 0 value. Modify the **passwd** and **group** files as follows:

passwd file: scan-user:x:0:0:Description:C:\Users\scan-user

group file: scangroup:x:0:0

- As the permissions differ for the scan-user account (depending on the type of image to be scanned), it is required to have 2 separate Windows scan hosts for provisioning, each with a unique local account and UID permissions.

Prior to initiating an on-demand scan, select specific scanhost pool which has the desired scan host. To avoid provisioning two separate Windows scan hosts, use a non-admin user account (nfsnobody), then set the UID mapping to 0 value.

Configuring scan host

NetBackup malware scanning feature requires configuration of an additional host (scan host). The scan host configuration can be performed through one of the following methods:

- Automated scripts: See [“Automated scan host configuration”](#) on page 678.
- Manually: See [“Manual scan host configuration”](#) on page 682.

Automated scan host configuration

Scan host can be configured automatically using one of the following options:

For Agentless host:

- **PowerShell:** PowerShell scripts can be used to configure Windows scan host. See [“Scan host configuration using PowerShell”](#) on page 679.
- **Shell:** Shell scripts can be used to configure Linux scan host by copying the required script to scan host. See [“Scan host configuration using Shell”](#) on page 680.

- **Ansible:** Ansible playbook can be used to configure one or more Linux and Windows scan hosts remotely.
See [“Scan host configuration using Ansible”](#) on page 681.

Note: The above automated configuration scripts currently only support installation of NetBackup Malware Scanner (Avira).

For NetBackup client as the scan host

- Configure NetBackup client as the scan host.
See [“Configuring NetBackup client as the scan host”](#) on page 688.
- If the status of the scanner host is activated, then the existing system with the NetBackup client can be used as scan host.
- Verify the status of the scanner host as follows:
 - On the left, click **Detection and reporting > Malware detection**.
 - On the **Malware detection** page, select **Malware detection settings > Manage malware scanner host pools** on the top-right corner to go to host pool list page.
 - Select the desired scan host. Then click **Actions > Manage hosts**.
The status of the scanner hosts is displayed.
 - To change the status of the scanner host, select the desired scanner host and click **Actions > Activate/Deactivate**.

Scan host configuration using PowerShell

This utility installs and configures the prerequisites required to run a malware scan on the scan host (Windows Server 2016 and above). Additionally, this utility can be used to install NetBackup Malware Scanner on the scan host.

For more information, refer to the `ReadMe.md` file located at [PowerShell ReadMe.md](#).

Prerequisites

- For installing prerequisite software using the package managers, software repositories must be configured.
- Windows Server version: 2016 and above
- Internet connectivity is required.

Steps to configure scan host using PowerShell

- 1 Clone the repository from GitHub and move it to your scan host as follows:

```
git clone https://github.com/VeritasOS/netbackup-scanhost-config.git
```
- 2 Provide the scan host details in the `inputs.json` file. Refer to the *Terminologies* section in [ReadMe.md](#) file for the complete list of options.
- 3 Open `powershell.exe` as Administrator.
- 4 Navigate to `netbackup-scanhost-config\powershell\` folder as follows:

```
cd netbackup-scanhost-config\powershell\
```
- 5 Run the following command:

```
.\configure-scanhost.ps1 --install
```
- 6 Use the information displayed at the end of script to register the scan host to NetBackup primary server.

Scan host configuration using Shell

This utility installs and configures the prerequisites required to run a malware scan on the scan host (RHEL (8.x, 9.x) / SUSE 12 and above). Additionally, this utility can be used to install NetBackup Malware Scanner on the scan host.

For more information, refer to the `ReadMe.md` file located at [Shell ReadMe.md](#).

Prerequisites

- RHEL version: 8.x, 9.x
- Internet connectivity is required and the subscription manager must be attached.
- Uses `jq` for parsing the `inputs.json` file.
- the default login shell must be `bash`.

Steps to configure scan host using Shell

- 1 Clone the repository from GitHub and move it to your scan host as follows:

```
git clone https://github.com/VeritasOS/netbackup-scanhost-config.git
```
- 2 Navigate to `netbackup-scanhost-config\shell` folder as follows:

```
cd netbackup-scanhost-config\shell
```
- 3 Provide the scan host details in the `inputs.json` file. Refer to the *Terminologies* section in [ReadMe.md](#) file for the complete list of options.

- `install_avira`: Installs NetBackup Malware Scanner if set to *true*, defaults to *false*.
 - `avira_package_path`: (Required only if `install_avira` is set to *true*). Local absolute path to the NetBackup Malware Scanner zip package (**NBAntimalwareClient**) which is available on the Veritas download center.
- 4 Run the following command:
- ```
sh configure-scanhost.sh [--verbose] [--install]
```
- 5 Use the information displayed at the end of script to register the scan host to NetBackup primary server.

## Scan host configuration using Ansible

Using Ansible, single/multiple scan hosts can be configured at once by providing the host details in `inventory/hosts.yml` file. NetBackup footprint is not required on the scan host. This utility installs and configures the prerequisites required to run a malware scan on the scan host (RHEL 8.x/9.x/ Windows Server 2016 and above). Additionally, this utility can be used to install NetBackup Malware Scanner on the scan host.

For more information, refer to the `ReadMe.md` file located at [Ansible ReadMe.md](#).

### Prerequisites

- The minimum required configuration for the scan host is 8 CPU and 32-GB RAM.
- For the supported operating systems of the scan host, refer to the [Software Compatibility List](#).
- NetBackup footprint is not required on the scan host. The existing systems with the NetBackup client or media server can be used as scan host, too.
- (Linux) The scan host must be reachable from the media server over SSH.

---

**Note:** SSH connection to scan host from the media server must be successful.

---

- Following are the platform specific requirements:  
(*For Windows*) openssh, nfs-client, vc runtime, non-administrator user and Avira configured using previously created non-administrator user.  
(*For Linux*) libnsl, cifs-utils, non-root user and Avira configured using previously created non-administrator user.

## Steps to configure scan host using Ansible

---

**Note:** Ensure that you perform all the steps in this procedure on Ansible control host.

---

- 1 Clone the repository from GitHub and move it to your Ansible control host as follows:

```
git clone
https://github.com/VeritasOS/netbackup-scanhost-config.git
```

- 2 Navigate to `netbackup-scanhost-config\ansible` folder as follows:

```
cd netbackup-scanhost-config\ansible
```

- 3 By default, the host key checking would happen before configuring the scan host. To add the fingerprint of the scan host for Linux hosts, manually perform SSH to the scan host as follows:

```
ssh-keyscan -H {{HOST}} >> ~/.ssh/known_hosts
```

- 4 Provide the scan host details in the `inventory/hosts.yml` file. Refer to the *Terminologies* section in [ReadMe.md](#) file for the complete list of options.

- `install_avira`: Installs NetBackup Malware Scanner if set to *true*, defaults to *false*.
- `avira_package_path`: (Required only if `install_avira` is set to *true*). Local absolute path to the NetBackup Malware Scanner zip package (**NBAntimalwareClient**) which is available on the Veritas download center.
- `ansible_user`: Scan host username who must be a user with Administrator or root/sudo privileges. When using the sudo privileges, provide the sudo password as follows:

```
ansible_sudo_pass=<password>
```

- `ansible_ssh_pass`: Scan host password.

- 5 Run the following to run the playbook:

```
ansible-playbook playbook.yml
```

- 6 Use the credentials displayed at the end of script to register the scan host to NetBackup primary server.

## Manual scan host configuration

The scan host must have NetBackup Malware Scanner (Avira) installed and must be reachable from the media server over SSH.

Configure the required share type such as NFS or SMB.

---

**Note:** For Linux scan host, NFS share type shows 4x better scan time than SMB share type.

---

**Notes:** Perform the following steps on the MSDP storage server:

- Configure NFS and SMB configurations. Also, NFS or SMB client must be on scan host.
- For an SMB share, ensure that the storage server is connected or joined to the Active Directory Domain and obtain an Active Directory domain details and a valid user credentials.
- Ensure that the user that is specified in the share type has required permission to mount.

For more information on the additional prerequisites (such as SMB/NFS client software) and scan host configuration steps, refer to *NetBackup Web UI Administrator Guide*.

## Scenario based scan host configuration

The configuration of an NFS share type depends on the platform and malware scanner tool. Refer to the following examples for configuring the scan host manually:

### For an agentless host:

- For Windows, NFS share type and Microsoft Defender Antivirus:  
See [“Configure malware scan host for Windows NFS share type and Microsoft Defender”](#) on page 684.
- For Linux, NFS share type:  
See [“Configure malware scan host for Linux NFS share type and Avira”](#) on page 686.

### For a NetBackup client that is the scan host:

- For NetBackup client as the scan host for Windows NFS share type and Microsoft Defender  
See [“Configuring NetBackup client as the scan host”](#) on page 688.

### For a Flex application that is the scan host

- The **Flex application** scan host is applicable only for NFS share type and Avira. For more information on configuring and creating NetBackup malware scanner instance for Flex application, see the *NetBackup Application Guide For Flex Appliance*.

## Configure malware scan host for Windows NFS share type and Microsoft Defender

NetBackup malware scanning feature requires configuration of an additional host (a scan-host).

Before configuring scan host ensure that the following prerequisites are met:

See “[Prerequisites for a scan host](#)” on page 671.

### Scan host configuration

#### 1 Install OpenSSH:

---

**Note:** For Windows 2019, OpenSSH server feature can be enabled.

---

- Download OpenSSH package from <https://github.com/PowerShell/Win32-OpenSSH/releases> and extract it to C:\Program Files folder.
- Add C:\Program Files to environment variable PATH.
- Open PowerShell and run it as an administrator.
- Navigate to C:\Program Files and run the following commands to install sshd and enable port 22:  

```
powershell.exe -ExecutionPolicy Bypass -File install-sshd.ps1
netsh advfirewall firewall add rule name=sshd dir=in
action=allow protocol=TCP localport=22
sc.exe config sshd start= auto
net start sshd
```

#### 2 Install NFS client by running the following command on PowerShell:

```
Install-WindowsFeature -Name NFS-Client
```

#### 3 Enable UID mapping:

- Run the following commands on PowerShell to enable NFS user mapping:

```
PS C:\Users\Administrator> Set-NfsMappingStore -EnableUNMLookup
$True -UNMServer localhost
PS C:\Users\Administrator> nfsadmin mapping
```

The following are the settings on localhost

```
Mapping Server Lookup : Enabled
Mapping Server : localhost
```

```
AD Lookup : Disabled
AD Domain
```

- Create the `passwd` and `group` files as follows:

---

**Note:** Ensure that the file extension is not created. The entry that is created must be in the file type format.

---

- C:\Windows\System32\drivers\etc\passwd file:

```
<scanuser>:x:<uid>:<uid>:Description:C:\Users\<scanuser>
```

For example,

```
C:\Windows\System32\drivers\etc\passwd -
scanuser:x:1000:1000:Description:C:\Users\scanuser
```

- C:\Windows\System32\drivers\etc\group file:

```
<scanuser>:x:<uid>:<uid>
```

For example,

```
C:\Windows\System32\drivers\etc\group - scanuser:x:1000:1000
```

---

**Note:** For scanning VMWare, Hyper-V and Cloud images on Windows scan host, enable `nfsadmin` mapping to UID/GID 0. Scan user must be an administrator.

```
passwd file content -
```

```
Administrator:x:0:0:Description:C:\Users\Administrator
```

```
group file content - Administrator:x:0:0
```

---

#### 4 Restart NFS client:

After updating `passwd/group` files, restart NFS client service using the following commands:

```
nfsadmin client stop
```

```
nfsadmin client start
```

- 5 Verify the ID (UID/GID) mapping for user by running the following command using PowerShell:

```
Get-NfsMappedIdentity -AccountName scanuser -AccountType User
```

```
UserIdentifier : 1001
GroupIdentifier : 1001
UserName : scanuser
PrimaryGroup :
SupplementaryGroups :
```

- 6 Install VC runtime:

Download and install VC runtime package from  
[https://aka.ms/vs/17/release/vc\\_redist.x64.exe](https://aka.ms/vs/17/release/vc_redist.x64.exe).

- 7 Configure the Malware scanner tool (Microsoft Defender Antivirus).

See “[Configuring Microsoft Defender Antivirus](#)” on page 665.

## Configure malware scan host for Linux NFS share type and Avira

NetBackup malware scanning feature requires configuration of an additional host (a scan-host).

Before configuring scan host ensure that the prerequisites mentioned in the following section are met:

See “[Prerequisites for a scan host](#)” on page 671.

### Scan host configuration

---

**Note:** For ease of understanding the following documented procedure, refer to [Video](#).

---

- 1 Install NFS client: `$ yum install nfs-utils -y`
- 2 Install libnsl: `$ yum install libnsl -y`
- 3 Create non-root user account for performing a scan: `$ useradd scanuser`
- 4 Set password of scan user (username: scanuser): `$ passwd scanuser`

- 5 Provide mount and unmount access to scanuser: `$ vim /etc/sudoers`

Add the following line:

```
scanuser ALL=(ALL) NOPASSWD: /bin/umount, /bin/mount
```

Install malware tool using scanuser: `$ su scanuser`

- 6 Download the latest available version of NetBackup Malware Scanner tool (Avira) from [Cohesity Support Downloads](#):

```
$ unzip NBAntiMalwareClient_<version>.zip
$ cd NBAntiMalwareClient_<version>_LinuxR_x86/
$ sh setup.sh
```

Or

If malware scanner is already installed and needs to be upgraded:

```
$ unzip NBAntiMalwareClient_<version>.zip
$ cd NBAntiMalwareClient_<version>_LinuxR_x86/
$ sh setup.sh
>> NetBackup Malware Scanner is already installed. Do you want
to update it? (y/n): default: y
Note: To replace all binaries at target location, enter option
-ALL
```

where `<version>` is the latest available version of NetBackup Malware Scanner tool (Avira)

- 7 Copy RSA key: `$ hostname`

Copy the hostname to notepad for later use.

```
$ ssh-keyscan <hostname> 2>/dev/null | grep ssh-rsa | awk '{print
$3}' | base64 -d | sha256sum
```

---

**Note:** Copy the RSA key to notepad for later use.

---

## 8 Create a scan host pool.

For more information on creating the scan host pool, refer to the following section:

See [“Configuring a scan host pool”](#) on page 689.

## 9 Validate malware scanner configuration through Web UI as follows:

The **Validate configuration** feature within NetBackup Web UI is available in NetBackup version 10.4 and higher. If NetBackup version is below 10.4 then create small size backup image using a policy type Standard or MS Windows and trigger scan using that image. If the NetBackup or the malware scan job fails, then the job will have the details needed to troubleshoot.

# Configuring NetBackup client as the scan host

NetBackup malware scanning feature requires configuration of an additional host (a scan-host).

Before configuring scan host ensure that the following prerequisites are met:

See [“Prerequisites for a scan host”](#) on page 671.

## Configuring NetBackup client as the scan host

### 1 Install NFS client by running the following command on PowerShell:

```
Install-WindowsFeature -Name NFS-Client
```

### 2 Enable UID mapping by running the following commands on PowerShell to enable NFS user mapping:

```
PS C:\Users\Administrator> Set-NfsMappingStore -EnableUNMLookup
$True -UNMServer localhost
```

```
PS C:\Users\Administrator> nfsadmin mapping
```

The following are the settings on localhost

```
Mapping Server Lookup : Enabled
Mapping Server : localhost
AD Lookup : Disabled
AD Domain
```

### 3 Run the configuration script as follows:

- **For Linux:** `/usr/opensv/netbackup/bin/goodies/nbscanhostconfigcmd -validate`

- For Windows:

```
install_path\NetBackup\bin\goodies\nbscanhostconfigcmd.exe"
-validate
```

#### 4 Restart NFS client:

After updating `passwd/group` files, restart NFS client service using the following commands:

```
nfsadmin client stop

nfsadmin client start
```

#### 5 Verify the ID (UID/GID) mapping for user by running the following command using PowerShell:

```
Get-NfsMappedIdentity -AccountName scanuser -AccountType User
```

```
UserIdentifier : 1001
GroupIdentifier : 1001
UserName : scanuser
PrimaryGroup :
SupplementaryGroups :
```

#### 6 Configure the Malware scanner tool (Microsoft Defender Antivirus).

See [“Configuring Microsoft Defender Antivirus”](#) on page 665.

For more information on setting up PBX communication, refer to the 'Configuring NetBackup Messaging Broker service to use PBX port' section in the *NetBackup Administrator's Guide, Volume I*.

## Configuring a scan host pool

Refer to the following topics to configure a scan host pool.

See [“Add an existing scan host”](#) on page 691.

See [“Validating the scan host pool configuration”](#) on page 692.

See [“Add a new host in a scan host pool”](#) on page 690.

## Prerequisites for scan host pool

Scan host pool is a group of scan hosts. Scan host pool configurations must be performed from NetBackup Web UI before the scan host configuration is completed.

- All the scan host added in the scan host pool must have same malware tool as that of the scan host pool.

- All the scan host added in the pool must have same share type as that of scan host pool.
- *(Applicable only for Agentless scan host)* To add scan host in a scan pool, credentials of scan host and RSA key are required. To get the RSA key of the scan host, refer to the following section:  
See [“Managing credentials for malware scanning”](#) on page 694.
- *(Applicable only for NetBackup client as the scan host)* Credentials must be added only for SMB share type. To add the credentials, refer to the following section:  
See [“Managing credentials for malware scanning”](#) on page 694.
- Before performing the scan, ensure that the scan hosts are active and available in scan host pool.

## Configure a new scan host pool

### To configure a new scan host pool

- 1 On left, select **Detection and reporting > Malware detection**.
- 2 At the top right, select **Malware detection settings > Manage malware scanner host pools** to go to the host pool list page.
- 3 Select **Add** to add a new host pool.
- 4 Enter the details such as **Host pool name**, **Malware scanner**, **Host type**, and **Type of share**.
- 5 Select **Save and add hosts**.

## Add a new host in a scan host pool

Use this procedure to add a new scan host in the scan host pool that is configured. See the following topic for prerequisites.

See [“Prerequisites for scan host pool”](#) on page 689.

### To add a new host in a scan host pool

- 1 On the left, click **Detection and reporting > Malware detection**.
- 2 Click **Malware detection** page, click **Malware detection settings > Manage malware scanner host pools** on the top-right corner.
- 3 On the **Malware scanner host pools** page, select the desired scan host pool and click **Manage hosts** from the action menu.
- 4 On the **Manage scanner hosts** page, click **Add new**.

- 5 (Applicable only for Agentless scan host) On the **Add scanner host to scanner host pool <Host pool name>** page, enter **Host name**.

(Applicable only for NetBackup client as the scan host) On the pop up window, select one or more clients which you want to add.

- 6 (Applicable only for Agentless scan host)
- Click on **Select existing credential** or **Add a new credential**.  
See [“Managing credentials for malware scanning”](#) on page 694.
  - Select the media server to validate credentials.
  - Click on **Validate credentials**. On successful validation, click **Save** to save the credentials.
  - Select from the following options:
    - To save the credentials and validate the configuration later, click **Save**.  
See [“Validating the scan host pool configuration”](#) on page 692.
    - To save the credentials and immediately validate the configuration, click **Save and validate configuration**.

---

**Note:** By default three parallel scans are supported per scan host and this limit is configurable. Having more scan hosts in the scan pool increases the number of parallel scans.

See [“Configure resource limits for malware detection”](#) on page 696.

---

## Managing a scan host

Refer to the following topics to manage a scan host:

- See [“Add an existing scan host”](#) on page 691.
- See [“Validating the scan host pool configuration”](#) on page 692.
- See [“Remove the scan host”](#) on page 693.
- See [“Activate or deactivate the scan host”](#) on page 693.
- See [“Managing credentials for malware scanning”](#) on page 694.

### Add an existing scan host

Use this procedure to add a same scan host in another scan host pool of same share type.

**To configure an existing scan host**

- 1 On left, click **Detection and reporting > Malware detection**.
- 2 On the **Malware detection** page, click **Malware detection settings > Manage malware scanner host pools** on the top right corner.
- 3 On the **Malware scanner host pools** page, select the desired scan host pool and click **Manage hosts** from the action menu.
- 4 On the **Manage scanner hosts** page, click **Add existing** to select pre-existing host.

---

**Note:** List includes all scan hosts from all scan host of agentless or agent based pools.

---

- 5 On the **Add existing malware scanner host** window, select the desired one or more scan hosts.
- 6 Click **Add**.

---

**Note:** *(Applicable only for NetBackup client as the scan host)* After adding the scan host to the scan host pool, user has to manually activate the scan host if it is deactivated.

---

## Validating the scan host pool configuration

*(Applicable only for Agentless scan host)* Use this procedure to validate the configuration for a new or an existing scan host in the scan host pool that is configured.

**To validate the scan host pool configuration**

- 1 On the left, click **Detection and reporting > Malware detection**.
- 2 Click **Malware detection** page, click **Malware detection settings** on the top-right corner.
- 3 After adding a new scan host or an existing scan host, on the **Manage scanner hosts** page, select the desired scan host and click **Validate configuration** from the action menu.

To add a new scan host or an existing scan host, see the following topics.

See [“Add a new host in a scan host pool”](#) on page 690.

See [“Add an existing scan host”](#) on page 691.

- 4 On the **Validate configuration** page, enter the details to search and select an image to validate the configuration.

---

**Note:** Validating the configuration is only supported for backup image of **Standard** policy type.

---

- 5 Select the backups to scan and click on **Validate configuration**.

---

**Note:** It is recommended to use backup image with small number of files. For large backups, IA creation may delay and test scan might fail.

---

- 6 After successful validation, click **Finish**.

The **Malware scanner host pools** page is displayed with the list of added scanner hosts.

## Remove the scan host

### To remove the scan host

- 1 On left, select **Detection and reporting > Malware detection**.
- 2 At the top right, select **Malware detection settings > Manage malware scanner host pools**.
- 3 On the **Malware scanner host pools** page, select the desired scan host pool and select **Actions > Manage hosts**.
- 4 Select the desired host and select **Delete** to remove scan host from scan host pool.

## Activate or deactivate the scan host

### To activate or deactivate the scan host

- 1 On left, select **Detection and reporting > Malware detection**.
- 2 At the top right, select **Malware detection settings > Manage malware scanner host pools**.
- 3 Select the desired scan host pool and select **Actions > Manage hosts**.
- 4 Select the desired host. Depending on the status of the scan host, from the **Actions** menu select **Activate** or **Deactivate**.

## Managing credentials for malware scanning

### To add new credentials

- 1 On the left, click **Detection and reporting > Malware detection**.
- 2 On the **Malware detection** page, select **Malware detection settings > Manage malware scanner host pools** on the top-right corner to go to host pool list page.
- 3 Select the desired scan host. Then click **Actions > Manage hosts**.
- 4 If the scan host connectivity type is **Agentless host**:
  - Select the desired host. Then click **Actions > Manage credentials**.
  - Select **Add a new credential** and click **Next**.
  - Add the details such as the **Credential name**, **Tag**, and **Description**.
  - On the **Host credentials** tab, add the **Host username**, **Host password**, **SSH port**, **RSA key**, and **Share type**.
    - To validate the SSH connection between the MSDP media server and the host, run the following command:

```
ssh username@remote_host_name
```
    - To verify the RSA key for a remote scan host, run the following command:

```
ssh-keyscan scan_host_name 2>/dev/null | grep ssh-rsa
```
    - To obtain the RSA key for the scan host, use the following command. Use the command from any Linux host with SSH connectivity to the scan host (this host can be the scan host itself):

```
ssh-keyscan scan_host_name 2>/dev/null | grep ssh-rsa | awk '{print $3}' | base64 -d | sha256sum
```

For example, the output is  
**33f697637ab3f0911c1d462d4bde8be3eec61a33403e8f6a88daecb415a31eef**  
- where the RSA key is  
**33f697637ab3f0911c1d462d4bde8be3eec61a33403e8f6a88daecb415a31eef**

---

**Note:** Ensure that you remove the – character from the RSA key when you copy.

The following host key algorithms are used to connect to scan host in the given order:

rsa-sha2-512, rsa-sha2-256, ssh-rsa

---

**5** If the scan host connectivity type is **NetBackup client**:

- Select the desired host. Then click **Actions > Manage credentials**.
- Select **Add a new credential** and click **Next**.

**To add existing credentials**

- 1** On the left, click **Detection and reporting > Malware detection**.
- 2** On the **Malware detection** page, select **Malware detection settings > Manage malware scanner host pools** on the top-right corner to go to host pool list page.
- 3** Select the desired scan host pool. Then click **Actions > Manage hosts**.
- 4** Select the desired host and click **Actions > Manage credentials**.
- 5** Select **Select existing credential**.
- 6** Select the desired credential and click **Select**.

**To edit existing credentials**

- 1** On the left, click **Detection and reporting > Malware detection**.
- 2** On the **Malware detection** page, select **Malware detection settings > Manage malware scanner host pools** on the top-right corner to go to host pool list page.
- 3** Select the desired scan host pool. Then click **Actions > Manage hosts**.
- 4** Select the desired host and click **Actions > Manage credentials**.
- 5** *(If the scan host connectivity type is Agentless host)* To edit the **Associate credentials** details of an existing credential, click **Actions > Edit** and edit the following required fields:
  - Tag
  - Description
  - Host credentials
  - Host password

- SSH port
- RSA key
- Share type

*(If the scan host connectivity type is NetBackup client and SMB share type):*  
 Associate one set of credentials with this host by either selecting an existing credential or adding a new credential. For more information, see the following:

[To add new credentials](#)

[To add existing credentials](#)

#### **To validate the scan host credentials**

(Applicable only if the scan host connectivity type is **Agentless host**)

- 1** On left, click **Detection and reporting > Malware detection**.
- 2** On the **Malware detection** page, select **Malware detection settings > Manage malware scanner host pools** on the top-right corner to go to host pool list page.
- 3** On the **Malware scanner host pools** page, click **Add** to add a new host pool.  
 The **Add scanner host pool** page appears.
- 4** After you provide the credentials for the scan host on the **Add scanner host pool** page, search for and select the media server.

---

**Note:** Only SSH credentials are validated by connecting to scan host from the selected media server. The media server must be a Linux media server with NetBackup version 10.3 or later.

---

- 5** Click **Validate credential**.
- 6** After the credentials are successfully validated, click **Save**.

## **Configure resource limits for malware detection**

#### **To configure resource limits for malware detection**

- 1** On the left, click **Detection and reporting > Malware detection**.
- 2** On the top right, click **Malware detection settings > Resource limits**.
- 3** Click **Edit** to edit the resource limit of the resource type.

- 4 Set the global limit which would be considered when resource limit is not set for a resource type.

Or, click **Add** to override the malware global settings.

- 5 Enter the new host name and set the limits.

---

**Note:** Resource type scan host: Number of scans per scan host. Default: 3, Minimum: 1, Maximum: 10

Resource type storage server: Number of scans per storage server. Default: 20, Minimum: 1, Maximum: 50

---

- 6 Click **Save**.

---

**Caution:** Setting the Instant Access limit to large value would lead to Storage server resources (memory, CPU, disk) being used for malware scanning purpose. It is advised to set the value based on the existing load on the storage server due to the backup or duplication operations.

---

---

**Note:** For NetBackup version 10.2 and later, the global parallel scans limit that is configured with the option **MALWARE\_DETECTION\_JOBS\_PER\_SCAN\_HOST** is not applicable. Configure the global parallel scans limit using the Web UI.

---

# Performing malware scan

This chapter includes the following topics:

- [Performing malware scan before recovery](#)
- [Perform a malware scan](#)

## Performing malware scan before recovery

The following table provides the scenarios when the **Scan for malware before recovery** option is enabled/disabled:

---

**Note:** For Hyper-V backup images, user cannot perform malware scan before recovery.

---

| Scenarios                                                                                                              | Enabled |
|------------------------------------------------------------------------------------------------------------------------|---------|
| If user does not have RBAC permissions to trigger malware scan.                                                        | No      |
| If primary copy is snapshot (NAS-Data-Protection) in any of the selected backup images.                                | No      |
| <b>Note:</b> In selected date range, user must select backup image as the primary copy to trigger recovery time scan.  |         |
| Images in selected date range must only be in the backup format (combination of backup and snapshot is not supported). |         |
| If scan host pool is not configured.                                                                                   | No      |

### To perform malware scan before recovery of files/folders

- 1 On the left, click **Recovery**.
- 2 Under **Regular recovery**, click **Start recovery**.

### 3 Select the following properties:

|                    |                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Source client      | The client that performed the backup.                                                                                         |
| Destination client | The client to which you want to restore the backup.                                                                           |
| Policy type        | The type of policy that is associated with the backup you want to restore.                                                    |
| Restore type       | The type of restore that you want to perform. The restore types that are available depend on the policy type that you choose. |

### 4 Click **Next**.

The following warning message is displayed when images which are not scanned are selected for recovery:

One or more images selected for recovery are not scanned.

### 5 In the Recovery details page:

- Edit the **Date range** in the **Use date picker** option.

Or

Click **Use backup history** to view and select specific images.

---

**Note:** The table displays all the backup image details for selected time frame. You can filter and sort the images based on the malware scan results, schedule type, or policy name.

---

- Click **Apply** to apply the date changes or add the selected images for recovery.

### 6 To perform the malware scan of files/folders selected for recovery, select the **Scan for malware before recovery** option.

User will be able to list **Most recent** files/folders when **Scan for malware before recovery** option is selected.

---

**Note:** The **Allow the selection of images that are malware-affected** option will be disabled if user selects **Scan for malware before recovery** option.

---

### 7 On the left, expand the **Source client** directory. Select any directories that you want to restore. Or in the right pane, select any files or directories. Click **Next**.

### 8 Select the **Restore target** and the **Recovery options**.

- 9 Select one of the following options under **Malware scan and recover option** for files infected with malware:
- If any files are infected with malware, recover only uninfected files (clean)
  - If any files are infected with malware, recover the latest clean copy of the files within the selected date range
  - If any files are infected with malware, recover all files, including infected files
  - If any files are infected with malware, do not perform the recovery job
- Select a malware scanner host pool and click **Next**.
- 10 In the Review page, view the summary of all the selections that you made, and click:
- **Start recovery**
- Or
- (Applicable when **Scan for malware before recovery** is selected) **Start scan and recovery**

You can see the progress of the restore job in the Activity monitor.

---

**Note:** For NAS-Data-Protection policy type multiple recovery jobs can be triggered for multi-volume restore. A comma separated list of Job IDs one per volume is displayed. The recovery job column would display only one Job ID NetBackup.

---

## Perform a malware scan

### To perform a malware scan

- 1 On the left, select **Detection and reporting > Malware detection**.
- 2 On the **Malware detection** page, select **Scan for malware**.
- 3 In the **Search by** option, select one of the following:
  - **Backup images**
  - **Assets by policy type**
  - **Assets by workload type**

For more information on the options for scanning, refer to the following on-demand scan:

- See [“Scanning backup images”](#) on page 702.
- See [“Assets by policy type”](#) on page 704.

- See “[Assets by workload type](#)” on page 706.
- 4 The following steps are applicable for scanning with the options **Assets by policy type** and **Assets by workload type**.
- From the **Client/Asset** table, select a client or an asset to scan.
  - Click **Next**.

---

**Note:** (Applicable only for **Assets by policy type** option) If the selected client in the previous step supports multiple policy types, then you have the option to select a single policy type for scanning.

---

- For the **Start date/time** and **End date/time** verify the date and the time range or update it.
- In the **Scanner host pool**, select the appropriate host pool name.
- (Applicable only for the **NAS-Data-Protection** policy type) In the **Volume** field, select the volume that is backed up for NAS devices.  
Volume-level filtering only fetches the top-level directories of the NAS-Data-Protection volume backup. Volume-level filtering is applicable only if the top-level directory is a volume. In this case you can select individual backup images with the **Backup images** option.
- From the **Current infection status**, select one of the following:
  - **Not scanned**
  - **Not infected**
  - **Infection detected by malware scan**
  - **Infection detected by file hash search**
  - **All**
- Click **Scan for malware**.  
Note that NetBackup is unable to scan more than 100 images. In that case, adjust the date range and try again.
- After the scan is initiated, the **Scan status** is displayed. Following are the status fields:
  - **Not scanned**
  - **Not infected**
  - **Infected**
  - **Failed**

---

**Note:** When we hover on failed status, the tool tip displays the reason for failed scan.

The backup images which failed in validation, are ignored. Malware scanning is supported for the backup images that are stored on storage with instant access capability for the supported policy type only.

---

- **Pending**
- **In progress**

## Scanning backup images

This section describes the procedure for scanning client backup images of a particular policy for malware.

### To scan policy of client backup images for malware

- 1 On the left, select **Detection and reporting > Malware detection**.
- 2 On the **Malware detection** page, select **Scan for malware**.
- 3 In the **Search by** option, select **Backup images**.

Select one of the following scan types:

- **Malware scan** - Select this option to scan images using default malware scan.
- **YARA scan** - Select this option to scan images using YARA rules.  
Click the **Select threat feeds** option.  
On the **Select threat feeds for scanning** dialog box, select the required YARA rules or a zip file of YARA rules that you have uploaded earlier.  
See [“About YARA scanning”](#) on page 740.

All the following steps are applicable for the scan type: Malware scan.

- 4 In the **Scanner host pool** option, search and select the appropriate host pool name from the list of scanner host pools listed in **Select malware scanner host pool**.

---

**Note:** Scan host from the selected scan host pool must be able to access the instant access mount created on the storage server which is configured with NFS/SMB share type.

---

- 5 In the search criteria, review and edit the following:
  - **Policy name**

Only supported policy types are listed.

- **Client name**  
Displays the clients that have backup images for a supported policy type.
- **Policy type**  
Displays all the supported policies which are enabled for malware scanning.

---

**Note:** The Nutanix-AHV policy displays Nutanix-AHV images if the backups are taken from a Nutanix-AHV policy and Protection plan backups.

---

---

**Warning:** The **Hypervisor** policy type displays Nutanix AHV and RHV images. NetBackup supports malware scanning only for Nutanix AHV images.

---

- **Type of backup**  
Any incremental backup images that do not have the NetBackup Accelerator feature enabled are not supported for the VMware workload.
- **Copies**  
If the selected copy does not support instant access, then the backup image is skipped for the malware scan.
- **Disk pool**  
MSDP (PureDisk), OST (for example, Data Domain) and AdvancedDisk storage type disk pools are listed.
- **Disk type**  
MSDP (PureDisk), OST (for example, Data Domain) and AdvancedDisk disk types are listed.
- **Infection status**  
The malware infected status of the backup images can be searched based on the following types: infection detected by malware scan, file hash search, not infected, not scanned or all.
- For the **Select the timeframe of backups**, verify the date and the time range or update it.
- On selecting the **Abort malware scan on detecting an infection** option, clean recovery would not be supported for infected images.

**6** Click **Search**.

**7** Select the search criteria and ensure that the selected scan host is active and available.

- 8 From the **Select the backups to scan** table select one or more images for scan.
- 9 Click **Scan for malware**.
- 10 After the scan is initiated, the **Scan status** is displayed.

The following are the status fields:

- **Not scanned**
- **Not infected**
- **Infected**
- **Failed**

Hover over the status to view the reason for the failed scan.

---

**Note:** Any backup images that fail the validation are ignored. Malware scanning is supported for the backup images that are stored on storage with instant access capability and for the supported policy types only. For backup images of VMware, Nutanix-AHV and Hyper-V stored on OST targets, malware scanning is supported only if media server with Instant Access capability is also present.

---

- **In progress**
- **Pending**

---

**Note:** You can cancel the malware scan for one or more in progress and pending jobs.

---

- **Infected - Malware scan aborted**

## Assets by policy type

This procedure is not applicable for YARA scanning.

This topic describes the procedure for scanning NAS-Data-Protection backup images for malware. NetBackup supports the policy types for malware scanning: Standard, MS-Windows, NAS-Data-Protection, Nutanix-AHV, Hypervisor (Nutanix AHV), Hyper-V, Universal-Share, Cloud object store, VMware or Cloud.

**To scan the supported assets by policy type, perform the following:**

- 1 On the left, click **Detection and reporting > Malware detection**.
- 2 On the **Malware detection** page, click **Scan for malware**.

- 3 In the **Search by** option, select **Assets by policy type**.
- 4 From the **Client/Asset** table, select a Client/Asset to scan.
- 5 Click **Next**.  
  
If the selected client in the previous step supports multiple policy types, you can select a single policy type for scanning.
- 6 For the **Start date/time** and **End date/time** verify the date and the time range or update it.  
  
The scan is initiated for a maximum of 100 images.
- 7 In the **Scanner host pool**, select the appropriate host pool name.
- 8 In the **Volume** field, **Select volume** backed up for NAS devices.

---

**Note:** Volume level filtering only fetches the top-level directories of the NAS-Data-Protection volume backup. Volume level filtering is applicable only if the top-level directory is a volume. In this case you have the option to select the individual backup images by using the **Backup images** option in the **Search by** option.

---

- 9 From the **Current infection status** list select one of the following:
  - **Not scanned**
  - **Not infected**
  - **Infection detected by malware scan**
  - **Infection detected by file hash search**
  - **All**

---

**Note:** For NAS-Data-Protection, any backup images that were created on the media server of earlier versions of NetBackup 10.4, select the **All** option for **Current status of malware scan**.

---

- 10 Click **Scan for malware**.

---

**Warning:** Scan is limited to only 100 images. Adjust the date range and try again.

---

- 11 After the scan is initiated, the **Scan status** is displayed. The following are the status fields:

- **Not scanned**
- **Not infected**
- **Infected**
- **Failed**

---

**Note:** Hover over the status to view the reason for the failed scan.

Any backup images that fail validation are ignored. Malware scanning is supported for the backup images that are stored on storage with instant access capability and for the supported policy types only.

---

- **Pending**
- **In progress**
- **Aborted on detection of malware**

More information is available on the malware scan status.

See [“View the malware scan status”](#) on page 708.

## Assets by workload type

This section describes the procedure for scanning VMware, Universal shares, Kubernetes, Nutanix, and Cloud VM assets for malware.

---

**Note:** For YARA scanning, only Kubernetes is supported.

---

**To scan the supported assets for malware, perform the following:**

- 1** On the left, select the supported workload under **Workloads**.
- 2** Select the resource which has backups completed.
- 3** Select **Actions > Scan for malware**.
- 4** On the **Malware scan** page, perform the following:
  - Select the date range for the scan by selecting **Start date/time** and **End date/time**.
  - Select **Scanner host pool**.
  - From the **Current infection status** list select one of the following:
    - **Not scanned**
    - **Not infected**

- Infection detected by malware scan
- Infection detected by file hash search
- All

**5** Click **Scan for malware**.

---

**Note:** The malware scanner host can initiate a scan of three images at the same time.

---

**6** After the scan starts, you can see the **Scan status** on **Malware detection**, the following fields are visible:

- Not scanned
- Not infected
- Infected
- Failed

---

**Note:** Any backup images that fail validation are ignored.

---

- In progress
- Pending

# Managing scan tasks for malware and YARA scanning

This chapter includes the following topics:

- [View the malware scan status](#)
- [Actions for malware scanned images](#)
- [Recover from malware-affected images \(clients protected by protection plan\)](#)
- [Recover from malware-affected images \(clients protected by policies\)](#)
- [Clean file recovery for virtual workload \(VMware\)](#)

## View the malware scan status

**To view the malware scan status**

- ◆ On the left, click **Detection and reporting > Malware detection**.

The following columns are displayed:

- Client - Name of the NetBackup client where the malware is detected.
- Backup time - Time when the backup was performed.
- Scan status - The scan status of the backup image. The different statuses are infected, not infected, failed, in progress, pending, canceled, infected-malware scan aborted, and cancellation in progress.
- Files infected - Indicates the number of files that were found infected during the scan.

- Scan progress - Indicates the percentage of scan completed.
- Total files - Indicates the count of files and folders as recorded in the catalog for the backup image (list of backup images in case of DNAS). For recovery time scan, the **Total files** column would only indicate the count of files selected for recovery.
- % infected - Provides the percentage of infected files as compared to **Total files**.

---

**Note:** Skipped files during recovery are considered as **Not-infected**.

---

- Elapsed time - Represents the time since scan request was accepted (Date of scan) till the time of completion of scan (End date of Scan). The elapsed time would consist of idle time, time spent in pending state. For resume of failed jobs it would include time spent from failure till the time when the resume operation was triggered.
- Scanned files - Indicates the number of files that are scanned.
- Schedule type - The backup type of the associated backup job
- Date of scan - Date when the scan was performed.
- Policy type - Type of the policy that was selected for scanning.
- Policy name - Name of the policy that was used for scanning.
- Malware scanner - Name of the malware scanner that was used for scanning.
- Scanner host pool - Indicates the host pool used for malware scanning.
- Malware scanner version - Version of the malware scanner that was used for scanning.
- (*Only for Hyper-V policy*) Display name - Name of the virtual machine on which Hyper-V policy is configured.

---

**Note:** To view additional columns that are not displayed, use the **Show or hide columns** pull down menu.

---



---

**Note:** For NetBackup Malware Scanner (Avira 2.3 and above) and Symantec Protection Engine, Scan progress and Scanned files are updated while scanning is in progress for NetBackup 10.3 and above.

---

# Actions for malware scanned images

Once you scan the backup images for malware detection, a tabular data is available on the **Malware detection** home page.

See [“View the malware scan status”](#) on page 708.

For each backup image, the following quick configurations are available.

## To expire all the copies

- 1 On the left, click **Detection and reporting > Malware detection**.
- 2 For the desired scan result, click **Actions > Expire all copies**.
- 3 Confirm to expire all the copies of the selected backup image.

---

**Note:** This option is available only for infected scan results.

---

## To view any infected files

- 1 On the left, click **Detection and reporting > Malware detection**.
- 2 For the desired scan result, click **Actions > View infected files**.

---

**Note:** This option is available only for infected scan results and scan type 'Recovery'.

---

- 3 In the **Infected files** table, search or the desired file, if needed.
- 4 If you want to export the list, click **Export list**.

---

**Note:** A list of infected files from the selected malware scanning result is exported in `.csv` format. The file name is of the following format:

`backupid_infected_files_timestamp.csv`

---

### To export the infected files list

- 1 On the left, click **Detection and reporting > Malware detection**.
- 2 For the desired malware affected, click **Actions > Export infected files list**.

---

**Note:** A `.csv` file contains backup time, names, hashes of the infected files and virus information.

For Microsoft Windows Defender, if real time protection is enabled, then hashes of the infected files are not created as files are not accessible.

---

### To export the unscannable files list

- 1 On the left, click **Detection and reporting > Malware detection**.
- 2 For the desired malware affected, click **Actions > Export unscannable files list**.

---

**Note:** A `.csv` file contains the list of files that the malware scanner skips due to issues such as file input or output errors, encrypted (password protected) files, etc.

---

### To cancel a malware scan

- 1 On the left, click **Detection and reporting > Malware detection**.
- 2 For the wanted scan result, click **Actions > Cancel malware scan**.

**Note:** You can only cancel the malware scan from the "in progress" and the "pending" states.

- 3 Click **Cancel scan** to confirm.

The status changes to **Cancellation in progress**.

---

**Note:** The **Cancel malware scan** is not supported for scan results with scan type 'Recovery'.

---

### To rescan an image

- 1 On the left, click **Detection and reporting > Malware detection**.
- 2 For the wanted scan result, click **Actions > Rescan image**.
- 3 Click **Rescan** to confirm.

- 4 For a bulk rescan, when you select one or more images with a different or an empty scanner host pool, you must select a new scanner host pool.
  - Click **Rescan image**.
  - Select a new scan host pool.  
The new scan host pool is applicable for all the selected images for this rescan.
  - Click **Rescan** to confirm.  
Rescan (and resume) is not supported for scan results with scan type recovery.
- 5 For a rescan of failed or canceled jobs, scanning is triggered from the point of failure (resumed) instead of from a complete scan, under the following conditions:
  - If the value of **Date of scan** is more than 48 hours, then the job is not resumed and the full scan is initiated. This action ensures that the malware signatures that are used for the scan do not differ significantly.
  - Supported for Standard or MS-Windows policy backup images that have a large number of files (> 500 KB). For a DNAS policy, it is supported for more than one stream.
  - Instant Access must have succeeded for the failed job.
  - Resume identifies the first instant access capable copy to scan, which can be different from the copy that was selected for the initial scan request.

After the job is resumed the existing scan result is moved from the state "failed" to "pending" and subsequently to an "in-progress" state. The progress update can continue from the point of failure. For a complete rescan the new scan result is displayed. If the user needs to perform a complete scan, then it can be started using the on-demand scan options.

#### **To delete the scan results**

- 1 On the left, click **Detection and reporting > Malware detection**.
- 2 Any scan results that are in a "failed" or "canceled" state can be deleted manually. Click **Actions > Delete scan results**.
- 3 Click **Yes** to confirm the deletion of the selected scan results.  
You can select a maximum of 20 scan results to delete.

#### To view the details of a scan result

- 1 On the left, click **Detection and reporting > Malware detection**.
- 2 Click **Actions > View details** to view details for the backup images with individual batch level.

---

**Note:** The **View details** option is available only for the scan results that are in "failed" or "in progress" state.

---

- 3 On the **View details** page, you can copy information to the Clipboard. Click **Actions > Copy failure details** or **Actions > Copy the scan results**.
- 4 Click **Close**.

## Recover from malware-affected images (clients protected by protection plan)

To restore from malware-affected recovery points, you must have the Administrator role or equivalent RBAC permissions. To recover a specific recovery point that is affected by malware, see the following topic:

See [“Recover from malware-affected images \(clients protected by policies\)”](#) on page 714.

---

**Note:** Recovery options are not supported for YARA scanning.

---

#### To recover from malware-affected images for clients protected by protection plan

- 1 On left pane select the supported **Workload**.
- 2 Locate the protected resource and click **Actions > Recover**.
- 3 On the **Recovery points** tab you can see **Malware scan** status of each recovery point, as follows:
  - **Not scanned**
  - **Not infected**
  - **Infected**
- 4 Select the recovery point.

- 5 Select **Allow the selection of recovery points that are malware-affected**. This option only displays if there are recovery points that contain malware-affected images.

---

**Note:** To restore from malware-affected recovery points, you must have the Administrator role or equivalent RBAC permissions.

---

- 6 Click **Recover** and select the type of recovery. Then follow the prompts.  
For more details on recovering a VM, see the *NetBackup for VMware Administrator's Guide*.

## Recover from malware-affected images (clients protected by policies)

To restore from malware-affected images, you must have the Administrator role or equivalent RBAC permissions. To recover a VMware asset that is affected by malware, see the following topic.

See [“Recover from malware-affected images \(clients protected by protection plan\)”](#) on page 713.

---

**Note:** Recovery options are not supported for YARA scanning.

---

### To recover from malware-affected images (clients protected by policies)

- 1 On the left, select **Recovery**.
- 2 On the **Regular recovery** card, select the link **Start recovery**.
- 3 Select the following properties:

|                    |                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Source client      | The client that performed the backup.                                                                                         |
| Destination client | The client to which you want to restore the backup.                                                                           |
| Policy type        | The type of policy that is associated with the backup you want to restore.                                                    |
| Restore type       | The type of restore that you want to perform. The restore types that are available depend on the policy type that you choose. |

- 4 Click **Next**.

- 5 Select the **Start date** and **End date**.

Or, click **Use backup history** to view and select specific images. Click **Select** to add the selected images for recovery.

---

**Note:** The table displays all the backup image details for the selected time frame. You can filter and sort the images based on the malware scan results, infection status, schedule type, policy type, or policy name.

---

- 6 To include any malware-infected images in the recovery, select **Allow the selection of images that are malware-affected**.

---

**Note:** The option **Allow the selection of images that are malware-affected** is disabled if you select the option **Scan for malware before recovery**.

See [“Performing malware scan before recovery”](#) on page 698.

---

- 7 On the left, expand the **Source client** directory. Select any directories that you want to restore. Or in the right pane, select any files or directories. Click **Next**.
- 8 Select the recovery target.
- 9 To restore any files that are malware-infected, click **Allow recovery of files infected by malware**. Otherwise, NetBackup only restores the files that are scanned and free from malware.

---

**Note:** By default, the **Allow recovery of files infected by malware** option is selected and cannot be changed when:

Malware scan is aborted on detection of malware for the selected image.

During malware scan when the **Abort malware scan on detecting an infection** option is selected.

---

- 10 Select any other recovery options that you want. Then click **Next**.
- 11 Review the recovery settings and then click **Start recovery**.

## Clean file recovery for virtual workload (VMware)

To restore from malware-affected images, you must have the Administrator role or equivalent RBAC permissions.

You can perform the following types of recovery:

- Recover a VMware asset that is affected by malware (with agent and agentless)
- Recover a specific recovery point that is affected by malware (with agent)

---

**Note:** Recovery time scan is not supported for YARA scanning.

---

## Recover a VMware asset that is affected by malware (with agent and agentless)

This procedure describes how to perform a VMware single file restore from a recovery point. You can perform this action with the VMware agent or with agentless.

### To recover a VMware asset that is affected by malware

- 1 On the left select **Workload > VMware**.
- 2 Search and click on the virtual machine to be recovered.
- 3 On the **Recovery points** tab, select the date for the recovery point.
- 4 Select **Allow the selection of recovery points that are malware-affected**. This option only displays if there are recovery points that contain malware-affected images.

---

**Note:** To restore from malware-affected recovery points, you must have the Administrator role or equivalent RBAC permissions.

---

- 5 Click **Recover** and select the type of recovery as **Restore files and folders**. Then follow the prompts.

---

**Note:** NetBackup now provides support for VMware single file restore clean recovery by selecting the **Allow recovery of files infected by malware** option in the **Recovery options**. This option overrides the default behavior.

---

For more details on recovering a VM, see the *NetBackup for VMware Administrator's Guide*.

## Recover a specific recovery point that is affected by malware (with agent)

This procedure describes how to perform a single file restore from the Recovery utility. You can perform this action with the VMware agent.

### To perform a single file restore from the Recovery utility

- 1 On the left, select **Recovery**.
- 2 On the **Regular recovery** card, select the link **Start recovery**.
- 3 Select the following properties:

|                    |                                                                                                                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policy type        | The type of policy that is associated with the backup you want to restore.<br><br>Select the policy type as VMware.                                                                                    |
| Source client      | The client that performed the backup. On the <b>Virtual machines search</b> tab, select the virtual machine and select <b>Apply</b> .                                                                  |
| Destination client | The client to which you want to restore the backup.                                                                                                                                                    |
| Restore type       | The type of restore that you want to perform. The restore types that are available depend on the policy type that you choose.<br><br><b>Note:</b> Clean recovery is supported only for normal backups. |

- 4 Select **Next**.
- 5 Edit the **Date range**.

Or, select **Use backup history** to view and select specific images. Select **Apply** to add the selected images for recovery.

---

**Note:** The table displays all the backup image details for the selected time frame. You can filter and sort the images based on the malware scan results, infection status, schedule type, policy type, or policy name.

---

- 6 To include any malware-infected images in the recovery, select **Allow the selection of images that are malware-affected**.
- 7 On the left, expand the **Source client** directory. Select any directories that you want to restore. Or in the right pane, select any files or directories. Select **Next**.
- 8 Select the recovery target.
- 9 To restore any files that are malware-infected, click **Allow recovery of files infected by malware**. Otherwise, NetBackup only restores the files that are scanned and free from malware.
- 10 Select any other recovery options that you want. Then select **Next**.
- 11 Review the recovery settings and then click **Start recovery**.

# Malware scan configuration parameters

This chapter includes the following topics:

- [MALWARE\\_SCAN\\_OPERATION\\_TIMEOUT](#)
- [MALWARE\\_DETECTION\\_CLEANUP\\_PERIOD](#)
- [MALWARE\\_DETECTION\\_TIMEOUT\\_PERIOD](#) option for NetBackup servers
- [FAIL\\_SAFE\\_SCAN\\_RETRY\\_COUNT](#)
- [Malware hash configuration parameters](#)
- [MALWARE\\_DETECTION\\_MALWARE\\_JOBS\\_CLEANUP\\_PERIOD](#)
- [MALWARE\\_DETECTION\\_WORKLIST\\_CLEANUP\\_PERIOD](#)
- [CLIENT\\_KEEP\\_LOG\\_DAYS](#)
- [VIRUS\\_SIGNATURE\\_UPDATE\\_INTERVAL](#)

## MALWARE\_SCAN\_OPERATION\_TIMEOUT

The **MALWARE\_SCAN\_OPERATION\_TIMEOUT** parameter is used to configure the duration of the scan operation that is allowed to run before timeout happens.

Scan operation for backup image can take a long time based upon the factors like backup size, number of files in the backup. By default, scan operation times out after 2 days. User can set the timeout value from 1 hour to 30 days.

**Table 45-1** MALWARE\_SCAN\_OPERATION\_TIMEOUT option information

| Usage                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Where to use                         | On NetBackup media servers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| How to use                           | <p>Use <code>nbgetconfig</code> or <code>nbsetconfig</code> commands to view, add, or change the value of the timeout.</p> <p>For information about these commands, see the <a href="#">NetBackup Commands Reference Guide</a>.</p> <p>Set the configuration key on the MSDP media server where <code>ScanManager (nbcs)</code> is started. For multiple MSDP media servers, set the configuration key on each server.</p> <p>Use the following format:</p> <p><b>MALWARE_SCAN_OPERATION_TIMEOUT = 120</b></p> <p>By default scan operation timeout value is 2880 minutes (2 days). The minimum supported value is 60 minutes (1 hour) and the maximum supported value is 43200 minutes (30 days).</p> |
| Equivalent NetBackup web UI property | No equivalent exists in the host properties.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## MALWARE\_DETECTION\_CLEANUP\_PERIOD

Malware detection performs automated cleanup of scan jobs which are older than 30 days in batches and displays the following state:

- Clean
- Failed
- Cancel

Cleanup runs every 12 hours after NetBackup has started.

**Table 45-2** Malware detection clean up option information

| Usage        | Description                                                                                      |
|--------------|--------------------------------------------------------------------------------------------------|
| Where to use | User can modify the configuration parameters in <code>bp.conf</code> file on the primary server. |

**Table 45-2** Malware detection clean up option information (*continued*)

| Usage      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| How to use | <p>Set the following parameters in <code>bp.conf</code> file:</p> <ul style="list-style-type: none"> <li>To change the cleanup period in days:<br/><b>MALWARE_DETECTION_CLEANUP_PERIOD = 45</b></li> </ul> <p><b>Note:</b> Value should be in number of days only. Although any integer value greater than 0 is accepted. NetBackup recommends not to set it to more than 6 month that is, 180 (days). If an invalid value is set, then the default value of 30 days is used.</p> <ul style="list-style-type: none"> <li>To switch off the cleanup period:<br/><b>MALWARE_DETECTION_CLEANUP_PERIOD = 0</b></li> <li>To change the scan job batch size:<br/><b>MALWARE_DETECTION_CLEANUP_BATCH_SIZE = 600 (setting batch size 600)</b></li> </ul> <p><b>Note:</b> You can set any value between 1 to 5000 for batch size. If you set invalid value then default value of 500 is used.</p> |

## MALWARE\_DETECTION\_TIMEOUT\_PERIOD option for NetBackup servers

The **MALWARE\_DETECTION\_TIMEOUT\_PERIOD** parameter is used to configure the duration of the scan operation that is allowed to run before timeout happens. Scan operation for backup image can take a long time based upon the factors like backup size, number of files in the backup. By default, scan operation times out after 2 days. User can set the timeout value in hours.

**Table 45-3** MALWARE\_DETECTION\_TIMEOUT\_PERIOD option information

| Usage        | Description                                                                                                                                                                                                                                                                                                              |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Where to Use | On NetBackup primary servers.                                                                                                                                                                                                                                                                                            |
| How to use   | <p>Use <code>nbgetconfig</code> or <code>nbsetconfig</code> commands to view, add, or change the value of the timeout.</p> <p>For information about these commands, see the <a href="#">NetBackup Commands Reference Guide</a>.</p> <p>Use the following format:</p> <p><b>MALWARE_DETECTION_TIMEOUT_PERIOD = 72</b></p> |

Table 45-3 MALWARE\_DETECTION\_TIMEOUT\_PERIOD option information  
(continued)

| Usage                                | Description                                  |
|--------------------------------------|----------------------------------------------|
| Equivalent NetBackup web UI property | No equivalent exists in the host properties. |

## FAIL\_SAFE\_SCAN\_RETRY\_COUNT

The **FAIL\_SAFE\_SCAN\_RETRY\_COUNT** parameter is used by the primary server to attempt the scan job on different scan host from the same scan host pool. The scan job is attempted depending on the value specified in the **FAIL\_SAFE\_SCAN\_RETRY\_COUNT** parameter when the scan job fails due to an issue related to scan host environment.

Following are the permissible values for **FAIL\_SAFE\_SCAN\_RETRY\_COUNT** parameter:

| Value | Description               |
|-------|---------------------------|
| 0     | Disabled                  |
| 1     | Default retry count       |
| 3     | Maximum retry count value |

## Malware hash configuration parameters

### FILE\_HASH\_SEARCH\_INTERVAL\_SECONDS

The **FILE\_HASH\_SEARCH\_INTERVAL\_SECONDS** parameter is used to configure the interval between search jobs that are triggered.

Table 45-4 FILE\_HASH\_SEARCH\_INTERVAL\_SECONDS option information

| Usage        | Description                                                                                                |
|--------------|------------------------------------------------------------------------------------------------------------|
| Where to use | User can modify the configuration parameters in <code>bp.conf</code> file on the NetBackup primary server. |

**Table 45-4** FILE\_HASH\_SEARCH\_INTERVAL\_SECONDS option information  
(continued)

| Usage      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| How to use | <p>Reduce the value of <b>FILE_HASH_SEARCH_INTERVAL_SECONDS</b> to decrease the time of identifying malware within the protected assets in a NetBackup domain.</p> <p>Use the following format:</p> <p><b>FILE_HASH_SEARCH_INTERVAL_SECONDS = 1800</b></p> <p>The default value is 28800 (8 hours). The minimum value is 1800 (30 minutes) and the maximum value is 86400 (24 hours).</p> <p><b>Note:</b> Restart the NetBackup Web Management Console service (<code>nbwmc</code>) for the new value to take effect.</p> |

## MALWARE\_HASH\_RETENTION\_DAYS

The **MALWARE\_HASH\_RETENTION\_DAYS** parameter is used to configure the number of days when a malware hash is treated as outdated.

**Table 45-5** MALWARE\_HASH\_RETENTION\_DAYS option information

| Usage        | Description                                                                                                                                                                                                                                        |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Where to use | User can modify the configuration parameters in <code>bp.conf</code> file on the NetBackup primary server.                                                                                                                                         |
| How to use   | <p>Reduce the value of <b>MALWARE_HASH_RETENTION_DAYS</b> to reduce the size of the malware hash values in the database.</p> <p>Use the following format:</p> <p><b>MALWARE_HASH_RETENTION_DAYS = 7</b></p> <p>The default value is 30 (days).</p> |

# MALWARE\_DETECTION\_MALWARE\_JOBS\_CLEANUP\_PERIOD

Malware detection performs automated cleanup of malware jobs which are older than 30 days in batches and in the following state:

- Scan complete
- Failed
- Cancel

Cleanup runs every 12 hours after NetBackup has started.

**Table 45-6** Malware detection malware jobs clean up option information

| Usage        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Where to use | User can modify the malware jobs cleanup period by setting the parameter in <code>bp.conf</code> file on the primary server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| How to use   | <p>Set the following parameters in <code>bp.conf</code> file:</p> <ul style="list-style-type: none"> <li>■ To change the cleanup period in days:<br/> <b>MALWARE_DETECTION_MALWARE_JOBS_CLEANUP_PERIOD = 45</b><br/> <b>Note:</b> Value must be in number of days only. An integer value greater than 0 is accepted, but NetBackup recommends not to set it to more than 6 month that is, 180 (days). If an invalid value is set, then the default value of 30 days is used.</li> <li>■ To switch off the cleanup period:<br/> <b>MALWARE_DETECTION_MALWARE_JOBS_CLEANUP_PERIOD = 0</b></li> <li>■ To change the scan job batch size:<br/> <b>MALWARE_DETECTION_CLEANUP_BATCH_SIZE = 600</b><br/> <b>Note:</b> You can set any value between 1 to 5000 for batch size. If you set invalid value then default value of 500 is used.</li> </ul> |

## MALWARE\_DETECTION\_WORKLIST\_CLEANUP\_PERIOD

Malware detection performs automated cleanup of worklists in batches and which are in the following state:

- Scan complete
- Failed
- Cancel

Cleanup runs every 12 hours after NetBackup has started.

**Table 45-7** Malware detection worklist clean up option information

| Usage        | Description                                                                                                                                |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Where to use | User can modify the malware detection worklist cleanup period by setting the parameter in <code>bp.conf</code> file on the primary server. |

**Table 45-7** Malware detection worklist clean up option information (*continued*)

| Usage      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| How to use | <p>Set the following parameters in <code>bp.conf</code> file:</p> <ul style="list-style-type: none"> <li>To switch off the worklist cleanup period:<br/> <b>MALWARE_DETECTION_WORKLIST_CLEANUP_PERIOD = 0</b><br/> <b>Note:</b> Any value greater than 0 will start the clean up of the worklists table.</li> <li>To change the scan job batch size:<br/> <b>MALWARE_DETECTION_CLEANUP_BATCH_SIZE = 600</b><br/> <b>Note:</b> You can set any value between 1 to 5000 for batch size. If you set invalid value then default value of 500 is used.</li> </ul> |

## CLIENT\_KEEP\_LOG\_DAYS

The **CLIENT\_KEEP\_LOG\_DAYS** parameter defines the duration for which NetBackup retains data from VxUL and Legacy logs. The logs can take up a significant amount of disk space (the log volume size is 25GB), therefore, it is recommended not to retain the logs for longer time than required. By default logs older than 7 days are deleted.

To modify the default settings, it is necessary to log in to the NetBackup malware scanner container via SSH and adjust the value of **CLIENT\_KEEP\_LOG\_DAYS** in the `bp.conf` file located at `/usr/opensv/netbackup/` folder.

## VIRUS\_SIGNATURE\_UPDATE\_INTERVAL

The **VIRUS\_SIGNATURE\_UPDATE\_INTERVAL** parameter specifies the validity period, in hours, for the malware signature definitions used by NetBackup. By default, the malware signature definitions remain valid for 4 hours. You can adjust this interval as required. Setting the value to **0** will update the malware signature definitions before every scan.

**Table 45-8** Virus signature update interval option information

| Usage        | Description                 |
|--------------|-----------------------------|
| Where to use | On NetBackup media servers. |

Table 45-8      Virus signature update interval option information (continued)

| Usage                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| How to use                            | <div>Set the following parameters in <code>bp.conf</code> file:</div> <div><div><div>■ To change the cleanup period in hours:</div><div><b>VIRUS_SIGNATURE_UPDATE_INTERVAL</b><br/><b>= 2</b></div><div><b>Note:</b> Value should be in number of hours only.</div></div><div><div>■ To update definition for every scan:</div><div><b>VIRUS_SIGNATURE_UPDATE_INTERVAL</b><br/><b>= 0</b></div></div></div> |
| Equivalent NetBackup web UI property: | No equivalent exists in the host properties.                                                                                                                                                                                                                                                                                                                                                                |

# Troubleshooting

This chapter includes the following topics:

- [Troubleshooting issues with malware scanning](#)

## Troubleshooting issues with malware scanning

### Failed to get response from NetBackup malware utility

*(Applicable on scan host RHEL 8.x and NFS version 4.x)* When scanning large size backup (~ 200 million files), following error is displayed on the Web UI for failed job:

```
Failed to get response from NetBackup malware utility.
```

While scan is in progress on scan host, NFS mount points are not accessible from scan host. Scan job remains in progress and timeout after two days. NFS exports on storage server are accessible.

**Workaround:** Ensure that you use NFS version 3 for mounting IA mounts on scan host over NFS by setting the following configuration in `/etc/nfsmount.conf` file on scan host:

```
grep Defaultvers /etc/nfsmount.conf Defaultvers=3
```

### Failed to connect to the scan host

SSH connection to scan host from media server failed.

**Workaround:** Verify the following scan host credentials:

- RSA (SHA256) key
- User name
- Password

Refer to *NetBackup Web UI Administrator's Guide* for the scan host configuration.

## Failed to determine the scan host OS

Error can be due to unsupported scan host.

**Workaround:** For a complete list of supported platforms for the scan host, refer to the *Software Compatibility list* document.

## Failed to copy NetBackup malware utility to the scan host

- Not enough space is available on the scan host.
- SSH user does not have access to the required directories on the scan host.

### Workaround

- On a Windows scan host, check for space availability in `C:\` folder.
- On a Linux scan host, check for space availability in `/tmp` folder.

## Failed to get the scan host credentials

Media server is not able to fetch the credentials to access scan host from the Primary.

**Workaround:** Check that credentials for scan host are specified.

## Time-out has occurred during the scan

Default scan operation time out is two days. Time to scan may vary depending on the factors such as workload type, network bandwidth, backup size.

**Workaround:** Scan time-out is configurable and can be changed by setting the **MALWARE\_SCAN\_OPERATION\_TIMEOUT** configuration key.

- Minimum value: 1 hour
- Maximum value: 30 days

## Failed to get response from NetBackup malware utility

Mismatch between `nbmalwareutil` binary and the `ScanManager`.

### Workaround:

Contact NetBackup support.

## Failed to launch the scanner

Malware scanner-specific failure message.

**Workaround:** Refer to `nbmalwarescanner` logs on the media server for agentless host type pools, or on scan host if it is agent based scan.

## Failed to mount the backup image

This error message appears for one of the following reasons:

- IA share is not accessible from the scan host.  
**Workaround:** Check IA configuration on storage server. Verify on activity monitor that IA job is successful.
- The backup image for which the scan was requested expired after the Instant Access (IA) mount was created. This causes the IA mount to be deleted along with the corresponding NFS export path, resulting in an NFS mount failure on the scan host.  
**Workaround:** Ensure that the backup image remains valid for the entire duration of the scan. Avoid initiating scans on images that may expire during the scan process.

## Failed to create Instant Access mount

Unable to create mount due to the following error in Instant Access:

```
Failed to fetch image details.
```

The backup image for which the scan was requested expired before the Instant Access (IA) mount creation. As a result, IA mount creation fails.

**Workaround:** Ensure that malware scans are not triggered for backup images that are close to their expiration time. Verify the image retention period before initiating the scan.

## Failed to unmount the backup image

IA share is busy or not accessible.

**Workaround:** Refer to `nbmalwarescanner` logs on the media server for agentless host type pools, or on scan host if it is agent based scan.

## Failed to run a scan

Generic failure during the scan of a backup image.

**Workaround:** Refer to `nbmalwarescanner` logs on the media server for agentless host type pools, or on scan host if it is agent based scan.

## Instant access mount created but not deleted by malware scan

Generic failure during the scan of a backup image.

**Workaround:**

- Verify if any scan is in progress.

- If no scan is in progress, then obtain the list of such instant access mounts with ID's of the instant access mount created using the GET IA API from the following directory:

```
/netbackup/recovery/workloads/{workload}/instant-access-mounts
```

- Using the DELETE API, delete the instant access mount:

```
/netbackup/recovery/workloads/{workload}/instant-access-mounts/{mountId}
```

## **All mount drives are exhausted**

Only five backup images can be mounted at the same time on windows scan host.

### **Workaround:**

- Ensure that scan host is not part of multiple NetBackup domains.
- Check if there are any Stale mounts on the scan host by running `net use`.
- Following drive letters are used for mounting the IA shares on the windows scan host. Ensure that they are not in use. L:\ M:\ N:\ O:\ P:\

## **Either the Windows Defender is not installed or the environment variable is not set**

Microsoft Windows Defender is not installed on the scan host or not configured properly.

**Workaround:** Ensure that Microsoft Windows Defender is installed on scan host.

Refer *NetBackup Web UI Administrator's Guide* for the scan host configuration.

## **Either Symantec protection engine is not installed or the environment variable is not set**

Symantec Protection Engine is not installed on the scan host or not configured properly.

**Workaround:** Ensure that Symantec Protection Engine is installed on scan host.

Refer *NetBackup Web UI Administrator's Guide* for the scan host configuration.

## **Failed to perform malware scan of the backup image**

Generic error for Scan failure.

**Workaround:** Contact NetBackup support.

## **Net bios name can be at most 15 chars long**

Storage server host name cannot be more than 15 characters for the SMB share support.

If Windows Server 2016 is used to set up Active Directory domain, then it does not allow a connection to a storage server with host name of length more than 15 characters.

**Workaround:** Ensure that the character limit is not more than 15 characters.

## Failed to run a scan

Generic failure during scanning backup image.

**Workaround:** Check for the following errors:

- Refer to `nbmalwarescanner` logs on the media server for agentless host type pools, or on scan host if it is agent based scan.
- Check for space on media server storage.
- Check for NFS service failure on media server.

## Too many infected files in the selected time range

Review the `nbmalwarescanner` to view the infected files list for the backup images in the selected date range.

**Workaround:** Update the date range or recovery files and folders selection to reduce the number of infected files. Retry the operation. You can also perform one of the following:

- Select the **Allow recovery of files impacted by malware** option which can be used to recover selective clean files.
- Skip that backup image from recovery.

## Large number of infected files

- There are too many infected files in the selected scan result. If the scan result has infected files greater than 5000, the following message is displayed:

`Large number of infected files. To view the complete list of infected files, export the list.`

**Workaround:** Export the infected file list in `.csv` format and download it to view it.

- There are many infected files in the selected scan result or the infected file paths are long to be captured in the database. Following error message is displayed:

`Large number of infected files.`

**Workaround:** This result cannot be exported or viewed.

: As the results cannot be exported or viewed, review the scan logs to view a detailed list of the infected files for the selected scan result.

## Scan operation is divided into parts

For large size backup, scan operation is divided into parts. For example, if total number of files in the backup are 1,000,000, the scan operation will be divided into two parts of 500,000 files each.

Each part would be created and scanned separately. Each part can be assigned with different scan host. The Malware detection UI displays only single entry for backup.

**Workaround:** Each divided part details can be obtained by using the REST API.

## The NB\_MALWARE\_SCANNER\_PATH environment variable is missing

When performing a malware scan operation with the NetBackup Malware Scanner installed on the scan host, it fails with the following error message:

```
Missing environment variable NB_MALWARE_SCANNER_PATH
```

**Workaround:** Ensure that NetBackup Malware Scanner is installed. Note the install location.

Login on the scan host as user using the same user credentials that were provided during scan host configuration on the primary server. Add the following lines to ~/.bashrc:

```
export
NB_MALWARE_SCANNER_PATH=<installLocation>/savapi-sdk-linux64/bin
export PATH=$PATH:$NB_MALWARE_SCANNER_PATH
```

## Failed to perform malware scan on Windows scan host

Malware scanning on Windows scan host may fail if there are cygwin mks toolkit installed.

**Workaround:** UNIX utilities are installed, however, defined scanuser cannot have those UNIX utilities in the PATH variable.

## Issues related to space and directory access on the scan host

| Error/Issue                                                                                                                                                                                                                                                                                                                                                                                                      | Description                                                                                                                                                                            | Workaround                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>Failed to open the file.</li> <li>Unable to create a directory.</li> <li>Failed to generate the result file.</li> <li>Failed to open the output file.</li> <li>Unable to create directory for result file.</li> <li>Failed to open the result file.</li> <li>Unable to create mount destination directory.</li> <li>Unable to create directory for a log file.</li> </ul> | <ul style="list-style-type: none"> <li>Not enough space is available on the scan host.</li> <li>SSH user does not have access to the required directories on the scan host.</li> </ul> | <ul style="list-style-type: none"> <li>On a Windows scan host, check space availability in C:\</li> <li>On a Linux scan host check space availability in /tmp</li> </ul> |

## Issue related to NAS-Data-Protection

- When upgrading NetBackup from previous version to NetBackup version 10.3 or later with the following options selected, the `No images match the search criteria` message is displayed:

| Options                                 | Fields                                                                                                                                                                                   |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Search by:</b> Backup images         | <b>Policy type:</b> NAS-Data-Protection<br><b>Copies:</b> Copy2<br><b>Malware scan status:</b> Not scanned (Default)                                                                     |
| <b>Search by:</b> Assets by policy type | <b>Policy type:</b> NAS-Data-Protection<br><b>Copies:</b> Copy2<br><b>Scanner host pool:</b> Select the required scanner host pool.<br><b>Malware scan status:</b> Not scanned (Default) |

### Workaround

To view the images that are backed up, ensure that you select the **Malware scan status** option as **All** to scan the NAS-Data-Protection backup images created on earlier version of NetBackup media server.

- **File write error**

**File write error**

While running a malware scan on NAS-Data Protection Policy, a `.tar.gz` file (~13 GB) was skipped with the following error message:

```
File write error
```

The NetBackup Malware Scanner, also known as Avira, extracts the contents of compressed or archived files to a staging volume prior to scanning. If there is insufficient space in the staging volume to extract the compressed or archived files, those files may be skipped during the scanning process and will be reported as unscannable files. It is possible to export a list of unscannable files from the scan results. The reason for skipping a file will be indicated as follows:

```
File write error
```

**Workaround:**

The default size of the staging volume is 10GB, which must be increased if there is a large number of compressed or archived files in the backup, or if the compressed or archived files are nested, such as a zip file containing `.jar` or `.war` files.

---

**Note:** In such instances, the user can resize the staging volume using the Flex Console. The maximum size for the staging volume is 50GB.

---

## Issues in scan performance

When using Instant Access mount points for malware scan (traditional malware scan) in NetBackup versions prior to 10.3, performance issues were observed.

**Workaround:** Upgrade to NetBackup media and storage server 10.3 or later. NetBackup 10.3 introduces the **dynamic scan** feature. This improves the instant access time as well as the scan performance.

The following table provides the differences between the traditional malware scan and dynamic scan:

| <b>Key scanning procedure</b>                                                        | <b>Traditional malware scan using Instant Access mount points</b>                                                                                           | <b>Dynamic scan</b>                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Instant access stage.                                                                | Analyzes the tar stream and builds each file's header and extent map file (LMDB database), which is time consuming for large number of files in the backup. | Restores TIR (catalog database) and IM (image metadata) information from fragment.                                                                                                                                                                                                                                                                                             |
| Instant access share (NFS/SMB) is mounted and user tries to list or access the file. | Accesses it's header file and reads the attribute from it.                                                                                                  | Query's the directory from catalog database to get all the files and directories which are under this directory. It can also query each files and directories attribute to the output.                                                                                                                                                                                         |
| Scan host opens a file                                                               | Opens and loads the LMDB database.                                                                                                                          | Builds the index in memory and reads directly from data container. <ul style="list-style-type: none"> <li>■ To get file's extent by locating and reading the tar header and analyze the content.</li> <li>■ To get SO list (PureDisk only) by searching the SO list from fragment FP map</li> <li>■ To build mapping table by inserting the SO list (PureDisk only)</li> </ul> |
| Scan host reads a file                                                               | Searches from LMDB database and reads from data container.                                                                                                  | If storage server is 3rd party storage vendor, it reads data through OST interface directly. If storage server is PureDisk, it searches from mapping table and reads data from data container.                                                                                                                                                                                 |

## Details of log file location for errors

The following table provides the details for the respective log files to be viewed depending on the use case:

**Table 46-1** Log file locations for Agentless scan host

| Use case       | Components on primary server | Components on media server  | Log file path                                                                                                                                        |
|----------------|------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configurations | nbwebbservice                | ncfnbcs                     | For primary server:                                                                                                                                  |
| Scan process   | nbwebbservice<br>bprd        | ncfnbcs<br>nbmalwarescanner | <ul style="list-style-type: none"> <li>■ /usr/openv/logs/nbwebbservice</li> <li>■ /usr/openv/netbackup/logs/bprd/</li> </ul>                         |
| Recovery       | nbwebbservice<br>bprd        |                             | For media server: <ul style="list-style-type: none"> <li>■ /usr/openv/logs/ncfnbcs</li> <li>■ /usr/openv/netbackup/logs/nbmalwarescanner/</li> </ul> |

**Table 46-2** Log file locations for NetBackup client as the scan host

| Use case       | Components on primary server | Components on the scan host client | Log file path                               |
|----------------|------------------------------|------------------------------------|---------------------------------------------|
| Configurations | nbwebbservice                | nbsubscriber                       | ■ /usr/openv/netbackup/logs/scanhostconfig/ |
| Scan process   | nbwebbservice<br>bprd        | nbsubscriber                       | ■ /usr/openv/logs/nbsubscriber/             |
| Recovery       | nbwebbservice<br>bprd        |                                    |                                             |

## SSH login is disabled by default

For VMWare VM backup scan, ensure that you use scan user with `uid=0`. SSH login is disabled by default and user may not enable it for security reasons.

### Workaround

In above scenario, perform the following:

If SSH login is disabled for the root user, then non-root scan user can be added to group 0 (root) to be able to scan all the files.

For example, `uid=1001(scanuser) gid=1001(scanuser) groups=1001(scanuser),0(root)`

## Malware status displayed as 'Not supported' for Hyper-V images

During upgrade, the malware status for Hyper-V images created in NetBackup version prior to 11.0.0.1 are displayed as **Not supported**. For newly backed up images post upgrade, default malware status for Hyper-V backup images will be displayed as **Not Scanned**.

### Workaround

User can perform malware scan on the Hyper-V images displayed as **Not supported**.

## Issues in VMware scan performance

When using Instant Access mount points for malware scan (traditional malware scan) for VMware backup images in NetBackup versions prior to 11.1, performance issues were observed.

### Workaround

Upgrade to NetBackup primary, media and storage server 11.1 or later. NetBackup 11.1 introduces the VxMS based Instant access feature for malware scanning of VMware backup images which is based on the dynamic scan feature. This improves the instant access time and scan performance.

**Note:** For more information on dynamic scan which was applicable for non-VMware workload, refer to [Issues in scan performance](#) section. VxMS based Instant Access is applicable for VMware backup images if it's backup policy has **Enable file recovery from VM backup** option enabled, that is, VxMS enabled backup, else it will continue using the traditional Instant Access method.

The following table provides the differences between the traditional malware scan and VxMS based Instant Access scan:

| Traditional malware scan                                                                                                                        | VxMS based Instant Access scan                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| To provide IA mount point for traditional malware scan for VMware backup image, it uses third party open source tool called <b>libguestFS</b> . | VxMS-based intelligent automation eliminates the need for any external tools for malware scanning. It relies on the VxMS catalog and records to retrieve files from the backup image. |
| Adding an extra layer of <b>libguestFS</b> extends IO durations and hinders malware scanning efficiency.                                        | VxMS offers a solution by utilizing VxMS-based records from the backup image, which allows for quicker execution of file operations.                                                  |

### **Traditional malware scan**

The ability to scan malware in batches is unavailable.

### **VxMS based Instant Access scan**

The VxMS-based IA scans extensive VMware backups in batches of 500,000 files, with each batch being handled by a different scan thread.

# Threat library

This chapter includes the following topics:

- [About threat library and YARA rule files](#)
- [Add threat feeds](#)

## About threat library and YARA rule files

A threat library is a set of threat feeds in the form of a rule file or a `.zip` file of multiple YARA rule files. You can add threat feeds that you can use when you want to scan images to detect malware.

## Add threat feeds

A threat feed can consist of YARA or other rules. Ensure that you have stored the required threat feeds or rule files at the required location.

See [“About YARA scanning”](#) on page 740.

### To add a threat feed

- 1 On the left, click **Detection and reporting > Threat library**.
- 2 Click **Add**.
- 3 On the **Add threat feed** dialog box, click **Upload threat feed file**. Select the required threat feed from the appropriate location. It can be a YARA rule file or a `.zip` file.

A YARA rule file can be of extension `.yar` or `.yara`.

**4** Enter the threat feed name.

**5** Click **Save**.

After you save the threat feeds, they are validated. Threat feeds with successful validation have the status as 'Valid'. If validation is not successful, the status is shown as 'Invalid'. Use the **View details** option to view the reasons for the invalid status of the threat feeds.

Only valid threat feeds can be used for YARA scanning.

# YARA scanning

This chapter includes the following topics:

- [About YARA scanning](#)
- [Workflow to configure YARA scanning](#)
- [Scanning backup images with YARA scanner](#)
- [Assets by workload type for YARA scanning](#)

## About YARA scanning

YARA stands for 'Yet Another Ridiculous Acronym'.

YARA scanner is a tool that uses YARA rules to find and classify malware and other malicious artifacts within files or memory. YARA allows users to define textual or binary patterns to create rules that identify specific malware families or types of threats.

### Support information

- YARA scanning is supported only for Linux platform with NFS share type.
- Recovery time scan is not supported for YARA.

See [“Workflow to configure YARA scanning”](#) on page 741.

# Workflow to configure YARA scanning

Table 48-1

| Step   | Description                                                                                                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Add a compute host that has YARA scanner configured on it. Specify the operation and the scanner type as YARA scanner when you add a compute host.<br><br>See <a href="#">"Add a compute host"</a> on page 626. |
| Step 2 | Add a threat feed with the required YARA rules.<br><br>See <a href="#">"Add threat feeds"</a> on page 738.                                                                                                      |
| Step 3 | Scan backup images with YARA scanner<br><br>See <a href="#">"Scanning backup images with YARA scanner"</a> on page 741.                                                                                         |

## Scanning backup images with YARA scanner

Use this topic to scan images with YARA scanner.

### To scan images with YARA scanner

- 1 On the left, click **Detection and reporting > Malware detection**.
- 2 Click **Scan for malware**.
- 3 In the **Search by** option, select **Backup images**.
- 4 Select **YARA scan** as the scan type.
- 5 Click the **Select threat feeds** option.  
  
On the dialog box, select the required YARA rule files or .zip file and click **Select**.
- 6 In the **search criteria**, review and edit the following:
  - Policy name - Only supported policy types are listed.
  - Client name - Displays the clients that have backup images for a supported policy type.
  - Policy type - Displays all the supported policies that are enabled for YARA scanning.
  - Type of backup - Any incremental backup images that do not have the NetBackup Accelerator feature enabled are not supported for the VMware workload.

- Copies - If the selected copy does not support instant access, then the backup image is skipped for the scan. (For NAS-Data-Protection policy type) Select the Copies as Copy 2.
- Disk pool - MSDP (PureDisk), OST (for example, Data Domain) and AdvancedDisk storage type disk pools are listed.
- Disk type - MSDP (PureDisk), OST (for example, Data Domain) and AdvancedDisk disk types are listed.
- Infection status - The malware-infected status of the backup images can be searched based on the following types: infection detected by malware scan, file hash search, not infected, not scanned or all.
- For the **Select the timeframe of backups**, verify the date and the time range or update it.
- On selecting the **Abort malware scan on detecting an infection** option, clean recovery would not be supported for infected images.

7 Click **Search**.

8 Select the search criteria and ensure that the selected compute host is active and available.

9 From the **Select the backups to scan** table select one or more images for scan.

10 Click **Scan for malware**.

11 After the scan is initiated, the **Scan status** is displayed.

The following are the status fields:

- Not scanned
- Not infected
- Infected
- Failed

Hover over the status to view the reason for the failed scan.

---

**Note:** Any backup images that fail the validation are ignored. Scanning is supported for the backup images that are stored on storage with instant access capability and for the supported policy types only.

---

- In progress
- Pending

---

**Note:** You can cancel the scan for one or more jobs that are in progress or are pending.

---

- Infected - Scan aborted

You can view the YARA scanning jobs on the **Activity monitor** UI.

## Assets by workload type for YARA scanning

This section describes the procedure for scanning Kubernetes assets for YARA.

### To scan Kubernetes assets for YARA

- 1 On the left, select the supported workload under Workloads.
- 2 Select the resource for which backups are completed.
- 3 Select **Actions > Scan for malware**.
- 4 On the **Malware scan** page, perform the following:
  - Select the date range for the scan by selecting **Start date/time** and **End date/time**.
  - Select scan type as **YARA scan**, and then select **Required threat feeds**.
  - From the Current infection status list select one of the following:
    - Not scanned
    - Not infected
    - Infection detected by malware scan
    - Infection detected by file hash search
    - All
- 5 Click **Scan for malware**.
- 6 After the scan starts, you can see the **Scan status on Malware detection**. The following fields are visible:
  - Not scanned
  - Not infected
  - Infected
  - Failed

---

**Note:** Any backup images that fail the validation are ignored.

---

- In progress
- Pending

# File hash calculation

This chapter includes the following topics:

- [About file hash calculation](#)
- [Workflow to configure file hash calculation](#)
- [Calculate file hashes for backup images](#)
- [Troubleshooting issues with file hash calculation](#)

## About file hash calculation

File hash calculation enables post-backup SHA-256 hash computation for files stored in NetBackup backup images. Hashes are calculated for regular files and files contained within stream-friendly compressed and archive formats as follows:

`tar, zip, gz, bz2, xz, 7z, rar (RAR 5 is not supported), tar.gz, tgz, tar.bz2, tbz2, tar.xz, txz, jar, war, deb, rpm, cab, iso, and udeb`

This feature enables hash-based threat hunting for regular, compressed and archive files by matching computed file hashes against curated Indicators of Compromise (IOC) stores that contain known malicious hashes.

The hash calculation job computes cryptographic hashes in a streaming manner and stores the hash metadata in the NetBackup catalog. These hashes are transferred to the file hash server, where they are indexed and made available for search operations across backup images at scale.

### Support information

- NetBackup primary 11.2 or later is required.
- Images for which hash calculation is performed must reside on NetBackup media server 11.2 or later.

- Compute hosts used for hash calculation are supported only on Linux (Red Hat or SUSE) clients version 11.2 or later. The clients must have the `libarchive` OS library installed.
- The NetBackup file hash server must be a NetBackup media server 11.2 or later.
- Standard, Windows and DNAS policy types are supported.
- Hash calculation is not supported for synthetic backup images, client-side encrypted backup images or compressed images.

See [“Workflow to configure file hash calculation”](#) on page 746.

## Workflow to configure file hash calculation

The following table provides a workflow that describes the end-to-end operation for compressed file hash calculation.

**Table 49-1** Workflow to configure file hash calculation

| Steps  | Description                                                                                                                                                                                                                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>Configure the file hash server:</b></p> <p>For more information on configuring the file hash server, see 'Configuring the file hash server' section in the <i>NetBackup™ Web UI Administrator's Guide</i>.</p>                                                                                                                                                                   |
| Step 2 | <p><b>Configure the compute host:</b></p> <p>Add a compute host that has the hash calculator configured.</p> <p>By default, all NetBackup Linux Red Hat and SUSE 11.2 clients include the hash calculator. When adding the compute host, specify the operation and select <b>Hash calculator</b> as the scanner type.</p> <p>See <a href="#">“Add a compute host”</a> on page 626.</p> |
| Step 3 | <p><b>Calculate hashes for files in backup images:</b></p> <p>See <a href="#">“Calculate file hashes for backup images”</a> on page 747.</p>                                                                                                                                                                                                                                           |
| Step 4 | <p><b>Search for files using the file hash:</b></p> <p>You can search the files using the file hash. For more information, see 'Searching the files using the file hash' section in the <i>NetBackup™ Web UI Administrator's Guide</i>.</p>                                                                                                                                            |

# Calculate file hashes for backup images

Use this procedure to calculate file hashes for backup images.

## To calculate file hashes

- 1 On the left, click **Detection and reporting > Malware detection**.
- 2 Click **Scan for malware**.
- 3 In the **Search by** option, select **Backup images**.
- 4 Select **Hash calculation** as the scan type.
- 5 In the **search criteria**, review and edit the following:
  - Policy name - Only supported policy types are listed.
  - Client name - Displays the clients that have backup images for a supported policy type.
  - Policy type - Displays all the supported policy types that are enabled for hash calculation.
  - Type of backup - Displays all the supported type of backups that are enabled for hash calculation.
  - Copies - If the selected copy does not support instant access, then the backup image is skipped for the hash calculation. (For NAS-Data-Protection policy type) Select the Copies as Copy 2.
  - Disk pool - MSDP (PureDisk), SpanFS, OST (for example, Data Domain) and AdvancedDisk storage type disk pools are listed.
  - Disk type - MSDP (PureDisk), SpanFS, OST (for example, Data Domain) and AdvancedDisk disk types are listed.
  - Infection status - The malware-infected status of the backup images can be searched based on the following types: infection detected by malware scan, file hash search, not infected, not scanned or all.
  - For the **Select the timeframe of backups**, verify the date and the time range or update it.
- 6 Click **Search**.
- 7 Select the search criteria and ensure that the selected compute host is active and available.
- 8 From the **Select the backups to scan** table, select one or more images for which hashes were previously calculated and that are not listed in the search results.

- 9 Click **Calculate file hash**.
- 10 After the hash calculation job is initiated, you can view progress on the **Activity monitor** UI.

During the hash calculation job, the generated hashes are immediately transferred to the **File Hash Server** and ingested. This allows the hashes to be searched and used instantly without any delay. If file hash transfer for another image is in progress, the file hashes are queued and transferred and ingested at regular intervals.

Advanced configuration parameters

Use the following advanced configuration parameters to customize file hash calculation behavior and optimize performance.

Table 49-2 Advanced file hash configuration parameters

| Parameter                         | Description                                                                                                         |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------|
| HASH_SCAN_MAX_FILE_SIZE_IN_MB     | Specifies the maximum file size (in MB) for hash calculation.<br><br>A value of 0 indicates no limit. Default: 200. |
| HASH_SCAN_NESTED_ARCHIVE_DEPTH    | Specifies the maximum depth for nested archive extraction.<br><br>A value of -1 indicates no limit. Default: 10.    |
| DISABLE_FHS_TRANSFER              | Controls automatic transfer of images to the file hash server during hash calculation.<br><br>Default: 1 (enabled). |
| FILE_HASH_BID_BATCH_INTERVAL      | Specifies the interval (in seconds) for file hash transfer.<br><br>Default: 86400.                                  |
| AUTO_CLEAN_FILE_HASH_FROM_CATALOG | Set to 1 on the primary server to automatically delete file hashes and reduce catalog size.                         |

For more information on other configurable parameters, refer to the following section:  
See [“Malware hash configuration parameters”](#) on page 721.

Troubleshooting issues with file hash calculation

Log files:

- **Web service logs:** Linux: `/usr/openv/logs/nbwebservice`

- **BPDBM logs:** Linux: `/usr/opensv/netbackup/logs/bpdbm`
- **BPRD logs:** Linux: `/usr/opensv/netbackup/logs/bprd`
- **NetBackup admin logs:** Linux: `/usr/opensv/netbackup/logs/admin/`
- **File hash server logs:** `/<file hash storage path>/hashdb/log`

## Network timeout during file hash search

The following error is encountered when performing a file hash search.

```
network connection broken
```

File hash search results in a network timeout (initial failure error code 4106), and subsequent searches continue to fail with error code 40.

This issue typically occurs when the file hash server services are not functioning correctly or become unresponsive.

### Workaround:

Restart the file hash server services to restore connectivity and allow hash search operations to complete successfully.

## Warning in hash calculation job activity monitor

- **Failed to transfer file hashes for image to the file hash server**

The following warning message appears in the job activity monitor:

```
File hash transfer queued for image
```

The above issue may be due to one of the following reasons:

- File hash server is not configured correctly.
- An earlier hash-only image transfer did not complete successfully.
- Hash-only images exist but were not transferred to the file hash server.

Check the following logs on the primary server:

- `bprd` logs for entries similar to:

```
immediate transfer of hash-only image <backup-id> to file hash server f
```

- `bpdbm` logs for entries similar to:

```
failed to create hash-only bid info file
```

### Workaround:

Verify hash-only image creation:

- Check for all hash-only images:

```
/usr/opensv/netbackup/bin/admincmd/bpimagelist -hash_only
```

- Check hash-only images for a specific parent backup:

```
/usr/opensv/netbackup/bin/admincmd/bpimagelist -hash_only -parent
<parent_backup_id>
```

- If no hash-only images are listed, then configure the file hash server by following the procedure described in the following section:

See [“Workflow to configure file hash calculation”](#) on page 746.

Retrigger the hash calculation job.

- If hash-only images are listed but not available on the file hash server, then manually initiate the transfer from the primary server using the following command:

```
/usr/opensv/netbackup/bin/goodies/nbfhsmgr -transfer
```

After the transfer completes, start hash database processing on the file hash server using the following command:

```
/usr/opensv/pdde/pdcr/bin/fhdbctl --op db_process start
```

- **Failed to transfer file hashes due to ongoing ingestion**

The following warning message appears in the job activity monitor:

```
File hash transfer queued for image
```

The above issue may be due to one of the following reasons:

- A previous hash ingestion process is still in progress or did not complete successfully.
- The file hash server database is locked by another ingestion job.

Check the file hash logs for the following message:

```
failed to acquire lock within 40s for systemtest5230h_1777303980.f

(waited 40s), another ingestion in progress
```

#### **Workaround:**

- Manually initiate the hash-only image transfer from the Primary Server using the following command:

```
/usr/opensv/netbackup/bin/goodies/nbfhsmgr -transfer
```

- Start database processing on the file hash server using the following command:

```
/usr/opensv/pdde/pdcr/bin/fhdbctl --op db_process start
```

- Monitor the file hash server logs to ensure that the ingestion completes successfully before retriggering the hash calculation job.

## Error on Web UI

Failed to validate the compute host. The following error message is displayed on the NetBackup Web UI:

```
Failed to validate the compute host.
```

The above issue may be due to one of the following reasons:

- The compute host was added and deleted multiple times.
- The compute host type is not correctly configured for malware scanning.

Check the `nbweb service` logs on the Primary Server for entries similar to:

```
Exception occurred while binding the queue,
closing the connection if opened.
java.io.IOException
at com.netbackup.messagequeue.service.MQServiceUtil.bindQueue
```

### Workaround:

- On the compute host, edit the `/usr/opensv/netbackup/bp.conf` file.
- Add the following entry:

```
MACHINE_NBU_TYPE = NB_SCAN_HOST
```

- Restart NetBackup services on the compute host:

```
Stop: /usr/opensv/netbackup/bin/bp.kill_all
Start: /usr/opensv/netbackup/bin/bp.start_all
```

- Re-validate the compute host from the Web UI.