Veritas NetBackup™ Deduplication Guide

UNIX, Windows, Linux

Release 8.1.1

VERITAS™

Veritas NetBackup™ Deduplication Guide

Last updated: 2018-02-23

Document version:NetBackup 8.1.1

Legal Notice

Copyright © 2018 Veritas Technologies LLC. All rights reserved.

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

This product may contain third-party software for which Veritas is required to provide attribution to the third party (“Third-party Programs”). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

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

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

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

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

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

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

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

https://sort.veritas.com/documents

Documentation feedback

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1 Introducing the NetBackup media server deduplication option 12

About the NetBackup deduplication options 12
New MSDP features in NetBackup 8.1.1 13

Chapter 2 Planning your deployment 14

Planning your MSDP deployment 15
NetBackup naming conventions 16
About MSDP deduplication nodes 17
About the NetBackup deduplication destinations 17
About MSDP storage capacity 18
About MSDP storage and connectivity requirements 19
Fibre Channel and iSCSI comparison for MSDP 21
About NetBackup media server deduplication 22
About MSDP storage servers 24
About MSDP load balancing servers 25
About MSDP server requirements 25
About MSDP unsupported configurations 27
About NetBackup Client Direct deduplication 27
About MSDP client deduplication requirements and limitations 28
About MSDP remote office client deduplication 29
About MSDP remote client data security 30
About remote client backup scheduling 30
About the NetBackup Deduplication Engine credentials 30
About the network interface for MSDP 31
About MSDP port usage 32
About MSDP optimized synthetic backups 33
About MSDP and SAN Client 33
About MSDP optimized duplication and replication 34
About MSDP performance 34
How file size may affect the MSDP deduplication rate 35
About MSDP stream handlers 35
MSDP deployment best practices 36
Use fully qualified domain names 36

About scaling MSDP 36
Send initial full backups to the storage server 37
Increase the number of MSDP jobs gradually 37
Introduce MSDP load balancing servers gradually 38
Implement MSDP client deduplication gradually 38
Use MSDP compression and encryption 39
About the optimal number of backup streams for MSDP 39
About storage unit groups for MSDP 39
About protecting the MSDP data 40
Save the MSDP storage server configuration 40
Plan for disk write caching 41

Chapter 3 Provisioning the storage 42

About provisioning the storage for MSDP 42
Do not modify MSDP storage directories and files 44
About adding additional MSDP storage 44
About volume management for NetBackup MSDP 45

Chapter 4 Licensing deduplication 46

About the MSDP license 46
Licensing NetBackup MSDP 47

Chapter 5 Configuring deduplication 48

Configuring MSDP server-side deduplication 50
Configuring MSDP client-side deduplication 53
About the MSDP Deduplication Multi-Threaded Agent 54
Configuring the Deduplication Multi-Threaded Agent behavior 56
MSDP mtstrm.conf file parameters 56
Configuring deduplication plug-in interaction with the Multi-Threaded Agent 61
About MSDP fingerprinting 62
About the MSDP fingerprint cache 63
Configuring the MSDP fingerprint cache behavior 64
MSDP fingerprint cache behavior options 64
About seeding the MSDP fingerprint cache for remote client deduplication 65
Configuring MSDP fingerprint cache seeding on the client 67
Configuring MSDP fingerprint cache seeding on the storage server 68
NetBackup seedutil options 70
Enabling 96-TB support for MSDP 71

About MSDP Encryption using KMS service 71
Upgrading KMS for MSDP 72
Configuring a storage server for a Media Server Deduplication Pool 73
MSDP storage path properties 88
MSDP network interface properties 91
Configuring a storage server for a PureDisk Deduplication Pool 91
About disk pools for NetBackup deduplication 101
Configuring a disk pool for deduplication 103
Media Server Deduplication Pool properties 110
Creating the data directories for 96-TB MSDP support 112
Adding volumes to a 96-TB Media Server Deduplication Pool 113
Configuring a Media Server Deduplication Pool storage unit 115
Media Server Deduplication Pool storage unit properties 117
MSDP storage unit recommendations 118
Configuring client attributes for MSDP client-side deduplication 119
Disabling MSDP client-side deduplication for a client 121
About MSDP compression 121
About MSDP encryption 123
MSDP compression and encryption settings matrix 124
Configuring encryption for MSDP backups 126
Configuring encryption for MSDP optimized duplication and replication 127
About the rolling data conversion mechanism for MSDP 128
Modes of rolling data conversion 129
MSDP encryption behavior and compatibilities 131
Configuring optimized synthetic backups for MSDP 132
About a separate network path for MSDP duplication and replication 133
Configuring a separate network path for MSDP duplication and replication 134
About MSDP optimized duplication within the same domain 135
About the media servers for MSDP optimized duplication within the same domain 138
Configuring MSDP optimized duplication within the same NetBackup domain 143
Configuring NetBackup optimized duplication or replication behavior 147
About MSDP replication to a different domain 150
Configuring MSDP replication to a different NetBackup domain 152
About NetBackup Auto Image Replication 153
About trusted master servers for Auto Image Replication 161
Adding a trusted master server 164

Removing a trusted master server 169
Enabling NetBackup clustered master server inter-node authentication 171
Configuring a target for MSDP replication to a remote domain 172
About configuring MSDP optimized duplication and replication bandwidth 177
About storage lifecycle policies 178
About the storage lifecycle policies required for Auto Image Replication 179
Creating a storage lifecycle policy 181
Storage Lifecycle Policy dialog box settings 184
About MSDP backup policy configuration 186
Creating a backup policy 187
Resilient Network properties 188
Resilient connection resource usage 191
Specifying resilient connections 192
Adding an MSDP load balancing server 194
About variable-length deduplication on NetBackup clients 195
About the MSDP pd.conf configuration file 197
Editing the MSDP pd.conf file 198
MSDP pd.conf file parameters 198
About the MSDP contentrouter.cfg file 215
About saving the MSDP storage server configuration 215
Saving the MSDP storage server configuration 216
Editing an MSDP storage server configuration file 217
Setting the MSDP storage server configuration 218
About the MSDP host configuration file 219
Deleting an MSDP host configuration file 219
Resetting the MSDP registry 220
About protecting the MSDP catalog 221
About the MSDP shadow catalog 221
About the MSDP catalog backup policy 222
Changing the MSDP shadow catalog path 223
Changing the MSDP shadow catalog schedule 224
Changing the number of MSDP catalog shadow copies 225
Configuring an MSDP catalog backup 226
MSDP drcontrol options 227
Updating an MSDP catalog backup policy 230
About MSDP FIPS compliance 232

Chapter 6 Configuring deduplication to the cloud with NetBackup CloudCatalyst 234

Using NetBackup CloudCatalyst to upload deduplicated data to the cloud 235
Optimized duplication is used to copy data from an MSDP storage server to a CloudCatalyst storage server (preferred use case) 235
Backups go directly to a CloudCatalyst storage server 237
CloudCatalyst requirements and limitations 238
Configuring a Linux media server as a CloudCatalyst storage server 239
Configuring a CloudCatalyst storage server for deduplication to the cloud 241
How to configure a NetBackup CloudCatalyst Appliance 241
How to configure a Linux media server as a CloudCatalyst storage server 244
Configuring a CloudCatalyst storage server as the target for the deduplications from MSDP storage servers 246
Configuring a storage lifecycle policy for NetBackup CloudCatalyst 247
About the CloudCatalyst esfs.json configuration file 248
About the CloudCatalyst cache 252
Differences between KMS and MSDP encryption for CloudCatalyst configurations 254
Controlling data traffic to the cloud when using CloudCatalyst 254
Configuring push or pull optimized duplication for CloudCatalyst 256
Decommissioning CloudCatalyst cloud storage 261
NetBackup CloudCatalyst workflow processes 261
Disaster Recovery for CloudCatalyst 266

Chapter 7 Monitoring deduplication activity 267

Monitoring the MSDP deduplication rate 267
Viewing MSDP job details 269
MSDP job details 269
About MSDP storage capacity and usage reporting 272
About MSDP container files 273
Viewing storage usage within MSDP container files 274
Viewing MSDP disk reports 275
About monitoring MSDP processes 276
Reporting on Auto Image Replication jobs 277

Chapter 8 Managing deduplication 278

Managing MSDP servers 279
Viewing MSDP storage servers 279
Determining the MSDP storage server state 279
Viewing MSDP storage server attributes 280
Setting MSDP storage server attributes 281
Changing MSDP storage server properties 282
Clearing MSDP storage server attributes 283
About changing the MSDP storage server name or storage path 284
Changing the MSDP storage server name or storage path 284
Removing an MSDP load balancing server 286
Deleting an MSDP storage server 287
Deleting the MSDP storage server configuration 288
Managing NetBackup Deduplication Engine credentials 289
Determining which media servers have deduplication credentials 289
Adding NetBackup Deduplication Engine credentials 289
Changing NetBackup Deduplication Engine credentials 290
Deleting credentials from a load balancing server 290
Managing Media Server Deduplication Pools 291
Viewing Media Server Deduplication Pools 291
Determining the Media Server Deduplication Pool state 291
Changing Media Server Deduplication Pool state 292
Viewing Media Server Deduplication Pool attributes 292
Setting a Media Server Deduplication Pool attribute 293
Changing a Media Server Deduplication Pool properties 294
Clearing a Media Server Deduplication Pool attribute 299
Determining the MSDP disk volume state 300
Changing the MSDP disk volume state 300
Inventorying a NetBackup disk pool 301
Deleting a Media Server Deduplication Pool 302
Deleting backup images 302
About MSDP queue processing 303
Processing the MSDP transaction queue manually 303
About MSDP data integrity checking 304
Configuring MSDP data integrity checking behavior 305
MSDP data integrity checking configuration parameters 307
About managing MSDP storage read performance 309
About MSDP storage rebasing 309
MSDP server-side rebasing parameters 311
About the MSDP data removal process 312

Resizing the MSDP storage partition 313
How MSDP restores work 314
Configuring MSDP restores directly to a client 315
About restoring files at a remote site 315
About restoring from a backup at a target master domain 316
Specifying the restore server 316

Chapter 9 Recovering MSDP 318

About recovering the MSDP catalog 318
Restoring the MSDP catalog from a shadow copy 319
Recovering from an MSDP storage server disk failure 321
Recovering from an MSDP storage server failure 322
Recovering the MSDP storage server after NetBackup catalog recovery 325

Chapter 10 Replacing MSDP hosts 326

Replacing the MSDP storage server host computer 326

Chapter 11 Uninstalling MSDP 329

About uninstalling MSDP 329
Deactivating MSDP 329

Chapter 12 Deduplication architecture 331

MSDP server components 331
Media server deduplication backup process 334
MSDP client components 337
MSDP client–side deduplication backup process 337

Chapter 13 Troubleshooting 342

About unified logging 342
About using the vxlogview command to view unified logs 343
Examples of using vxlogview to view unified logs 344
About legacy logging 345
Creating NetBackup log file directories for MSDP 347
NetBackup MSDP log files 347
Troubleshooting MSDP installation issues 354
MSDP installation on SUSE Linux fails 354
Troubleshooting MSDP configuration issues 355
MSDP storage server configuration fails 355
MSDP database system error (220) 355

MSDP server not found error 356
License information failure during MSDP configuration 356
The disk pool wizard does not display an MSDP volume 357
Troubleshooting MSDP operational issues 357
Verify that the MSDP server has sufficient memory 358
MSDP backup or duplication job fails 358
MSDP client deduplication fails 360
MSDP volume state changes to DOWN when volume is unmounted 361
MSDP errors, delayed response, hangs 362
Cannot delete an MSDP disk pool 362
MSDP media open error (83) 363
MSDP media write error (84) 365
MSDP no images successfully processed (191) 368
MSDP storage full conditions 368
Troubleshooting MSDP catalog backup 369
Viewing MSDP disk errors and events 370
MSDP event codes and messages 370
Troubleshooting CloudCatalyst issues 373
CloudCatalyst logs 373
Problems encountered while using the Cloud Storage Server Configuration Wizard 375
Disk pool problems 377
Problems during cloud storage server configuration 378
Status 191: No images were successfully processed 380
Media write error (84) if due to a full local cache directory 380
Trouble restarting ESFS after the CloudCatalyst storage server is down 381
Restarting the vxesfsd process 381
Problems restarting vxesfsd 382
CloudCatalyst troubleshooting tools 383

Appendix A Migrating to MSDP storage 386

Migrating from PureDisk to the NetBackup MSDP 386
Migrating from another storage type to MSDP 387

Index 389

Chapter 1

Introducing the NetBackup media server deduplication option

This chapter includes the following topics:

- About the NetBackup deduplication options
- New MSDP features in NetBackup 8.1.1

About the NetBackup deduplication options

Veritas NetBackup provides the deduplication options that let you deduplicate data everywhere, as close to the source of data as you require.

Deduplication everywhere provides the following benefits:

- Reduce the amount of data that is stored.
- Reduce backup bandwidth.
- Reduce backup windows.
- Reduce infrastructure.

Deduplication everywhere lets you choose at which point in the backup process to perform deduplication. NetBackup can manage your deduplication wherever you implement it in the backup stream.

Table 1-1 describes the options for deduplication.

Table 1-1 NetBackup deduplication options

Type	Description
Media server deduplication	NetBackup clients send their backups to a NetBackup media server, which deduplicates the backup data. A NetBackup media server hosts the NetBackup Deduplication Engine, which writes the data to a **Media Server Deduplication Pool** on the target storage and manages the deduplicated data See "About NetBackup media server deduplication" on page 22.
Client deduplication	With NetBackup MSDP client deduplication, clients deduplicate their backup data and then send it directly to the storage server, which writes it to the storage. The network traffic is reduced greatly. See "About NetBackup Client Direct deduplication" on page 27.
NetBackup appliance deduplication	Veritas provides several hardware and a software solutions that include NetBackup deduplication. The NetBackup appliances have their own documentation set: https://www.veritas.com/content/support/en_US/Appliances.html

New MSDP features in NetBackup 8.1.1

Starting from NetBackup 8.1.1, MSDP is now FIPS validated and can be operated in FIPS mode. (See "About MSDP FIPS compliance" on page 232.)

NetBackup incorporates Key Management Server (KMS) with MSDP. KMS is a master server-based symmetric Key Management Service that ensures a secure data path for MSDP. (See "About MSDP Encryption using KMS service" on page 71.)

You can now choose between fixed-length deduplication and variable-length deduplication. In variable-length deduplication, NetBackup processes the data, calculates the size boundaries, and segments the data in variable sizes. Each data segment is assigned a unique ID and NetBackup intelligently evaluates whether any data segment with the same ID exists so that it is not backed up again. Variable-length deduplication improves the deduplication rates, reduces backup storage, improves the backup performance, and lowers the overall cost that is spent on data protection.

The following topic contains more information:

See "About variable-length deduplication on NetBackup clients" on page 195.

Chapter 2

Planning your deployment

This chapter includes the following topics:

- Planning your MSDP deployment
- NetBackup naming conventions
- About MSDP deduplication nodes
- About the NetBackup deduplication destinations
- About MSDP storage capacity
- About MSDP storage and connectivity requirements
- About NetBackup media server deduplication
- About NetBackup Client Direct deduplication
- About MSDP remote office client deduplication
- About the NetBackup Deduplication Engine credentials
- About the network interface for MSDP
- About MSDP port usage
- About MSDP optimized synthetic backups
- About MSDP and SAN Client
- About MSDP optimized duplication and replication
- About MSDP performance
- About MSDP stream handlers
- MSDP deployment best practices

Planning your MSDP deployment

Table 2-1 provides an overview of planning your deployment of NetBackup deduplication.

Table 2-1 Deployment overview

Step	Deployment task	Where to find the information
Step 1	Learn about deduplication nodes and storage destinations	See "About MSDP deduplication nodes" on page 17. See "About the NetBackup deduplication destinations" on page 17.
Step 2	Understand the storage capacity and requirements	See "About MSDP storage capacity" on page 18. See "About MSDP storage and connectivity requirements" on page 19.
Step 3	Determine which type of deduplication to use	See "About NetBackup media server deduplication" on page 22. See "About NetBackup Client Direct deduplication" on page 27. See "About MSDP remote office client deduplication" on page 29.
Step 4	Determine the requirements for deduplication hosts	See "About MSDP storage servers" on page 24. See "About MSDP server requirements" on page 25. See "About MSDP client deduplication requirements and limitations" on page 28. See "About the network interface for MSDP" on page 31. See "About MSDP port usage" on page 32. See "About scaling MSDP" on page 36. See "About MSDP performance" on page 34.
Step 5	Determine the credentials for deduplication	See "About the NetBackup Deduplication Engine credentials" on page 30.
Step 6	Read about compression and encryption	See "About MSDP compression" on page 121. See "About MSDP encryption" on page 123.
Step 7	Read about optimized synthetic backups	See "About MSDP optimized synthetic backups" on page 33.
Step 8	Read about deduplication and SAN Client	See "About MSDP and SAN Client" on page 33.
Step 9	Read about optimized duplication and replication	See "About MSDP optimized duplication and replication" on page 34.
Step 10	Read about stream handlers	See "About MSDP stream handlers" on page 35.

Table 2-1 Deployment overview *(continued)*

Step	Deployment task	Where to find the information
Step 11	Read about best practices for implementation	See "MSDP deployment best practices" on page 36.
Step 12	Determine the storage requirements and provision the storage	See "About provisioning the storage for MSDP" on page 42. See "About MSDP storage and connectivity requirements" on page 19. See "About MSDP storage capacity" on page 18. See "MSDP storage path properties" on page 88.
Step 13	License MSDP	See "About the MSDP license" on page 46. See "Licensing NetBackup MSDP" on page 47.
Step 14	Configure MSDP	See "Configuring MSDP server-side deduplication" on page 50. See "Configuring MSDP client-side deduplication" on page 53.
Step 15	Migrate from other storage to NetBackup deduplication	See "Migrating from another storage type to MSDP" on page 387.

NetBackup naming conventions

NetBackup has rules for naming logical constructs, such as clients, disk pools, backup policies, storage lifecycle policies, and so on. Generally, names are case-sensitive. The following set of characters can be used in user-defined names and passwords:

- Alphabetic (A-Z a-z) (names are case-sensitive)
- Numeric (0-9)
- Period (.)
- Plus (+)
- Minus (-)
  Do not use a minus as the first character.
- Underscore (_)

Note: No spaces are allowed.

The naming conventions for the NetBackup Deduplication Engine differ from these NetBackup naming conventions.

See “About the NetBackup Deduplication Engine credentials” on page 30.

About MSDP deduplication nodes

A media server deduplication node comprises the following:

Storage server	The storage server deduplicates the backups, writes the data to the storage, and manages the storage. See “About MSDP storage servers” on page 24.
Load balancing servers	Load balancing servers assist the storage server by deduplicating backups. Load balancing servers are optional. See “About MSDP load balancing servers” on page 25.
Storage	See “About the NetBackup deduplication destinations” on page 17.
Clients	The clients may include the clients that deduplicate their own data (Client Direct). See “About NetBackup Client Direct deduplication” on page 27.

Multiple media server deduplication nodes can exist. Nodes cannot share servers or storage.

Each node manages its own storage. Deduplication within each node is supported; deduplication between nodes is not supported.

See “About NetBackup media server deduplication” on page 22.

See “About MSDP storage servers” on page 24.

About the NetBackup deduplication destinations

Several destinations exist for the NetBackup deduplication, as shown in the following table.

Table 2-2 NetBackup deduplication storage destinations

Destination	Description
Media Server Deduplication Pool	A NetBackup **Media Server Deduplication Pool** represents the disk storage that is attached to a NetBackup media server. NetBackup deduplicates the data and hosts the storage. If you use this destination, use this guide to plan, implement, configure, and manage deduplication and the storage. When you configure the storage server, select **Media Server Deduplication Pool** as the storage type. The **Media Server Deduplication Pool** can be hosted on the following systems: ■ A NetBackup media server. ■ A NetBackup 5200 series appliance or NetBackup 5300 series appliance.
PureDisk Deduplication Pool	A NetBackup **PureDisk Deduplication Pool** represents a storage pool on a NetBackup 5000 series appliance. NetBackup deduplicates the data, and the NetBackup 5000 series appliance hosts the storage. **Note:** NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only. If you use a NetBackup 5000 series appliance for storage, use the following documentation: ■ The NetBackup 5000 series appliance documentation to plan, implement, configure, and manage the appliance, which includes the storage: http://www.veritas.com/docs/TECH145661 ■ This guide to configure backups and deduplication in NetBackup. When you configure the storage server, select **PureDisk Deduplication Pool** as the storage type.

About MSDP storage capacity

The following table describes the maximum deduplication storage capacity for a single **Media Server Deduplication Pool**:

Table 2-3 Maximum MSDP storage capacities

Maximum capacity	Description
64 TBs	For all supported systems, NetBackup supports up to 64 TBs of storage in a single **Media Server Deduplication Pool**. See "About provisioning the storage for MSDP" on page 42.
96 TBs	NetBackup supports 96 TBs of storage in a new **Media Server Deduplication Pool** on the supported versions of the following operating systems: ■ Red Hat Linux ■ SUSE Linux See "About provisioning the storage for MSDP" on page 42.

NetBackup reserves 4 percent of the storage space for the deduplication database and transaction logs. Therefore, a storage full condition is triggered at a 96-percent threshold. If you use separate storage for the deduplication database, NetBackup still uses the 96-percent threshold to protect the data storage from any possible overload.

If your storage requirements exceed the capacity of a **Media Server Deduplication Pool**, you can use more than one media server deduplication node.

See "About MSDP deduplication nodes" on page 17.

For the operating system versions that NetBackup supports for deduplication, see the NetBackup operating system compatibility list available through the following URL:

http://www.netbackup.com/compatibility

About MSDP storage and connectivity requirements

The following subsections describe the storage and the connectivity requirements for the NetBackup Media Server Deduplication Option.

Storage media

The following are the minimum requirements for single stream read or write performance for each disk volume. Greater individual data stream capability or aggregate capability may be required to satisfy your objectives for writing to and reading from disk.

Up to 32 TBs of storage	130 MB/sec. 200 MB/sec for enterprise-level performance.
32 to 48 TBs of storage	200 MB/sec. Veritas recommends that you store the data and the deduplication database on separate disk volumes, each with 200 MB/sec read or write speed. Neither should be stored on the system disk.
48 to 64 TBs of storage	250 MB/sec. Veritas recommends that you store the data and the deduplication database on separate disk volumes, each with 250 MB/sec read or write speed. Neither should be stored on the system disk.
96 TBs of storage	250 MB/sec. 96 TBs of storage require four separate volumes, each with 250 MB/sec read or write speed. You cannot use the system disk of the storage server host for any of the required volumes.

Local disk storage may leave you vulnerable in a disaster. SAN disk can be remounted at a newly provisioned server with the same name.

NetBackup requires the exclusive use of the disk resources. If the storage is also used for purposes other than backups, NetBackup cannot manage disk pool capacity or manage storage lifecycle policies correctly. Therefore, NetBackup must be the only entity that uses the storage.

NetBackup **Media Server Deduplication Pool** does not support the following storage types for deduplication storage:

- Network Attached Storage (that is, file based storage protocols) such as CIFS or NFS.
- The ZFS file system.

The NetBackup compatibility lists are the definitive source for supported operating systems, computers, and peripherals. See the compatibility lists available at the following website:

http://www.netbackup.com/compatibility

The storage must be provisioned and operational before you can configure deduplication in NetBackup.

See “About provisioning the storage for MSDP” on page 42.

Storage connection

The storage must be direct-attached storage (DAS), internal disks, or connected by a dedicated, low latency storage area network (Fibre Channel or iSCSI).

A storage area network should conform to the following criteria:

Latency	Maximum 0.1-millisecond latency per round trip.
Bandwidth	Enough bandwidth on the storage network to satisfy your throughput objectives. Veritas supports iSCSI on storage networks with at least 10-Gigabit Ethernet network bandwidth. Veritas recommends the Fibre Channel storage networks with at least 4-Gigabit network bandwidth.
HBAs	The storage server should have an HBA or HBAs dedicated to the storage. Those HBAs must have enough bandwidth to satisfy your throughput objectives.

See "Fibre Channel and iSCSI comparison for MSDP" on page 21.

Fibre Channel and iSCSI comparison for MSDP

Deduplication is a CPU and memory intensive process. It also requires dedicated and high-speed storage connectivity for the best performance. That connectivity helps to ensure the following:

- Consistent storage performance.
- Reduced packet loss during network congestion.
- Reduced storage deadlocks.

The following table compares both the Fibre Channel and the iSCSI characteristics that affect deduplication storage performance. By design, Fibre Channel provides the greatest opportunity to meet performance objectives. To achieve the results that are required for NetBackup MSDP storage, iSCSI may require other optimizations that are described in the following table.

Table 2-4 Fibre Channel and iSCSI characteristics

Item	Fibre Channel	iSCSI
Genesis	Storage networking architecture that is designed to handle the same block storage format that storage devices use.	Storage network protocol that is built on top of TCP/IP to use the same wiring as the rest of the enterprise.

Table 2-4 Fibre Channel and iSCSI characteristics *(continued)*

Item	Fibre Channel	iSCSI
Protocol	FCP is a thin, single-purpose protocol that provides lossless, in-order frame delivery and low switch latency.	iSCSI is a multiple layer implementation that facilitates data transfers over intranets and long distances. The SCSI protocol expects lossless, in-order delivery, but iSCSI uses TCP/IP, which experiences packet loss and out-of-order delivery.
Host CPU load	Low. Fibre Channel frame processing is offloaded to dedicated low-latency HBAs.	Higher. Most iSCSI implementations use the host processor to create, send, and interpret storage commands. Therefore, Veritas requires dedicated network interfaces on the storage server to reduce storage server load and reduce latency.
Latency	Low.	Higher.
Flow control	A built-in flow control mechanism that ensures data is sent to a device when it is ready to accept it.	No built-in flow control. Veritas recommends that you use the Ethernet priority-based flow control as defined in the IEEE 802.1Qbb standard.
Deployment	Difficult.	Easier than Fibre Channel, but more difficult to deploy to meet the criteria for MSDP. The required dedicated network interfaces add to deployment difficult. Other optimizations for carrying storage traffic also add to deployment difficult. Other optimizations include flow control, jumbo framing, and multi-path I/O.

Although Veritas supports iSCSI for connectivity to **Media Server Deduplication Pool** storage, Veritas recommends Fibre Channel. Veritas believes that Fibre Channel provides better performance and stability than iSCSI. iSCSI instability may manifest as status 83 and status 84 error messages.

See “MSDP media open error (83)” on page 363.

See “MSDP media write error (84)” on page 365.

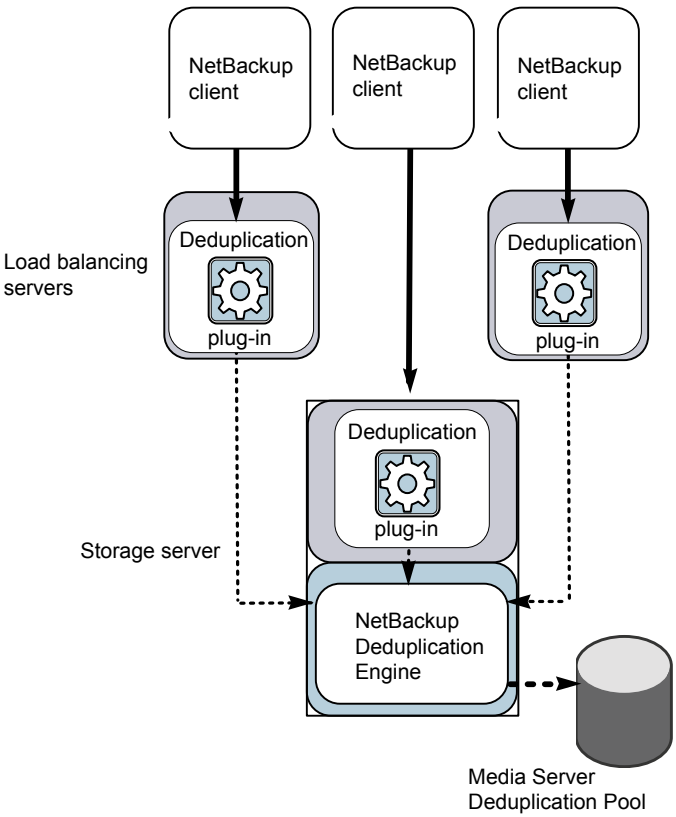
About NetBackup media server deduplication

With media server deduplication, the NetBackup client software creates the image of backed up files as for a normal backup. The client sends the backup image to a media server, which hosts the plug-in that duplicates the backup data. The media

server can be the storage server or a load balancing server if one is configured. The deduplication plug-in breaks the backup image into segments and compares the segments to all of the segments that are stored in that deduplication node. The plug-in then sends only the unique segments to the NetBackup Deduplication Engine on the storage server. The Deduplication Engine writes the data to a **Media Server Deduplication Pool**.

Figure 2-1 shows NetBackup media server deduplication. The deduplication storage server is a media server on which the deduplication core components are enabled. The storage destination is a **Media Server Deduplication Pool**.

Figure 2-1 NetBackup media server deduplication



More detailed information is available.

See “About MSDP deduplication nodes” on page 17.

See “About MSDP storage servers” on page 24.

See “About MSDP load balancing servers” on page 25.

See “About MSDP server requirements” on page 25.

See “About MSDP unsupported configurations” on page 27.

See “MSDP server components” on page 331.

See “Media server deduplication backup process” on page 334.

About MSDP storage servers

A storage server is an entity that writes to and reads from the storage. One host functions as the storage server, and only one storage server exists for each NetBackup deduplication node. The host must be a NetBackup media server. Although the storage server components run on a media server, the storage server is a separate logical entity.

See “About MSDP deduplication nodes” on page 17.

The MSDP storage server does the following:

- Receives the backups from clients and then deduplicates the data.
- Receives the deduplicated data from clients or from other media servers.
  You can configure NetBackup clients and other NetBackup media servers to deduplicate data also. In which case, the storage server only receives the data after it is deduplicated.
  See “About NetBackup Client Direct deduplication” on page 27.
  See “About MSDP load balancing servers” on page 25.
- Writes the deduplicated data to and reads the deduplicated data from the disk storage.
- Manages that storage.
- Manages the deduplication processes.

How many storage servers (and by extension, nodes) you configure depends on your storage requirements. It also depends on whether or not you use optimized duplication or replication, as follows:

- Optimized duplication in the same domain requires at least two deduplication nodes in the same domain. The following are the required storage servers:
  - One for the backup storage, which is the source for the duplication operations.
  - Another to store the copies of the backup images, which are the target for the duplication operations.

  See “About MSDP optimized duplication within the same domain” on page 135.

- Auto Image Replication to another domain requires the following storage servers:
  - One for the backups in the originating NetBackup domain. This storage server writes the NetBackup client backups to the storage. It is the source for the duplication operations.
  - Another in the remote NetBackup domain for the copies of the backup images. This storage server is the target for the duplication operations that run in the originating domain.

  See "About NetBackup Auto Image Replication" on page 153.

About MSDP load balancing servers

You can configure other NetBackup media servers to help deduplicate data. They perform file fingerprint calculations for deduplication, and they send the unique data segments to the storage server. These helper media servers are called load balancing servers.

A NetBackup media server becomes a load balancing server when two things occur:

- You enable the media server for deduplication load balancing duties.
  You do so when you configure the storage server or later by modifying the storage server properties.
- You select it in the storage unit for the deduplication pool.

See "Introduce MSDP load balancing servers gradually" on page 38.

Load balancing servers also perform restore and duplication jobs.

Load balancing servers can be any supported server type for deduplication. They do not have to be the same type as the storage server.

Note: Load balancing for CloudCatalyst storage servers or CloudCatalyst appliances is supported. See the following topic for configuration considerations.

See "Configuring push or pull optimized duplication for CloudCatalyst" on page 256.

About MSDP server requirements

The host computer's CPU and memory constrain how many jobs can run concurrently. The storage server requires enough capability for deduplication and for storage management unless you offload some of the deduplication to load balancing servers.

Table 2-5 shows the minimum requirements for MSDP servers. NetBackup deduplication servers are always NetBackup media servers.

Processors for deduplication should have a high clock rate and high floating point performance. Furthermore, high throughput per core is desirable. Each backup stream uses a separate core.

Intel and AMD have similar performance and perform well on single core throughput.

Newer SPARC processors, such as the SPARC64 VII, provide the single core throughput that is similar to AMD and Intel. Alternatively, UltraSPARC T1 and T2 single core performance does not approach that of the AMD and Intel processors. Tests show that the UltraSPARC processors can achieve high aggregate throughput. However, they require eight times as many backup streams as AMD and Intel processors to do so.

Table 2-5 MSDP server minimum requirements

Component	Storage server	Load balancing server
CPU	Veritas recommends at least a 2.2-GHz clock rate. A 64-bit processor is required. At least four cores are required. Veritas recommends eight cores. For 64 TBs of storage, Intel x86-64 architecture requires eight cores.	Veritas recommends at least a 2.2-GHz clock rate. A 64-bit processor is required. At least two cores are required. Depending on throughput requirements, more cores may be helpful.
RAM		4 GBs.
Operating system	The operating system must be a supported 64-bit operating system. See the operating system compatibility list for your NetBackup release on the Veritas Support website. http://www.netbackup.com/compatibility	The operating system must be a supported 64-bit operating system. See the operating system compatibility list for your NetBackup release on the following website. http://www.netbackup.com/compatibility

A Veritas tech note provides detailed information about and examples for sizing the hosts for deduplication. Information includes the number of the NICs or the HBAs for each server to support your performance objectives.

Note: In some environments, a single host can function as both a NetBackup master server and as a deduplication server. Such environments typically run fewer than 100 total backup jobs a day. (Total backup jobs means backups to any storage destination, including deduplication and non-deduplication storage.) If you perform more than 100 backups a day, deduplication operations may affect master server operations.

See “About MSDP performance” on page 34.

See "About MSDP queue processing" on page 303.

About MSDP unsupported configurations

The following items describe some configurations that are not supported:

- NetBackup media server deduplication and Veritas Backup Exec deduplication cannot reside on the same host. If you use both NetBackup and Backup Exec deduplication, each product must reside on a separate host.
- NetBackup does not support clustering of deduplication storage servers or load balancing servers.
- Deduplication within each media server deduplication node is supported; global deduplication between nodes is not supported.

About NetBackup Client Direct deduplication

With NetBackup Client Direct deduplication (also known as *client-side deduplication*), the client hosts the plug-in that duplicates the backup data. The NetBackup client software creates the image of backed up files as for a normal backup. Next, the deduplication plug-in breaks the backup image into segments and compares the segments to all of the segments that are stored in that deduplication node. The plug-in then sends only the unique segments to the NetBackup Deduplication Engine on the storage server. The engine writes the data to a **Media Server Deduplication Pool**.

Client deduplication does the following:

- Reduces network traffic. The client sends only unique file segments to the storage server. Duplicate data is not sent over the network.
- Distributes some deduplication processing load from the storage server to clients. (NetBackup does not balance load between clients; each client deduplicates its own data.)

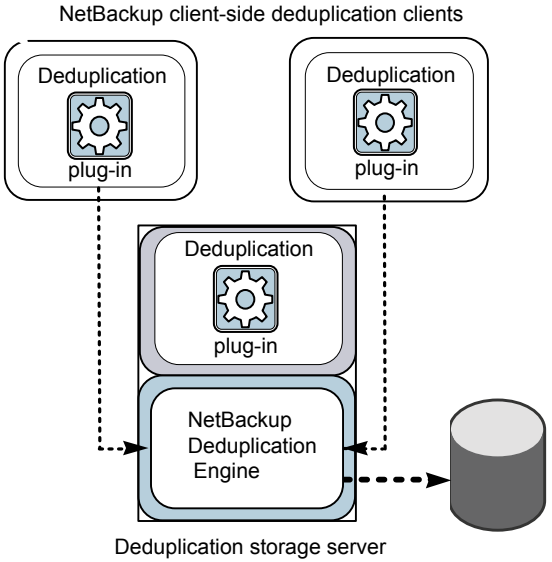
NetBackup Client Deduplication is a solution for the following cases:

- Remote office or branch office backups to the data center.
  NetBackup provides resilient network connections for remote office backups.
  See "About MSDP remote office client deduplication" on page 29.
- LAN connected file server
- Virtual machine backups.

Client-side deduplication is also a useful solution if a client host has unused CPU cycles or if the storage server or load balancing servers are overloaded.

Figure 2-2 shows client deduplication. The deduplication storage server is a media server on which the deduplication core components are enabled. The storage destination is a **Media Server Deduplication Pool**

Figure 2-2 NetBackup client deduplication



More information is available.

See "About MSDP client deduplication requirements and limitations" on page 28.

See "About MSDP remote office client deduplication" on page 29.

See "MSDP client components" on page 337.

See "MSDP client–side deduplication backup process" on page 337.

About MSDP client deduplication requirements and limitations

The clients that deduplicate their own data and the master server must use the same name to resolve the storage server. The name must be the host name under which the NetBackup Deduplication Engine credentials were created. If they do not use the same name, backups fail. In some environments, careful configuration may be required to ensure that the client and the master server use the same name for the storage server. Such environments include those that use VLAN tagging and those that use multi-homed hosts.

NetBackup does not support the following for client-side deduplication:

- Multiple copies per job. For the jobs that specify multiple copies, the backup images are sent to the storage server and may be deduplicated there. Multiple copies are configured in a NetBackup backup policy.
- NDMP hosts. The backup jobs fail if you try to use client-side deduplication for NDMP hosts.

For the systems on which NetBackup supports client-side deduplication, see the NetBackup compatibility lists at the following URL:

http://www.netbackup.com/compatibility

The clients that deduplicate their own data conform to the standard NetBackup release level compatibility. The *NetBackup Release Notes* for each release defines the compatibility between NetBackup releases. To take advantage of any new features, improvements, and fixes, Veritas recommends that the clients and the servers be at the same release and revision.

The *NetBackup Release Notes* is available through the following URL:

http://www.veritas.com/docs/DOC5332

About MSDP remote office client deduplication

WAN backups require more time than local backups in your own domain. WAN backups have an increased risk of failure when compared to local backups. To help facilitate WAN backups, NetBackup provides the capability for resilient network connections. A resilient connection allows backup and restore traffic between a client and NetBackup media servers to function effectively in high-latency, low-bandwidth networks such as WANs.

The use case that benefits the most from resilient connections is client-side deduplication at a remote office that does not have local backup storage. The following items describe the advantages:

- Client deduplication reduces the time that is required for WAN backups by reducing the amount of data that must be transferred.
- The resilient connections provide automatic recovery from network failures and latency (within the parameters from which NetBackup can recover).

When you configure a resilient connection, NetBackup uses that connection for the backups. Use the NetBackup **Resilient Network** host properties to configure NetBackup to use resilient network connections.

See “Resilient Network properties” on page 188.

See “Specifying resilient connections” on page 192.

The `pd.conf FILE_KEEP_ALIVE_INTERVAL` parameter lets you configure the frequency of keep-alive operations on idle sockets.

See "MSDP pd.conf file parameters" on page 198.

You can improve the performance of the first backup for a remote client.

See "About seeding the MSDP fingerprint cache for remote client deduplication" on page 65.

About MSDP remote client data security

Resilient connection traffic is not encrypted. The NetBackup deduplication process can encrypt the data before it is transmitted over the WAN. Veritas recommends that you use the deduplication encryption to protect your data during your remote client backups.

See "About MSDP encryption" on page 123.

NetBackup does not encrypt the data during a restore job. Therefore, Veritas recommends that you restore data to the original remote client over a private network.

See "How MSDP restores work" on page 314.

About remote client backup scheduling

NetBackup backup policies use the time zone of the master server for scheduling jobs. If your remote clients are in a different time zone than your NetBackup master server, you must compensate for the difference. For example, suppose the master server is in Finland (UTC+2) and the remote client is in London (UTC+0). If the backup policy has a window from 6pm to 6am, backups can begin at 4pm on the client. To compensate, you should set the backup window from 8pm to 8am. Alternatively, it may be advisable to use a separate backup policy for each time zone in which remote clients reside.

About the NetBackup Deduplication Engine credentials

The NetBackup Deduplication Engine requires credentials. The deduplication components use the credentials when they communicate with the NetBackup Deduplication Engine. The credentials are for the deduplication engine, not for the host on which it runs.

You enter the NetBackup Deduplication Engine credentials when you configure the storage server.

The following are the rules for the credentials:

- The user name and the password can be up to 62 characters in length. The user name and the password cannot be empty.
- You can use characters in the printable ASCII range (0x20-0x7E) except for the following characters:
  - Asterisk (*)
  - Backward slash (\) and forward slash (/)
  - Double quote (")
  - Left parenthesis [(] and right parenthesis [)]
  - Less than (<) and greater than (>) sign.
  - Caret sign (^).
  - Percent sign (%).
  - United States dollar sign ($).
  - Spaces.
  - Leading and trailing quotes.

Note: Record and save the credentials in case you need them in the future.

Caution: You cannot change the NetBackup Deduplication Engine credentials after you enter them. Therefore, carefully choose and enter your credentials. If you must change the credentials, contact your Veritas support representative.

About the network interface for MSDP

If the MSDP storage server has more than one network interface, NetBackup uses the default interface for all deduplication traffic. (Deduplication traffic includes backups, restores, duplication, and replication.) The host operating system determines which network interface is the default. However, you can configure the network interface or interfaces that NetBackup uses, as follows:

Configure a specific interface	To use a specific interface, you can enter that interface name when you configure the deduplication storage server. NetBackup uses this interface for all deduplication traffic unless you also configure a separate interface for duplication and replication. See "MSDP network interface properties" on page 91. See "Configuring a storage server for a Media Server Deduplication Pool" on page 73.
Configure an interface for duplication and replication traffic	You can configure a separate network interface for the duplication and the replication traffic. The backup and restore traffic continues to use the default interface or the specific configured interface. See "About a separate network path for MSDP duplication and replication" on page 133. See "Configuring a separate network path for MSDP duplication and replication" on page 134.

The NetBackup `REQUIRED_INTERFACE` setting does not affect deduplication processes.

About MSDP port usage

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

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

Table 2-6 Deduplication ports

Port	Usage
10082	The NetBackup Deduplication Engine (`spoold`). Open this port between the hosts that deduplicate data. Hosts include load balancing servers and the clients that deduplicate their own data.
10102	The NetBackup Deduplication Manager (`spad`). Open this port between the hosts that deduplicate data. Hosts include load balancing servers and the clients that deduplicate their own data.

About MSDP optimized synthetic backups

Optimized synthetic backups are a more efficient form of synthetic backup. A media server uses messages to instruct the storage server which full and incremental backup images to use to create the synthetic backup. The storage server constructs (or synthesizes) the backup image directly on the disk storage. Optimized synthetic backups require no data movement across the network.

The optimized synthetic backup method provides the following benefits:

- Faster than a synthetic backup.
  Regular synthetic backups are constructed on the media server. They are moved across the network from the storage server to the media server and synthesized into one image. The synthetic image is then moved back to the storage server.
- Requires no data movement across the network.
  Regular synthetic backups use network traffic.

See "Configuring optimized synthetic backups for MSDP" on page 132.

In NetBackup, the **OptimizedImage** attribute enables optimized synthetic backups. It applies to both storage servers and deduplication pools. Beginning with NetBackup 7.1, the **OptimizedImage** attribute is enabled by default on storage servers and media server deduplication pools. For the storage servers and the disk pools that you created in NetBackup releases earlier than 7.1, you must set the **OptimizedImage** attribute on them so they support optimized synthetic backups.

See "Setting MSDP storage server attributes" on page 281.

See "Setting a Media Server Deduplication Pool attribute" on page 293.

Table 2-7 MSDP requirements and limitations for optimized synthetic backups

What	Description
Requirements	The target storage unit's deduplication pool must be the same deduplication pool on which the source images reside.
Limitations	NetBackup does not support storage unit groups as a destination for optimized synthetic backups. If NetBackup cannot produce the optimized synthetic backup, NetBackup creates the more data-movement intensive synthetic backup.

About MSDP and SAN Client

SAN Client is a NetBackup optional feature that provides high speed backups and restores of NetBackup clients. Fibre Transport is the name of the NetBackup

high-speed data transport method that is part of the SAN Client feature. The backup and restore traffic occurs over a SAN.

SAN clients can be used with the deduplication option; however, the deduplication must occur on the media server, not the client. Configure the media server to be both a deduplication storage server (or load balancing server) and an FT media server. The SAN client backups are then sent over the SAN to the deduplication server/FT media server host. At that media server, the backup stream is deduplicated.

Do not enable client-side deduplication on SAN Clients. The data processing for deduplication is incompatible with the high-speed transport method of Fibre Transport. Client-side deduplication relies on two-way communication over the LAN with the media server. A SAN client streams the data to the FT media server at a high rate over the SAN.

About MSDP optimized duplication and replication

NetBackup supports several methods for optimized duplication and replication of deduplicated data.

The following table lists the duplication methods NetBackup supports between media server deduplication pools.

Table 2-8 NetBackup OpenStorage optimized duplication and replication methods

Optimized duplication method	Description
Within the same NetBackup domain	See "About MSDP optimized duplication within the same domain" on page 135.
To a remote NetBackup domain	See "About NetBackup Auto Image Replication" on page 153.

About MSDP performance

Many factors affect performance, especially the server hardware and the network capacity.

Table 2-9 provides information about performance during backup jobs for a deduplication storage server. The deduplication storage server conforms to the minimum host requirements. Client deduplication or load balancing servers are not used.

See "About MSDP server requirements" on page 25.

Table 2-9 MSDP job load performance for an MSDP storage server

When	Description
Normal operation	Normal operation is when all clients have been backed up once. Approximately 15 to 20 jobs can run concurrently and with high performance under the following conditions: ■ The hardware meets minimum requirements. (More capable hardware improves performance.) ■ No compression. If data is compressed, the CPU usage increases quickly, which reduces the number of concurrent jobs that can be handled. ■ The deduplication rate is between 50% and 100%. The deduplication rate is the percentage of data already stored so it is not stored again. ■ The amount of data that is stored is between 30% to 90% of the capacity of the storage.
Storage approaches full capacity	NetBackup maintains the same number of concurrent backup jobs as during normal operation under the following conditions: ■ The hardware meets minimum requirements. (More capable hardware improves performance.) ■ The amount of data that is stored is between 85% to 90% of the capacity of the storage. However, the average time to complete the jobs increases significantly.

How file size may affect the MSDP deduplication rate

The small file sizes that are combined with large file segment sizes may result in low initial deduplication rates. However, after the deduplication engine performs file fingerprint processing, deduplication rates improve. For example, a second backup of a client shortly after the first does not show high deduplication rates. But the deduplication rate improves if the second backup occurs after the file fingerprint processing.

How long it takes the NetBackup Deduplication Engine to process the file fingerprints varies.

About MSDP stream handlers

NetBackup provides the stream handlers that process various backup data stream types. Stream handlers improve backup deduplication rates by processing the underlying data stream.

For data that has already been deduplicated, the first backup with a new stream handler produces a lower deduplication rate. After that first backup, the deduplication rate should surpass the rate from before the new stream handler was used.

Veritas continues to develop additional stream handlers to improve backup deduplication performance.

MSDP deployment best practices

Because Veritas recommends minimum host and network requirements only, deduplication performance may vary greatly depending on your environment. Veritas provides best-practice guidelines to help you use deduplication effectively regardless of the capabilities of your hosts.

Veritas recommends that you consider the following practices when you implement NetBackup deduplication.

Use fully qualified domain names

Veritas recommends that you use fully qualified domain names for your NetBackup servers (and by extension, your deduplication servers). Fully qualified domain names can help to avoid host name resolution problems, especially if you use client-side deduplication.

Deduplication servers include the storage server and the load balancing servers (if any).

See “MSDP media write error (84)” on page 365.

About scaling MSDP

You can scale deduplication processing to improve performance by using load balancing servers or client deduplication or both.

If you configure load balancing servers, those servers also perform deduplication. The deduplication storage server still functions as both a deduplication server and as a storage server. NetBackup uses standard load balancing criteria to select a load balancing server for each job. However, deduplication fingerprint calculations are not part of the load balancing criteria.

To completely remove the deduplication storage server from deduplication duties, do the following for every storage unit that uses the deduplication disk pool:

- Select **Only use the following media servers.**
- Select all of the load balancing servers but do not select the deduplication storage server.

The deduplication storage server performs storage server tasks only: storing and managing the deduplicated data, file deletion, and optimized duplication.

If you configure client deduplication, the clients deduplicate their own data. Some of the deduplication load is removed from the deduplication storage server and loading balancing servers.

Veritas recommends the following strategies to scale MSDP:

- For the initial full backups of your clients, use the deduplication storage server. For subsequent backups, use load balancing servers.
- Enable client-side deduplication gradually.
  If a client cannot tolerate the deduplication processing workload, be prepared to move the deduplication processing back to a server.

Send initial full backups to the storage server

If you intend to use load balancing servers or client deduplication, use the storage server for the initial full backups of the clients. Then, send subsequent backups through the load balancing servers or use client deduplication for the backups. Doing so provides information about the total deduplication load. You can then allocate jobs to best balance the load among your hosts.

Deduplication uses the same fingerprint list regardless of which host performs the deduplication. So you can deduplicate data on the storage server first, and then subsequent backups by another host use the same fingerprint list. If the deduplication plug-in can identify the last full backup for the client and the policy combination, it retrieves the fingerprint list from the server. The list is placed in the fingerprint cache for the new backup.

See “About MSDP fingerprinting” on page 62.

Veritas also recommends that you implement load balancing servers and client deduplication gradually. Therefore, it may be beneficial to use the storage server for backups while you implement deduplication on other hosts.

Increase the number of MSDP jobs gradually

Veritas recommends that you increase the **Maximum concurrent jobs** value gradually. (The **Maximum concurrent jobs** is a storage unit setting.) Doing so provides information about the total deduplication load. The initial backup jobs (also known as initial seeding) require more CPU and memory than successive jobs. After initial seeding, the storage server can process more jobs concurrently. You can then gradually increase the jobs value over time.

See “About MSDP performance” on page 34.

Introduce MSDP load balancing servers gradually

Veritas recommends that you add load balancing servers only after the storage server reaches maximum CPU utilization. Then, introduce load balancing servers one at a time. It may be easier to evaluate how your environment handles traffic and easier to troubleshoot any problems with fewer hosts added for deduplication.

Many factors affect deduplication server performance.

See "About MSDP performance" on page 34.

Because of the various factors, Veritas recommends that you maintain realistic expectations about using multiple servers for deduplication. If you add one media server as a load balancing server, overall throughput should be faster. However, adding one load balancing server may not double the overall throughput rate, adding two load balancing servers may not triple the throughput rate, and so on.

If all of the following apply to your MSDP environment, your environment may be a good candidate for load balancing servers:

- The deduplication storage server is CPU limited on any core.
- Memory resources are available on the storage server.
- Network bandwidth is available on the storage server.
- Back-end I/O bandwidth to the deduplication pool is available.
- Other NetBackup media servers have CPU available for deduplication.

Gigabit Ethernet should provide sufficient performance in many environments. If your performance objective is the fastest throughput possible with load balancing servers, you should consider 10 Gigabit Ethernet.

Implement MSDP client deduplication gradually

If you configure clients to deduplicate their own data, do not enable all of those clients at the same time. Implement client deduplication gradually, as follows:

- Use the storage server for the initial backup of the clients.
- Enable deduplication on only a few clients at a time.
  Doing so provides information about deduplication affects the clients other jobs. It also may be easier to evaluate how your environment handles traffic and easier to troubleshoot any problems

If a client cannot tolerate the deduplication processing workload, be prepared to move the deduplication processing back to the storage server.

Use MSDP compression and encryption

Do not use compression or encryption in a NetBackup policy; rather, use the compression or the encryption that is part of the deduplication process.

See "About MSDP compression" on page 121.

See "About MSDP encryption" on page 123.

About the optimal number of backup streams for MSDP

A backup stream appears as a separate job in the NetBackup Activity Monitor. Various methods exist to produce streams. In NetBackup, you can use backup policy settings to configure multiple streams. The NetBackup for Oracle agent lets you configure multiple streams; also for Oracle the RMAN utilities can provide multiple backup channels.

For client deduplication, the optimal number of backup streams is two.

Media server deduplication can process multiple streams on multiple cores simultaneously. For large datasets in applications such as Oracle, media server deduplication leverages multiple cores and multiple streams. Therefore, media server deduplication may be a better solution when the application can provide multiple streams or channels.

More detailed information about backup streams is available.

http://www.veritas.com/docs/TECH77575

About storage unit groups for MSDP

You can use a storage unit group as a backup destination for NetBackup MSDP. All of the storage units in the group must have a **Media Server Deduplication Pool** as the storage destination.

Storage unit groups avoid a single point of failure that can interrupt backup service.

The best storage savings occur when a backup policy stores its data in the same deduplication destination disk pool instead of across multiple disk pools. For this reason, the **Failover** method for the **Storage unit selection** uses the least amount of storage. All of the other methods are designed to use different storage every time the backup runs. Veritas recommends that you select the **Failover** method for the **Storage unit selection** type.

Table 2-10 MSDP requirements and limitations for storage unit groups

What	Description
Requirements	A group must contain storage units of one storage destination type only. That is, a group cannot contain both **Media Server Deduplication Pool** storage units and storage units with other storage types.
Limitations	NetBackup does not support the following for storage unit groups: ■ Optimized duplication of deduplicated data. If you use a storage unit group as a destination for optimized duplication of deduplicated data, NetBackup uses regular duplication. See "About MSDP optimized duplication within the same domain" on page 135. ■ Optimized synthetic backups. If NetBackup cannot produce the optimized synthetic backup, NetBackup creates the more data-movement intensive synthetic backup. See "About MSDP optimized synthetic backups" on page 33.

About protecting the MSDP data

Veritas recommends the following methods to protect the deduplicated backup data:

- Use NetBackup optimized duplication to copy the images to another deduplication node at an off-site location.
  Optimized duplication copies the primary backup data to another deduplication pool. It provides the easiest, most efficient method to copy data off-site yet remain in the same NetBackup domain. You then can recover from a disaster that destroys the storage on which the primary copies reside by retrieving images from the other deduplication pool.
  See "Configuring MSDP optimized duplication within the same NetBackup domain" on page 143.
- Use NetBackup replication to copy the deduplicated data to another NetBackup domain off-site.
  See "Configuring MSDP replication to a different NetBackup domain" on page 152.

Veritas also recommends that you back up the MSDP catalog.

See "About protecting the MSDP catalog" on page 221.

Save the MSDP storage server configuration

Veritas recommends that you save the storage server configuration. Getting and saving the configuration can help you with recovery of your environment. For disaster

recovery, you may need to set the storage server configuration by using a saved configuration file.

If you save the storage server configuration, you must edit it so that it includes only the information that is required for recovery.

See "About saving the MSDP storage server configuration" on page 215.

See "Saving the MSDP storage server configuration" on page 216.

See "Editing an MSDP storage server configuration file" on page 217.

Plan for disk write caching

Storage components may use hardware caches to improve read and write performance. Among the storage components that may use a cache are disk arrays, RAID controllers, or the hard disk drives themselves.

If your storage components use caches for disk write operations, ensure that the caches are protected from power fluctuations or power failure. If you do not protect against power fluctuations or failure, data corruption or data loss may occur.

Protection can include the following:

- A battery backup unit that supplies power to the cache memory so write operations can continue if power is restored within sufficient time.
- An uninterruptible power supply that allows the components to complete their write operations.

If your devices that have caches are not protected, Veritas recommends that you disable the hardware caches. Read and write performance may decline, but you help to avoid data loss.

Chapter 3

Provisioning the storage

This chapter includes the following topics:

- About provisioning the storage for MSDP
- Do not modify MSDP storage directories and files
- About adding additional MSDP storage
- About volume management for NetBackup MSDP

About provisioning the storage for MSDP

NetBackup requires that the storage is exposed as a directory path.

Provision the storage as follows:

Up to 64 TBs	See Up to 64 TBs of storage.
96 TBs	See 96-TBs of storage.

How many storage instances you provision depends on your storage requirements for your backups. If your requirements are greater than one deduplication node can accommodate, you can configure more than one node.

See “About MSDP deduplication nodes” on page 17.

Optimized duplication and replication also can affect the number of nodes you provison.

See “About MSDP optimized duplication and replication” on page 34.

Other NetBackup requirements may affect how you provision the storage.

See “About MSDP storage and connectivity requirements” on page 19.

How to provision the storage is beyond the scope of the NetBackup documentation. Consult the storage vendor's documentation.

See “About the NetBackup deduplication destinations” on page 17.

See “Planning your MSDP deployment” on page 15.

Up to 64 TBs of storage

Provision the backup storage so that it appears as a single mount point to the operating system.

Because the storage requires a directory path, do not use only the root node (/) or drive letter (E:\) as the storage path. (That is, do not mount the storage as a root node (/) or a drive letter (E:\).

If you use a separate disk volume for the deduplication database, provision a 1-TB volume on a different mount point than the backup data storage.

96-TBs of storage

NetBackup supports 96 TBs of storage in a single **Media Server Deduplication Pool** on certain operating systems.

See “About MSDP storage capacity” on page 18.

Support requires four separate volumes on the storage server host.

Before you configure the MSDP storage server, you must provision the volumes as described in Table 3-1. Each volume must conform to the following items:

- Formatted with a file system that NetBackup supports for MSDP. The same file system must be used for all volumes.
- Reside on a separate disk from the other volumes that you allocate for the MSDP storage.
- Mounted on a separate mount point on the computer that you want to use as the MSDP storage server
  Veritas recommends that you use a descriptive naming convention for the mount point names.

Table 3-1 Volumes for 96-TB Media Server Deduplication Pool support

Size	Description	Suggested mount point
1 TB	The volume for the MSDP catalog (the deduplication database).	`/msdp/cat`

Table 3-1 Volumes for 96-TB Media Server Deduplication Pool support *(continued)*

Size	Description	Suggested mount point
32 TBs	The first volume for the MSDP storage. This volume contains backup data, configuration files, and log files.	`/msdp/vol0`
32 TBs	The second volume for the MSDP storage. This volume contains backup data.	`/msdp/vol1`
32 TBs	The third volume for the MSDP storage. This volume contains backup data.	`/msdp/vol2`

Do not modify MSDP storage directories and files

Unless you are directed to do so by the NetBackup documentation or by a Veritas support representative, do not do the following:

- Add files to the deduplication storage directories or database directories.
- Delete files from the deduplication storage directories or database directories.
- Modify files in the deduplication storage directories or database directories.
- Move files within the deduplication storage directories or database directories.
- Change the permissions of the directories and files within the deduplication storage directories or database directories.

Failure to follow these directives can result in operational failures and data loss.

About adding additional MSDP storage

The storage for a NetBackup **Media Server Deduplication Pool** is exposed as a single disk volume. You cannot add another volume to an existing **Media Server Deduplication Pool**.

To increase the capacity of a **Media Server Deduplication Pool**, grow the existing volume.

See “Resizing the MSDP storage partition” on page 313.

About volume management for NetBackup MSDP

If you use a tool to manage the volumes for NetBackup **Media Server Deduplication Pool** storage, Veritas recommends that you use the Veritas InfoScale Storage. InfoScale Storage includes the Veritas Volume Manager and the Veritas File System.

For supported systems, see the InfoScale hardware compatibility list at the Veritas website:

http://www.veritas.com/

Note: Although InfoScale Storage supports NFS, NetBackup does not support NFS targets for **Media Server Deduplication Pool** storage. Therefore, **Media Server Deduplication Pool** does not support NFS with InfoScale Storage.

Chapter 4

Licensing deduplication

This chapter includes the following topics:

- About the MSDP license
- Licensing NetBackup MSDP

About the MSDP license

NetBackup deduplication is licensed separately from base NetBackup.

The license enables both NetBackup media server deduplication and NetBackup client deduplication. The license is a front-end capacity license. It is based on the size of the data to be backed up, not on the size of the deduplicated data.

If you remove the license or if it expires, you cannot create new deduplication disk pools. you also cannot create the storage units that reference NetBackup deduplication pools. NetBackup does not delete the disk pools or the storage units that reference the disk pools. You can use them again if you enter a valid license.

The license also enables the **Use Accelerator** feature on the NetBackup policy **Attributes** tab. Accelerator increases the speed of full backups for files systems. Accelerator works with deduplication storage units as well as with other storage units that do not require the deduplication option. More information about Accelerator is available.

See the *NetBackup Administrator's Guide, Volume I*:

http://www.veritas.com/docs/DOC5332

Before you try to install or upgrade to a NetBackup version that supports deduplication, you should determine on which operating systems Veritas supports deduplication. See the NetBackup operating system compatibility list:

http://www.netbackup.com/compatibility

See “Licensing NetBackup MSDP” on page 47.

Licensing NetBackup MSDP

If you installed the license for deduplication when you installed or upgraded NetBackup, you do not need to perform this procedure.

Enter the license on the NetBackup master server. The following procedure describes how to use the **NetBackup Administration Console** to enter the license key.

To license NetBackup MSDP

1. On the **Help** menu of the **NetBackup Administration Console** on the NetBackup master server, select **License Keys**.
2. In the **NetBackup License Keys** dialog box, click **New**.
3. In the **Add a New License Key** dialog box, enter the license key and click **Add** or **OK**.
4. In the **NetBackup License Key** dialog box, click **Close**.
5. Restart all the NetBackup services and daemons.

Chapter 5

Configuring deduplication

This chapter includes the following topics:

- Configuring MSDP server-side deduplication
- Configuring MSDP client-side deduplication
- About the MSDP Deduplication Multi-Threaded Agent
- Configuring the Deduplication Multi-Threaded Agent behavior
- Configuring deduplication plug-in interaction with the Multi-Threaded Agent
- About MSDP fingerprinting
- About the MSDP fingerprint cache
- Configuring the MSDP fingerprint cache behavior
- About seeding the MSDP fingerprint cache for remote client deduplication
- Configuring MSDP fingerprint cache seeding on the client
- Configuring MSDP fingerprint cache seeding on the storage server
- Enabling 96-TB support for MSDP
- About MSDP Encryption using KMS service
- Configuring a storage server for a Media Server Deduplication Pool
- Configuring a storage server for a PureDisk Deduplication Pool
- About disk pools for NetBackup deduplication
- Configuring a disk pool for deduplication
- Creating the data directories for 96-TB MSDP support

- Adding volumes to a 96-TB Media Server Deduplication Pool
- Configuring a Media Server Deduplication Pool storage unit
- Configuring client attributes for MSDP client-side deduplication
- Disabling MSDP client-side deduplication for a client
- About MSDP compression
- About MSDP encryption
- MSDP compression and encryption settings matrix
- Configuring encryption for MSDP backups
- Configuring encryption for MSDP optimized duplication and replication
- About the rolling data conversion mechanism for MSDP
- Modes of rolling data conversion
- MSDP encryption behavior and compatibilities
- Configuring optimized synthetic backups for MSDP
- About a separate network path for MSDP duplication and replication
- Configuring a separate network path for MSDP duplication and replication
- About MSDP optimized duplication within the same domain
- Configuring MSDP optimized duplication within the same NetBackup domain
- About MSDP replication to a different domain
- Configuring MSDP replication to a different NetBackup domain
- About configuring MSDP optimized duplication and replication bandwidth
- About storage lifecycle policies
- About the storage lifecycle policies required for Auto Image Replication
- Creating a storage lifecycle policy
- About MSDP backup policy configuration
- Creating a backup policy
- Resilient Network properties
- Specifying resilient connections

- Adding an MSDP load balancing server
- About variable-length deduplication on NetBackup clients
- About the MSDP pd.conf configuration file
- Editing the MSDP pd.conf file
- About the MSDP contentrouter.cfg file
- About saving the MSDP storage server configuration
- Saving the MSDP storage server configuration
- Editing an MSDP storage server configuration file
- Setting the MSDP storage server configuration
- About the MSDP host configuration file
- Deleting an MSDP host configuration file
- Resetting the MSDP registry
- About protecting the MSDP catalog
- Changing the MSDP shadow catalog path
- Changing the MSDP shadow catalog schedule
- Changing the number of MSDP catalog shadow copies
- Configuring an MSDP catalog backup
- Updating an MSDP catalog backup policy
- About MSDP FIPS compliance

Configuring MSDP server-side deduplication

This topic describes how to configure media server deduplication in NetBackup.

Table 5-1 describes the configuration tasks.

The *NetBackup Administrator's Guide* describes how to configure a base NetBackup environment.

See the *NetBackup Administrator's Guide, Volume I*:

http://www.veritas.com/docs/DOC5332

Table 5-1 MSDP configuration tasks

Step	Task	Procedure
Step 1	Install the license for deduplication	See "Licensing NetBackup MSDP" on page 47.
Step 2	Create NetBackup log file directories on the master server and the media servers	See "NetBackup MSDP log files" on page 347. See "Creating NetBackup log file directories for MSDP" on page 347.
Step 3	Configure the Deduplication Multi-Threaded Agent behavior	The Deduplication Multi-Threaded Agent uses the default configuration values that control its behavior. You can change those values if you want to do so. See "About the MSDP Deduplication Multi-Threaded Agent" on page 54. See "Configuring the Deduplication Multi-Threaded Agent behavior" on page 56. See "Configuring deduplication plug-in interaction with the Multi-Threaded Agent" on page 61.
Step 4	Configure the fingerprint cache behavior	Configuring the fingerprint cache behavior is optional. See "About the MSDP fingerprint cache" on page 63. See "Configuring the MSDP fingerprint cache behavior" on page 64.
Step 5	Enable support for 96-TB MSDP	Before you configure a storage server that hosts a 96-TB **Media Server Deduplication Pool**, you must enable support for that size storage. See "Enabling 96-TB support for MSDP" on page 71.
Step 6	Configure a deduplication storage server	How many storage servers you configure depends on: your storage requirements and on whether or not you use optimized duplication or replication. When you configure a storage server, the wizard also lets you configure a disk pool and a storage unit. See "About MSDP storage servers" on page 24. See "MSDP storage path properties" on page 88. See "About MSDP optimized duplication and replication" on page 34. Which type of storage server to configure depends on the storage destination. See "About the NetBackup deduplication destinations" on page 17. See "Configuring a storage server for a Media Server Deduplication Pool" on page 73.

Table 5-1 MSDP configuration tasks *(continued)*

Step	Task	Procedure
Step 7	Configure a disk pool	If you already configured a disk pool when you configured the storage server, you can skip this step. How many disk pools you configure depends on: your storage requirements and on whether or not you use optimized duplication or replication. See "About disk pools for NetBackup deduplication" on page 101. See "Configuring a disk pool for deduplication" on page 103.
Step 8	Create the data directories for 96-TB support	For a 96-TB **Media Server Deduplication Pool**, you must create the data directories under the mount points for the storage directories. See "Creating the data directories for 96-TB MSDP support" on page 112.
Step 9	Add the other volumes for 96-TB support	For a 96-TB **Media Server Deduplication Pool**, you must add the second and third volumes to the disk pool. See "Adding volumes to a 96-TB Media Server Deduplication Pool" on page 113.
Step 10	Configure a storage unit	See "Configuring a Media Server Deduplication Pool storage unit" on page 115.
Step 11	Enable encryption	Encryption is optional. See "Configuring encryption for MSDP backups" on page 126.
Step 12	Configure optimized synthetic backups	Optimized synthetic backups are optional. See "Configuring optimized synthetic backups for MSDP" on page 132.
Step 13	Configure MSDP restore behavior	Optionally, you can configure NetBackup to bypass media servers during restores. See "How MSDP restores work" on page 314. See "Configuring MSDP restores directly to a client" on page 315.
Step 14	Configure optimized duplication copy	Optimized duplication is optional. See "About MSDP optimized duplication within the same domain" on page 135.
Step 15	Configure replication	Replication is optional. See "About MSDP replication to a different domain" on page 150.

Table 5-1 MSDP configuration tasks *(continued)*

Step	Task	Procedure
Step 16	Configure a backup policy	Use the deduplication storage unit as the destination for the backup policy. If you configured replication, use the storage lifecycle policy as the storage destination. See "About MSDP backup policy configuration" on page 186. See "Creating a backup policy" on page 187.
Step 17	Specify advanced deduplication settings	Advanced settings are optional. See "About the MSDP pd.conf configuration file" on page 197. See "Editing the MSDP pd.conf file" on page 198. See "MSDP pd.conf file parameters" on page 198.
Step 18	Protect the MSDP data and catalog	See "About protecting the MSDP data" on page 40. See "About protecting the MSDP catalog" on page 221.

Configuring MSDP client-side deduplication

This topic describes how to configure client deduplication in NetBackup. Media server deduplication must be configured before you can configure client-side deduplication.

See "Configuring MSDP server-side deduplication" on page 50.

Table 5-2 Client deduplication configuration tasks

Step	Task	Procedure
Step 1	Configure media server deduplication	See "Configuring MSDP server-side deduplication" on page 50.
Step 2	Learn about client deduplication	See "About NetBackup Client Direct deduplication" on page 27.
Step 3	Configure a resilient connection for remote office clients	Resilient connections are optional. See "About MSDP remote office client deduplication" on page 29. See "Resilient Network properties" on page 188. See "Specifying resilient connections" on page 192.
Step 4	Enable client-side deduplication	See "Configuring client attributes for MSDP client-side deduplication" on page 119.

Table 5-2 Client deduplication configuration tasks *(continued)*

Step	Task	Procedure
Step 5	Configure remote client fingerprint cache seeding	Configuring remote client fingerprint cache seeding is optional. See "Configuring MSDP fingerprint cache seeding on the client" on page 67. See "About seeding the MSDP fingerprint cache for remote client deduplication" on page 65. See "Configuring MSDP fingerprint cache seeding on the storage server" on page 68.
Step 6	Configure client-direct restores	Configuring client-direct restores is optional. If you do not do so, restores travel through the NetBackup media server components. See "Configuring MSDP restores directly to a client" on page 315.

About the MSDP Deduplication Multi-Threaded Agent

The MSDP deduplication process can use a Multi-Threaded Agent for most data sources. The Multi-Threaded Agent runs alongside the deduplication plug-in on both the clients and the media servers. The agent uses multiple threads for asynchronous network I/O and CPU core calculations. During a backup, this agent receives data from the deduplication plug-in through shared memory and processes it using multiple threads to improve throughput performance. When inactive, the agent uses minimal resources.

The NetBackup Deduplication Multi-Threaded Agent improves backup performance for any host that deduplicates data: the storage server, load balancing servers, or clients that deduplicate their own data. For each host on which you want to use the Multi-Threaded Agent, you must configure the deduplication plug-in to use it.

The Deduplication Multi-Threaded Agent uses the default configuration values that control its behavior. You can change those values if you want to do so. The following table describes the Multi-Threaded Agent interactions and behaviors. It also provides links to the topics that describe how to configure those interactions and behaviors.

Table 5-3 Interactions and behaviors

Interaction	Procedure
Multi-Threaded Agent behavior and resource usage	See "Configuring the Deduplication Multi-Threaded Agent behavior" on page 56.

Table 5-3 Interactions and behaviors *(continued)*

Interaction	Procedure
Whether or not the deduplication plug-in sends backups to the Multi-Threaded Agent	See "Configuring deduplication plug-in interaction with the Multi-Threaded Agent" on page 61.
The clients that should use the Deduplication Multi-Threaded Agent for backups	See "Configuring deduplication plug-in interaction with the Multi-Threaded Agent" on page 61.
The backup policies that should use the Deduplication Multi-Threaded Agent	See "Configuring deduplication plug-in interaction with the Multi-Threaded Agent" on page 61.

Table 5-4 describes the operational notes for MSDP multithreading. If the Multi-Threaded Agent is not used, NetBackup uses the single-threaded mode.

Table 5-4 Multi-Threaded Agent requirements and limitations

Item	Description
Supported systems	NetBackup supports the Multi-Threaded Agent on Linux, Solaris, and Windows operating systems.
Unsupported use cases	NetBackup does not use the Multi-Threading Agent for the following use cases: ■ Virtual synthetic backups ■ NetBackup Accelerator ■ `SEGKSIZE` is greater than 128 (`pd.conf` file) ■ `DONT_SEGMENT_TYPES` enabled (`pd.conf` file) ■ `MATCH_PDRO = 1` (`pd.conf` file) See "MSDP pd.conf file parameters" on page 198.
Policy-based compression or encryption	If NetBackup policy-based compression or encryption is enabled on the backup policy, NetBackup does not use the Deduplication Multi-Threaded Agent. Veritas recommends that you use the MSDP compression and encryption rather than NetBackup policy-based compression and encryption. See "About MSDP compression" on page 121. See "About MSDP encryption" on page 123.

Configuring the Deduplication Multi-Threaded Agent behavior

The `mtstrm.conf` configuration file controls the behavior of the NetBackup Deduplication Multi-Threaded Agent.

See "About the MSDP Deduplication Multi-Threaded Agent" on page 54.

If you change the `mtstrm.conf` file on a host, it changes the settings for that host only. If you want the same settings for all of the hosts that deduplicate data, you must change the `mtstrm.conf` file on all of the hosts.

To configure the Multi-Threaded Agent behavior

1. Use a text editor to open the `mtstrm.conf` file.

   The `mtstrm.conf` file resides in the following directories:

   - UNIX: `/usr/openv/lib/ost-plugins/`
   - Windows: *`install_path`*`\Veritas\NetBackup\bin\ost-plugins`

2. To change a behavior, specify a new value.

   See "MSDP mtstrm.conf file parameters" on page 56.

3. Save and close the file.

4. Restart the Multi-Threaded Agent on the host, as follows:

   - On UNIX:

     ```
     /usr/openv/pdde/pdag/bin/mtstrmd -terminate
     /usr/openv/pdde/pdag/bin/mtstrmd
     ```

   - On Windows, use the Windows Services manager. The service name is NetBackup Deduplication Multi-Threaded Agent.

MSDP mtstrm.conf file parameters

The `mtstrm.conf` configuration file controls the behavior of the Deduplication Multi-threaded Agent. The default values balance performance with resource usage.

A procedure exists that describes how to configure these parameters.

The `pd.conf` file resides in the following directories:

- (UNIX) `/usr/openv/lib/ost-plugins/`
- (Windows) *`install_path`*`\Veritas\NetBackup\bin\ost-plugins`

See "Configuring the Deduplication Multi-Threaded Agent behavior" on page 56.

The `mtstrm.conf` file is comprised of three sections. The parameters must remain within their sections. For descriptions of the parameters, see the following sections:

- Logging parameters
- Process parameters
- Threads parameters

The `mtstrm.conf` file resides in the following directories:

- UNIX: `/usr/openv/lib/ost-plugins/`
- Windows: *`install_path`*`\Veritas\NetBackup\bin\ost-plugins`

Logging parameters

The following table describes the logging parameters of the `mtstrm.conf` configuration file.

Table 5-5 Logging parameters (mtstrm.conf file)

Logging Parameter	Description
`LogPath`	The directory in which the `mtstrmd.log` files are created. Default values: ■ Windows: `LogPath=`*`install_path`*`\Veritas\pdde\\..\netbackup\logs\pdde` ■ UNIX: `LogPath=/var/log/puredisk`

`Logging`	Specify what to log:
	Default value: `Logging=short,thread`.
	Possible values:
	`minimal: Critical, Error, Authentication, Bug`
	`short : all of the above plus Warning`
	`long : all of the above plus Info`
	`verbose: all of the above plus Notice`
	`full : all of the above plus Trace messages (everything)`
	`none : disable logging`
	To enable or disable other logging information, append one of the following to the logging value, without using spaces:
	`,thread : enable thread ID logging.`
	`,date : enable date logging.`
	`,timing : enable high-resolution timestamps`
	`,silent : disable logging to console`

Table 5-5 Logging parameters (mtstrm.conf file) *(continued)*

Logging Parameter	Description
`Retention`	How long to retain log files (in days) before NetBackup deletes them. Default value: `Retention=7`. Possible values: 0-9, inclusive. Use 0 to keep logs forever.
`LogMaxSize`	The maximum log size (MB) before NetBackup creates a new log file. The existing log files that are rolled over are renamed `mtstrmd.log.<date/time stamp>` Default value: `LogMaxSize=500`. Possible value: 1 to the maximum operating system file size in MBs, inclusive.

Process parameters

The following table describes the process parameters of the `mtstrm.conf` configuration file.

Table 5-6 Process parameters (mtstrm.conf file)

Process Parameter	Description
`MaxConcurrentSessions`	The maximum number of concurrent sessions that the Multi-Threaded Agent processes. If it receives a backup job when the `MaxConcurrentSessions` value is reached, the job runs as a single-threaded job. By default, the deduplication plug-in sends backup jobs to the Multi-Threaded Agent on a first-in, first-out basis. However, you can configure which clients and which backup policies the deduplication plug-in sends to the Multi-Threaded Agent. The `MTSTRM_BACKUP_CLIENTS` and `MTSTRM_BACKUP_POLICIES` parameters in the `pd.conf` control the behavior. Filtering the backup jobs that are sent to the Multi-Threaded Agent can be very helpful on the systems that have many concurrent backup jobs. See "MSDP pd.conf file parameters" on page 198. Default value: `MaxConcurrentSessions=` (calculated by NetBackup; see the following paragraph). NetBackup configures the value for this parameter during installation or upgrade. The value is the hardware concurrency value of the host divided by the `BackupFpThreads` value (see Table 5-7). (For the purposes of this parameter, the *hardware concurrency* is the number of CPUs or cores or hyperthreading units.) On media servers, NetBackup may not use all hardware concurrency for deduplication. Some may be reserved for other server processes. For more information about hardware concurrency, see the `pd.conf` file `MTSTRM_BACKUP_ENABLED` parameter description. See "MSDP pd.conf file parameters" on page 198. Possible values: 1-32, inclusive. **Warning:** Veritas recommends that you change this value only after careful consideration of how the change affects your system resources. With default configuration values, each session uses approximately 120 to 150 MBs of memory. The memory that is used is equal to (`BackupReadBufferCount` * `BackupReadBufferSize`) + (3 * `BackupShmBufferSize`) + `FpCacheMaxMbSize` (if enabled).
`BackupShmBufferSize`	The size of the buffers (MB) for shared memory copying. This setting affects three buffers: The shared memory buffer itself, the shared memory receive buffer in the `mtstrmd` process, and the shared memory send buffer on the client process. Default value: `BackupShmBufferSize=2` (UNIX) or `BackupShmBufferSize=8` (Windows). Possible values: 1-16, inclusive.

Table 5-6 Process parameters (mtstrm.conf file) *(continued)*

Process Parameter	Description
`BackupReadBufferSize`	The size (MB) of the memory buffer to use per session for read operations from a client during a backup. Default value: `BackupReadBufferSize=32`. Possible values: 16-128, inclusive.
`BackupReadBufferCount`	The number of memory buffers to use per session for read operations from a client during a backup. Default value: `BackupReadBufferCount=3`. Possible values: `1` to `10`, inclusive.
`BackupBatchSendEnabled`	Determines whether to use batch message protocols to send data to the storage server for a backup. Default value: `BackupBatchSendEnabled=1`. Possible values: `0` (disabled) or `1` (enabled).
`FpCacheMaxMbSize`	The maximum amount of memory (MB) to use per session for fingerprint caching. Default value: `FpCacheMaxMbSize=20`. Possible values: 0-1024, inclusive.
`SessionCloseTimeout`	The amount of time to wait in seconds for threads to finish processing when a session is closed before the agent times-out with an error. Default value: 180. Possible values: 1-3600.
`SessionInactiveThreshold`	The number of minutes for a session to be idle before NetBackup considers it inactive. NetBackup examines the sessions and closes inactive ones during maintenance operations. Default value: 480. Possible values: 1-1440, inclusive.

Threads parameters

The following table describes the threads parameters of the `mtstrm.conf` configuration file.

Table 5-7 Threads parameters (mtstrm.conf file)

Threads Parameter	Description
`BackupFpThreads`	The number of threads to use per session to fingerprint incoming data. Default value: `BackupFpThreads=` (calculated by NetBackup; see the following explanation). NetBackup configures the value for this parameter during installation or upgrade. The value is equal to the following hardware concurrency threshold values. ■ Windows and Linux: The threshold value is 2. ■ Solaris: The threshold value is 4. For more information about hardware concurrency, see the `pd.conf` file `MTSTRM_BACKUP_ENABLED` parameter description. See "MSDP pd.conf file parameters" on page 198.
`BackupSendThreads`	The number of threads to use per session to send data to the storage server during a backup operation. Default value: `BackupSendThreads=1` for servers and `BackupSendThreads=2` for clients. Possible values: 1-32, inclusive.
`MaintenanceThreadPeriod`	The frequency at which NetBackup performs maintenance operations, in minutes. Default value: 720. Possible values: 0-10080, inclusive. Zero (0) disables maintenance operations.

Configuring deduplication plug-in interaction with the Multi-Threaded Agent

You can control the interaction between the NetBackup deduplication plug-in and the Multi-Threaded Agent. Several settings in the `pd.conf` file on a host control the interaction. A change in a `pd.conf` file changes the settings for that host only. If you want the same settings for all of the hosts that deduplicate data, you must change the `pd.conf` file on all of the hosts.

See "About the MSDP pd.conf configuration file" on page 197.

To configure deduplication plug-in interaction with the Multi-Threaded Agent

1 Use a text editor to open the `pd.conf` file.

The `pd.conf` file resides in the following directories:

- (UNIX) `/usr/openv/lib/ost-plugins/`

- (Windows) *install_path*\Veritas\NetBackup\bin\ost-plugins

2. To change a setting, specify a new value. The following are the settings that control the interaction:

   - MTSTRM_BACKUP_CLIENTS
   - MTSTRM_BACKUP_ENABLED
   - MTSTRM_BACKUP_POLICIES
   - MTSTRM_IPC_TIMEOUT

   These settings are described in another topic.

   See "MSDP pd.conf file parameters" on page 198.

3. Save and close the file.
4. Restart the NetBackup Remote Manager and Monitor Service (nbrmms) on the host.

About MSDP fingerprinting

NetBackup uses a unique identifier to identify each file and each file segment that is backed up. The deduplication plug-in reads the backup image and separates the image into files. The plug-in separates the files into segments. For each segment, the plug-in calculates the hash key (or *fingerprint*) that identifies each data segment. To create a hash, every byte of data in the segment is read and added to the hash.

NetBackup 8.0 and previous versions use fingerprinting calculations that are based on the MD5-like algorithm. Starting with NetBackup 8.1, the fingerprinting calculations are based on a more secure SHA-2 algorithm. On a system that is upgraded to the 8.1 version, every new segment is computed with the SHA-2 algorithm. A data rolling conversion task works in the background to convert the existing MD5-like fingerprints to SHA-2 fingerprints, gradually.

See "About the rolling data conversion mechanism for MSDP" on page 128.

NetBackup 8 .1 can handle both fingerprint types, and the new server is compatible with old clients and old servers. When you perform a backup from an old client to a new server or when you duplicate data from an old server to a new server, conversion from MD5-like to SHA-2 occurs inline on the new server before the data is saved to the disk. Similarly, when you duplicate data from a new server to an old server, conversion from SHA-2 to MD5-like occurs inline on the new server before the data is sent to the old server.

Notes and restrictions that there are some known issues for the compatibility support.

- The fingerprint conversion requires additional computation time. The interaction between old clients and old servers and new server is slower than if both the client and the server are new.
- You cannot restore data that is backed up using SHA-2 algorithm on a media server that uses the MD5-like algorithm. However, you may choose to restore the SHA-2 fingerprint data on a new media server.
- Similarly, you cannot use client-direct restore to restore data that is backed up using Client Direct deduplication on a media server that uses the MD5-like algorithm. However, you may choose to restore the data on a new media server.
- If you are using two types of media servers for load balancing, where one media server uses MD5-like algorithm and the other media server uses the SHA-2 algorithm, the initial backup may lose deduplication ratio. Therefore, split the old media servers and the new media servers into different groups, and create different storage unit for each of them.
- When data is backed up from a NetBackup 7.5 or previous version client, using Client Direct deduplication, most of the data is transferred over the network and deduplicated on the server. This may save storage, but it does not reduce network throughput. It is recommended that you upgrade the NetBackup client to the latest version.

See “About the MSDP fingerprint cache” on page 63.

See “Media server deduplication backup process” on page 334.

See “MSDP client–side deduplication backup process” on page 337.

About the MSDP fingerprint cache

NetBackup uses *fingerprints* to identify the file segments in the backup data. NetBackup writes only unique data segments to a **Media Server Deduplication Pool**. If a segment already is in storage, NetBackup does not store it again.

See “About MSDP fingerprinting” on page 62.

The storage server maintains an index cache of the fingerprints in RAM. For each backup job, a client requests a list of the fingerprints from its last backup from the server.

The NetBackup Deduplication Engine (`spoold`) loads a percentage of the fingerprints into the cache at startup. After startup, the Engine loads the remaining fingerprints.

You can configure the cache loading behavior.

See “Configuring the MSDP fingerprint cache behavior” on page 64.

You can also control the fingerprint cache seeding for clients.

See “About seeding the MSDP fingerprint cache for remote client deduplication” on page 65.

Configuring the MSDP fingerprint cache behavior

You can configure the cache loading behavior.

See “About the MSDP fingerprint cache” on page 63.

To configure MSDP fingerprint cache behavior

1. On the storage server, open the `contentrouter.cfg` file in a text editor; it resides in the following directory:
   - (UNIX) *storage_path*`/etc/puredisk`
   - (Windows) *storage_path*`\etc\puredisk`
2. Edit the parameters that control the behavior.

   See “MSDP fingerprint cache behavior options” on page 64.

MSDP fingerprint cache behavior options

Table 5-8 describes the parameters that control the behavior. All of these options are in the `contentrouter.cfg` file.

The parameters are stored in the `contentrouter.cfg` file.

See “About the MSDP contentrouter.cfg file” on page 215.

Table 5-8 Cache load parameters

Behavior	Description
`CacheLoadThreadNum`	The number of threads to use to load the remaining fingerprints. The `CacheLoadThreadNum` in the `contentrouter.cfg` file controls the number of threads. NetBackup begins loading fingerprints from the next container number after the startup fingerprint loading. The default is one.
`MaxCacheSize`	The percentage of RAM to use for the fingerprint cache. The `MaxCacheSize` in the `contentrouter.cfg` file controls percentage of RAM. The default is 75%.

About seeding the MSDP fingerprint cache for remote client deduplication

Veritas provides a method for *seeding* the fingerprint cache for a new client. The use case that benefits the most from seeding is the first backup of a remote client over a high latency network such as a WAN. The performance of the first backup is then similar to the performance of an existing client.

An important consideration is the client from which to seed the cache. When you choose a similar client, consider the following:

- If most of the information is the operating system files, use any client with the same operating system.
- If most of the information is data, finding a client with the same data may be unlikely. Therefore, consider physically moving a copy of the data to the datacenter. Back up that data on a similar client, and then use that client and policy for the seed.
- The more similar the clients are, the greater the cache hit rate is.

Two methods exist to configure cache seeding. You can use either method. The following table describes the seeding configuration methods.

Table 5-9 Seeding configuration methods

Host on which to configure seeding	Description
On the client	Configure seeding on the client for one or only a few clients. See "Configuring MSDP fingerprint cache seeding on the client" on page 67.
On the storage server	The use case that benefits the most is many clients to seed, and they can use the fingerprint cache from a single host. See "Configuring MSDP fingerprint cache seeding on the storage server" on page 68.

To ensure that NetBackup uses the seeded backup images, the first backup of a client after you configure seeding must be a full backup with a single stream. Specifically, the following two conditions must be met in the backup policy:

- The **Attributes** tab **Allow multiple data streams** attribute must be unchecked.
- The backup selection cannot include any**NEW_STREAM** directives.

If these two conditions are not met, NetBackup may use multiple streams. If the **Attributes** tab **Limit jobs per policy** is set to a number less than the total number

of streams, only those streams use the seeded images to populate the cache. Any streams that are greater than the **Limit jobs per policy** value do not benefit from seeding, and their cache hit rates may be close to 0%.

After the first backup, you can restore the original backup policy parameter settings.

The following items are example of informational messages that show that seeding occurred:

Activity Monitor Job Details

```
1/2/2015 2:18:23 AM - Info nbmaster1(pid=6340)
StorageServer=PureDisk:nbmaster1; Report=PDDO
Stats for (nbmaster1): scanned: 3762443 KB, CR
sent: 1022 KB, CR sent over FC: 0 KB, dedup:
100.0%, cache hits: 34364 (100.0%)
```

```
1/2/2015 2:18:24 AM - Info nbmaster1(pid=6340)
StorageServer=PureDisk:nbmaster1; Report=PDDO
Stats for (nbmaster1): scanned: 1 KB, CR sent:
0 KB, CR sent over FC: 0 KB, dedup: 100.0%
```

Deduplication plug-in log (`pdplugin.log`) on the client

```
01/02/15 02:15:17 [4452] [4884] [DEBUG] PDSTS:
cache_util_get_cache_dir: enter
db=/nbmaster1#1/2, scp='', bc=opscenter1,
bp=seedfinal, bl=4096
```

```
01/02/15 02:15:17 [4452] [4884] [DEBUG] PDSTS:
cache_util_get_cache_dir: new backup, using
existing client seeding directory
```

```
01/02/15 02:15:17 [4452] [4884] [DEBUG] PDSTS:
cache_util_get_cache_dir: exit
db=/nbmaster1#1/2, scp='', bc=opscenter1,
bp=seedfinal, bl=4096,
cachedir_buf='/nbmaster1#1/2/#pdseed/opscenter1'
err=0
```

See "NetBackup MSDP log files" on page 347.

Deduplication proxy server log (`nbostpxy.log`) on the client

```
02:15:17.417 [4452.4884] [DEBUG] [dummy] [11:bptm:6340:nbmaster1] [DEBUG]
PDSTS: cache_util_get_cache_dir: enter
db=/nbmaster1#1/2, scp='', bc=opscenter1,
bp=seedfinal, bl=4096

02:15:17.433 [4452.4884] [DEBUG] [dummy] [11:bptm:6340:nbmaster1] [DEBUG]
PDSTS: cache_util_load_fp_cache_nbu: enter
dir_path=/nbmaster1#1/2/#pdseed/opscenter1,
t=16s, me=1024

02:15:17.449 [4452.4884] [DEBUG] [dummy] [11:bptm:6340:nbmaster1] [DEBUG]
PDSTS: cache_util_load_fp_cache_nbu: adding
'nbmaster1_1420181254_C1_F1.img' to cache list
(1)

02:15:17.449 [4452.4884] [DEBUG] [dummy] [11:bptm:6340:nbmaster1] [DEBUG]
PDSTS: cache_util_load_fp_cache_nbu: opening
/nbmaster1#1/2/#pdseed/opscenter1/nbmaster1_1420181254_C1_F1.img
for image cache (1/1)

02:15:29.585 [4452.4884] [DEBUG] [dummy] [11:bptm:6340:nbmaster1] [DEBUG]
PDVFS: pdvfs_lib_log: soRead: segment
c32b0756d491871c45c71f811fbd73af already
present in cache.

02:15:29.601 [4452.4884] [DEBUG] [dummy] [11:bptm:6340:nbmaster1] [DEBUG]
PDVFS: pdvfs_lib_log: soRead: segment
346596a699bd5f0ba5389d4335bc7429 already
present in cache.
```

See "NetBackup MSDP log files" on page 347.

For more information about seeding, see the following Veritas tech note:

http://www.veritas.com/docs/TECH144437

See "About the MSDP fingerprint cache" on page 63.

Configuring MSDP fingerprint cache seeding on the client

Seeding on the client requires the following:

- A client name
- A policy name
- A date after which to stop using the similar client's fingerprint cache.

Information about when to use this seeding method and how to choose a client from which to seed is available.

See "About seeding the MSDP fingerprint cache for remote client deduplication" on page 65.

Warning: Do not use this procedure on the storage server or the load balancing server. If you do, it affects all clients that are backed up by that host.

To seed the MSDP fingerprint cache on the client

- Before the first backup of the remote client, edit the `FP_CACHE_CLIENT_POLICY` parameter in the `pd.conf` file on the remote client.

  Specify the setting in the following format:

  clienthostmachine,*backuppolicy*,*date*

clienthostmachine	The name of the existing similar client from which to seed the cache. **Note:** NetBackup treats long and short host names differently, so ensure that you use the client name as it appears in the policy that backs it up.
backuppolicy	The backup policy for that client.
date	The last date in mm/dd/yyyy format to use the fingerprint cache from the existing similar client. After this date, NetBackup uses the fingerprints from the client's own backup.

  See "Editing the MSDP pd.conf file" on page 198.

  See "MSDP pd.conf file parameters" on page 198.

Configuring MSDP fingerprint cache seeding on the storage server

On the storage server, the NetBackup `seedutil` utility creates a special seeding directory for a client. It populates the seeding directory with image references to another client and policy's backup images. The following is the pathname of the seeding directory:

database_path/databases/catalog/2/#pdseed/*client_name*

(By default, NetBackup uses the same path for the storage and the catalog; the *database_path* and the *storage_path* are the same. If you configure a separate path for the deduplication database, the paths are different.)

When a backup runs, NetBackup loads the fingerprints from the #pdseed directory for the client. (Assuming that no fingerprints exist for that client in the usual catalog location.)

Information about when to use this seeding method and how to choose a client from which to seed is available.

See "About seeding the MSDP fingerprint cache for remote client deduplication" on page 65.

To seed the fingerprint cache from the storage server

1. Before the first backup of the remote client, specify the clients and the policy in the following format:

   UNIX: `/usr/openv/pdde/pdag/bin/seedutil -seed -sclient client_name -spolicy policy_name -dclient destination_client_name`

   Windows: `install_path\Veritas\pdde\seedutil -seed -sclient client_name -spolicy policy_name -dclient destination_client_name`

   Note: NetBackup treats long and short host names differently, so ensure that you use the client name as it appears in the policy that backs it up.

   See "NetBackup seedutil options" on page 70.

2. Repeat the command for each client that you want to seed with fingerprints.
3. Verify that the seeding directories for the clients were created by using the following command:

   ```
   seedutil -list_clients
   ```

4. Back up the clients.
5. After the client or clients are backed up, remove the seeding directories for the clients. The following is the command syntax:

   ```
   seedutil -clear client_name
   ```

   After one full backup for the client or clients, NetBackup clears the seeding directory automatically. If the first backup fails, the seeded data remains for successive attempts. Although NetBackup clears the seeding directory automatically, Veritas recommends that you clear the client seeding directories manually.

NetBackup seedutil options

The following is the usage statement for the `seedutil` utility:

`seedutil [-v log_level] [-seed -sclient source_client_name -spolicy policy_name -dclient destination_client_name [-backupid backup_id]] [-clear client_name] [-clear_all] [-list_clients] [-list_images client_name] [-help]`

The following items describe the options:

`-backupid backup_id`	The backup ID from which to copy the data for seeding.
`-clear client_name`	Clear the contents of the seed directory specified by the *client_name*.
`-clear_all`	Clear the contents of all of the seed directories.
`-dclient destination_client_name`	The name of the new client for which you are seeding the data.
`-help`	Display help for the command.
`-list_clients`	List all of the clients that have been configured for seeding.
`-list_images client_name`	List the contents of the seeding directory for the specified client.
`-sclient source_client_name`	The client from which to copy the data for seeding. **Note:** NetBackup treats long and short host names differently, so ensure that you use the client name as it appears in the policy that backs it up.
`-seed`	Configure seeding.
`-spolicy policy_name`	The NetBackup policy that backed up the client that you want to use for the seeding data.
`-v log_level`	The log level.

The following are the directories in which the command resides:

- UNIX: `/usr/openv/pdde/pdag/bin`

- Windows: `C:\Program Files\Veritas\pdde`

Enabling 96-TB support for MSDP

Before you configure a storage server for a 96-TB **Media Server Deduplication Pool**, you must enable support for the multiple volumes that are required.

See "About MSDP storage capacity" on page 18.

See "About provisioning the storage for MSDP" on page 42.

To enable support for a 96-TB NetBackup MSDP

- On the NetBackup media server that you want to use as the MSDP storage server, create an empty `nbapp-release` file in the `/etc` directory. The following is an example that shows how to use the `touch` command to create the file:

  ```
  touch /etc/nbapp-release
  ```

About MSDP Encryption using KMS service

NetBackup incorporates Key Management Server (KMS) with Media Server Deduplication Pool.

MSDP encryption carries out segment-level encryption and assigns a unique encryption key for every data segment. A customer key is retrieved from NetBackup KMS to encrypt the segment key. The customer key is refreshed regularly and KMS service rotates the user key frequently (every 3 months by default).

You can configure the KMS service from the NetBackup Administration Console or the NetBackup command line during storage server configuration.

Note: You cannot disable the MSDP KMS service once you enable it.

You can use the following commands to get the status of the KMS mode:

- For UNIX:

  ```
  /usr/openv/pdde/pdcr/bin/crcontrol --getmode
  ```

- For Windows:

  ```
  <install_path>\Veritas\pdde\crcontrol.exe --getmode
  ```

For enabling KMS, refer to the following topics:

See "Configuring a storage server for a Media Server Deduplication Pool" on page 73.

Upgrading KMS for MSDP

During the NetBackup upgrade, KMS rolling conversion runs along with MSDP encryption rolling conversion.

The supported NetBackup upgrade paths are:

- NetBackup 8.0 to 8.1.1
- NetBackup 8.1 to 8.1.1

Since KMS services were introduced in NetBackup 8.0, upgrades from pre-8.0 NetBackup versions are not supported.

For additional information, refer to the *Configuring KMS* section in the *Veritas NetBackup Security and Encryption Guide*.

Before you upgrade KMS, complete the following steps:

1 Create an empty database using the following command:

- For UNIX:

  `/usr/openv/netbackup/bin/nbkms -createemptydb`

- For Windows:

  `<install_path>\Veritas\NetBackup\bin\nbkms.exe -createemptydb`

  Enter the following parameters when you receive a prompt:

  - Enter the HMK passphrase
    Enter a password that you want to set as the host master key (HMK) passphrase. Press Enter to use a randomly generated HMK passphrase. The passphrase is not displayed on the screen.
  - Enter HMK ID
    Enter a unique ID to associate with the host master key. This ID helps you to determine an HMK associated with any key store.
  - Enter KPK passphrase
    Enter a password that you want to set as the key protection key (KPK) passphrase. Press Enter to use a randomly generated HMK passphrase. The passphrase is not displayed on the screen.
  - Enter KPK ID
    Enter a unique ID to associate with the key protection key. This ID helps you to determine a KPK associated with any key store.

  After the operation completes successfully, run the following command on the master server to start KMS:

- For UNIX:

  `/usr/openv/netbackup/bin/nbkms`

- For Windows:

  <install_path>\Veritas\NetBackup\bin\nbkms.exe

2 Create a key group and an active key by entering the following commands:

- For UNIX:

  /usr/openv/netbackup/bin/admincmd/nbkmsutil -createkg -kgname msdp

  /usr/openv/netbackup/bin/admincmd/nbkmsutil -createkey -kgname msdp -keyname name –activate

- For Windows:

  <install_path>\Veritas\NetBackup\bin\nbkms.exe -createkg -kgname msdp

  <install_path>\Veritas\NetBackup\bin\nbkms.exe -createkey -kgname msdp -keyname name –activate

  Enter a password that you want set as the key passphrase.

3 Create a `kms.cfg` configuration file at the following location:

- On UNIX:

  /usr/openv/pdde/kms.cfg

- On Windows:

  <install_path>\Veritas\pdde\kms.cfg

  Add the following content to the `kms.cfg` file:

```
[KMSOptions]
KMSEnable=true
KMSKeyGroupName=YourKMSKeyGroupName
KMSServerName= YourKMSServerName
KMSType=0
```

After completing the steps, you can upgrade MSDP.

Configuring a storage server for a Media Server Deduplication Pool

Configure in this context means to configure a NetBackup media server as a storage server for a **Media Server Deduplication Pool**.

See “About MSDP storage servers” on page 24.

The type of storage.	Select **Media Server Deduplication Pool** for the type of disk storage.
The credentials for the deduplication engine.	See "About the NetBackup Deduplication Engine credentials" on page 30.
The storage paths.	See "MSDP storage path properties" on page 88.
The network interface.	See "About the network interface for MSDP" on page 31.
The load balancing servers, if any.	See "About MSDP storage servers" on page 24.

When you configure the storage server, the wizard also lets you create a disk pool and storage unit.

Prerequisite	For a 96-TB **Media Server Deduplication Pool**, you must create the required directories before you configure the storage server. See "Creating the data directories for 96-TB MSDP support" on page 112.

To configure a NetBackup storage server for a Media Server Deduplication Pool

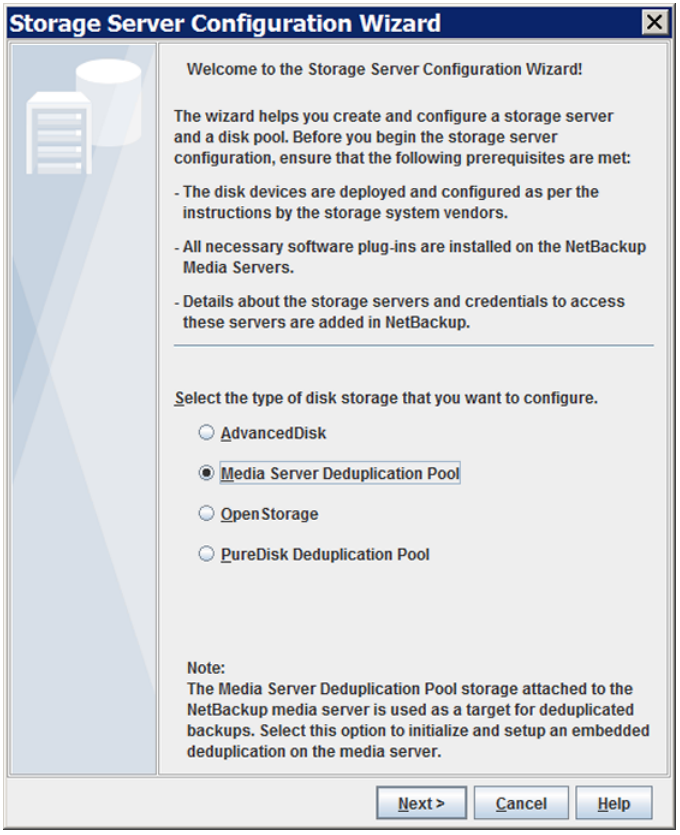
1. In the **NetBackup Administration Console**, select either **NetBackup Management** or **Media and Device Management**.
2. In the right pane, click **Configure Disk Storage Servers**.

   The **Storage Server Configuration Wizard Welcome** panel appears.

3 On the **Welcome** panel, select **Media Server Deduplication Pool** from the drop-down menu.

The types of storage servers that you can configure depend on the options for which you are licensed.

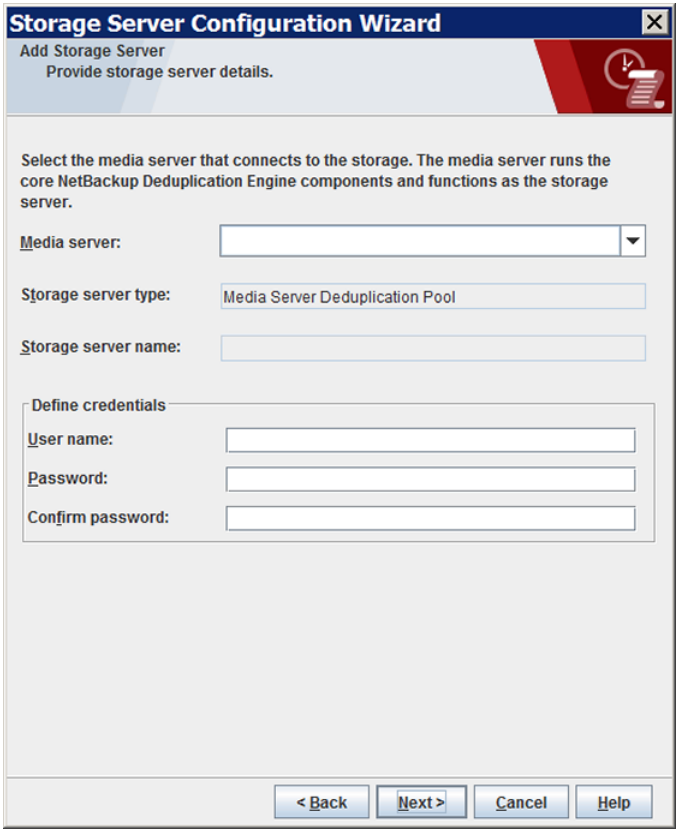
The following is an example of the wizard panel:



After you select **Media Server Deduplication Pool**, click **Next**. The **Add Storage Server** wizard panel appears.

4 On the **Add Storage Server** panel, select or enter the appropriate information.

The following is an example of the wizard panel:



Media server Select the media server that you want to configure as the storage server.

You can add deduplication load balancing servers on the next wizard panel.

Username Enter the user name for the NetBackup Deduplication Engine.

See "About the NetBackup Deduplication Engine credentials" on page 30.

Password Enter the password for the NetBackup Deduplication Engine.

Confirm password To confirm the password, re-enter the password.

After you enter the information, click **Next**.

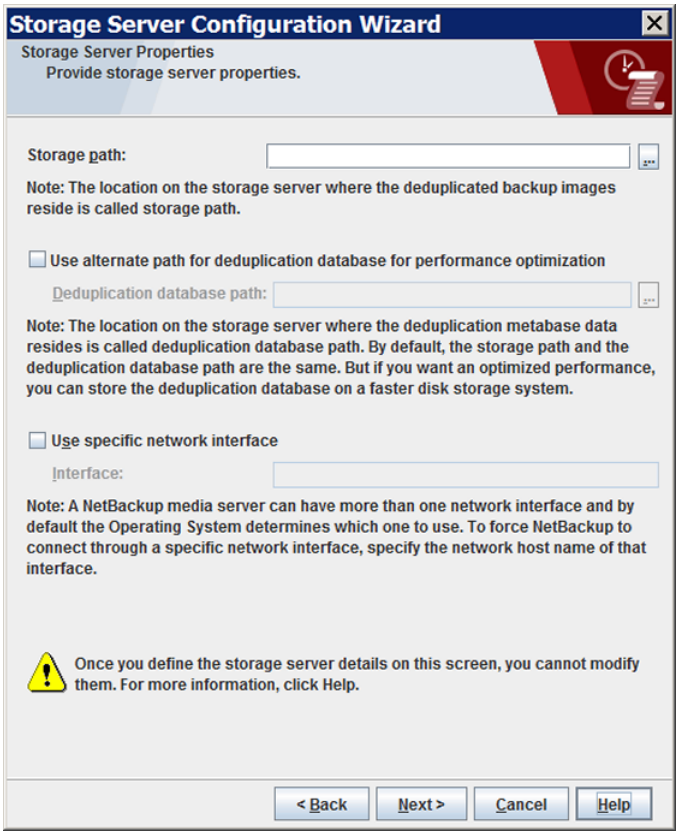
The **Storage Server Properties** panel appears.

5 On the **Storage Server Properties** panel, enter or select the properties for the deduplication storage server.

See “MSDP storage path properties” on page 88.

See “MSDP network interface properties” on page 91.

The following is an example of the wizard panel:



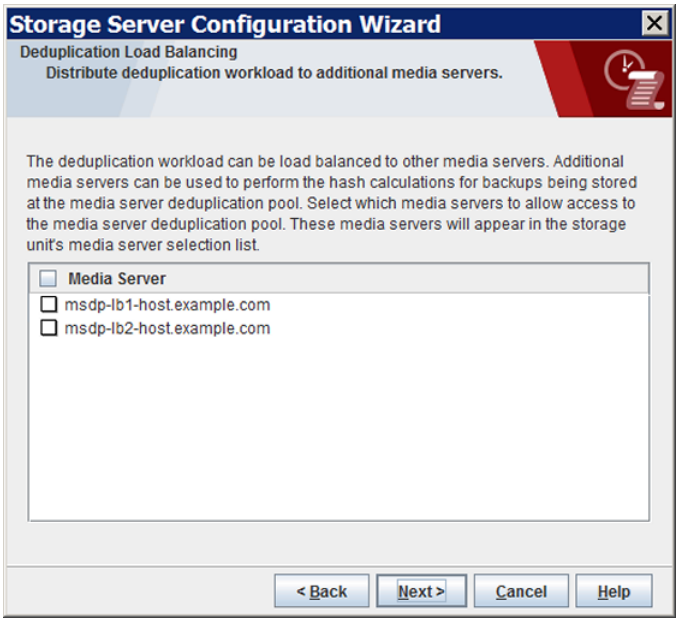
After you click **Next**, the behavior depends on whether you have media servers installed, as follows:

No media servers installed	The **Storage Server Encryption** panel appears. Go to step 8.
Media servers are installed.	The **Deduplication Load Balancing** panel appears. Continue to step 6.

6 On the **Deduplication Load Balancing** panel, select other NetBackup media servers to use for deduplication. Selecting load balancing servers is optional.

See "About MSDP load balancing servers" on page 25.

The following is an example of the wizard panel:



For the media servers that you select, NetBackup enables their deduplication functionality and populates them with the NetBackup Deduplication Engine credentials you entered on a previous panel.

When you click **Next**, the **Storage Server Encryption** panel appears next.

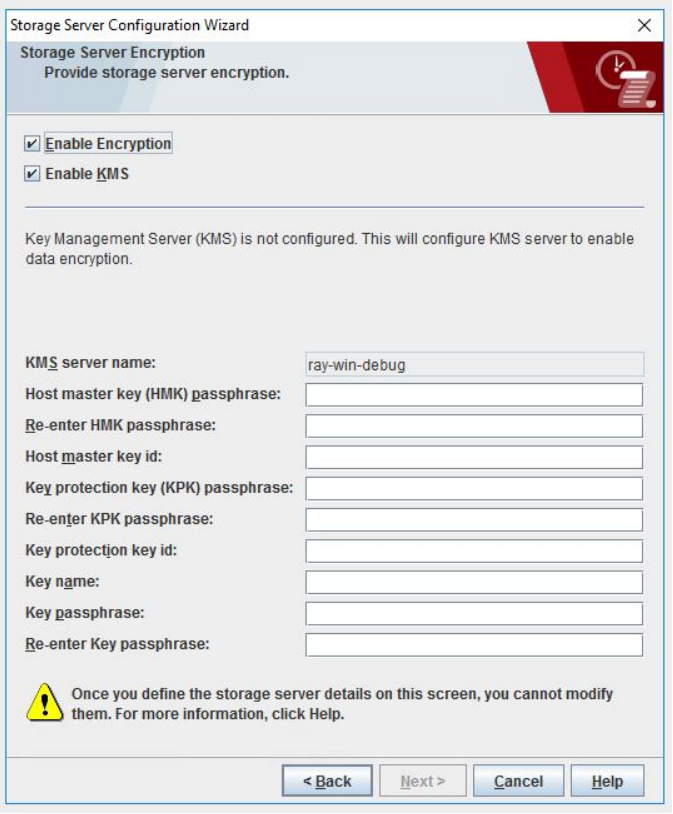
Note: Load balancing for CloudCatalyst storage servers or CloudCatalyst appliances is supported. See the following topic for configuration considerations.

See "Configuring push or pull optimized duplication for CloudCatalyst" on page 256.

---

7 On the **Storage Server Encryption** panel, you can enable encryption and KMS for the Media Server Deduplication Pool. The **Enable KMS** option is available when you select **Enable Encryption**.

The following is an example of the wizard panel:



See “About MSDP encryption” on page 123.

See “About MSDP Encryption using KMS service” on page 71.

- If you select **Enable KMS** for the first time, as a one-time KMS configuration, you must enter the following information:

Option	Description
KMS server name	The name of the Key Management Server.
Host master key (HMK) passphrase	Enter a password that you want to set as the host master key (HMK) passphrase.
Host master key id	Enter a unique ID to associate with the host master key. This ID helps you to determine an HMK associated with any key store.

Option	Description
Key protection key (KPK) passphrase	Enter a password that you want to set as the key protection key (KPK) passphrase. This ID helps you to determine a KPK associated with any key store.
Key protection key id	Enter a unique ID to associate with the key protection key.
Key name	Enter a name of the key.
Key passphrase	Enter a password that you want set as the key passphrase.

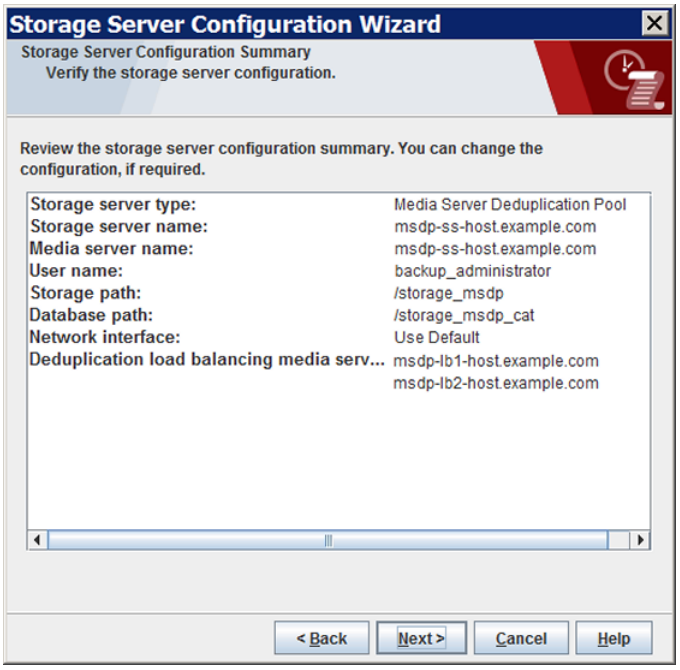
- If you select **Enable KMS** and if KMS is already configured on the Master Server, you must enter the following information:

Option	Description
Key name	Enter a name of the key.
Key passphrase	Enter a password that you want set as the key passphrase.

When you click **Next**, the **Storage Server Configuration Summary** panel appears next.

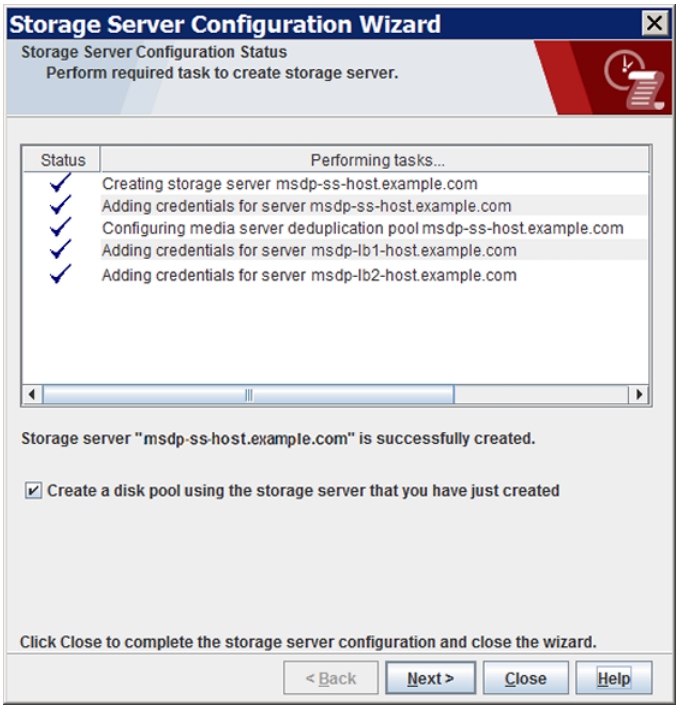
8 On the **Storage Server Configuration Summary** panel, verify the selections. If OK, click **Next** to configure the storage server.

The following is an example of the wizard panel:



The **Storage Server Creation Status** panel appears.

9 The **Storage Server Configuration Status** wizard panel describes the status of the operation.



After the storage server is created, you can do the following:

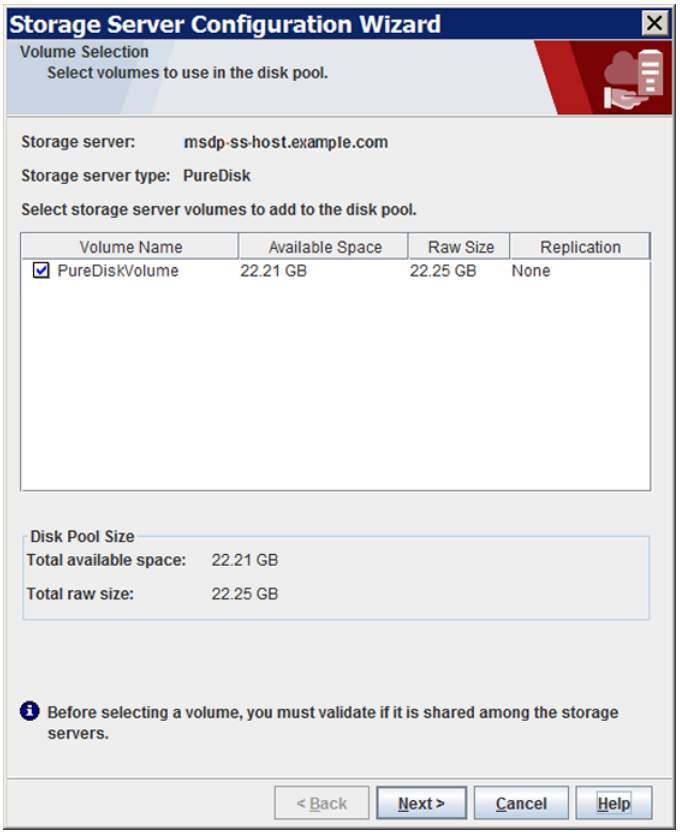
Configure a disk pool	Ensure that **Create a disk pool using the storage server that you have just created** is selected and then click **Next**. The **Select Volumes** panel appears. Continue to the next step.
Exit	Click **Close**. You can configure a disk pool at another time.

If storage server creation fails, troubleshooting help is available.

See "Troubleshooting MSDP configuration issues" on page 355.

10 On the **Select Volumes** panel, select the volume for this disk pool. All of storage in the **Storage Path** that you configured in the **Storage Server Configuration Wizard** is exposed as a single volume. The **PureDiskVolume** is a virtual name for that storage.

The following is an example of the wizard panel:

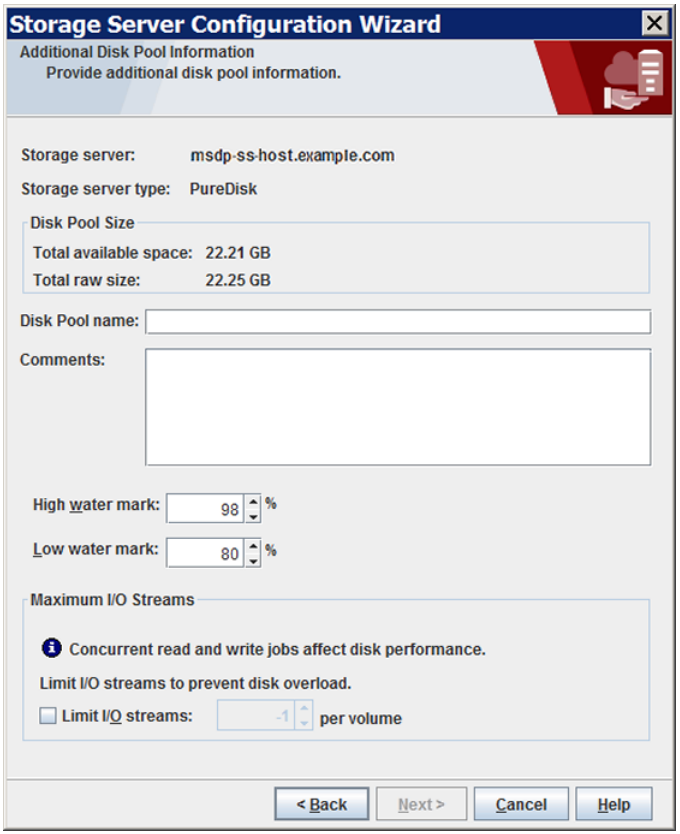


After you select the **PureDiskVolume** volume, click **Next**. The **Additional Disk Pool Information** wizard panel appears.

11 On the **Additional Disk Pool Information** panel, enter the values for this disk pool.

See "Media Server Deduplication Pool properties" on page 110.

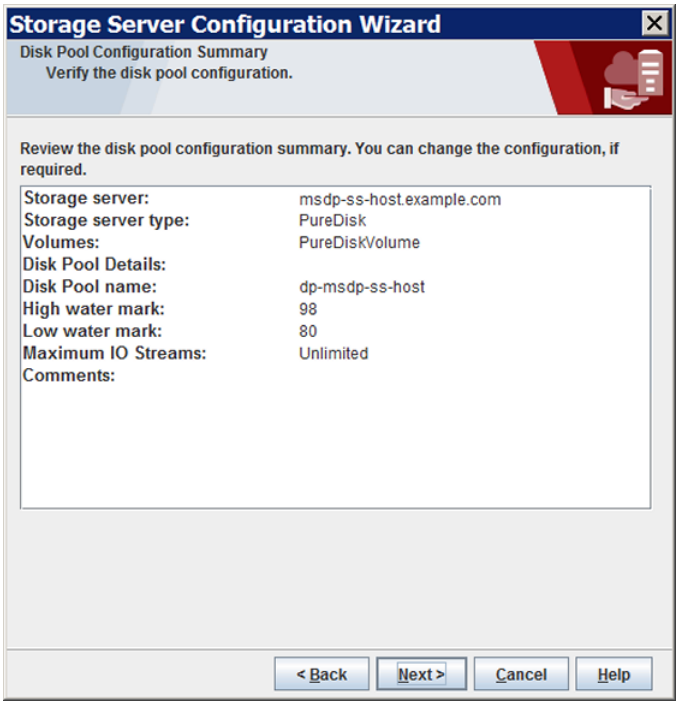
The following is an example of the wizard panel:



After you enter the appropriate information or select the necessary options, click **Next**. The **Disk Pool Configuration Summary** wizard panel appears.

12 On the **Disk Pool Configuration Summary** panel, verify the selections. If OK, click **Next**.

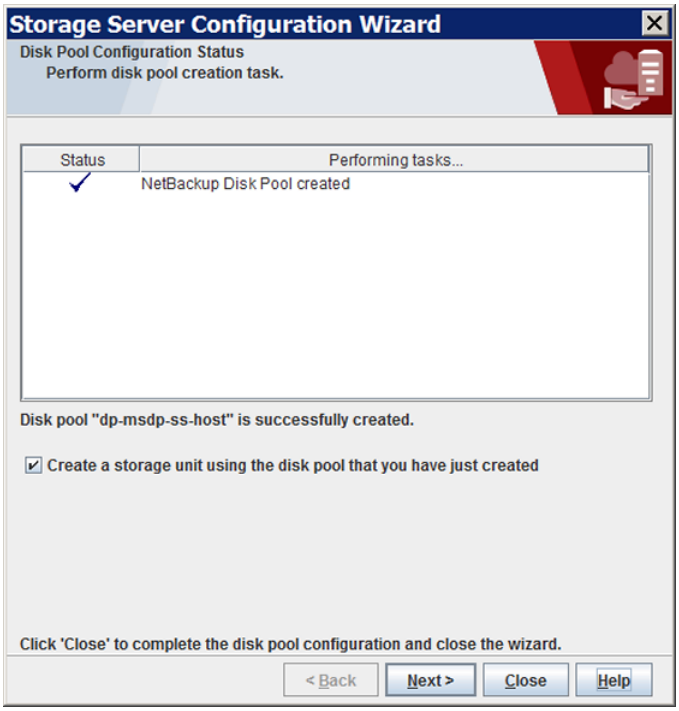
The following is an example of the wizard panel:



To configure the disk pool, click **Next**. The **Disk Pool Configuration Status** wizard panel appears.

13 The **Disk Pool Configuration Status** wizard panel describes the progress of the operation.

The following is an example of the wizard panel:



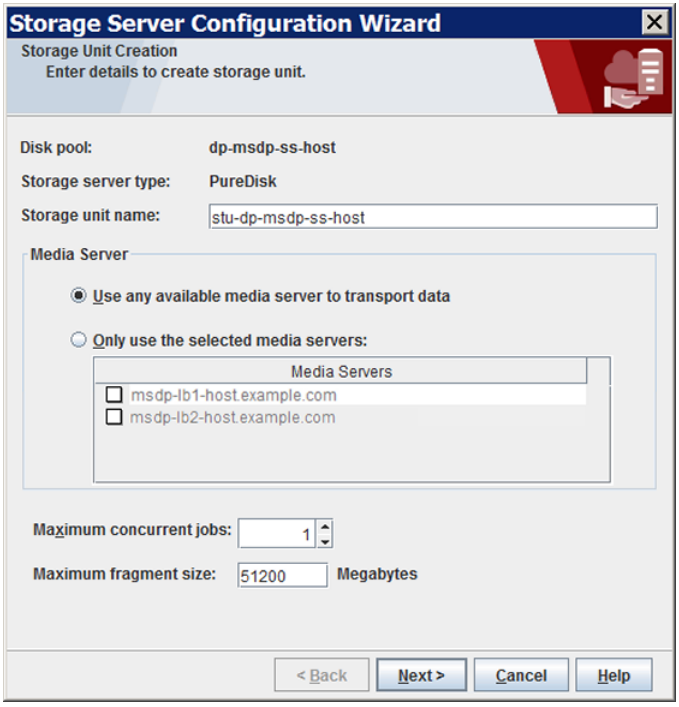
After the disk pool is created, you can do the following:

Configure a storage unit	Ensure that **Create a storage unit using the disk pool that you have just created** is selected and then click **Next**. The **Storage Unit Creation** wizard panel appears. Continue to the next step.
Exit	Click **Close**. You can configure one or more storage units later. See "Configuring a Media Server Deduplication Pool storage unit" on page 115.

14 Enter the appropriate information for the storage unit.

See "Media Server Deduplication Pool storage unit properties" on page 117.

The following is an example of the wizard panel:



After you enter the appropriate information or select the necessary options, click **Next** to create the storage unit.

15 After NetBackup configures the storage unit, the **Finished** panel appears. Click **Finish** to exit from the wizard.

MSDP storage path properties

NetBackup requires that the storage is exposed as a directory path. The following table describes the storage path properties for a **Media Server Deduplication Pool** on the storage server:

Table 5-10 MSDP storage path properties

Property	Description

Storage path	The path to the storage. The storage path is the directory in which NetBackup stores the raw backup data. Backup data should not be stored on the system disk.
	
	Because the storage requires a directory path, do not use only the root node (`/`) or drive letter (`E:\`) as the storage path. (That is, do not mount the storage as a root node (`/`) or a drive letter (`E:\`).
	
	For a 96-TB **Media Server Deduplication Pool**, you must enter the path name of the mount point for the volume that you consider the first 32-TB storage volume. The following is an example of a volume naming convention for the mount points for the backups:
	
	`/msdp/vol0  <--- The first volume`
	`/msdp/vol1`
	`/msdp/vol2`
	
	NetBackup supports 96-TB deduplication pools on a subset of supported systems.
	
	See "About MSDP storage capacity" on page 18.
	
	See "About provisioning the storage for MSDP" on page 42.
	
	See "Creating the data directories for 96-TB MSDP support" on page 112.
	
	You can use the following characters in the storage path name:
	
	■ Any of the 26 letters of the International Standards Organization (ISO) Latin-script alphabet, both uppercase (capital) letters and lowercase (small) letters. These are the same letters as the English alphabet.
	■ Any integer from 0 to 9, inclusive.
	■ A space character.
	■ Any of the following characters:
	UNIX: `_-:./\`
	Windows: `_-:.\` (a colon (`:`) is allowed only after a drive letter (for example, `G:\MSDP_Storage`)
	
	NetBackup requirements for the deduplication storage paths may affect how you expose the storage.
	
	See "About MSDP storage and connectivity requirements" on page 19.

Table 5-10 MSDP storage path properties *(continued)*

Property	Description
Use alternate path for deduplication database	By default, NetBackup uses the storage path for the MSDP database (that is, the MSDP catalog) location. The MSDP database is different than the NetBackup catalog. Select this option to use a location other than the default for the deduplication database. For a 96-TB **Media Server Deduplication Pool**, you must select this option. See "About provisioning the storage for MSDP" on page 42. For performance optimization, Veritas recommends that you use a separate disk volume for the deduplication database than for the backup data.
Database path	If you selected **Use alternate path for deduplication database**, enter the path name for the database. The database should not be stored on the system disk. For a 96-TB **Media Server Deduplication Pool**, you must enter the path name of the partition that you created for the MSDP catalog. For example, if the naming convention for your mount points is `/msdp/volx`, Veritas recommends the following for the MSDP catalog directory: `/msdp/cat` See "About provisioning the storage for MSDP" on page 42. For performance optimization, Veritas recommends that you use a separate disk volume for the deduplication database than for the backup data. You can use the following characters in the path name: ■ Any of the 26 letters of the International Standards Organization (ISO) Latin-script alphabet, both uppercase (capital) letters and lowercase (small) letters. These are the same letters as the English alphabet. ■ Any integer from 0 to 9, inclusive. ■ A space character. ■ Any of the following characters: UNIX: `_-:./\` Windows: `_-:.\` (a colon (`:`) is allowed only after a drive letter (for example, `F:\MSDP_Storage`)

If the directory or directories do not exist, NetBackup creates them and populates them with the necessary subdirectory structure. If the directory or directories exist, NetBackup populates them with the necessary subdirectory structure.

Caution: You cannot change the paths after NetBackup configures the deduplication storage server. Therefore, decide during the planning phase where and how you want the deduplicated backup data to be stored and then carefully enter the paths.

MSDP network interface properties

The following table describes the network interface properties for a **Media Server Deduplication Pool** storage server.

Caution: You cannot change the network interface after NetBackup configures the deduplication storage server. Therefore, enter the properties carefully.

Table 5-11 MSDP network interface properties

Property	Description
Use specific network interface	Select this option to specify a network interface for the deduplication traffic. If you do not specify a network interface, NetBackup uses the operating system host name value. See "About the network interface for MSDP" on page 31.
Interface	If you selected **Use specific network interface**, enter the interface name.

Configuring a storage server for a PureDisk Deduplication Pool

Note: NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only.

Configure in this context means to configure a PureDisk Storage Pool Authority as a storage server in NetBackup.

See "About the NetBackup deduplication destinations" on page 17.

When you configure a storage server for MSDP, you specify the following:

- The type of storage.
  Select **PureDisk Deduplication Pool** for the type of disk storage.
- The credentials for the PureDisk Storage Pool Authority.
- A media server to use as a backup server and deduplication server. Also, other media servers to use as load balancing servers, if any.

When you configure the storage server, the wizard also lets you configure a disk pool and storage unit also.

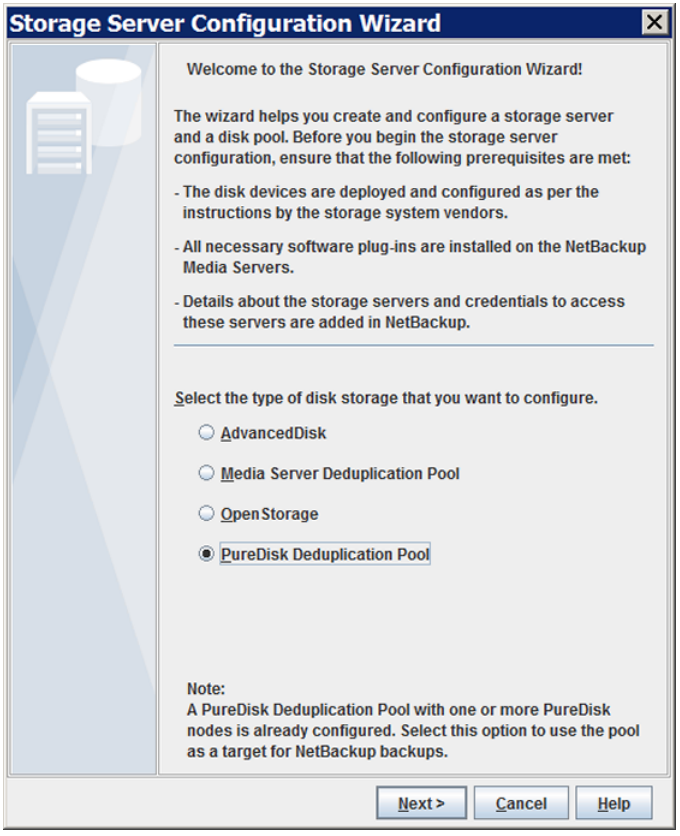
To configure a NetBackup storage server for a PureDisk Deduplication Pool by using the wizard

1. In the **NetBackup Administration Console**, select either **NetBackup Management** or **Media and Device Management**.
2. In the right pane, click **Configure Disk Storage Servers**.

   The **Storage Server Configuration Wizard Welcome** panel appears.
3. On the **Welcome** panel, select **Media Server Deduplication Pool** from the drop-down menu.

   The types of storage servers that you can configure depend on the options for which you are licensed.

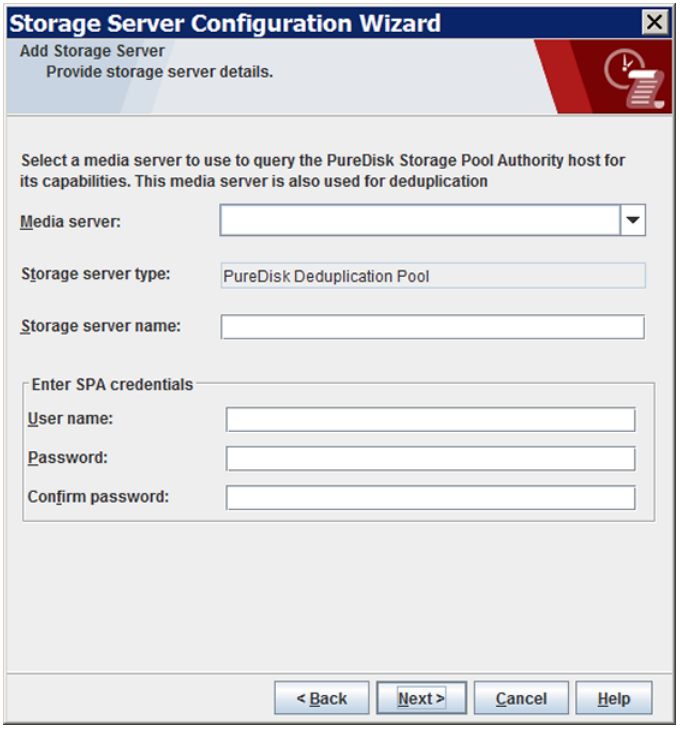
   The following is an example of the wizard panel:



   After you select **Media Server Deduplication Pool**, click **Next.** The **Add Storage Server** wizard panel appears.

4 On the **Add Storage Server** panel, select or enter the appropriate information.

The following is an example of the wizard panel:



Media server	Select a media server to use to query the NetBackup 5000 series appliance for its capabilities. That media server also is used for deduplication. You can add other deduplication load balancing servers on the next wizard panel.
Storage server name	Enter the host name of the NetBackup 5000 series appliance in the **Storage server name** field.
Username	Enter the user name for the NetBackup 5000 series appliance.
Password	Enter the password for the NetBackup 5000 series appliance.
Confirm password	To confirm the password, re-enter the password.

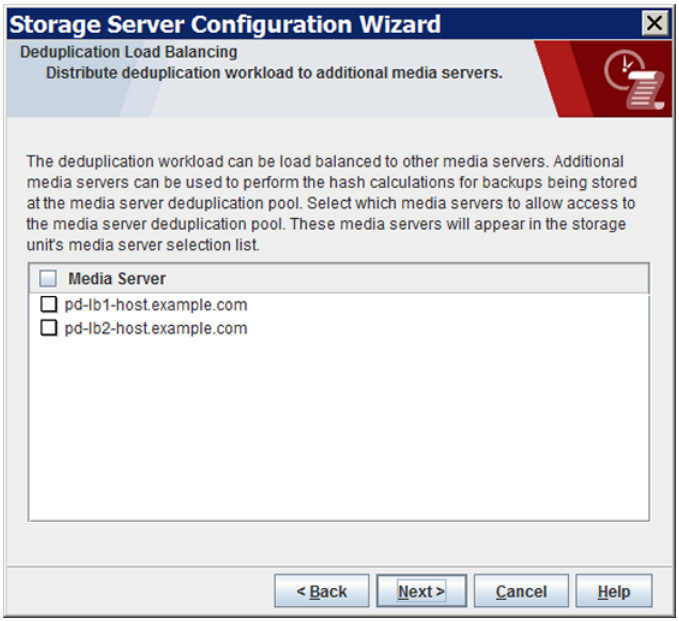
After you enter the information, click **Next**.

The **Configure Additional Media Servers** panel appears.

5 On the **Deduplication Load Balancing** panel select other NetBackup media servers to use for deduplication load balancing. The wizard populates the media servers that you select with the Storage Pool Authority credentials you entered on a previous panel. Selecting load balancing servers is optional.

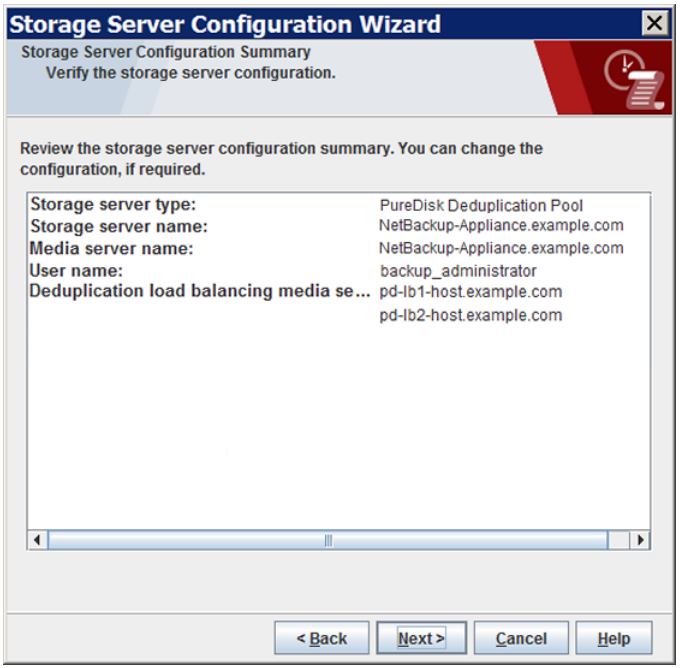
See "About MSDP load balancing servers" on page 25.

The following is an example of the wizard panel:



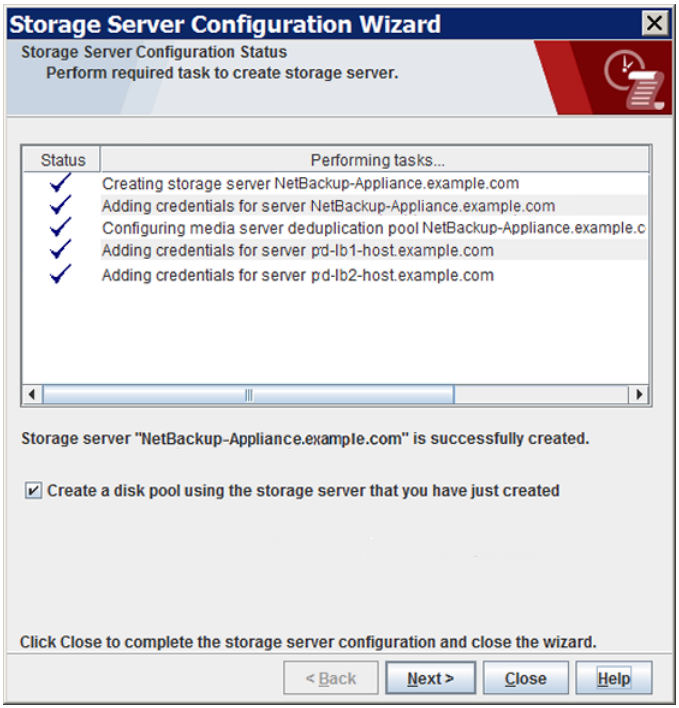
When you click **Next**, the **Storage Server Configuration Summary** panel appears next.

6 On the **Storage Server Configuration Summary** panel, verify the selections. If OK, click **Next**.



The **Storage Server Creation Status** panel appears. It describes the status of the wizard actions.

7 The **Storage Server Configuration Status** wizard panel describes the status of the operation, as follows:



After the storage server is created, you can do the following:

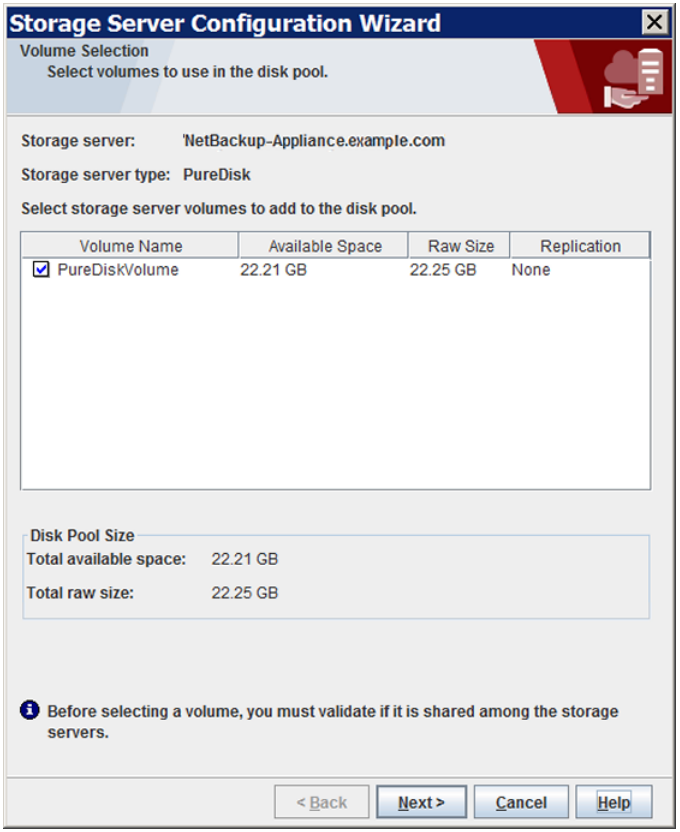
Configure a disk pool	Ensure that **Create a disk pool using the storage server that you have just created** is selected and then click **Next**. The **Select Volumes** panel appears. Continue to the next step.
Exit	Click **Close**. You can configure a disk pool at another time.

If storage server creation fails, troubleshooting help is available.

See "Troubleshooting MSDP configuration issues" on page 355.

8 On the **Volume Selection** panel, select the volume for this disk pool. All of storage of the NetBackup 5000 series appliance is exposed as a single volume. The **PureDiskVolume** is a virtual name for that storage.

The following is an example of the wizard panel:

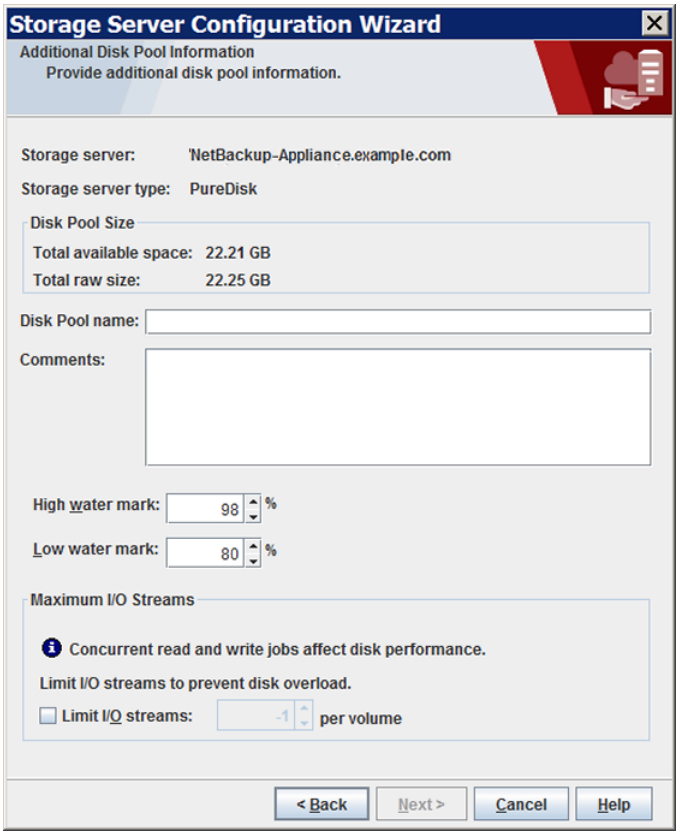


After you select the **PureDiskVolume** volume, click **Next**. The **Additional Disk Pool Information** wizard panel appears.

9 On the **Additional Disk Pool Information** panel, enter the values for this disk pool.

See "Media Server Deduplication Pool properties" on page 110.

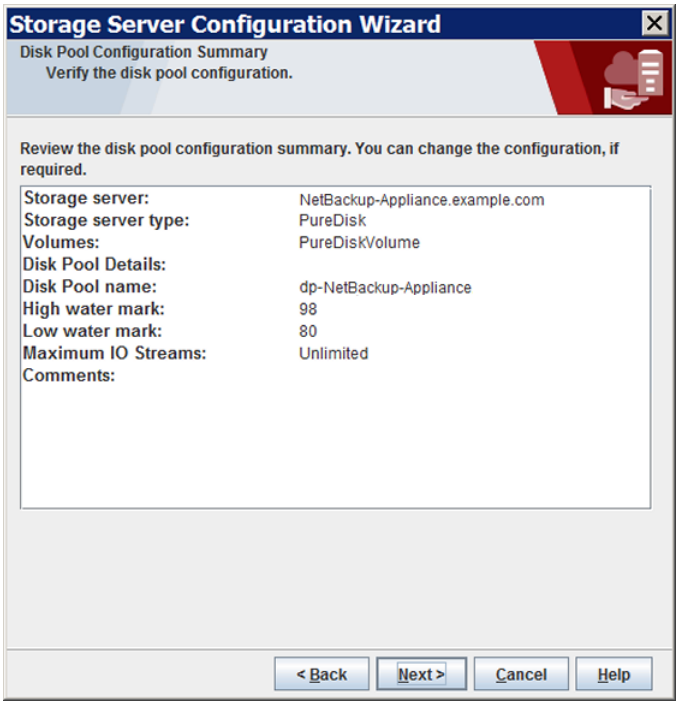
The following is an example of the wizard panel:



After you enter the appropriate information or select the necessary options, click **Next**. The **Disk Pool Configuration Summary** wizard panel appears.

10 On the **Disk Pool Configuration Summary** panel, verify the selections. If OK, click **Next**.

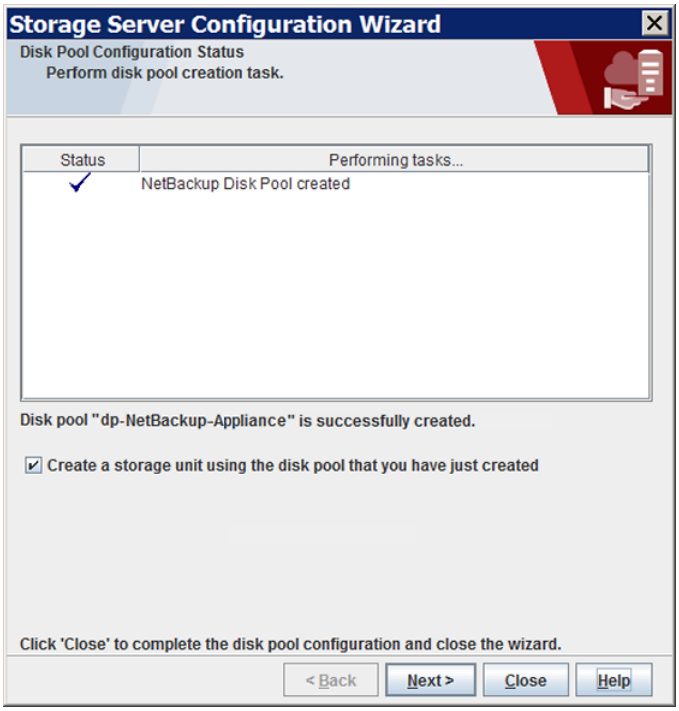
The following is an example of the wizard panel:



To configure the disk pool, click **Next**. The **Disk Pool Configuration Status** wizard panel appears.

11 The **Disk Pool Configuration Status** wizard panel describes the progress of the operation.

The following is an example of the wizard panel:



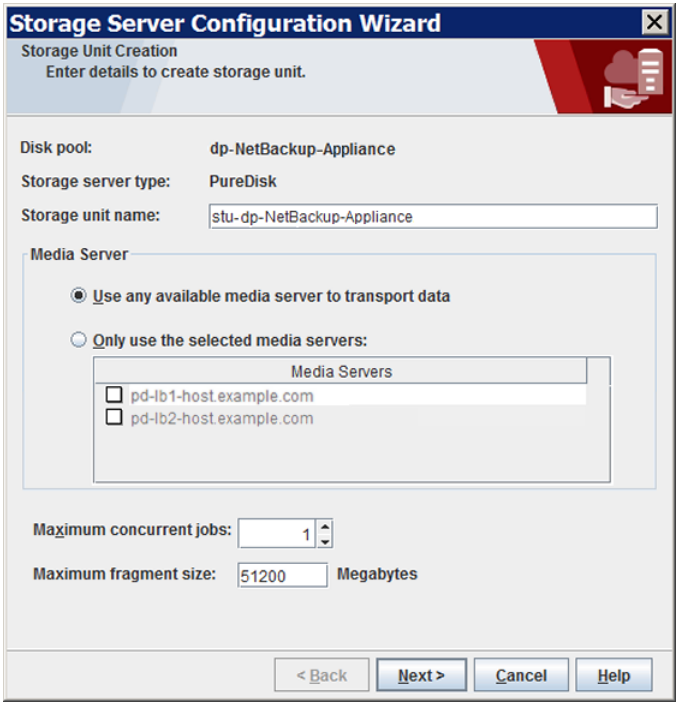
After the disk pool is created, you can do the following:

Configure a storage unit	Ensure that **Create a storage unit using the disk pool that you have just created** is selected and then click **Next**. The **Storage Unit Creation** wizard panel appears. Continue to the next step.
Exit	Click **Close**. You can configure one or more storage units later. See "Configuring a Media Server Deduplication Pool storage unit" on page 115.

12 Enter the appropriate information for the storage unit.

See “Media Server Deduplication Pool storage unit properties” on page 117.

The following is an example of the wizard panel:



After you enter the appropriate information or select the necessary options, click **Next** to create the storage unit.

13 After NetBackup configures the storage unit, the **Finished** panel appears. Click **Finish** to exit from the wizard.

About disk pools for NetBackup deduplication

NetBackup deduplication disk pools represent the storage for deduplicated backup data. NetBackup servers or NetBackup clients deduplicate the backup data that is stored in a deduplication disk pool.

Two types of deduplication pools exist, as follows:

- A NetBackup **Media Server Deduplication Pool** represents the disk storage that is attached to a NetBackup media server. NetBackup deduplicates the data and hosts the storage.

NetBackup requires exclusive ownership of the disk resources that comprise the deduplication pool. If you share those resources with other users, NetBackup cannot manage deduplication pool capacity or storage lifecycle policies correctly.

- A NetBackup **PureDisk Deduplication Pool** represents a PureDisk storage pool on a NetBackup 5000 series appliance. NetBackup deduplicates the data, and PureDisk hosts the storage.

  Note: NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only.

How many deduplication pools you configure depends on your storage requirements. It also depends on whether or not you use optimized duplication or replication, as described in the following table:

Table 5-12 Deduplication pools for duplication or replication

Type	Requirements
Optimized duplication within the same NetBackup domain	Optimized duplication in the same domain requires the following deduplication pools: ■ At least one for the backup storage, which is the source for the duplication operations. The source deduplication pool is in one deduplication node. ■ Another to store the copies of the backup images, which is the target for the duplication operations. The target deduplication pool is in a different deduplication node. See "About MSDP optimized duplication within the same domain" on page 135.
Auto Image Replication to a different NetBackup domain	Auto Image Replication deduplication pools can be either replication source or replication target. The replication properties denote the purpose of the deduplication pool. The deduplication pools inherit the replication properties from their volumes. See "About the replication topology for Auto Image Replication" on page 158. Auto Image Replication requires the following deduplication pools: ■ At least one replication source deduplication pool in the originating domain. A replication source deduplication pool is one to which you send your backups. The backup images on the source deduplication pool are replicated to a deduplication pool in the remote domain or domains. ■ At least one replication target deduplication pool in a remote domain or domains. A replication target deduplication pool is the target for the duplication operations that run in the originating domain. See "About NetBackup Auto Image Replication" on page 153.

Configuring a disk pool for deduplication

The NetBackup **Storage Server Configuration Wizard** lets you configure one disk pool during storage server configuration. To configure additional disk pools, launch the **Disk Pool Configuration Wizard**. Before you can configure a NetBackup disk pool, a NetBackup deduplication storage server must exist.

See "About disk pools for NetBackup deduplication" on page 101.

When you configure a deduplication disk pool, you specify the following:

- The type of disk pool: **PureDisk**. **PureDisk** is the type for the following disk pools:
  - A **Media Server Deduplication Pool** on the disk storage that is attached to a NetBackup deduplication media server.
  - A **PureDisk Deduplication Pool**, which represents storage on a NetBackup 5000 series appliance.
- The deduplication storage server to query for the disk storage to use for the pool.
- The disk volume to include in the pool.
  NetBackup exposes the storage as a single volume.
- The disk pool properties.
  See "Media Server Deduplication Pool properties" on page 110.

Veritas recommends that disk pool names be unique across your enterprise.

To configure a deduplication disk pool by using the wizard

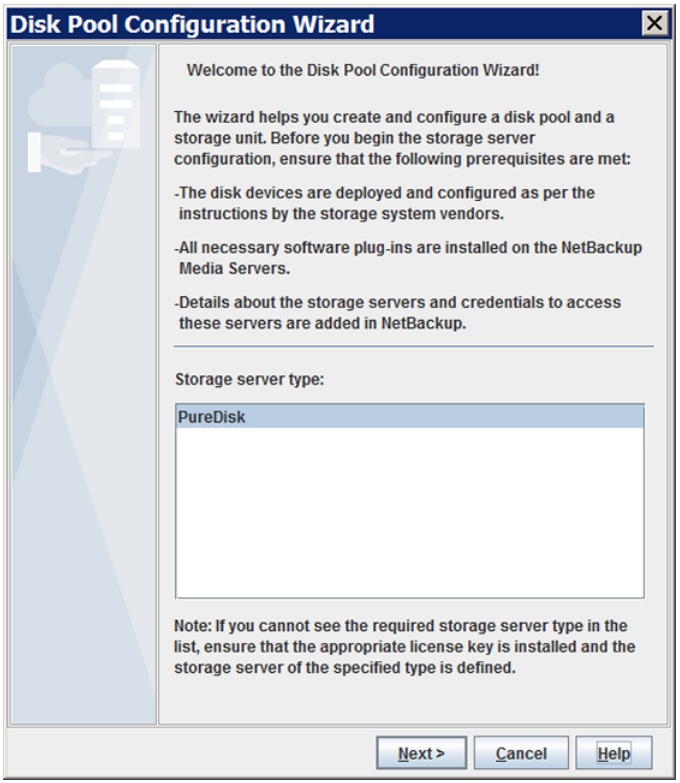
1. In the **NetBackup Administration Console**, select either **NetBackup Management** or **Media and Device Management**.
2. From the list of wizards in the right pane, click **Configure Disk Pool**.
3. Click **Next** on the welcome panel of the wizard.

   The **Disk Pool** panel appears.

4 On the **Disk Pool** panel, select **PureDisk** in the **Type** windows.

The types of disk pools that you can configure depend on the options for which you are licensed.

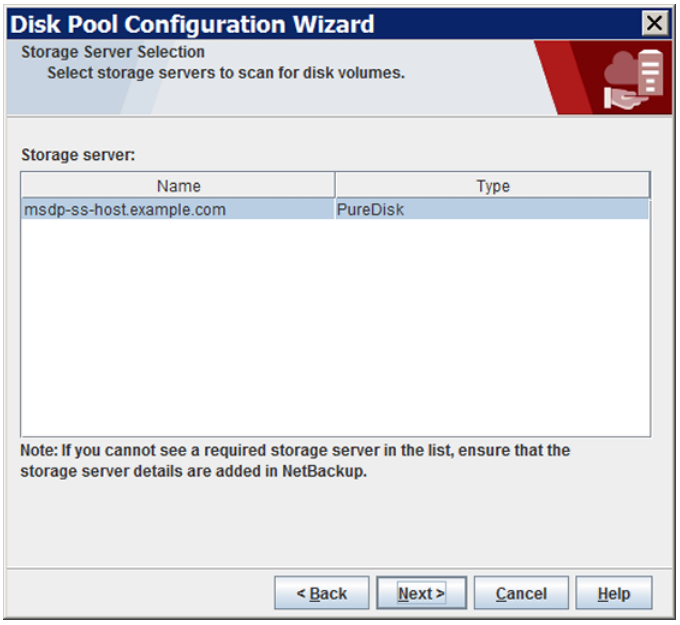
The following is an example of the wizard panel:



After you select the disk pool **Type**, click **Next**. The **Select Storage Server** wizard panel appears.

5 On the **Select Storage Server** panel, select the storage server for this disk pool. The wizard displays the deduplication storage servers that are configured in your environment. For a **PureDisk Deduplication Pool**, the storage server is the NetBackup 5000 series appliance.

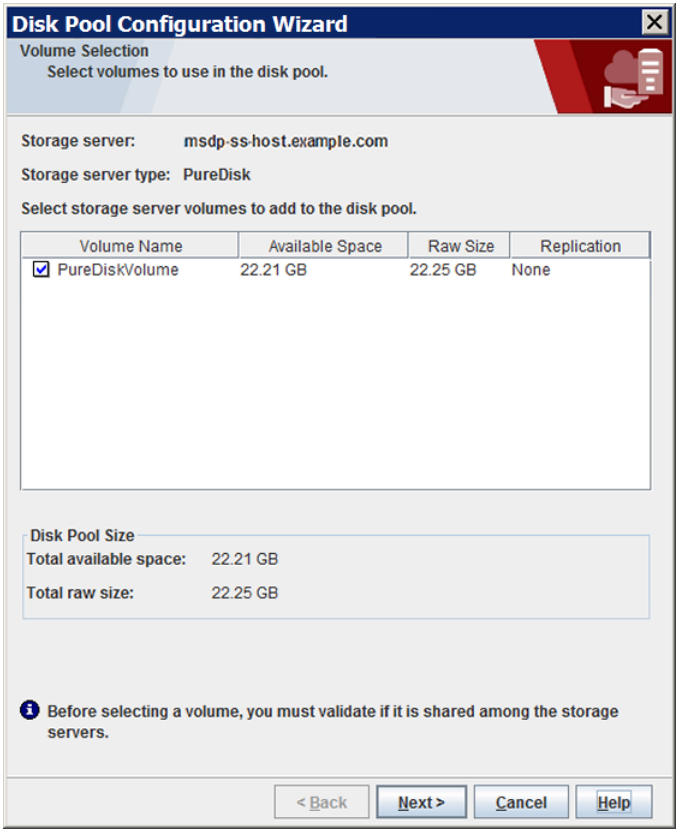
The following is an example of the wizard panel:



Click **Next**. The **Volume Selection** wizard panel appears.

6 On the **Volume Selection** panel, select the volume for this disk pool.

The following is an example of the wizard panel:



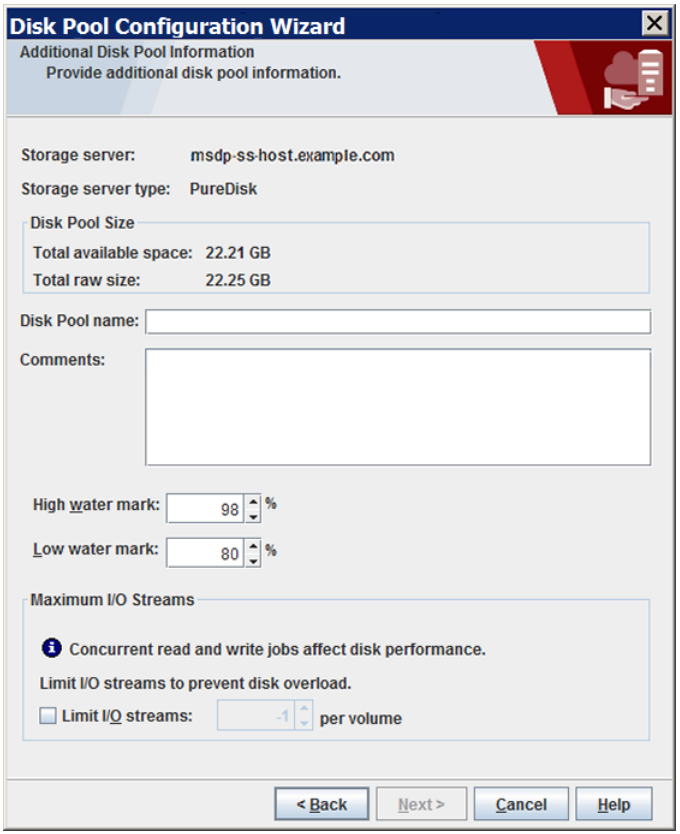
Media Server Deduplication Pool	All of storage in the **Storage Path** that you configured in the **Storage Server Configuration Wizard** is exposed as a single volume. The **PureDiskVolume** is a virtual name for that storage.
PureDisk Deduplication Pool	All of storage in the NetBackup 5000 series appliance is exposed as a single volume. The **PureDiskVolume** is a virtual name for that storage.

After you select the **PureDiskVolume** volume, click **Next**. The **Additional Disk Pool Information** wizard panel appears.

7 On the **Additional Disk Pool Information** panel, enter the values for this disk pool.

See "Media Server Deduplication Pool properties" on page 110.

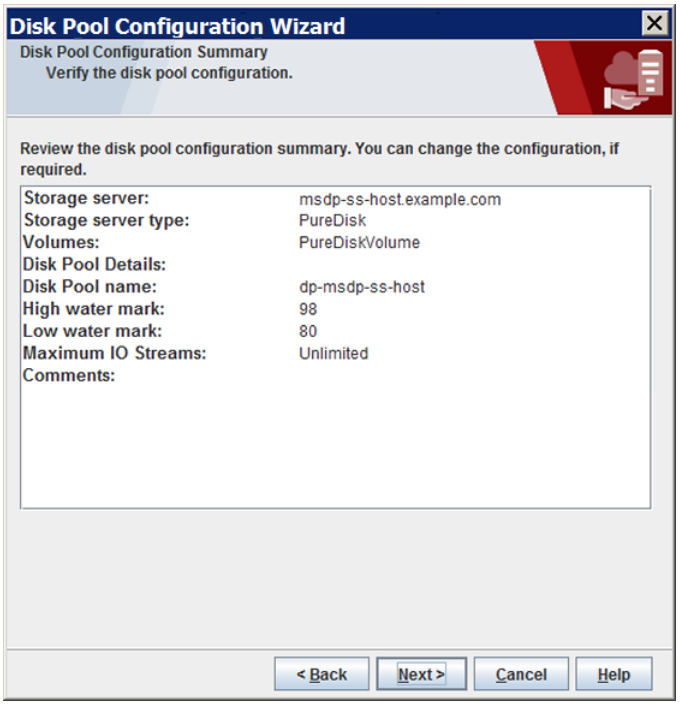
The following is an example of the wizard panel:



After you enter the appropriate information or select the necessary options, click **Next**. The **Disk Pool Configuration Summary** wizard panel appears.

8 On the **Disk Pool Configuration Summary** panel, verify the selections. If OK, click **Next**.

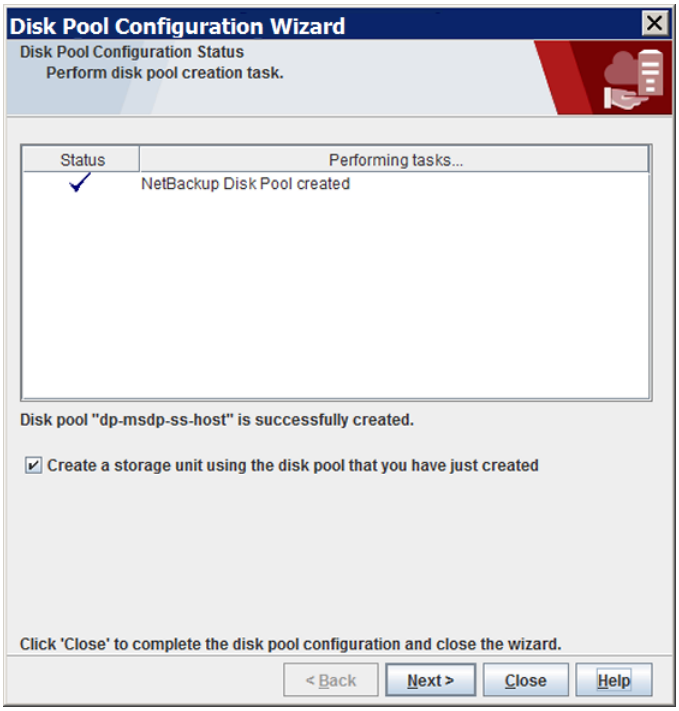
The following is an example of the wizard panel:



To configure the disk pool, click **Next**. The **Disk Pool Configuration Status** wizard panel appears.

9 The **Disk Pool Configuration Status** wizard panel describes the progress of the operation.

The following is an example of the wizard panel:



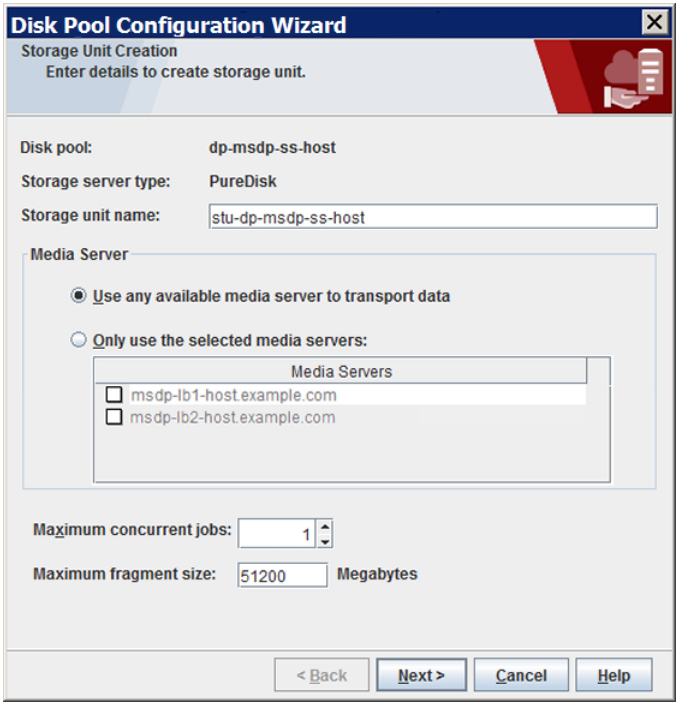
After the disk pool is created, you can do the following:

Configure a storage unit	Ensure that **Create a storage unit using the disk pool that you have just created** is selected and then click **Next**. The **Storage Unit Creation** wizard panel appears. Continue to the next step.
Exit	Click **Close**. You can configure one or more storage units later. See "Configuring a Media Server Deduplication Pool storage unit" on page 115.

10 Enter the appropriate information for the storage unit.

See “Media Server Deduplication Pool storage unit properties” on page 117.

The following is an example of the wizard panel:



After you enter the appropriate information or select the necessary options, click **Next** to create the storage unit.

11 After NetBackup configures the storage unit, the **Finished** panel appears. Click **Finish** to exit from the wizard.

Media Server Deduplication Pool properties

Table 5-13 describes the disk pool properties.

Table 5-13 Media server deduplication pool properties

Property	Description
Storage server	The storage server name. The storage server is the same as the NetBackup media server to which the storage is attached.

Table 5-13 Media server deduplication pool properties *(continued)*

Property	Description
Storage server type	For a **Media Server Deduplication Pool**, the storage type is **PureDisk**.
Disk volumes	For a **Media Server Deduplication Pool**, all disk storage is exposed as a single volume. **PureDiskVolume** is a virtual name for the storage that is contained within the directories you specified for the storage path and the database path.
Total available space	The amount of space available in the disk pool.
Total raw size	The total raw size of the storage in the disk pool.
Disk Pool name	The disk pool name. Enter a name that is unique across your enterprise.
Comments	A comment that is associated with the disk pool.
High water mark	The **High water mark** indicates that the volume is full. When the volume reaches the **High water mark**, NetBackup fails any backup jobs that are assigned to the storage unit. NetBackup also does not assign new jobs to a storage unit in which the deduplication pool is full. The **High water mark** includes the space that is committed to other jobs but not already used. The default is 98%.
Low water mark	The **Low water mark** has no affect on the **PureDiskVolume**.
Limit I/O streams	Select to limit the number of read and write streams (that is, jobs) for each volume in the disk pool. A job may read backup images or write backup images. By default, there is no limit. If you select this property, also configure the number of streams to allow per volume. When the limit is reached, NetBackup chooses another volume for write operations, if available. If not available, NetBackup queues jobs until a volume is available. Too many streams may degrade performance because of disk thrashing. Disk thrashing is excessive swapping of data between RAM and a hard disk drive. Fewer streams can improve throughput, which may increase the number of jobs that complete in a specific time period.

Table 5-13 Media server deduplication pool properties *(continued)*

Property	Description
per volume	Select or enter the number of read and write streams to allow per volume. Many factors affect the optimal number of streams. Factors include but are not limited to disk speed, CPU speed, and the amount of memory.

Creating the data directories for 96-TB MSDP support

NetBackup requires that each storage volume contain a directory named `data`.

You must create the `data` directories on the second and third volumes that are required for 96-TB support. (NetBackup creates the required `data` directory on the volume that you specify in the **Storage Server Configuration Wizard**.)

Prerequisite

- The volumes must be formatted with the file systems that NetBackup supports for MSDP and mounted on the storage server.
  See "About provisioning the storage for MSDP" on page 42.
- The storage server must be configured already.
  See "Configuring a storage server for a Media Server Deduplication Pool" on page 73.

To create the data directories for 96-TB MSDP support

- In both the second and third volumes for the **Media Server Deduplication Pool**, create a `data` subdirectory at the volumes's mount points, as follows:

  mount_point/data

  The following is an example of the mount points for the three required storage volumes:

```
/msdp/vol0  <--- NetBackup creates the data directory in this volume
/msdp/vol1  <--- Create a data directory in this volume
/msdp/vol2  <--- Create a data directory in this volume
```

Adding volumes to a 96-TB Media Server Deduplication Pool

When you configure a storage server for a 96-TB **Media Server Deduplication Pool**, you specify the pathname of the first storage volume. Before you can use the **Media Server Deduplication Pool**, you must add the other two volumes to the disk pool.

See “About provisioning the storage for MSDP” on page 42.

See “Configuring a storage server for a Media Server Deduplication Pool” on page 73.

To add the other volumes to a 96-TB Media Server Deduplication Pool

1. On the MSDP storage server, use the `crcontrol` utility to add the second and third 32-TB volumes to the disk pool. You must include the `data` directories as part of the pathname. The following is the command syntax:

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --dsaddpartition pathname
   ```

   The following two examples show how to add the pathnames for `/msdp/vol1` and `/msdp/vol2` volumes:

   ```
   # /usr/openv/pdde/pdcr/bin/crcontrol --dsaddpartition /msdp/vol1/data
   Partition /msdp/vol1/data was added successfully.

   # /usr/openv/pdde/pdcr/bin/crcontrol --dsaddpartition /msdp/vol2/data
   Partition /msdp/vol2/data was added successfully
   ```

   After the next polling cycle of the NetBackup Remote Manager and Monitor Service, the NetBackup Administration Console displays the new, expanded capacity for the disk pool.

   Note: For a **Media Server Deduplication Pool**, NetBackup exposes the storage as a single volume in the **NetBackup Administration Console**. Therefore, if you have a 96-TB **Media Server Deduplication Pool**, the number of volumes is 1 even though three volumes are used for the storage.

2. On the MSDP storage server, you can use the `crcontrol` utility to verify that the **Media Server Deduplication Pool** contains the new volumes. If the volumes were added correctly, there should be three mount points as follows:

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --dsstat 2 | grep Mount

   Mount point count: 3
   ================ Mount point   1 ================
   ================ Mount point   2 ================
   ================ Mount point   3 ================
   ```

3. To display detailed information about the disk pool, use the `crcontrol --dsstat 3` command, as follows:

   ```
   /usr/openv/pdde/pdcr/bin/crcontrol --dsstat 3
   ```

Configuring a Media Server Deduplication Pool storage unit

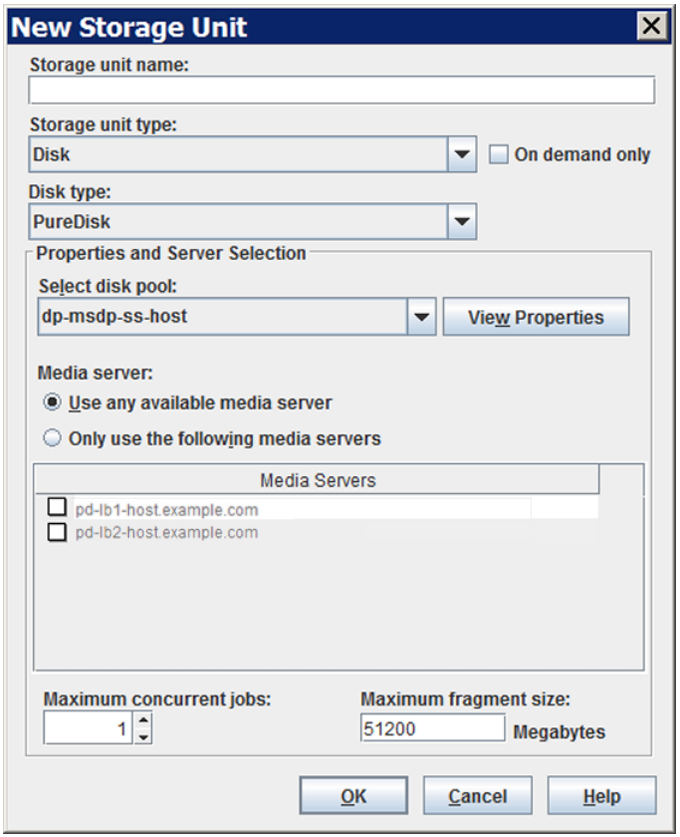
A NetBackup deduplication storage unit represents the storage in either a **Media Server Deduplication Pool** or a **PureDisk Deduplication Pool**. Create one or more storage units that reference the disk pool.

See "About disk pools for NetBackup deduplication" on page 101.

The **Disk Pool Configuration Wizard** lets you create a storage unit; therefore, you may have created a storage unit when you created a disk pool. To determine if storage units exist for the disk pool, see the **NetBackup Management > Storage > Storage Units** window of the Administration Console.

To configure a storage unit from the Actions menu

1. In the **NetBackup Administration Console**, expand **NetBackup Management > Storage > Storage Units**.
2. On the **Actions** menu, select **New > Storage Unit**.



3. Complete the fields in the **New Storage Unit** dialog box.

   For a storage unit for optimized duplication destination, select **Only use the following media servers**. Then select the media servers that are common between the two deduplication nodes.

   See "Media Server Deduplication Pool storage unit properties" on page 117.

Media Server Deduplication Pool storage unit properties

The following are the configuration options for a storage unit that has a **Media Server Deduplication Pool** as a target.

Table 5-14 Media Server Deduplication Pool storage unit properties

Property	Description
Storage unit name	A unique name for the new storage unit. The name can describe the type of storage. The storage unit name is the name used to specify a storage unit for policies and schedules. The storage unit name cannot be changed after creation.
Storage unit type	Select **Disk** as the storage unit type.
Disk type	Select **PureDisk** for the disk type for a **Media Server Deduplication Pool**.
Disk pool	Select the disk pool that contains the storage for this storage unit. All disk pools of the specified **Disk type** appear in the **Disk pool** list. If no disk pools are configured, no disk pools appear in the list.
Media server	The **Media server** setting specifies the NetBackup media servers that can deduplicate the data for this storage unit. Only the deduplication storage server and the load balancing servers appear in the media server list. Specify the media server or servers as follows: ■ To allow any server in the media server list to deduplicate data, select **Use any available media server**. ■ To use specific media servers to deduplicate the data, select **Only use the following media servers**. Then, select the media servers to allow. NetBackup selects the media server to use when the policy runs.
Maximum fragment size	For normal backups, NetBackup breaks each backup image into fragments so it does not exceed the maximum file size that the file system allows. You can enter a value from 20 MBs to 51200 MBs. For a FlashBackup policy, Veritas recommends that you use the default, maximum fragment size to ensure optimal deduplication performance. For more information, see the *NetBackup Snapshot Client Administrator's Guide*: http://www.veritas.com/docs/DOC5332

Table 5-14 Media Server Deduplication Pool storage unit properties *(continued)*

Property	Description
Maximum concurrent jobs	The **Maximum concurrent jobs** setting specifies the maximum number of jobs that NetBackup can send to a disk storage unit at one time. (Default: one job. The job count can range from 0 to 256.) This setting corresponds to the Maximum concurrent write drives setting for a Media Manager storage unit. NetBackup queues jobs until the storage unit is available. If three backup jobs are scheduled and **Maximum concurrent jobs** is set to two, NetBackup starts the first two jobs and queues the third job. If a job contains multiple copies, each copy applies toward the **Maximum concurrent jobs** count. **Maximum concurrent jobs** controls the traffic for backup and duplication jobs but not restore jobs. The count applies to all servers in the storage unit, not per server. If you select multiple media servers in the storage unit and 1 for **Maximum concurrent jobs**, only one job runs at a time. The number to enter depends on the available disk space and the server's ability to run multiple backup processes. **Warning:** A Maximum concurrent jobs setting of 0 disables the storage unit.

MSDP storage unit recommendations

You can use storage unit properties to control how NetBackup performs, as follows:

Configure a favorable client-to-server ratio

For a favorable client-to-server ratio, you can use one disk pool and configure multiple storage units to separate your backup traffic. Because all storage units use the same disk pool, you do not have to partition the storage.

For example, assume that you have 100 important clients, 500 regular clients, and four media servers. You can use two media servers to back up your most important clients and two media servers to back up you regular clients.

The following example describes how to configure a favorable client-to-server ratio:

- Configure the media servers for NetBackup deduplication and configure the storage.
- Configure a disk pool.

- Configure a storage unit for your most important clients (such as STU-GOLD). Select the disk pool. Select **Only use the following media servers**. Select two media servers to use for your important backups.
- Create a backup policy for the 100 important clients and select the STU-GOLD storage unit. The media servers that are specified in the storage unit move the client data to the deduplication storage server.
- Configure another storage unit (such as STU-SILVER). Select the same disk pool. Select **Only use the following media servers**. Select the other two media servers.
- Configure a backup policy for the 500 regular clients and select the STU-SILVER storage unit. The media servers that are specified in the storage unit move the client data to the deduplication storage server.

Backup traffic is routed to the wanted data movers by the storage unit settings.

Note: NetBackup uses storage units for media server selection for write activity (backups and duplications) only. For restores, NetBackup chooses among all media servers that can access the disk pool.

Throttle traffic to the media servers

You can use the **Maximum concurrent jobs** settings on disk pool storage units to throttle the traffic to the media servers. Effectively, this setting also directs higher loads to specific media servers when you use multiple storage units for the same disk pool. A higher number of concurrent jobs means that the disk can be busier than if the number is lower.

For example, two storage units use the same set of media servers. One of the storage units (STU-GOLD) has a higher **Maximum concurrent jobs** setting than the other (STU-SILVER). More client backups occur for the storage unit with the higher **Maximum concurrent jobs** setting.

Configuring client attributes for MSDP client-side deduplication

To configure client deduplication, set an attribute in the NetBackup master server **Client Attributes** host properties. If the client is in a backup policy in which the storage destination is a **Media Server Deduplication Pool**, the client deduplicates its own data.

To specify the clients that deduplicate backups

1. In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Master Servers**.
2. In the details pane, select the master server.
3. On the **Actions** menu, select **Properties**.
4. Select the **Client Attributes** properties.
5. On the **General** tab of the **Client Attributes** properties, add the clients that you want to deduplicate their own data to the **Clients** list, as follows:
   - Click **Add**.
   - In the **Add Client** dialog box, enter a client name or browse to select a client. Then click **Add**.
     Repeat for each client that you want to add.
   - When you finish adding clients, click **Close**.
6. Select one of the following **Deduplication Location** options:
   - **Always use the media server** disables client deduplication. By default, all clients are configured with the **Always use the media server** option.
   - **Prefer to use client-side deduplication** uses client deduplication if the deduplication plug-in is active on the client. If it is not active, a normal backup occurs; client deduplication does not occur.
   - **Always use client-side deduplication** uses client deduplication. If the deduplication backup job fails, NetBackup retries the job.

   You can override the **Prefer to use client-side deduplication** or **Always use client-side deduplication** host property in the backup policies.

   Note: NetBackup Client Direct deduplication is supported in a CloudCatalyst duplication to cloud scenario. However, Client Direct deduplication is not supported in a scenario where the backup is uploaded directly to the cloud and no duplication is configured.

   See **Disable client-side deduplication** in the *NetBackup Administrator's Guide, Volume I*:

   http://www.veritas.com/docs/DOC5332

See “Disabling MSDP client-side deduplication for a client” on page 121.

Disabling MSDP client-side deduplication for a client

You can remove a client from the list of clients that deduplicate their own data. If you do so, a deduplication server backs up the client and deduplicates the data.

To disable MSDP client deduplication for a client

1. In the NetBackup Administration Console, expand **NetBackup Management > Host Properties > Master Servers**.
2. In the details pane, select the master server.
3. On the **Actions** menu, select **Properties**.
4. On the **Host Properties Client Attributes General** tab, select the client that deduplicates its own data.
5. In the **Deduplication Location** drop-down list, select **Always use the media server**.
6. Click **OK**.

About MSDP compression

NetBackup deduplication hosts provide compression for the deduplicated data. It is separate from and different than NetBackup policy-based compression.

Compression is configured by default on all MSDP hosts. Therefore, backups, duplication traffic, and replication traffic are compressed on all MSDP hosts. The data also is compressed on storage.

Table 5-15 describes the compression options.

A different topic describes the interaction of the encryption and the compression settings for MSDP.

See “MSDP compression and encryption settings matrix” on page 124.

Table 5-15 MSDP compression options

Option	Description
Compression for backups	For backups, the deduplication plug-in compresses the data after it is deduplicated. The data remains compressed during transfer from the plug-in to the NetBackup Deduplication Engine on the storage server. The Deduplication Engine writes the encrypted data to the storage. For restore jobs, the process functions in the reverse direction. The `COMPRESSION` parameter in the `pd.conf` file on each MSDP host controls compression and decompression for that host. By default, backup compression is enabled on all MSDP hosts. Therefore, compression and decompression occur on the following hosts as necessary: ■ The clients that deduplicate their own data (that is, client-side deduplication). ■ The load balancing servers. ■ The storage server. MSDP compression cannot occur on normal NetBackup clients (that is, the clients that do not deduplicate their own data). **Note:** Do not enable backup compression by selecting the **Compression** option on the **Attributes** tab of the **Policy** dialog box. If you do, NetBackup compresses the data before it reaches the plug-in that deduplicates it. Consequently, deduplication rates are very low. Also, NetBackup does not use the Deduplication Multi-Threaded Agent if policy-based encryption is configured. See "About the MSDP Deduplication Multi-Threaded Agent" on page 54.
Compression for duplication and replication	For duplication and replication, the deduplication plug-in compresses the data for transfer. The data remains compressed during transfer from the plug-in to the NetBackup Deduplication Engine on the storage server and remains compressed on the storage. The `OPTDUP_COMPRESSION` parameter in the `pd.conf` file controls compression for duplication and replication. By default, duplication and replication compression is enabled on all MSDP hosts. Therefore, duplication and replication compression occurs on the following MSDP servers: ■ The load balancing servers. ■ The storage server. Duplication and replication compression does not apply to clients. NetBackup chooses the least busy host to initiate and manage each duplication job and replication job. To ensure that compression occurs for all optimized duplication and replication jobs: do not change the default setting of the `OPTDUP_COMPRESSION` parameter.

See "About the MSDP pd.conf configuration file" on page 197.

See "Use MSDP compression and encryption" on page 39.

About MSDP encryption

NetBackup provides encryption for the deduplicated data. It is separate from and different than NetBackup policy-based encryption. By default, MSDP encryption is disabled.

Table 5-16 describes the encryption options.

A different topic describes the interaction of the encryption and the compression settings for MSDP.

See "MSDP compression and encryption settings matrix" on page 124.

Table 5-16 MSDP encryption options

Option	Description
Backup encryption	For backups, the deduplication plug-in encrypts the data after it is deduplicated. The data remains encrypted during transfer from the plug-in to the NetBackup Deduplication Engine on the storage server. The Deduplication Engine writes the encrypted data to the storage. For restore jobs, the process functions in the reverse direction. The MSDP `pd.conf` file `ENCRYPTION` parameter controls backup encryption for individual hosts. By default, backup encryption is disabled on all MSDP hosts. If you want backup encryption, you must enable it on the following MSDP hosts: ■ The clients that deduplicate their own data (that is, client-side deduplication). ■ The MSDP load balancing servers. ■ The MSDP storage server. See "Configuring encryption for MSDP backups" on page 126. **Note:** Do not enable backup encryption by selecting the **Encryption** option on the **Attributes** tab of the **Policy** dialog box. If you do, NetBackup encrypts the data before it reaches the plug-in that deduplicates it. Consequently, deduplication rates are very low. Also, NetBackup does not use the Deduplication Multi-Threaded Agent if policy-based encryption is configured. See "About the MSDP Deduplication Multi-Threaded Agent" on page 54.

Table 5-16 MSDP encryption options *(continued)*

Option	Description
Duplication and replication encryption	For duplication and replication, the deduplication plug-in on MSDP servers encrypts the data for transfer. The data is encrypted during transfer from the plug-in to the NetBackup Deduplication Engine on the target storage server and remains encrypted on the target storage. The MSDP `pd.conf` file `OPTDUP_ENCRYPTION` parameter controls duplication and replication encryption for individual hosts. By default, duplication and replication encryption is disabled on the MSDP storage server and on the MSDP load balancing servers. If you want duplication and replication encryption, you must enable it on the following MSDP servers: ■ The load balancing servers. ■ The storage server. Duplication and replication encryption does not apply to clients. NetBackup chooses the least busy host to initiate and manage each duplication job and replication job. See "Configuring encryption for MSDP optimized duplication and replication" on page 127.

NetBackup 8.0 introduced the Advanced Encryption Standard 256 bit, CTR (AES) encryption algorithm to Media Server Deduplication Pool (MSDP). The AES encryption algorithm replaces the older Blowfish encryption algorithm.

See "About the rolling data conversion mechanism for MSDP" on page 128.

See "MSDP encryption behavior and compatibilities" on page 131.

MSDP compression and encryption settings matrix

Four MSDP `pd.conf` file parameters control the compression and the encryption for individual hosts. Table 5-17 shows the matrix for the outcomes for the compression and the encryption parameters.

Table 5-17 Compression and encryption settings and outcomes

Parameters	Default: Compress both the backups and duplication and replication	Settings A: Compress and encrypt the backups	Settings B: Compress the backups and compress and encrypt duplication and replication	Settings C: Compress and encrypt backups and compress duplication and replication	Settings D: Compress and encrypt both backups and duplication and replication
ENCRYPTION	0	1	0	1	1
COMPRESSION	1	1	1	1	1
OPTDUP_ENCRYPTION	0	0	1	0	1
OPTDUP_COMPRESSION	1	0	1	1	1
Outcomes on the disk pools	Backup MSDP: Encryption: 0 Compression: 1 Target MSDP: Encryption: 0 Compression: 1	Backup MSDP: Encryption: 1 Compression: 1 Target MSDP: Encryption: 1 Compression: 1	Backup MSDP: Encryption: 0 Compression: 1 Target MSDP: Encryption: 1 Compression: 1	Backup MSDP: Encryption: 1 Compression: 1 Target MSDP: Encryption: 1 Compression: 1	Backup MSDP: Encryption: 1 Compression: 1 Target MSDP Encryption: 1 Compression: 1
Notes		See the following note.		See the following note.	See the following note.

Note: Settings A and C have the same outcome on target storage as setting D because of the interaction of compression and encryption for the backups. If the backups are encrypted and compressed, they are also encrypted and compressed during optimized duplication and replication and encrypted and compressed on target storage. The OPTDUP_ENCRYPTION setting is ignored.

For client-side deduplication clients, a parameter on the storage server can override the pd.conf file ENCRYPTION parameter.

See "Configuring encryption for MSDP backups" on page 126.

See "About MSDP compression" on page 121.

See "About MSDP encryption" on page 123.

See "About the MSDP pd.conf configuration file" on page 197.

Configuring encryption for MSDP backups

Two procedures exist to configure encryption during backups for MSDP, as follows:

Configure encryption on individual hosts	Use this procedure to configure encryption on individual MSDP hosts. The `ENCRYPTION` parameter in the MSDP `pd.conf` file controls encryption for that host. The parameter applies only to the host on which you modify the `pd.conf`, as follows: See "To configure backup encryption on a single host" on page 126.
Configure encryption for all Client Direct clients	Use this procedure to configure encryption for all of your clients that deduplicate their own data (that is, client-side deduplication). If you use this procedure, you do not have to configure each client-side deduplication client individually. The `ServerOptions` parameter in the MSDP `contentrouter.cfg` file controls encryption for all client-side deduplication clients. This parameter supersedes the `pd.conf` file `ENCRYPTION` setting on client-side deduplication hosts. See "To configure backup encryption on all client-side deduplication clients" on page 127.

To ensure that encryption occurs for all backups jobs, configure it on all MSDP hosts. MSDP hosts include the MSDP storage server, the MSDP load balancing servers, and the NetBackup Client Direct deduplication clients.

See "About MSDP encryption" on page 123.

To configure backup encryption on a single host

1. Use a text editor to open the `pd.conf` file on the host.

   The `pd.conf` file resides in the following directories:

   - (UNIX) `/usr/openv/lib/ost-plugins/`
   - (Windows) *`install_path`*`\Veritas\NetBackup\bin\ost-plugins`

   See "MSDP pd.conf file parameters" on page 198.

2. For the line that begins with `#ENCRYPTION`, remove the pound sign (or hash sign, `#`) in column 1.

3 In that same line, replace the `0` (zero) with a `1`.

Note: The spaces to the left and right of the equal sign (=) in the file are significant. Ensure that the space characters appear in the file after you edit the file.

4 On the client-side deduplication clients and on the MSDP load balancing servers, ensure that the `LOCAL_SETTINGS` parameter in the `pd.conf` file is set to `1`. Doing so ensures that the setting on the current host has precedence over the server setting.

5 Save and close the file.

6 If the host is the storage server or a load balancing server, restart the NetBackup Remote Manager and Monitor Service (`nbrmms`) on the host.

To configure backup encryption on all client-side deduplication clients

1 On the storage server, open the `contentrouter.cfg` file in a text editor; it resides in the following directory:

- (UNIX) *storage_path*`/etc/puredisk`
- (Windows) *storage_path*`\etc\puredisk`

2 Add `agent_crypt` to the `ServerOptions` line of the file. The following line is an example:

```
ServerOptions=fast,verify_data_read,agent_crypt
```

Configuring encryption for MSDP optimized duplication and replication

The `OPTDUP_ENCRYPTION` parameter in the `pd.conf` file on the MSDP host controls duplication and replication encryption for that host. The data that is encrypted during transfer remains encrypted on the target storage.

Use this procedure to configure encryption for optimized duplication and replication on MSDP storage servers and on MSDP load balancing servers. To ensure that encryption occurs for all optimized duplication and replication jobs, configure it on all MSDP servers.

By default, optimized duplication encryption is disabled on all MSDP hosts.

See "About MSDP encryption" on page 123.

To configure replication and duplication encryption on an MSDP server

1. Use a text editor to open the `pd.conf` file on the MSDP server.

   The `pd.conf` file resides in the following directories:

   - (UNIX) `/usr/openv/lib/ost-plugins/`
   - (Windows) *`install_path`*`\Veritas\NetBackup\bin\ost-plugins`

2. For the line that begins with `#OPTDUP_ENCRYPTION`, remove the pound sign (or hash sign, `#`) in column 1.

3. In that same line, replace the `0` (zero) with a `1`.

   Note: The spaces to the left and right of the equal sign (=) in the file are significant. Ensure that the space characters appear in the file after you edit the file.

   See "MSDP pd.conf file parameters" on page 198.

4. On load balancing servers, ensure that the `LOCAL_SETTINGS` parameter is set to `1`. Doing so ensures that the `ENCRYPTION` setting on the load balancing server is used.

5. Save and close the file.

6. Restart the NetBackup Remote Manager and Monitor Service (`nbrmms`) on the host.

About the rolling data conversion mechanism for MSDP

To ensure that data is encrypted and secured with the highest standards, NetBackup uses the AES encryption algorithm and SHA-2 fingerprinting algorithm beginning with the 8.1 release. Specifically, MSDP uses AES-256 and SHA-512/256.

In NetBackup 8.1, with the introduction of the AES and the SHA-2 algorithms, we want to convert the data that is encrypted and computed with the older algorithms (Blowfish and MD5-like) to the newer algorithms (AES-256 and SHA-512/256).

The environments that are upgraded to NetBackup 8.1 may include Blowfish encrypted data and the MD5-like fingerprints that need to be converted to the new format. To handle the conversion and secure the data, a new internal task converts the current data container to the AES-256 encryption and the SHA-512/256 fingerprint algorithm. This new task is referred to as the rolling data conversion.

The conversion begins automatically after an upgrade to NetBackup 8.0. You can control some aspects of the conversion process or stop it entirely.

Rolling data conversion traverses all existing data containers. If the data is encrypted with the Blowfish algorithm, the data is re-encrypted with the AES-256 algorithm. Then a new SHA-512/256 fingerprint is generated. After the conversion, the data container has an additional `.map` file, in addition to the `.bhd` and `.bin` files. The `.map` file contains the mapping between the SHA-512/256 and the MD5-like fingerprints. It is used for the compatibility between SHA-512/256 fingerprints and MD5-like fingerprints. The `.bhd` file includes the SHA-512/256 fingerprints.

When you upgrade to NetBackup 8.1.1, there might be encrypted data that is not encrypted using a customer key. The encrypted data must be encrypted by a customer key and to handle the data conversion and secure the data, a new internal task encrypts the existing data using a customer key. After the encryption and the fingerprint rolling conversion completes, the KMS rolling conversion begins.

Modes of rolling data conversion

MSDP uses the rolling data conversion mechanism to convert Blowfish encrypted data to AES-256 encrypted data, and MD5-like fingerprints to SHA-512/256 fingerprints, in parallel. There are two modes of data conversion: normal mode and fast mode.

- Normal mode: By default, the data conversion process starts in a normal mode for an upgraded system. Similar to compaction, the data conversion runs only when no backup, restore, or Content Router Queue Processing (CRQP) jobs are active.

  In the normal mode, the time for data conversion depends on the following factors:

  - Total size of the storage
  - Power of the CPU
  - Workload on the system

  Data conversion in the normal mode may take a longer time.

  Veritas tests in a controlled environment showed that for a single 1-TB mount point, the conversion speed is about 50MB/s in normal mode.

- Fast mode: In the fast mode, the data conversion disables cyclic redundancy checks and compaction. The rolling data conversion runs while backup, restore, duplication, or CRQP jobs are active.

  Veritas tests in a controlled environment showed that for a single 1-TB mount point, the conversion speed is about 105MB/s in fast mode.

Note: The performance numbers shown were observed in the Veritas test environment and are not a guarantee of performance in your environment.

In a new installation of NetBackup 8.1, the rolling data conversion is marked as **Finished** and does not start in the future. For an upgrade to NetBackup 8.1, the rolling data conversion is enabled by default and works in the background after the MSDP conversion completes. Only the data that existed before upgrade is converted. All new data uses the new SHA-512/256 fingerprint and does not need conversion.

While in **Fast mode**, the rolling data conversion affects the performance of backup, restore, duplication, and replication jobs. To minimize this effect, use the **Normal mode**, which pauses the conversion when the system is busy, but slows down the conversion process. The **Fast mode** keeps the conversion active regardless of system state.

You can manage and monitor the rolling data conversion using the following `crcontrol` command options.

Table 5-18 MSDP `crcontrol` command options for rolling data conversion

Option	Description
`--dataconverton`	To start the data conversion process, use the `--dataconverton` option: Windows: *`install_path`*`\Veritas\pdde\Crcontrol.exe --dataconverton` UNIX: `/usr/openv/pdde/pdcr/bin/crcontrol --dataconverton`
`--dataconvertoff`	To stop the data conversion process, use the `--dataconverton` option: Windows: *`install_path`*`\Veritas\pdde\Crcontrol.exe --dataconvertoff` UNIX: `/usr/openv/pdde/pdcr/bin/crcontrol --dataconvertoff`

Table 5-18 MSDP `crcontrol` command options for rolling data conversion *(continued)*

Option	Description
`--dataconvertstate`	To determine the mode of data conversion and the conversion progress, use the `--dataconvertstate` option: Windows: *`install_path`*`\Veritas\pdde\Crcontrol.exe --dataconvertstate` UNIX: `/usr/openv/pdde/pdcr/bin/crcontrol --dataconvertstate`
`--dataconvertmode`	To switch between the normal mode and fast mode of data conversion, use the `--dataconvertmode` option: Windows: *`install_path`*`\Veritas\pdde\Crcontrol.exe --dataconvertmode` *`mode`* UNIX: `/usr/openv/pdde/pdcr/bin/crcontrol --dataconvertmode <mode>` The default value for the *<mode>* variable is 0, which stands for the normal mode. To switch data conversion from normal mode to fast mode, enter 1 for the value of the *<mode>*variable.

MSDP encryption behavior and compatibilities

MSDP supports multiple encryption algorithms. Therefore, it manages both the Blowfish and the AES encrypted data to ensure data compatibility.

For restore operations, MSDP recognizes the Blowfish data and the AES data to be able to restore the old backup images.

The following tables describe the encryption behavior for backup, duplication, and replication operations when the encryption is in progress.

Table 5-19 Encryption behavior for a backup operation to a NetBackup 8.0 storage server

Type of client	Data encryption format
Client with NetBackup 8.0, including the Client Direct deduplication	AES

Table 5-19 Encryption behavior for a backup operation to a NetBackup 8.0 storage server *(continued)*

Type of client	Data encryption format
Client with NetBackup version earlier than 8.0, excluding Client Direct deduplication	AES
Client with NetBackup version earlier than 8.0, using the Client Direct deduplication	AES (using inline data conversion)
Load balancing server with NetBackup version 8.0	AES
Load balancing server with NetBackup version earlier than 8.0	AES (using inline data conversion)

Table 5-20 Encryption behavior for optimized duplication and Auto Image Replication operations to a NetBackup 8.0 target server

Type of source storage	Data encryption format for the duplication or the replication data that is encrypted with AES	Data encryption format for the duplication or the replication data that is encrypted with Blowfish
Source server with NetBackup 8.0	AES	AES (using inline data conversion)
Source server with NetBackup version earlier than 8.0	Not applicable	AES (using inline data conversion)

Note: Inline data conversion takes place simultaneously while the backup, duplication, or replication operations are in progress.

Configuring optimized synthetic backups for MSDP

To configure optimized synthetic backups for MSDP, you must select the **Synthetic backup** policy attribute.

To configure optimized synthetic backups for MSDP

1. Configure a **Standard** or **MS-Windows** backup policy.

   See "Creating a backup policy" on page 187.

2. Select the **Synthetic backup** attribute on the **Schedule Attribute** tab of the backup policy.

See "Setting MSDP storage server attributes" on page 281.

See "Creating a backup policy" on page 187.

About a separate network path for MSDP duplication and replication

You can use a different network for MSDP duplication and replication traffic rather than the one you use for MSDP backups. Both the duplication and the replication data traffic and the control traffic travel over the separate network. Your MSDP traffic uses two different networks, as follows:

Backups and restores	For backups and restores, NetBackup uses the network interface that was configured during the storage server configuration. Both the backup and restore traffic and the control traffic travel over the *backup* network. See "About the network interface for MSDP" on page 31.
Duplication and replication	For the duplication and the replication traffic, configure your host operating systems to use a different network than the one you use for backups and restores. Both the duplication and the replication data traffic and the control traffic travel over the *duplication and replication* network. See "Configuring a separate network path for MSDP duplication and replication" on page 134. When you configure the optimized duplication or replication target, ensure that you select the host name that represents the *duplication and replication* network.

See "About MSDP optimized duplication within the same domain" on page 135.

See "About MSDP replication to a different domain" on page 150.

Configuring a separate network path for MSDP duplication and replication

You can use a different network for MSDP duplication and replication traffic rather than the one you use for MSDP backups. Both the duplication and the replication data traffic and the control traffic travel over the separate network.

See "About a separate network path for MSDP duplication and replication" on page 133.

This procedure describes how to use the storage servers `hosts` files to route the traffic onto the separate network.

The following are the prerequisites:

- Both the source and the destination storage servers must have a network interface card that is dedicated to the other network.
- The separate network must be operational and using the dedicated network interface cards on the source and the destination storage servers.
- On UNIX MSDP storage servers, ensure that the Name Service Switch first checks the local `hosts` file for before querying the Domain Name System (DNS). See the operating system documentation for information about the Name Service Switch.

To configure a separate network path for MSDP duplication and replication

1. On the source storage server, add the destination storage servers's dedicated network interface to the operating system `hosts` file. If *TargetStorageServer* is the name of the destination host on the network that is dedicated for duplication, the following is an example of the `hosts` entry in IPv4 notation:

   ```
   10.10.10.1    TargetStorageServer.example.com    TargetStorageServer
   ```

   Veritas recommends that you always use the fully qualified domain name when you specify hosts.

2. On the destination storage server, add the source storage servers's dedicated network interface to the operating system `hosts` file. If *SourceStorageServer* is the name of the source host on the network that is dedicated for duplication, the following is an example of the `hosts` entry in IPv4 notation:

   ```
   10.80.25.66    SourceStorageServer.example.com    SourceStorageServer
   ```

   Veritas recommends that you always use the fully qualified domain name when specifying hosts.

3 To force the changes to take effect immediately, flush the DNS cache. See the operating system documentation for how to flush the DNS cache.

4 From each host, use the `ping` command to verify that each host resolves the name of the other host.

```
SourceStorageServer.example.com> ping TargetStorageServer.example.com
TargetStorageServer.example.com> ping SourceStorageServer.example.com
```

If the `ping` command returns positive results, the hosts are configured for duplication and replication over the separate network.

5 When you configure the target storage server, ensure that you select the host name that represents the alternate network path.

About MSDP optimized duplication within the same domain

Optimized duplication within the same domain copies the deduplicated backup images between **Media Server Deduplication Pools** within the same domain. The source and the destination storage must use the same NetBackup master server.

The optimized duplication operation is more efficient than normal duplication. Only the unique, deduplicated data segments are transferred. Optimized duplication reduces the amount of data that is transmitted over your network.

Optimized duplication is a good method to copy your backup images off-site for disaster recovery.

The following table describes the supported sources and targets.

Table 5-21 MSDP optimized duplication source and targets

Source storage	Target storage
Media Server Deduplication Pool	**Media Server Deduplication Pool**
Media Server Deduplication Pool	**PureDisk Deduplication Pool**
PureDisk Deduplication Pool	**PureDisk Deduplication Pool**
PureDisk Deduplication Pool	**Media Server Deduplication Pool**

Note: A **PureDisk Deduplication Pool** in NetBackup represents the storage on a NetBackup 5000 series appliance. NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only.

By default, NetBackup does not retry failed optimized duplication jobs invoked by NetBackup Vault of the `bpduplicate` command. You can change that behavior.

See "Configuring NetBackup optimized duplication or replication behavior" on page 147.

You can use a separate network for the duplication traffic.

See "About a separate network path for MSDP duplication and replication" on page 133.

See "Configuring MSDP optimized duplication within the same NetBackup domain" on page 143.

Review the following requirements and limitations.

About MSDP optimized duplication requirements

The following are the requirements for optimized duplication within the same NetBackup domain:

- The source storage and the destination storage must have at least one media server in common.
  See "About the media servers for MSDP optimized duplication within the same domain" on page 138.
- In the storage unit you use for the destination for the optimized duplication, you must select only the common media server or media servers.
  If you select more than one, NetBackup assigns the duplication job to the least busy media server. If you select a media server or servers that are not in common, the optimized duplication job fails.
  For more information about media server load balancing, see the *NetBackup Administrator's Guide, Volume I*:
  http://www.veritas.com/docs/DOC5332
- The destination storage unit cannot be the same as the source storage unit.

About MSDP optimized duplication limitations

The following are limitations for optimized duplication within the same NetBackup domain:

- If an optimized duplication job fails after the configured number of retries, NetBackup does not run the job again.
  By default, NetBackup retries an optimized duplication job three times. You can change the number of retries.
  See "Configuring NetBackup optimized duplication or replication behavior" on page 147.

- NetBackup does not support MSDP optimized duplication to storage unit groups. If you use a storage unit group as a destination for optimized duplication, NetBackup uses regular duplication.
- Optimized duplication does not support multiple copies. If NetBackup is configured to make multiple new copies from the (source) copy of the backup image, the following occurs:
  - In a storage lifecycle policy, one duplication job creates one optimized duplication copy. If multiple optimized duplication destinations exist, a separate job exists for each destination. This behavior assumes that the device for the optimized duplication destination is compatible with the device on which the source image resides.

    If multiple remaining copies are configured to go to devices that are not optimized duplication capable, NetBackup uses normal duplication. One duplication job creates those multiple copies.
  - For other duplication methods, NetBackup uses normal duplication. One duplication job creates all of the copies simultaneously. The other duplication methods include the following: NetBackup Vault, the `bpduplicate` command line, and the duplication option of the **Catalog** utility in the **NetBackup Administration Console**.
- For optimized duplication between two **PureDisk Deduplication Pools**, NetBackup reports that the deduplication rate is 100%. However, deduplication does not occur during optimized duplication. Therefore, ignore the deduplication rate statistics.

  Note: NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only.

- The copy operation uses the maximum fragment size of the source storage unit, not the setting for the destination storage unit. The optimized duplication copies the image fragments as is. For greater efficiency, the duplication does not resize and reshuffle the images into a different set of fragments on the destination storage unit.
- If the destination is a **PureDisk Deduplication Pool**, that PureDisk storage domain can be the destination of duplication from one NetBackup domain only. If you try to duplicate from MSDP storage in more than one NetBackup domain, optimized duplication does not function correctly.

  Note: NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only.

About the media servers for MSDP optimized duplication within the same domain

For optimized **Media Server Deduplication Pool** duplication within the same domain, the source storage and the destination storage must have at least one media server in common. The common server initiates, monitors, and verifies the duplication operation. The common server requires credentials for both the source storage and the destination storage. (For deduplication, the credentials are for the NetBackup Deduplication Engine, not for the host on which it runs.)

Which media server initiates the duplication operation determines if it is a push or a pull operation, as follows:

- If the media server is co-located physically with the source storage server, it is push duplication.
- If the media server is co-located physically with the destination storage server, it is a pull duplication.

Technically, no advantage exists with a push duplication or a pull duplication. However, the media server that initiates the duplication operation also becomes the write host for the new image copies.

A storage server or a load balancing server can be the common server. The common server must have the credentials and the connectivity for both the source storage and the destination storage.

About MSDP push duplication within the same domain

Figure 5-1 shows a push configuration for optimized duplication within the same domain. The local deduplication node contains normal backups; the remote deduplication node is the destination for the optimized duplication copies. Load balancing server LB_L2 has credentials for both storage servers; it is the common server.

Figure 5-1 Push duplication environment

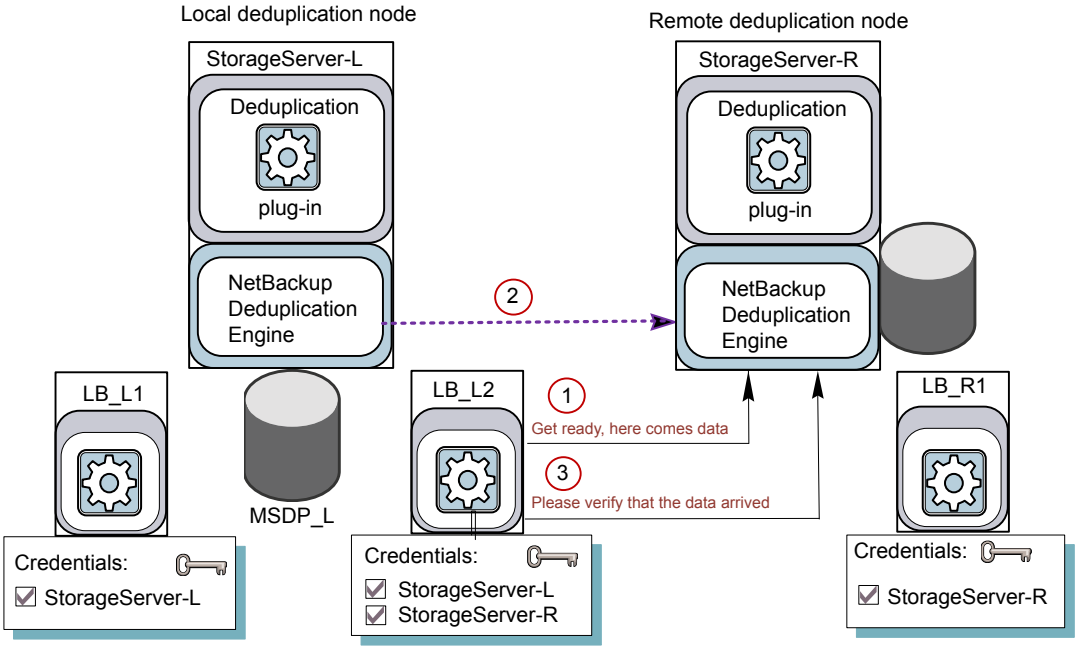


Figure 5-2 shows the settings for the storage unit for the normal backups for the local deduplication node. The disk pool is the **MSDP_L** in the local environment. Because all hosts in the local node are co-located, you can use any available media server for the backups.

Figure 5-2 Storage unit settings for backups to MSDP_L

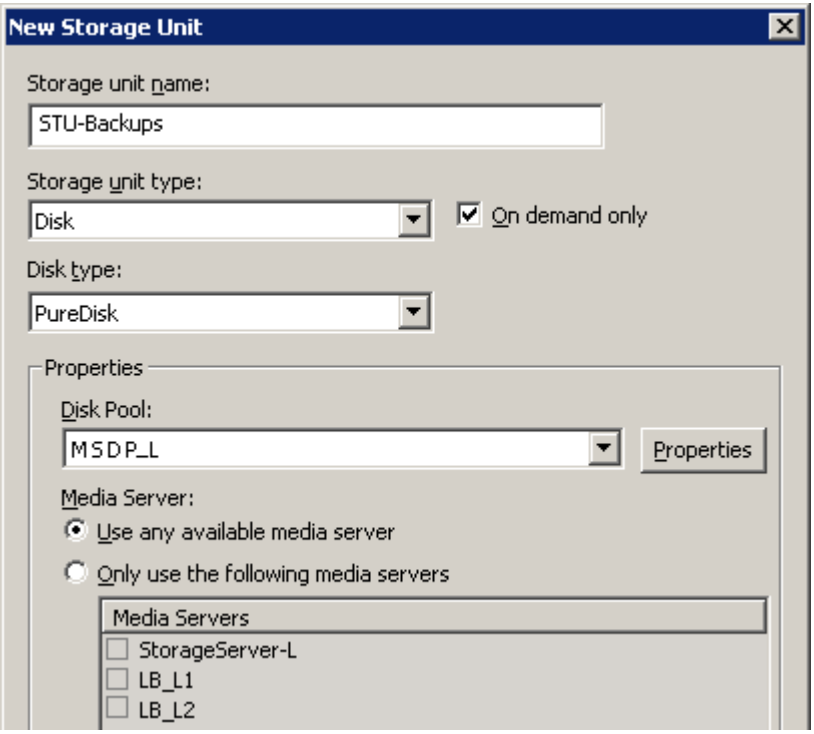
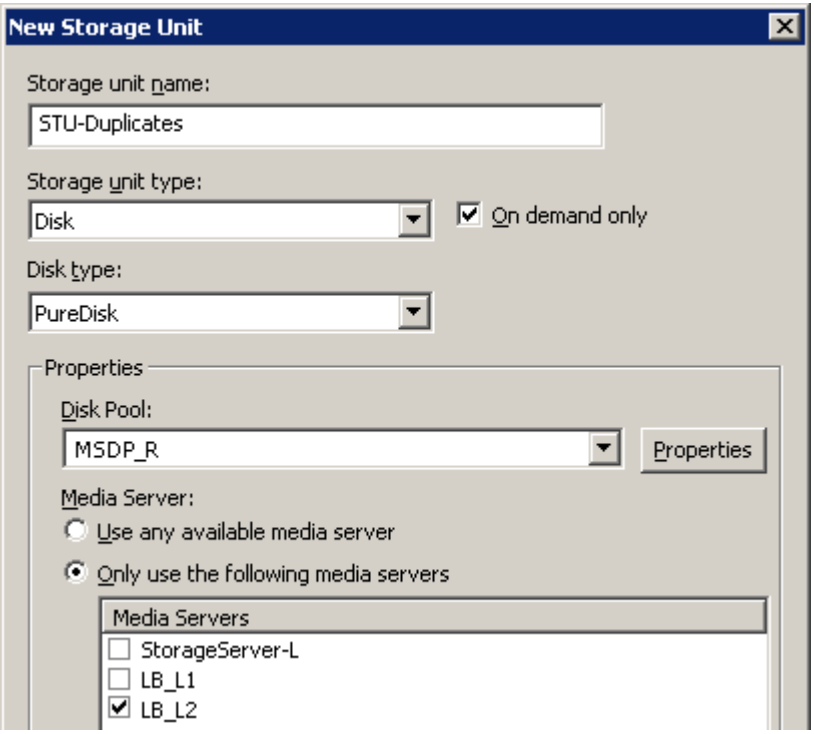


Figure 5-3 shows the storage unit settings for the optimized duplication. The destination is the **MSDP_R** in the remote environment. You must select the common server, so only load balancing server LB_L2 is selected.

Figure 5-3 Storage unit settings for duplication to MSDP_R



If you use the remote node for backups also, select **StorageServer-R** and load balancing server **LB_R1** in the storage unit for the remote node backups. If you select server **LB_L2**, it becomes a load balancing server for the remote **Media Server Deduplication Pool**. In such a case, data travels across your WAN.

You can use a load balancing server when you duplicate between two NetBackup deduplication pools.

About MSDP pull duplication within the same domain

Figure 5-4 shows a pull configuration for optimized duplication within the same domain. Deduplication node A contains normal backups; deduplication node B is the destination for the optimized duplication copies. Host B has credentials for both nodes; it is the common server.

Figure 5-4 Pull duplication

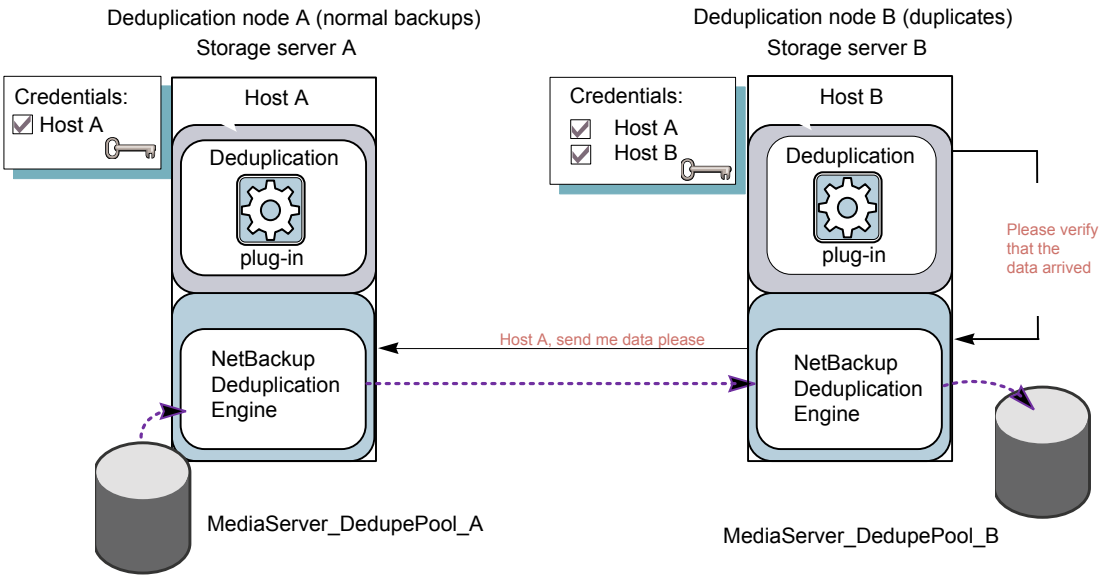
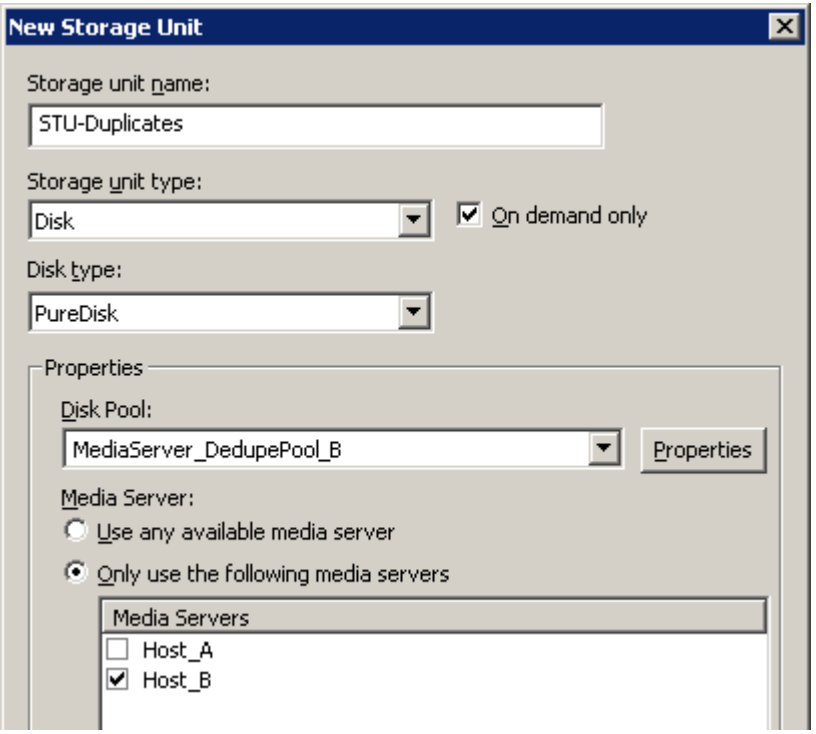


Figure 5-5 shows the storage unit settings for the duplication destination. They are similar to the push example except host B is selected. Host B is the common server, so it must be selected in the storage unit.

Figure 5-5 Pull duplication storage unit settings



If you use node B for backups also, select host B and not host A in the storage unit for the node B backups. If you select host A, it becomes a load balancing server for the node B deduplication pool.

Configuring MSDP optimized duplication within the same NetBackup domain

You can configure optimized duplication from a **Media Server Deduplication Pool** to other deduplication storage within the same NetBackup domain.

Table 5-22 How to configure optimized duplication of deduplicated data

Step	Action	Description
Step 1	Review optimized duplication	See "About MSDP optimized duplication within the same domain" on page 135.

Table 5-22 How to configure optimized duplication of deduplicated data *(continued)*

Step	Action	Description
Step 2	Configure the storage servers	See "Configuring a storage server for a Media Server Deduplication Pool" on page 73. One server must be common between the source storage and the destination storage. Which you choose depends on whether you want a push or a pull configuration. See "About the media servers for MSDP optimized duplication within the same domain" on page 138. For a push configuration, configure the common server as a load balancing server for the storage server for your normal backups. For a pull configuration, configure the common server as a load balancing server for the storage server for the copies at your remote site. Alternatively, you can add a server later to either environment. (A server becomes a load balancing server when you select it in the storage unit for the deduplication pool.)
Step 3	Configure the deduplication pools	If you did not configure the deduplication pools when you configured the storage servers, use the **Disk Pool Configuration Wizard** to configure them. See "Configuring a disk pool for deduplication" on page 103.
Step 4	Configure the storage unit for backups	In the storage unit for your backups, do the following: **1** For the **Disk type**, select **PureDisk**. **2** For the **Disk pool**, select your **Media Server Deduplication Pool** or **PureDisk Deduplication Pool**. **Note:** NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only. If you use a pull configuration, do not select the common media server in the backup storage unit. If you do, NetBackup uses it to deduplicate backup data. (That is, unless you want to use it for a load balancing server for the source deduplication node.) See "Configuring a Media Server Deduplication Pool storage unit" on page 115.

Table 5-22 How to configure optimized duplication of deduplicated data *(continued)*

Step	Action	Description
Step 5	Configure the storage unit for duplication	Veritas recommends that you configure a storage unit specifically to be the target for the optimized duplication. Configure the storage unit in the deduplication node that performs your normal backups. Do not configure it in the node that contains the copies. In the storage unit that is the destination for your duplicated images, do the following: **1** For the **Disk type**, select **PureDisk**. **2** For the **Disk pool**, the destination can be a **Media Server Deduplication Pool** or a **PureDisk Deduplication Pool**. **Note:** NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only. Also select **Only use the following media servers**. Then, select the media server or media servers that are common to both the source storage server and the destination storage server. If you select more than one, NetBackup assigns the duplication job to the least busy media server. If you select only a media server (or servers) that is not common, the optimized duplication job fails. See "Configuring a Media Server Deduplication Pool storage unit" on page 115.
Step 6	Configure optimized duplication bandwidth	Optionally, you can configure the bandwidth for replication. See "About configuring MSDP optimized duplication and replication bandwidth" on page 177.
Step 7	Configure optimized duplication behaviors	Optionally, you can configure the optimized duplication behavior. See "Configuring NetBackup optimized duplication or replication behavior" on page 147. See "About configuring MSDP optimized duplication and replication bandwidth" on page 177.

Table 5-22 How to configure optimized duplication of deduplicated data *(continued)*

Step	Action	Description
Step 8	Configure a storage lifecycle policy for the duplication	Configure a storage lifecycle policy only if you want to use one to duplicate images. The storage lifecycle policy manages both the backup jobs and the duplication jobs. Configure the lifecycle policy in the deduplication environment that performs your normal backups. Do not configure it in the environment that contains the copies. When you configure the storage lifecycle policy, do the following: ■ The first operation must be a **Backup**. For the **Storage** for the **Backup** operation, select the storage unit that is the target of your backups. That storage unit may use a **Media Server Deduplication Pool** or a **PureDisk Deduplication Pool**. These backups are the primary backup copies; they are the source images for the duplication operation. ■ For the second, child **Operation**, select **Duplication**. Then, select the storage unit for the destination deduplication pool. That pool may be a **Media Server Deduplication Pool** or a **PureDisk Deduplication Pool**. **Note:** NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only. See "About storage lifecycle policies" on page 178. See "Creating a storage lifecycle policy" on page 181.
Step 9	Configure a backup policy	Configure a policy to back up your clients. Configure the backup policy in the deduplication environment that performs your normal backups. Do not configure it in the environment that contains the copies. ■ If you use a storage lifecycle policy to manage the backup job and the duplication job: Select that storage lifecycle policy in the **Policy storage** field of the Policy **Attributes** tab. ■ If you do not use a storage lifecycle policy to manage the backup job and the duplication job: Select the storage unit that contains your normal backups. These backups are the primary backup copies. **Note:** NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only. See "About MSDP backup policy configuration" on page 186. See "Creating a backup policy" on page 187.

Table 5-22 How to configure optimized duplication of deduplicated data *(continued)*

Step	Action	Description

Step 10	Configure NetBackup Vault for the duplication	Configure Vault duplication only if you use NetBackup Vault to duplicate the images.
		
		Configure Vault in the deduplication environment that performs your normal backups. Do not configure it in the environment that contains the copies.
		
		For Vault, you must configure a Vault profile and a Vault policy.
		
		■ Configure a Vault profile.
		  ■ On the Vault **Profile** dialog box **Choose Backups** tab, choose the backup images in the source **Media Server Deduplication Pool** or a **PureDisk Deduplication Pool**.
		  ■ On the **Profile** dialog box **Duplication** tab, select the destination storage unit in the **Destination Storage unit** field.
		■ Configure a Vault policy to schedule the duplication jobs. A Vault policy is a NetBackup policy that is configured to run Vault jobs.
		
		Note: NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only.

Step 11	Duplicate by using the `bpduplicate` command	Use the NetBackup `bpduplicate` command only if you want to duplicate images manually. Duplicate from a **Media Server Deduplication Pool** or a **PureDisk Deduplication Pool** to another **Media Server Deduplication Pool** or another **PureDisk Deduplication Pool** in the same domain. **Note:** NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only. See the *NetBackup Commands Reference Guide*: http://www.veritas.com/docs/DOC5332

Configuring NetBackup optimized duplication or replication behavior

You can configure some optimized duplication and replication behaviors for NetBackup. The behaviors depend on how NetBackup duplicates the images, as described in the following table.

Table 5-23 Optimized duplication behavior

Behavior	Description
Duplication by using NetBackup Vault or the `bpduplicate` command	If you use NetBackup Vault or the `bpduplicate` command for duplication, you can configure the following behaviors: ■ Number of optimized duplication attempts. You can change the number of times NetBackup retries an optimized duplication job before it fails the jobs. See "To configure the number of duplication attempts" on page 148. ■ Optimized duplication failover. By default, if an optimized duplication job fails, NetBackup does not run the job again. You can configure NetBackup to use normal duplication if an optimized duplication job fails. See "To configure optimized duplication failover" on page 149.
Duplication or replication by using a storage lifecycle policy	If a storage lifecycle policy optimized duplication or replication job fails, NetBackup waits 2 hours and retries the job again. NetBackup repeats the retry behavior until the job succeeds or the source backup image expire. You can change the number of hours for the wait period. See "To configure the storage lifecycle policy wait period" on page 149.

If you use a storage lifecycle policy for duplication, do not configure optimized duplication behavior for NetBackup Vault or the `bpduplicate` command, and vice versa. NetBackup behavior may not be predictable.

Caution: These settings affect all optimized duplication jobs; they are not limited to a specific NetBackup storage option.

To configure the number of duplication attempts

◆ On the master server, create a file named `OPT_DUP_BUSY_RETRY_LIMIT`. Add an integer to the file that specifies the number of times to retry the job before NetBackup fails the job.

The file must reside on the master server in the following directory (depending on the operating system):

■ UNIX: `/usr/openv/netbackup/db/config`

- Windows: *install_path*\NetBackup\db\config.

To configure optimized duplication failover

- On the master server, add the following configuration option:

  RESUME_ORIG_DUP_ON_OPT_DUP_FAIL = TRUE

  See "Setting NetBackup configuration options by using the command line" on page 149.

  Alternatively on UNIX systems, you can add the entry to the bp.conf file on the NetBackup master server.

To configure the storage lifecycle policy wait period

1. in the **NetBackup Administration Console**, expand **NetBackup Management** > **Host Properties** > **Master Servers**. Select the master server, and then on the **Actions** menu click **Properties**.
2. Select **SLP Parameters**.
3. Change the **Extended image retry interval** to the new value.
4. Click **OK**.

Setting NetBackup configuration options by using the command line

Veritas recommends that you use the **NetBackup Administration Console Host Properties** to configure NetBackup properties.

However, some properties cannot be set by using the **Administration Console**. You can set those properties by using the following NetBackup commands:

For a NetBackup server: bpsetconfig

For a NetBackup client: nbsetconfig

Configuration options are key and value pairs, as shown in the following examples:

- CLIENT_READ_TIMEOUT = 300
- LOCAL_CACHE = NO
- RESUME_ORIG_DUP_ON_OPT_DUP_FAIL = TRUE
- SERVER = server1.example.com

You can specify some options multiple times, such as the SERVER option.

To set configuration options by using the command line

1. In a command window or shell window on the host on which you want to set the property, invoke the appropriate command. The command depends on the operating system and the NetBackup host type (client or server), as follows:

   UNIX — On a NetBackup client:

   ```
   /usr/openv/netbackup/bin/nbsetconfig
   ```

   On a NetBackup server:

   ```
   /usr/openv/netbackup/bin/admincmd/bpsetconfig
   ```

   Windows — On a NetBackup client:

   ```
   install_path\NetBackup\bin\nbsetconfig.exe
   ```

   On a NetBackup server:

   ```
   install_path\NetBackup\bin\admincmd\bpsetconfig.exe
   ```

2. At the command prompt, enter the key and the value pairs of the configuration options that you want to set, one pair per line.

   You can change existing key and value pairs.

   You can add key and value pairs.

   Ensure that you understand the values that are allowed and the format of any new options that you add.

3. To save the configuration changes, type the following, depending on the operating system:

   Windows: `Ctrl + Z Enter`

   UNIX: `Ctrl + D Enter`

About MSDP replication to a different domain

NetBackup supports replication to storage in a different domain. NetBackup Auto Image Replication is the method used to replicate backup images. (Backup image replication is not the same as snapshot replication, which may occur in the same domain.) You can replicate from one source to one or more destinations.

Table 5-24 describes the MSDP replication source and targets that NetBackup supports.

Table 5-24 NetBackup media server deduplication replication targets

Source storage	Target storage
Media Server Deduplication Pool	A **Media Server Deduplication Pool**, which can be hosted on the following systems: ■ A NetBackup media server. ■ A NetBackup 5200 series appliance or NetBackup 5300 series appliance.
PureDisk Deduplication Pool	A **PureDisk Deduplication Pool** on a NetBackup 5000 series appliance. A **PureDisk Deduplication Pool** is a **PureDisk Storage Pool** exposed to NetBackup by the NetBackup 5000 series appliance . A **PureDisk Deduplication Pool** can be the destination of replication from one NetBackup domain only. If you try to replicate from MSDP storage in more than one NetBackup domain, replication does not function correctly. **Note:** NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only.

Auto Image Replication does not support replicating from a storage unit group. That is, the source copy cannot be in a storage unit group.

If a replication job fails, NetBackup retries the replication until it succeeds or the source images expire. You can change the retry interval behavior.

See "Configuring NetBackup optimized duplication or replication behavior" on page 147.

If a job fails after it replicates some of the images, NetBackup does not run a separate image cleanup job for the partially replicated images. The next time the replication runs, that job cleans up the image fragments before it begins to replicate the images.

You can use a separate network for the duplication traffic.

See "About a separate network path for MSDP duplication and replication" on page 133.

See "Configuring MSDP replication to a different NetBackup domain" on page 152.

See "About MSDP optimized duplication and replication" on page 34.

Configuring MSDP replication to a different NetBackup domain

Table 5-25 describes the tasks that are required to replicate backup images from one **Media Server Deduplication Pool** to another in a different NetBackup domain.

Optionally, you can use a separate network for the optimized duplication traffic.

See "About a separate network path for MSDP duplication and replication" on page 133.

Table 5-25 NetBackup MSDP replication configuration tasks

Step	Task	Procedure
Step 1	Learn about MSDP replication	See "About MSDP replication to a different domain" on page 150. See "About NetBackup Auto Image Replication" on page 153.
Step 2	Determine if you need to configure a trust relationship with the target NetBackup domain	A trust relationship is optional. See "About trusted master servers for Auto Image Replication" on page 161.
Step 3	Add the remote storage server as a replication target	See "Configuring a target for MSDP replication to a remote domain" on page 172. See "Viewing the replication topology for Auto Image Replication" on page 159.

Table 5-25 NetBackup MSDP replication configuration tasks *(continued)*

Step	Task	Procedure
Step 4	Configure a storage lifecycle policy	The following are the options when you configure the SLP operations: ■ If you configured a trust relationship with the target domains, you can specify one of the following options: ■ **All replication target storage servers (across different NetBackup domains)** NetBackup automatically creates an import SLP in the target domain when the replication job runs. ■ **A specific Master Server**. If you choose this option, you then select **Target master server** and **Target import SLP**. You must create an import SLP in the target domain before you configure an SLP in the source domain. ■ If you did *not* configure a trust relationship with the target domains, **All replication target storage servers (across different NetBackup domains)** is selected by default. You cannot choose a specific target storage server. NetBackup automatically creates an import SLP in the target domain when the replication job runs. See "About storage lifecycle policies" on page 178. See "About the storage lifecycle policies required for Auto Image Replication" on page 179. See "Creating a storage lifecycle policy" on page 181.
Step 5	Configure replication bandwidth	Optionally, you can configure the bandwidth for replication. See "About configuring MSDP optimized duplication and replication bandwidth" on page 177.

About NetBackup Auto Image Replication

The backups that are generated in one NetBackup domain can be replicated to storage in one or more target NetBackup domains. This process is referred to as Auto Image Replication.

The ability to replicate backups to storage in other NetBackup domains, often across various geographical sites, helps facilitate the following disaster recovery needs:

- One-to-one model
  A single production datacenter can back up to a disaster recovery site.
- One-to-many model
  A single production datacenter can back up to multiple disaster recovery sites.
  See "One-to-many Auto Image Replication model" on page 155.

- Many-to-one model
  Remote offices in multiple domains can back up to a storage device in a single domain.
- Many-to-many model
  Remote datacenters in multiple domains can back up multiple disaster recovery sites.

NetBackup supports Auto Image Replication from a **Media Server Deduplication Pool** in one NetBackup domain to a **Media Server Deduplication Pool** in another domain.

Notes about Auto Image Replication

- Although Auto Image Replication is a disaster recovery solution, you cannot restore to clients in the primary (or originating) domain from the target master domain.
- Auto Image Replication does not support synthetic backups or optimized synthetic backups.
- Auto Image Replication does not support spanning volumes in a disk pool. NetBackup fails backup jobs to the disk pools that span volumes if the backup job is in a storage lifecycle policy that also contains a replication operation.
- Auto Image Replication does not support replicating from a storage unit group. That is, the source copy cannot be in a storage unit group.
- The ability to perform Auto Image Replication between different versions of NetBackup does not overrule the basic image compatibility rules. For example, a database backup that was taken in one NetBackup domain can be replicated to a NetBackup domain of an earlier version. However, the older server may not be able to successfully restore from the newer image.
  See the following article for information about version compatibility and interoperability:
  http://www.netbackup.com/compatibility
- Synchronize the clocks of the master servers in the source and the target domains so that the master server in the target domain can import the images as soon as they are ready. The master server in the target domain cannot import an image until the image creation time is reached. Time zone differences are not a factor because the images use Coordinated Universal Time (UTC).

Process Overview

Table 5-26 is an overview of the process, generally describing the events in the originating and target domains.

NetBackup uses storage lifecycle policies in the source domain and the target domain to manage the Auto Image Replication operations.

See "About the storage lifecycle policies required for Auto Image Replication" on page 179.

Table 5-26 Auto Image Replication process overview

Event	Domain in which event occurs	Event description
1	Originating master server (Domain 1)	Clients are backed up according to a backup policy that indicates a storage lifecycle policy as the **Policy storage** selection. The SLP must include at least one **Replication** operation to similar storage in the target domain.
2	Target master server (Domain 2)	The storage server in the target domain recognizes that a replication event has occurred. It notifies the NetBackup master server in the target domain.
3	Target master server (Domain 2)	NetBackup imports the image immediately, based on an SLP that contains an import operation. NetBackup can import the image quickly because the metadata is replicated as part of the image. (This import process is not the same as the import process available in the **Catalog** utility.)
4	Target master server (Domain 2)	After the image is imported into the target domain, NetBackup continues to manage the copies in that domain. Depending on the configuration, the media server in Domain 2 can replicate the images to a media server in Domain 3.

One-to-many Auto Image Replication model

In this configuration, all copies are made in parallel. The copies are made within the context of one NetBackup job and simultaneously within the originating storage server context. If one target storage server fails, the entire job fails and is retried later.

All copies have the same **Target Retention**. To achieve different **Target Retention** settings in each target master server domain, either create multiple source copies or cascade duplication to target master servers.

Cascading Auto Image Replication model

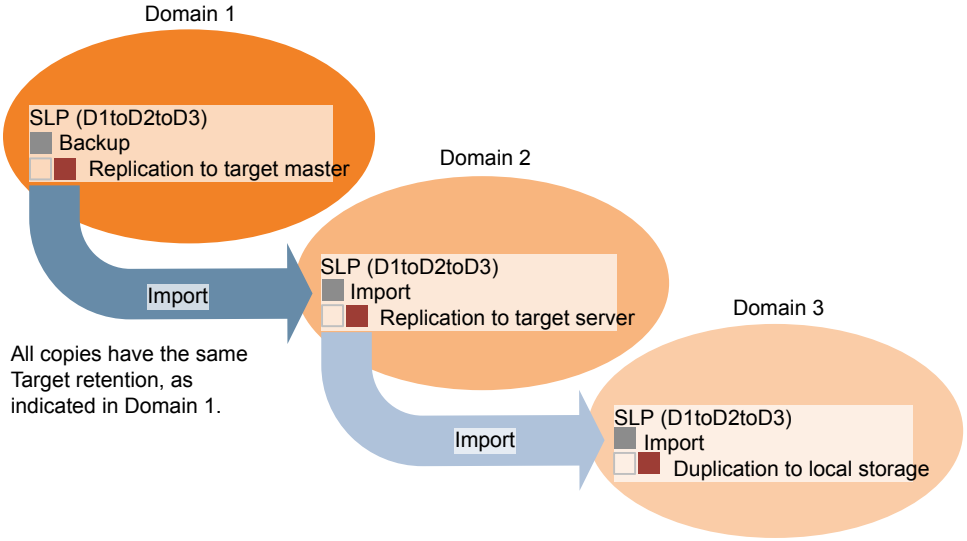
Replications can be cascaded from the originating domain to multiple domains. Storage lifecycle policies are set up in each domain to anticipate the originating image, import it and then replicate it to the next target master.

Figure 5-6 represents the following cascading configuration across three domains.

- The image is created in Domain 1, and then replicated to the target Domain 2.
- The image is imported in Domain 2, and then replicated to a target Domain 3.

- The image is then imported into Domain 3.

Figure 5-6 Cascading Auto Image Replication



In the cascading model, the originating master server for Domain 2 and Domain 3 is the master server in Domain 1.

Note: When the image is replicated in Domain 3, the replication notification event indicates that the master server in Domain 2 is the originating master server. However, after the image is imported successfully into Domain 3, NetBackup correctly indicates that the originating master server is in Domain 1.

The cascading model presents a special case for the Import SLP that replicates the imported copy to a target master. (This master server that is neither the first nor the last in the string of target master servers.)

The Import SLP must include at least one operation that uses a **Fixed** retention type and at least one operation that uses a **Target Retention** type. So that the Import SLP can satisfy these requirements, the import operation must use a **Target Retention**.

Table 5-27 shows the difference in the import operation setup.

Table 5-27 Import operation difference in an SLP configured to replicate the imported copy

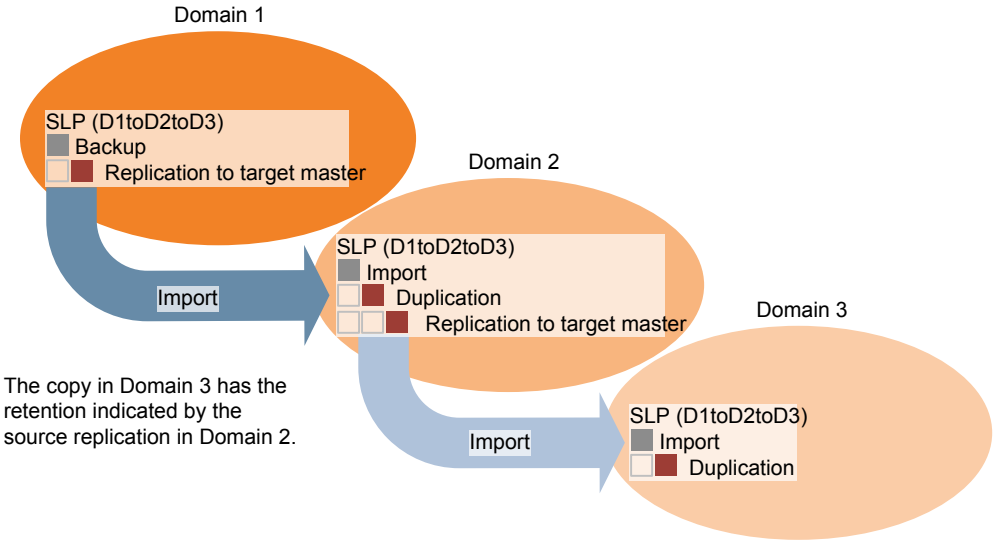
Import operation criteria	Import operation in a cascading model
The first operation must be an import operation.	Same; no difference.
A replication to target master must use a **Fixed** retention type	Same; no difference.
At least one operation must use the **Target retention**.	Here is the difference: To meet the criteria, the import operation must use **Target retention**.

The target retention is embedded in the source image.

In the cascading model that is represented in Figure 5-6, all copies have the same **Target Retention**—the **Target Retention** indicated in Domain 1.

For the copy in Domain 3 to have a different target retention, add an intermediary replication operation to the Domain 2 storage lifecycle policy. The intermediary replication operation acts as the source for the replication to target master. Since the target retention is embedded in the source image, the copy in Domain 3 honors the retention level that is set for the intermediary replication operation.

Figure 5-7 Cascading replications to target master servers, with various target retentions



About the domain relationship for replication

For a **Media Server Deduplication Pool** target: the relationship between the originating domain and the target domain or domains is established in the originating domain. Specifically, by configuring the target storage server in the **Replication** tab of the **Change Storage Server** dialog box of the source storage server.

See "Configuring a target for MSDP replication to a remote domain" on page 172.

Before you configure the replication relationship, you can add the target master server as a trusted host.

See "About trusted master servers for Auto Image Replication" on page 161.

Caution: Choose the target storage server carefully. A target storage server must not also be a storage server for the originating domain.

About the replication topology for Auto Image Replication

For Auto Image Replication, the disk volumes have the properties that define the replication relationships between the volumes. The knowledge of the volume properties is considered the replication topology. The following are the replication properties that a volume can have:

Source	A source volume contains the backups of your clients. The volume is the source for the images that are replicated to a remote NetBackup domain. Each source volume in an originating domain has one or more replication partner target volumes in a target domain.
Target	A target volume in the remote domain is the replication partner of a source volume in the originating domain.
None	The volume does not have a replication attribute.

NetBackup exposes the storage for a **Media Server Deduplication Pool** as a single volume. Therefore, there is always a one-to-one volume relationship for MSDP.

You configure the replication relationships in the source domain. To do so, you add target storage servers in the **Replication** tab of the **Change Storage Server** dialog box of the source storage server.

See "Configuring a target for MSDP replication to a remote domain" on page 172.

NetBackup discovers the replication topology when you configure the replication relationships. NetBackup discovers topology changes when you use the **Refresh** option of the **Change Disk Pool** dialog box.

See "Changing a Media Server Deduplication Pool properties" on page 294.

NetBackup includes a command that can help you understand your replication topology. Use the command in the following situations:

- After you configure the replication targets.
- After you configure the storage server and before you configure disk pools.
- After changes to the volumes that comprise the storage.

See "Viewing the replication topology for Auto Image Replication" on page 159.

Viewing the replication topology for Auto Image Replication

A volume that is a source of replication must have at least one replication partner that is the target of the replication. NetBackup lets you view the replication topology of the storage.

See "About the replication topology for Auto Image Replication" on page 158.

To view the replication topology for Auto Image Replication

- Run the `bpstsinfo` command, specifying the storage server name and the server type. The following is the command syntax:

- Windows: *install_path*\NetBackup\bin\admincmd\bpstsinfo -lsuinfo -storage_server *host_name* -stype *server_type*
- UNIX: /usr/openv/netbackup/bin/admincmd/bpstsinfo -lsuinfo -storage_server *host_name* -stype *server_type*

The following are the options and arguments for the command:

-storage_server *host_name*	The name of the target storage server.
-stype **PureDisk**	Use PureDisk for a **Media Server Deduplication Pool**,.

Save the output to a file so that you can compare the current topology with the previous topology to determine what has changed.

See "Sample volume properties output for MSDP replication" on page 160.

Sample volume properties output for MSDP replication

The following two examples show output from the bpstsinfo -lsuinfo command for two NetBackup deduplication storage servers. The first example is the output from the source disk pool in the originating domain. The second example is from the target disk pool in the remote master server domain.

The two examples show the following:

- All of the storage in a deduplication disk pool is exposed as one volume: PureDiskVolume.
- The PureDiskVolume of the deduplication storage server bit1.datacenter.example.com is the source for the replication operation.
- The PureDiskVolume of the deduplication storage server target_host.dr-site.example.com is the target of the replication operation.

```
> bpstsinfo -lsuinfo -storage_server bit1.datacenter.example.com -stype PureDisk
LSU Info:
        Server Name: PureDisk:bit1.datacenter.example.com
        LSU Name: PureDiskVolume
        Allocation : STS_LSU_AT_STATIC
        Storage: STS_LSU_ST_NONE
        Description: PureDisk storage unit (/bit1.datacenter.example.com#1/2)
        Configuration:
        Media: (STS_LSUF_DISK | STS_LSUF_ACTIVE | STS_LSUF_STORAGE_NOT_FREED |
         STS_LSUF_REP_ENABLED | STS_LSUF_REP_SOURCE)
        Save As : (STS_SA_CLEARF | STS_SA_IMAGE | STS_SA_OPAQUEF)
        Replication Sources: 0 ( )
```

```
        Replication Targets: 1 ( PureDisk:target_host.dr-site.example.com:PureDiskVolume )
        Maximum Transfer: 2147483647
        Block Size: 512
        Allocation Size: 0
        Size: 74645270666
        Physical Size: 77304328192
        Bytes Used: 138
        Physical Bytes Used: 2659057664
        Resident Images: 0

> bpstsinfo -lsuinfo -storage_server target_host.dr-site.example.com -stype PureDisk
LSU Info:
        Server Name: PureDisk:target_host.dr-site.example.com
        LSU Name: PureDiskVolume
        Allocation : STS_LSU_AT_STATIC
        Storage: STS_LSU_ST_NONE
        Description: PureDisk storage unit (/target_host.dr-site.example.com#1/2)
        Configuration:
        Media: (STS_LSUF_DISK | STS_LSUF_ACTIVE | STS_LSUF_STORAGE_NOT_FREED |
         STS_LSUF_REP_ENABLED | STS_LSUF_REP_TARGET)
        Save As : (STS_SA_CLEARF | STS_SA_IMAGE | STS_SA_OPAQUEF)
        Replication Sources: 1 ( PureDisk:bit1:PureDiskVolume )
        Replication Targets: 0 ( )
        Maximum Transfer: 2147483647
        Block Size: 512
        Allocation Size: 0
        Size: 79808086154
        Physical Size: 98944983040
        Bytes Used: 138
        Physical Bytes Used: 19136897024
        Resident Images: 0
```

About trusted master servers for Auto Image Replication

NetBackup provides the ability to establish a trust relationship between replication domains. A trust relationship is optional. The following items describe how a trust relationship affects Auto Image Replication:

No trust relationship	NetBackup replicates to all defined target storage servers. You cannot select a specific host or hosts as a target.

Trust relationship	You can select a subset of your trusted domains as a target for replication. NetBackup then replicates to the specified domains only rather than to all configured replication targets. This type of Auto Image Replication is known as Targeted A.I.R.

With Targeted A.I.R., when establishing trust between the source and the remote target server, you need to establish trust in both the domains.

1. In the source master server, add the target master server as a trusted server.
2. In the target master server, add the source master server as a trusted server.

The following diagram illustrates the different tasks for adding trusted master servers.

Figure 5-8 Tasks to establish a trust relationship between master servers for Targeted A.I.R.

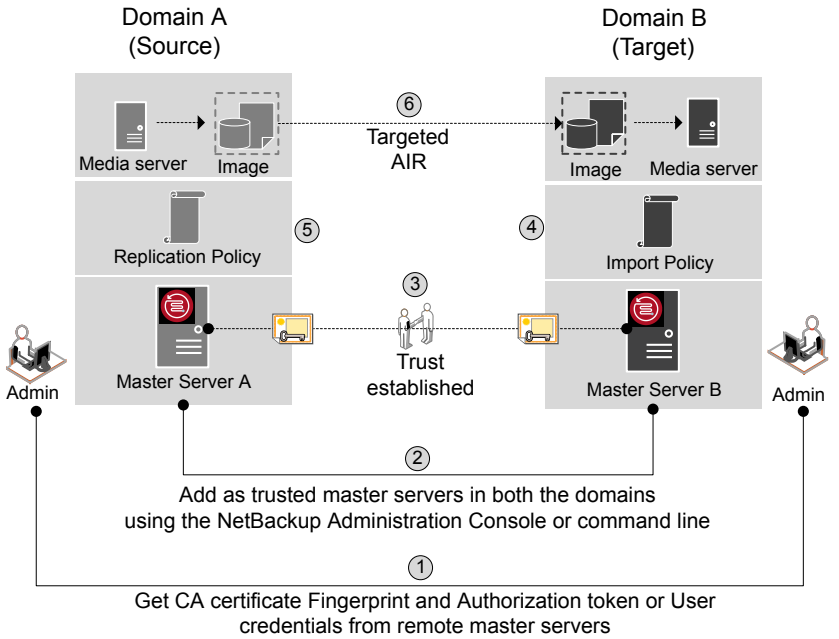


Table 5-28 Tasks to establish a trust relationship between master servers for Targeted A.I.R.

Step	Task	Procedure
Step 1	Administrators of both the source and target master servers must obtain each other's CA certificate fingerprint and authorization tokens or the user credentials. This activity must be performed offline. **Note:** Veritas recommends using an authentication token to connect to the remote master server. An authentication token provides restricted access and allows secure communication between both the hosts. The use of user credentials (user name and password) may present a possible security breach.	To obtain the authorization tokens, use the `bpnbat` command to login and `nbcertcmd` to get the authorization tokens. To obtain the SHA1 fingerprint of root certificate, use the `nbcertcmd -displayCACertDetail` command. To perform this task, see the NetBackup Commands Reference Guide. **Note:** When you run the commands, keep the target as the remote server.
Step 2	Establish trust between the source and the target domains. ■ On the source master server, add the target master server as trusted server. ■ On the target master server, add the source master server as trusted server.	To perform this task in the Veritas Administration Console, see the following topic: See "Adding a trusted master server" on page 164. To perform this task using the `nbseccmd`, see the NetBackup Commands Reference Guide.
Step 3	After you have added the source and target trusted servers, they have each other's host ID-based certificates. The certificates are used during each communication. Master Server A has a certificate issued by Master Server B and vice versa. Before communication can occur, Master Server A presents the certificate issued by Master Server B and vice versa. The communication between the source and target master servers is now secured.	To understand the use of host ID-based certificates, see the Veritas Security and Encryption Guide.
Step 4	Create an import storage lifecycle policy in the target domain.	See "About storage lifecycle policies" on page 178.
Step 5	Create a replication storage lifecycle policy in the source domain using the specific target master server and storage lifecycle policy. The backups that are generated in one NetBackup domain can be replicated to storage in one or more target NetBackup domains.	See "About storage lifecycle policies" on page 178.

Table 5-28 Tasks to establish a trust relationship between master servers for Targeted A.I.R. *(continued)*

Step	Task	Procedure
Step 6	The backups that are generated in one NetBackup domain can be replicated to storage in one or more target NetBackup domains. This process is referred to as Auto Image Replication.	See "About NetBackup Auto Image Replication" on page 153.

If your source and target trusted servers use different NetBackup versions, consider the following.

Note: When you upgrade both the source and the target master server to version 8.1 or later, you need to update the trust relationship. Run the following command:

```
nbseccmd -setuptrustedmaster -update
```

See the NetBackup Commands Reference Guide.

Table 5-29 Trust setup methods for different NetBackup versions

Source server version	Target server version	Trust setup method
8.1 and later	8.1 and later	Add a trusted master server using authorization token. Complete action on both the servers.
8.1 and later	8.0 or earlier	On the source server, add the target as the trusted master server using the remote (target) server's credentials.
8.0 or earlier	8.1 and later	On the source server, add the target as the trusted master server using the remote (target) server's credentials.

Adding a trusted master server

You can configure a trust relationship between multiple NetBackup domains. To do so, in the source domain and the target domain you must add a trust relationship.

A trust relationship between domains helps with replication operations.

See "About trusted master servers for Auto Image Replication" on page 161.

See "Configuring MSDP replication to a different NetBackup domain" on page 152.

Perform the following steps on both the source and the target server.

Before you begin

- Identify the NetBackup versions that are installed on the source and the target servers.
- Obtain the authorization tokens of the remote server.
  Use the `bpnbat` command to log in and `nbcertcmd` to get the authorization tokens.
  To perform this task, see the NetBackup Commands Reference Guide.
- Obtain the fingerprints for the remote server.
  To obtain the SHA1 fingerprint of root certificate, use the `nbcertcmd -displayCACertDetail` command.
  To perform this task, see the NetBackup Commands Reference Guide.
- Ensure that you have one of the following permissions:
  - System administrator permissions with `root` permissions for UNIX and administrator permissions for Windows, and a NetBackupCLI user for a 3.1 NetBackup appliance.
  - Access to NetBackup Administrator console, where you have **<username> ADMIN=ALL** permissions through `auth.conf`.
  - Enhanced audit user permissions through `authalias.conf`.

  For more information, see the NetBackup Security and Encryption Guide.
- If NBAC is enabled, ensure that both the target and the source master server have the same NBAC configuration.
- If the either the source or the target server master server is on version 8.0 or earlier, ensure that the **Enable insecure communication with NetBackup 8.0 and earlier hosts** option on **Security Management > Global Security Settings > Secure Communication** tab is selected.

To add a trusted master server

1. In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Master Servers** in the left pane.
2. In the right pane, select the master server.
3. On the **Actions** menu, click **Properties**.
4. In the properties dialog box left pane, select **Servers**.
5. In the **Servers** dialog box, select the **Trusted Master Servers** tab.
6. On the **Trusted Master Servers** tab, click **Add**.

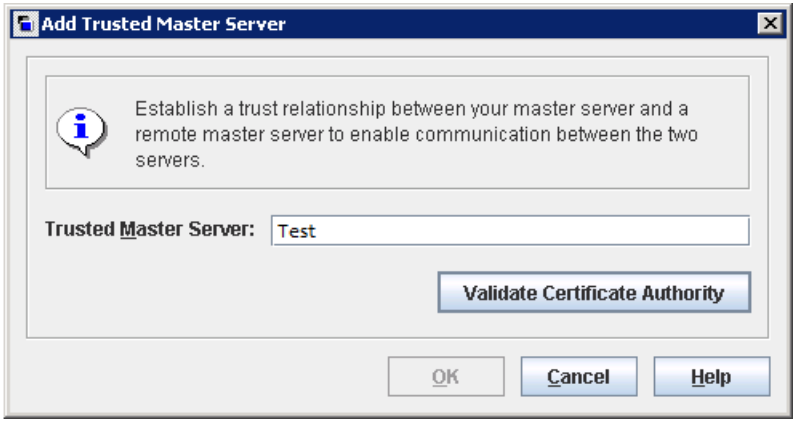
   The **Add Trusted Master Server** dialog box appears.

7 In the **Add Trusted Master Server** dialog box, enter the fully-qualified host name of the remote master server.

8 Click **Validate Certificate Authority**.

Depending on the NetBackup version of the target server, the next screens are displayed.

The following is an example of the dialog box:

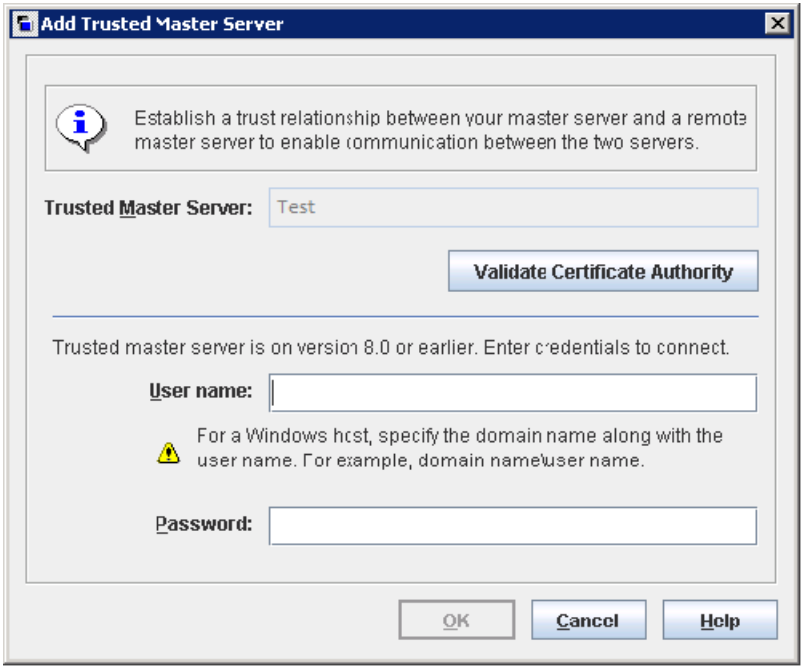


9 If the target server is on version 8.0 or earlier:

In the **Add Trusted Master Server** dialog box, enter the **Username** and **Password** of the remote master server host.

Skip steps 10 through 12.

The following is an example of the dialog box:



10 If both the source and the target server are on version 8.1 or later:

In the **Validate Certificate Authority** dialog box, verify if the CA certificate fingerprint of the remote server is correct.

11 To proceed, click **Yes**.

Or

If the fingerprints don't match, click **No**.

Contact the remote server admin to provide the correct fingerprints.

12 In the **Add Trusted Master Server** dialog box, enter the trusted master server details.

- Select **Specify Authentication Token of the trusted master server** and enter the token details of the remote master server.

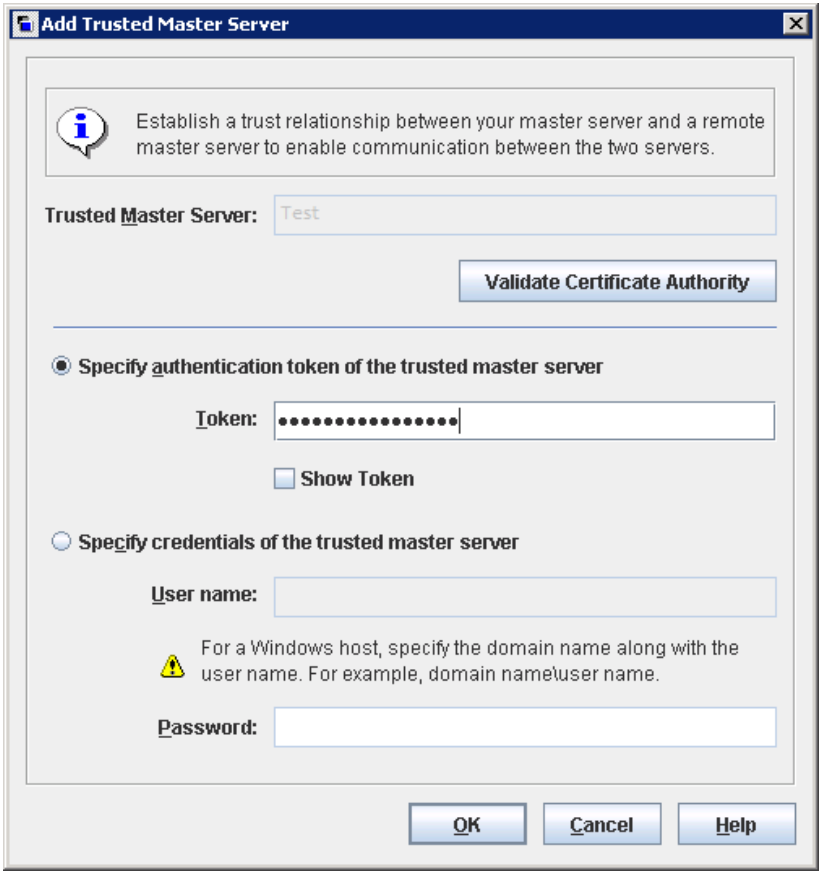
Note: To view the token you have entered, select **Show Token**.

Or

- Select **Specify credentials of the trusted master server** and enter the user name and password.
  To establish trust with a 3.1 NetBackup master appliance, use the NetBackupCLI credentials.

Note: Veritas recommends using an authentication token to connect to the remote master server. An authentication token provides restricted access and allows secure communication between both the hosts. The use of user credentials (user name and password) may present a possible security breach.

The following is an example of the dialog box:



13 Click **OK**.

14 Perform the same procedure on the remote master server of the master server you have added above.

Skip this step if the target server is on version 8.0 or earlier.

Note: You will not be able to fetch the host properties of a trusted master server from **Host Properties** > **Client** lists.

Removing a trusted master server

To remove a trusted master server, you must perform the following procedure on both the source and the target server.

Note: If either your source or the target server is on version 8.0 or earlier, follow the procedure that is prescribed in the respective guide.

To remove a trusted master server

1. Ensure that all replication jobs to the trusted target master server are complete. You can use `nbstlutil stlilist` to list the state of all storage lifecycle policy-managed operations. To cancel jobs use `nbstlutil cancel`.

   See the NetBackup Commands Reference Guide for information about the `nbstlutil` command.

2. Delete all storage lifecycle policies (SLPs) that use the trusted master as a destination.

   Note: Before deleting a storage lifecycle policy, ensure that there are no backup policies that indicate the SLP for the **Policy storage**.

3. In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Master Servers** in the left pane.
4. In the right pane, select the master server.
5. On the **Actions** menu, click **Properties**.
6. In the properties dialog box left pane, select **Servers**.
7. In the **Servers** dialog box, select the **Trusted Master Servers** tab.
8. On the **Trusted Master Servers** tab, select the trusted master server that you want to remove and click **Remove**.

   The **Remove Server** confirmation dialog box is displayed.
9. Click **Yes**.
10. When you finish removing trusted master servers, click **OK**.
11. Restart the `nbsl` service.
12. Repeat the steps on the source master server.

Note: In case of multiple NICs, if you have established trust using more that one host NIC and if you remove the trust relationship with any one host NIC, the trust with all the other host NICs is broken.

Enabling NetBackup clustered master server inter-node authentication

NetBackup requires inter-node authentication among the master servers in a cluster. For authentication, you must provision an authentication certificate on all of the nodes of the cluster. The certificates are used to establish SSL connections between the NetBackup hosts. The inter-node authentication allows the following NetBackup functionality:

NetBackup Administration Console	The NetBackup Administration Console in master server clusters requires the NetBackup authentication certificates for correct functionality.
Targeted A.I.R. (Auto Image Replication)	Auto Image Replication in which a master server is in a cluster requires inter-node authentication among the hosts in that cluster. The NetBackup authentication certificates provide the means to establish the proper trust relationships. Provision the certificates on the cluster hosts before you add the trusted master server. This requirement applies regardless of whether the clustered mastered server is the source of the replication operation or the target. See "About trusted master servers for Auto Image Replication" on page 161.

To enable clustered master server inter-node authentication

- On the active node of the NetBackup master server cluster, run the following NetBackup command:
  - Windows: *install_path*\NetBackup\bin\admincmd\bpnbaz -setupat
  - UNIX: /usr/openv/netbackup/bin/admincmd/bpnbaz -setupat

  NetBackup creates the certificates on every node in the master server cluster.

  The following is example output:

```
# bpnbaz -setupat
You will have to restart NetBackup services on this machine after
the command completes successfully.
Do you want to continue(y/n)y
Gathering configuration information.
Please be patient as we wait for 10 sec for the security services
to start their operation.
Generating identity for host 'bit1.remote.example.com'
Setting up security on target host: bit1.remote.example.com
```

```
nbatd is successfully configured on NetBackup Master Server.
Operation completed successfully.
```

Configuring a target for MSDP replication to a remote domain

Use the following procedure to configure a target for replication from a **Media Server Deduplication Pool** in an originating domain to a deduplication pool in another target domain. NetBackup supports several deduplication targets.

See "About MSDP replication to a different domain" on page 150.

Configuring the target storage server is only one step in the process of configuring MSDP replication.

See "Configuring MSDP replication to a different NetBackup domain" on page 152.

Note: About clustered master servers: If you add a trusted master server for replication operations, you must enable inter-node authentication on all of the nodes in the cluster. Enable the authentication before you begin the following procedure. This requirement applies regardless of whether the clustered mastered server is the source of the replication operation or the target.

See "About trusted master servers for Auto Image Replication" on page 161.

See "Enabling NetBackup clustered master server inter-node authentication" on page 171.

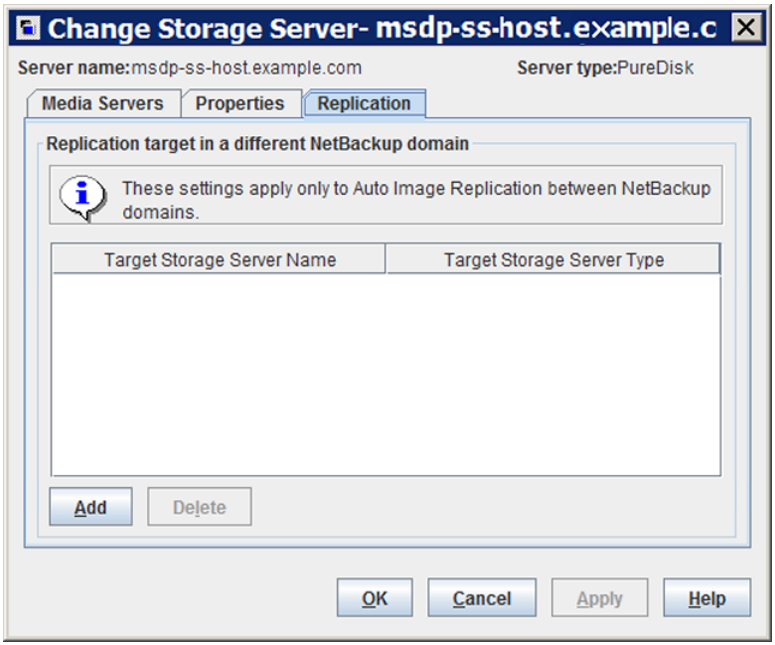
Caution: Choose the target storage server or servers carefully. A target storage server must not also be a storage server for the source domain. Also, a disk volume must not be shared among multiple NetBackup domains.

To configure a Media Server Deduplication Pool as a replication target

1. In the **NetBackup Administration Console**, expand **Media and Device Management > Credentials > Storage Server**.
2. Select the MSDP storage server.
3. On the **Edit** menu, select **Change**.

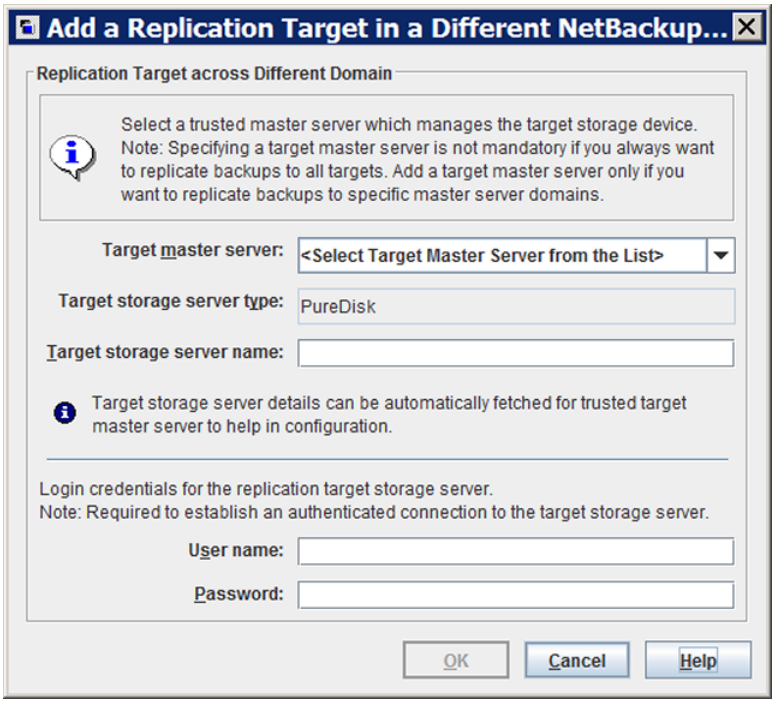
4 In the **Change Storage Server** dialog box, select the **Replication** tab.

The following is an example of the **Change Storage Server** dialog box **Replication** tab:



5 On the **Replication** tab, click **Add**. The **Add a Replication Target Across a Different NetBackup Domain** dialog box appears.

The following is an example of the dialog box.



6 In the **Add a Replication Target Across a Different NetBackup Domain** dialog box, complete one or more of the following procedures depending on your requirements:

Add a trusted master server

Add a trusted master server if you want to replicate backup images to a subset of available targets.

To add a trusted master server

1. In the **Target master server** drop-down list, select **Add a new trusted master server**.
2. Complete the fields in the **Add a New Trusted Master Server** dialog box. Click **OK** after you complete the fields.

   See "Target options for MSDP replication" on page 176.
3. Repeat the first two steps until you have finished adding trusted master servers.
4. To add a replication target, continue with the next procedure.

See "About trusted master servers for Auto Image Replication" on page 161.

Select a trusted master server and replication target

Select a trusted master server if you want to replicate backup images to a subset of available targets.

To select a trusted master server and replication target

1. In the **Target master server** drop-down list, select the master server of the domain to which you want to replicate data.

   All trusted master servers are in the drop-down list.
2. In the **Target storage server type** drop-down list, select the type of target storage server.

   All available target types are in the drop-down list.
3. In the **Target storage server name** drop-down list, select the storage server that hosts the target deduplication pool. All available storage servers in the target domain are in the drop-down list.

   After you select the target storage server, NetBackup populates the **User name** field with the **User name** of the NetBackup Deduplication Engine of the target host.
4. Enter the **Password** for the deduplication service on the target storage server.
5. Click **OK**.

See "Target options for MSDP replication" on page 176.

Enter a replication target	Enter a replication target if you did not configure trusted master servers. To enter a replication target **1** In the **Target storage server name** field, enter the name of the target storage server. **2** Enter the **User name** and **Password** for the NetBackup Deduplication Engine on the target storage server. **3** Click **OK**. See "Target options for MSDP replication" on page 176.

7 After all replication targets are added, click **OK**.

8 For the deduplication pools in each domain, open the **Change Disk Pool** dialog box and click **Refresh**.

Configuring a replication target configures the replication properties of the disk volumes in both domains. However, you must refresh the deduplication pools so thatNetBackup reads the new volume properties.

See "Changing a Media Server Deduplication Pool properties" on page 294.

Target options for MSDP replication

The following table describes the target options for replication to a NetBackup **Media Server Deduplication Pool**.

Table 5-30 MSDP target replication options

Option	Description
Target master server	All trusted master servers are in the drop-down list. Select the master server for the target domain to which you want to replicate backups. To add the master server of another domain as a trusted master, select **Add a new Trusted Master Server**. Configuring a trust relationship is required only if you want to choose a specific target for replication.

Table 5-30 MSDP target replication options *(continued)*

Option	Description
Target storage server type	The target storage server type must be **PureDisk**. If a trusted master server is configured, **PureDisk** is selected by default. If a trusted master server is *not* configured, NetBackup populates this field when it connects with the storage server you enter in the **Target storage server name** field.
Target storage server name	If a trusted master server is configured, select the target storage server. If a trusted master server is *not* configured, enter the name of the target storage server. The drop-down list shows all the storage servers that match the **Target storage server type**.
User name	When you configure a replication target, NetBackup populates the **User name** field with user account of the target storage server, as follows: ■ For an MSDP target, the NetBackup Deduplication Engine user name. ■ For a PureDisk storage target, the PureDisk Storage Pool Authority user name. NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only.
Password	Enter the password for the NetBackup Deduplication Engine.

About configuring MSDP optimized duplication and replication bandwidth

Each optimized duplication or Auto Image Replication job is a separate process or stream. The number of duplication or replication jobs that run concurrently determines the number of jobs that contend for bandwidth. You can control how much network bandwidth that optimized duplication and Auto Image Replication jobs consume.

Two different configuration file settings control the bandwidth that is used, as follows:

`bandwidthlimit`

The `bandwidthlimit` parameter in the `agent.cfg` file is the global bandwidth setting. You can use this parameter to limit the bandwidth that all replication jobs use. It applies to jobs in which a **Media Server Deduplication Pool** is the source. Therefore, configure it on the source storage server.

If `bandwidthlimit` is greater than zero, all of the jobs share the bandwidth. That is, the bandwidth for each job is the `bandwidthlimit` divided by the number of jobs.

If `bandwidthlimit=0`, total bandwidth is not limited. However, you can limit the bandwidth that each job uses. See the following `OPTDUP_BANDWIDTH` description.

If you specify bandwidth limits, optimized duplication and replication traffic to any destination is limited.

By default, `bandwidthlimit=0`.

The `agent.cfg` file resides in the following directory:

- UNIX: *`storage_path`*`/etc/puredisk`
- Windows: *`storage_path`*`\etc\puredisk`

`OPTDUP_BANDWIDTH`

The `OPTDUP_BANDWIDTH` parameter in the `pd.conf` file specifies the per job bandwidth.

`OPTDUP_BANDWIDTH` applies only if the `bandwidthlimit` parameter in the `agent.cfg` file is zero.

If `OPTDUP_BANDWIDTH` and `bandwidthlimit` are both `0`, bandwidth per replication job is not limited.

By default, `OPTDUP_BANDWIDTH = 0`.

See "About the MSDP pd.conf configuration file" on page 197.

See "Editing the MSDP pd.conf file" on page 198.

See "MSDP pd.conf file parameters" on page 198.

See "Configuring MSDP optimized duplication within the same NetBackup domain" on page 143.

See "Configuring MSDP replication to a different NetBackup domain" on page 152.

About storage lifecycle policies

A storage lifecycle policy (SLP) is a storage plan for a set of backups. An SLP is configured within the **Storage Lifecycle Policies** utility.

An SLP contains instructions in the form of storage operations, to be applied to the data that is backed up by a backup policy. Operations are added to the SLP that determine how the data is stored, copied, replicated, and retained. NetBackup retries the copies as necessary to ensure that all copies are created.

SLPs offer the opportunity for users to assign a classification to the data at the policy level. A data classification represents a set of backup requirements, which makes it easier to configure backups for data with different requirements. For example, email data and financial data.

SLPs can be set up to provide staged backup behavior. They simplify data management by applying a prescribed behavior to all the backup images that are included in the SLP. This process allows the NetBackup administrator to leverage the advantages of disk-based backups in the near term. It also preserves the advantages of tape-based backups for long-term storage.

The **SLP Parameters** properties in the **NetBackup Administration Console** allow administrators to customize how SLPs are maintained and how SLP jobs run.

Best-practice information about SLPs appears in the following document:

http://www.veritas.com/docs/TECH208536

For more information, see the NetBackup Administrator's Guide, Volume I.

About the storage lifecycle policies required for Auto Image Replication

To replicate images from one NetBackup domain to another NetBackup domain requires two storage lifecycle policies. The following table describes the policies and their requirements:

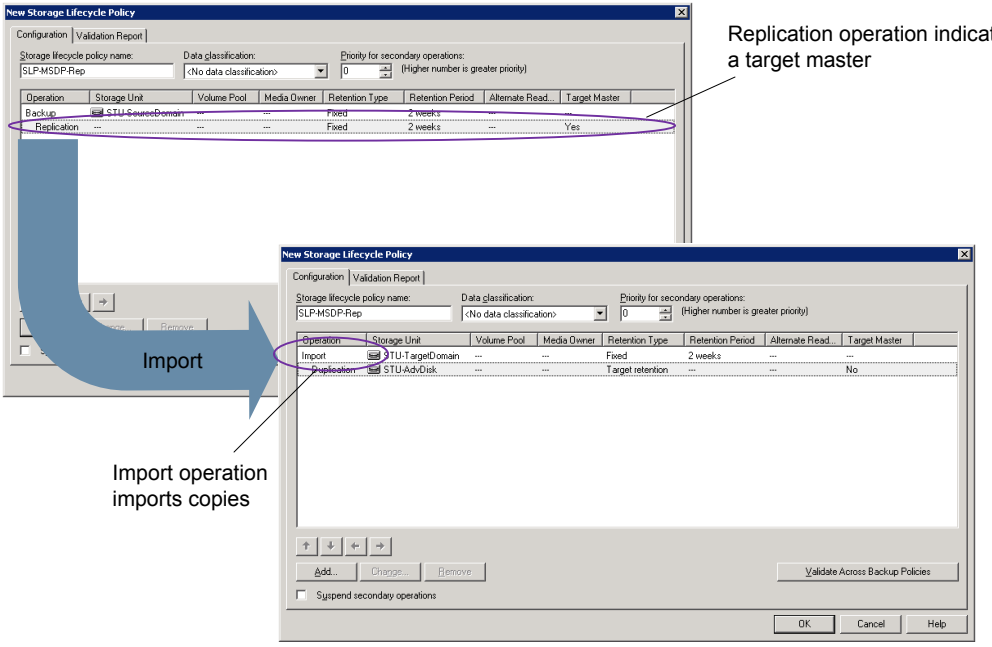
Table 5-31 SLP requirements for Auto Image Replication

Domain	Storage lifecycle policy requirements
Domain 1 (Source domain)	The Auto Image Replication SLP in the source domain must meet the following criteria: ■ The first operation must be a **Backup** operation to a **Media Server Deduplication Pool**. Indicate the exact storage unit from the drop-down list. Do not select **Any Available**. **Note:** The target domain must contain the same type of storage to import the image. ■ At least one operation must be a **Replication** operation to a **Media Server Deduplication Pool** in another NetBackup domain. You can configure multiple **Replication** operations in an Auto Image Replication SLP. The **Replication** operation settings determine whether the backup is replicated to all replication targets in all master server domains or only to specific replication targets. See "About trusted master servers for Auto Image Replication" on page 161. ■ The SLP must be of the same data classification as the **Import** SLP in Domain 2.
Domain 2 (Target domain)	If replicating to all targets in all domains, in each domain NetBackup automatically creates an **Import** SLP that meets all the necessary criteria. **Note:** If replicating to specific targets, you must create the **Import** SLP before creating the Auto Image Replication SLP in the originating domain. The **Import** SLP must meet the following criteria: ■ The first operation in the SLP must be an **Import** operation. NetBackup must support the **Destination storage** as a target for replication from the source storage. Indicate the exact storage unit from the drop-down list. Do not select **Any Available**. ■ The SLP must contain at least one operation that has the **Target retention** specified. ■ The SLP must be of the same data classification as the SLP in Domain 1. Matching the data classification keeps a consistent meaning to the classification and facilitates global reporting by data classification. See the following topic for more information about **Replication** operation configuration:

Figure 5-9 shows how the SLP in the target domain is set up to replicate the images from the originating master server domain.

Figure 5-9 Storage lifecycle policy pair required for Auto Image Replication

SLP on master server in the source domain



SLP that imports the copies to the target domain

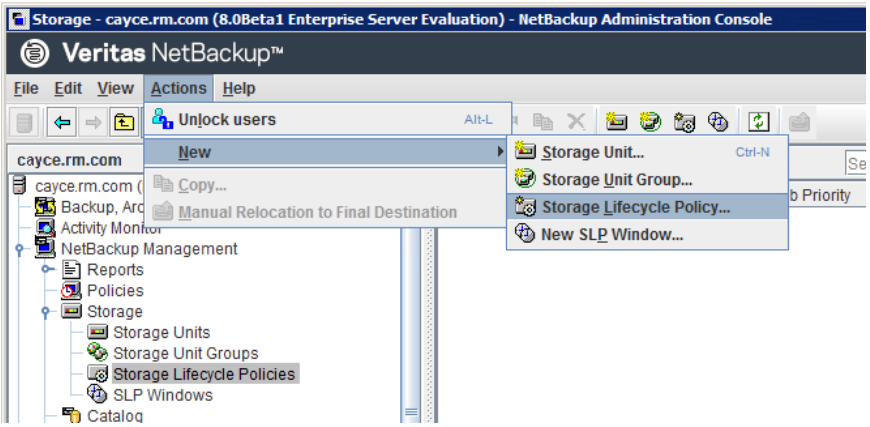
Note: Restart `nbstserv` after you make changes to the underlying storage for any operation in an SLP.

Creating a storage lifecycle policy

A storage lifecycle policy (SLP) is a storage plan for a set of backups. The operations in an SLP are the backup instructions for the data. Use the following procedure to create an SLP that contains multiple storage operations.

To add a storage operation to a storage lifecycle policy

1. In the **NetBackup Administration Console**, select **NetBackup Management > Storage > Storage Lifecycle Policies**.
2. Click **Actions > New > New Storage Lifecycle Policy** (Windows) or **Actions > New > Storage Lifecycle Policy** (UNIX).



3. In the **New Storage Lifecycle Policy** dialog box, enter a **Storage lifecycle policy name**.

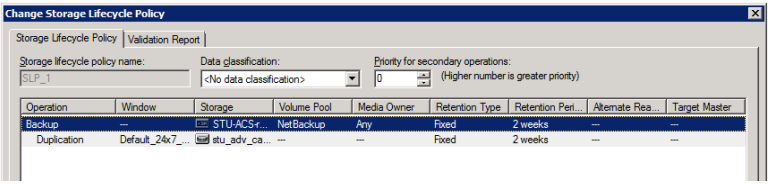
   See “NetBackup naming conventions” on page 16.

4 Add one or more operations to the SLP. The operations are the instructions for the SLP to follow and apply to the data that is specified in the backup policy.

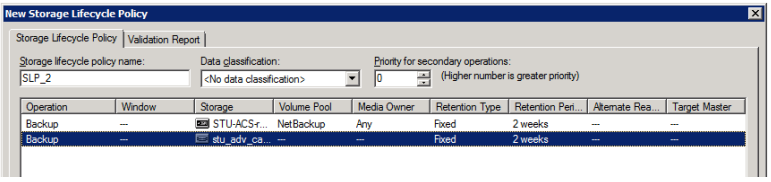
If this is the first operation added to the SLP, click **Add**.

If this is not the first operation in the SLP, add an operation that is either hierarchical or non-hierarchical:

To create a hierarchical operation, select an operation to become the source of the next operation. Click **Add**. The new operation is a child of the selected operation. The child is indented under the parent operation.



To create a non-hierarchical operation, do not select an operation. A non-hierarchical operation means that the operation does not have a parent and child relationship with another operation. The new operation is not indented.



5 In the **Properties** tab of the **New Storage Operation** dialog box, select an **Operation** type. If you're creating a child operation, the SLP displays only those operations that are valid based on the parent operation that you've selected.

The name of the operation reflects its purpose in the SLP:

- **Backup**
- **Duplication**
- **Import**
- **Replication**
  See "About NetBackup Auto Image Replication" on page 153.

6 Configure the properties for the operation.

7 The **Window** tab displays for the following operation types: **Backup From Snapshot**, **Duplication**, **Import**, **Index From Snapshot**, and **Replication**. If you'd like to control when the secondary operation runs, create a window for the operation.

8 Click the **Advanced** button in the **Properties** tab to display options about how the window should behave if the window closes and a secondary operation is not yet complete.

9 Click **OK** to create the operation.

10 Add additional operations to the SLP as needed. (See step 4.)

11 Change the hierarchy of the operations in the SLP if necessary.

12 Click **OK** to create the SLP. NetBackup validates the SLP when it is first created and whenever it is changed.

13 Configure a backup policy and select a storage lifecycle policy as the **Policy storage**.

See "Creating a backup policy" on page 187.

Storage Lifecycle Policy dialog box settings

The **New Storage Lifecycle Policy** dialog box and the **Change Storage Lifecycle Policy** dialog box contain the following settings.

Figure 5-10 Storage Lifecycle Policy tab

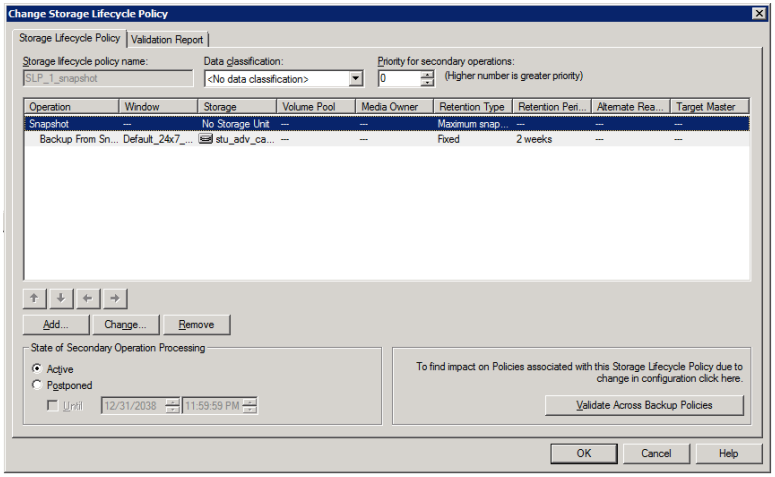


Table 5-32 Storage Lifecycle Policy tab

Setting	Description
Storage lifecycle policy name	The **Storage lifecycle policy name** describes the SLP. The name cannot be modified after the SLP is created.
Data classification	The **Data classification** defines the level or classification of data that the SLP is allowed to process. The drop-down menu contains all of the defined classifications as well as the **Any** classification, which is unique to SLPs. The **Any** selection indicates to the SLP that it should preserve all images that are submitted, regardless of their data classification. It is available for SLP configuration only and is not available to configure a backup policy. In an Auto Image Replication configuration where the master server domains run different versions of NetBackup, see the following topic for special considerations: See "About the storage lifecycle policies required for Auto Image Replication" on page 179. The **Data classification** is an optional setting. One data classification can be assigned to each SLP and applies to all operations in the SLP. If a data classification is selected (other than **Any**), the SLP stores only those images from the policies that are set up for that data classification. If no data classification is indicated, the SLP accepts images of any classification or no classification. The **Data classification** setting allows the NetBackup administrator to classify data based on relative importance. A classification represents a set of backup requirements. When data must meet different backup requirements, consider assigning different classifications. For example, email backup data can be assigned to the silver data classification and financial data backup may be assigned to the platinum classification. A backup policy associates backup data with a data classification. Policy data can be stored only in an SLP with the same data classification. Once data is backed up in an SLP, the data is managed according to the SLP configuration. The SLP defines what happens to the data from the initial backup until the last copy of the image has expired.
Priority for secondary operations	The **Priority for secondary operations** option is the priority that jobs from secondary operations have in relationship to all other jobs. The priority applies to the jobs that result from all operations except for **Backup** and **Snapshot** operations. Range: 0 (default) to 99999 (highest priority). For example, you may want to set the **Priority for secondary operations** for a policy with a gold data classification higher than for a policy with a silver data classification. The priority of the backup job is set in the backup policy on the **Attributes** tab.

Table 5-32 Storage Lifecycle Policy tab *(continued)*

Setting	Description
Operations	Use the **Add**, **Change**, and **Remove** buttons to create a list of operations in the SLP. An SLP must contain one or more operations. Multiple operations imply that multiple copies are created. The list also contains the columns that display information about each operation. Not all columns display by default. For column descriptions, see the following topic:
Arrows	Use the arrows to indicate the indentation (or hierarchy) of the source for each copy. One copy can be the source for many other copies.
Active and **Postponed**	The **Active** and **Postponed** options appear under **State of Secondary Operation Processing** and refer to the processing of all duplication operations in the SLP. **Note:** The **Active** and **Postponed** options apply to duplication operations that create tar-formatted images. For example, those created with `bpduplicate`. The **Active** and **Postponed** options do not affect the images that are duplicated as a result of OpenStorage optimized duplication, NDMP, or if one or more destination storage units are specified as part of a storage unit group. ■ Enable **Active** to let secondary operations continue as soon as possible. When changed from **Postponed** to **Active**, NetBackup continues to process the images, picking up where it left off when secondary operations were made inactive. ■ Enable **Postponed** to postpone the secondary operations for the entire SLP. **Postponed** does not postpone the creation of duplication jobs, it postpones the creation of images instead. The duplication jobs continue to be created, but they are not run until secondary operations are active again. All secondary operations in the SLP are inactive indefinitely unless the administrator selects **Active** or until the **Until** option is selected and an activation date is indicated.
Validate Across Backup Policies button	Click this button to see how changes to this SLP can affect the policies that are associated with this SLP. The button generates a report that displays on the **Validation Report** tab. This button performs the same validation as the `-conflict` option performs when used with the `nbstl` command.

About MSDP backup policy configuration

When you configure a backup policy, for the **Policy storage** select a storage unit that uses a deduplication pool.

For a storage lifecycle policy, for the **Storage unit** select a storage unit that uses a deduplication pool.

For VMware backups, select the **Enable file recovery from VM backup** option when you configure a VMware backup policy. The **Enable file recovery from VM backup** option provides the best deduplication rates.

NetBackup deduplicates the client data that it sends to a deduplication storage unit.

Creating a backup policy

The easiest method to set up a backup policy is to use the **Policy Configuration Wizard**. This wizard guides you through the setup process by automatically choosing the best values for most configurations.

Not all policy configuration options are presented through the wizard. For example, calendar-based scheduling and the **Data Classification** setting. After the policy is created, modify the policy in the **Policies** utility to configure the options that are not part of the wizard.

Note: Do not use the Policy Configuration Wizard to configure policies for Replication Director.

Using the Policy Configuration Wizard to create a backup policy

Use the following procedure to create a backup policy with the Policy Configuration Wizard.

To create a backup policy with the Policy Configuration Wizard

1. In the **NetBackup Administration Console**, in the left pane, click **NetBackup Management**.
2. In the right pane, click **Create a Policy** to begin the **Policy Configuration Wizard**.
3. Select **File systems, databases, applications**.
4. Click **Next** to start the wizard and follow the prompts.

Click **Help** on any wizard panel for assistance while running the wizard.

Creating a backup policy without using the Policy Configuration Wizard

Use the following procedure to create a backup policy in the **NetBackup Administration Console** without using the Policy Configuration Wizard.

To create a policy without the Policy Configuration Wizard

1. In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Policies**.
2. On the **Actions** menu, click **New > Policy**.
3. Type a unique name for the new policy in the **Add a New Policy** dialog box.

   See "NetBackup naming conventions" on page 16.
4. If necessary, clear the **Use Policy Configuration Wizard** check box.
5. Click **OK**.
6. Configure the attributes, the schedules, the clients, and the backup selections for the new policy.

Resilient Network properties

The **Resilient Network** properties appear for the master server, for media servers, and for clients. For media servers and clients, the **Resilient Network** properties are read only. When a job runs, the master server updates the media server and the client with the current properties.

The **Resilient Network** properties let you configure NetBackup to use resilient network connections for backups and restores. A resilient connection allows backup and restore traffic between a client and a NetBackup media server to function effectively in high-latency, low-bandwidth networks such as WANs. The data travels across a wide area network (WAN) to media servers in a central datacenter.

NetBackup monitors the socket connections between the remote client and the NetBackup media server. If possible, NetBackup re-establishes dropped connections and resynchronizes the data stream. NetBackup also overcomes latency issues to maintain an unbroken data stream. A resilient connection can survive network interruptions of up to 80 seconds. A resilient connection may survive interruptions longer than 80 seconds.

The NetBackup Remote Network Transport Service manages the connection between the computers. The Remote Network Transport Service runs on the master server, the client, and the media server that processes the backup or restore job. If the connection is interrupted or fails, the services attempt to re-establish a connection and synchronize the data.

NetBackup protects only the network socket connections that the NetBackup Remote Network Transport Service (`nbrntd`) creates. Examples of the connections that are not supported are:

- Clients that back up their own data (deduplication clients and SAN clients)

- Granular Recovery Technology (GRT) for Exchange Server or SharePoint Server
- NetBackup `nbfsd` process.

NetBackup protects connections only after they are established. If NetBackup cannot create a connection because of network problems, there is nothing to protect.

Resilient connections apply between clients and NetBackup media servers, which includes master servers when they function as media servers. Resilient connections do not apply to master servers or media servers if they function as clients and back up data to a media server.

Resilient connections can apply to all of the clients or to a subset of clients.

Note: If a client is in a different subdomain than the server, add the fully qualified domain name of the server to the client's hosts file. For example, `india.veritas.org` is a different subdomain than `china.veritas.org`.

When a backup or restore job for a client starts, NetBackup searches the **Resilient Network** list from top to bottom looking for the client. If NetBackup finds the client, NetBackup updates the resilient network setting of the client and the media server that runs the job. NetBackup then uses a resilient connection.

Figure 5-11 Master server Resilient Network host properties

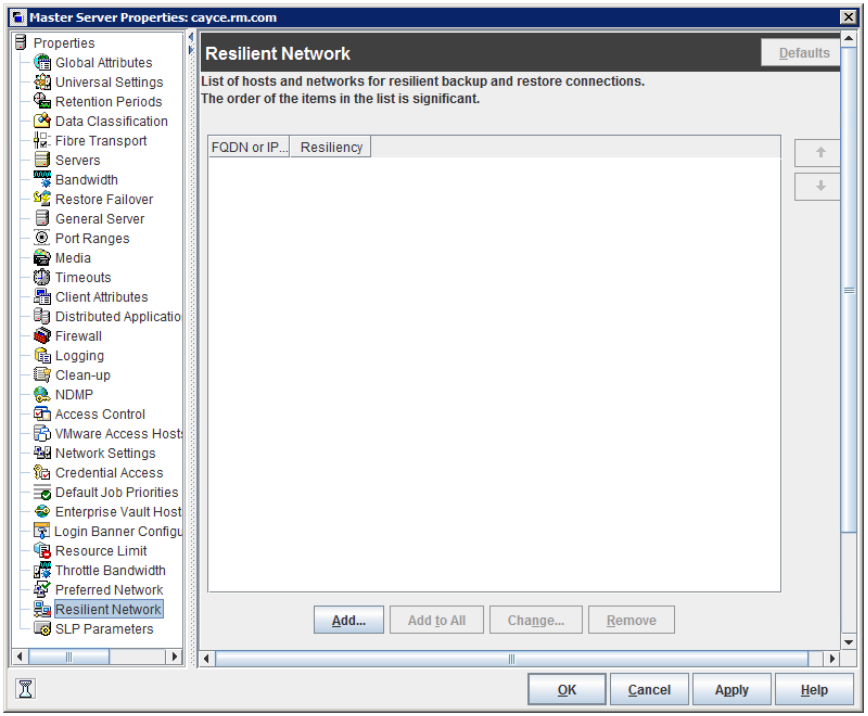


Table 5-33 describes the **Resilient Network** properties.

Table 5-33 Resilient Network dialog box properties

Property	Description
Host Name or IP Address	The **Host Name or IP Address** of the host. The address can also be a range of IP addresses so you can configure more than one client at once. You can mix IPv4 addresses and ranges with IPv6 addresses and subnets. If you specify the host by name, Veritas recommends that you use the fully qualified domain name. Use the arrow buttons on the right side of the pane to move up or move down an item in the list of resilient networks.
Resiliency	**Resiliency** is either **ON** or **OFF**.

Note: The order is significant for the items in the list of resilient networks. If a client is in the list more than once, the first match determines its resilient connection status. For example, suppose you add a client and specify the client IP address and specify **On** for **Resiliency**. Suppose also that you add a range of IP addresses as **Off**, and the client IP address is within that range. If the client IP address appears before the address range, the client connection is resilient. Conversely, if the IP range appears first, the client connection is not resilient.

The resilient status of each client also appears as follows:

- In the **NetBackup Administration Console**, select **NetBackup Management > Policies** in the left pane and then select a policy. In the right pane, a **Resiliency** column shows the status for each client in the policy.
- In the **NetBackup Administration Console**, select **NetBackup Management > Host Properties > Clients** in the left pane. In the right pane, a **Resiliency** column shows the status for each client.

Other NetBackup properties control the order in which NetBackup uses network addresses.

The NetBackup resilient connections use the SOCKS protocol version 5.

Resilient connection traffic is not encrypted. Veritas recommends that you encrypt your backups. For deduplication backups, use the deduplication-based encryption. For other backups, use policy-based encryption.

Resilient connections apply to backup connections. Therefore, no additional network ports or firewall ports must be opened.

Note: If multiple backup streams run concurrently, the Remote Network Transport Service writes a large amount of information to the log files. In such a scenario, Veritas recommends that you set the logging level for the Remote Network Transport Service to 2 or less. Instructions to configure unified logs are in a different guide.

See the NetBackup Logging Reference Guide.

Resilient connection resource usage

Resilient connections consume more resources than regular connections, as follows:

- More socket connections are required per data stream. Three socket connections are required to accommodate the Remote Network Transport Service that runs on both the media server and the client. Only one socket connection is required for a non-resilient connection.

- More sockets are open on media servers and clients. Three open sockets are required rather than one for a non-resilient connection. The increased number of open sockets may cause issues on busy media servers.
- More processes run on media servers and clients. Usually, only one more process per host runs even if multiple connections exist.
- The processing that is required to maintain a resilient connection may reduce performance slightly.

Specifying resilient connections

Use the following procedure to specify resilient connections for NetBackup clients.

See "Resilient Network properties" on page 188.

Alternatively, you can use the `resilient_clients` script to specify resilient connections for clients:

- Windows: *`install_path`*`\NetBackup\bin\admincmd\resilient_clients`
- UNIX: `/usr/openv/netbackup/bin/admincmd/resilient_clients`

To specify resilient connections

1. In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Master Servers** in the left pane.
2. In the right pane, select the master server on which to specify properties.
3. On the **Actions** menu, click **Properties**.
4. In the properties dialog box left pane, select **Resilient Network**.
5. In the **Resilient Network** dialog box, use the following buttons to manage resiliency for clients:

Add

To add resilient settings

1. Click **Add**.

   The **Add Resilient Network Settings** dialog box appears

2. Enter a client host name, an IP address, or an address range.

   If you specify the client host by name, Veritas recommends that you use the fully qualified domain name.

   For address ranges, use Classless Inter-Domain Routing (CIDR) notation (for example, **192.168.100.0/24** or **fd00::/8**).

3. Ensure that the **Resiliency On** option is selected.
4. Click **Add**.
5. Repeat until you have finished entering clients or address ranges.
6. When you finish adding network settings, click **Close**.

Add To All

If you select multiple hosts in the **NetBackup Administration Console**, the entries in the **Resilient Network** list may appear in different colors, as follows:

- The entries that appear in black type are configured on all of the hosts.
- The entries that appear in gray type are configured on some of the hosts only.

For the entries that are configured on some of the hosts only, you can add them to all of the hosts. To do so, select them and click **Add To All**.

Change

To change resilient settings

1. Select the client host name, the IP address, or the address range.
2. Click **Change**.

   The **Change Resilient Network Settings** dialog box appears

3. Select the desired **Resiliency** setting.
4. Click **OK**.

Remove

Remove the select host or address rang

1. Select the client host name, the IP address, or the address range.
2. Click **Remove**.

   The client is removed immediately; a confirmation dialog box does not appear.

Move an item in the list of items

1. Select the client host name, the IP address, or the address range.
2. Click the appropriate button to move up the item or move down the item.

   The order of the items in the list is significant.

   See "Resilient Network properties" on page 188.

6. After specifying resilient connections, click **OK**.

   The settings are propagated to the affected hosts through normal NetBackup inter-host communication, which can take up to 15 minutes.

7. If you want to begin a backup immediately, restart the NetBackup services on the master server.

Adding an MSDP load balancing server

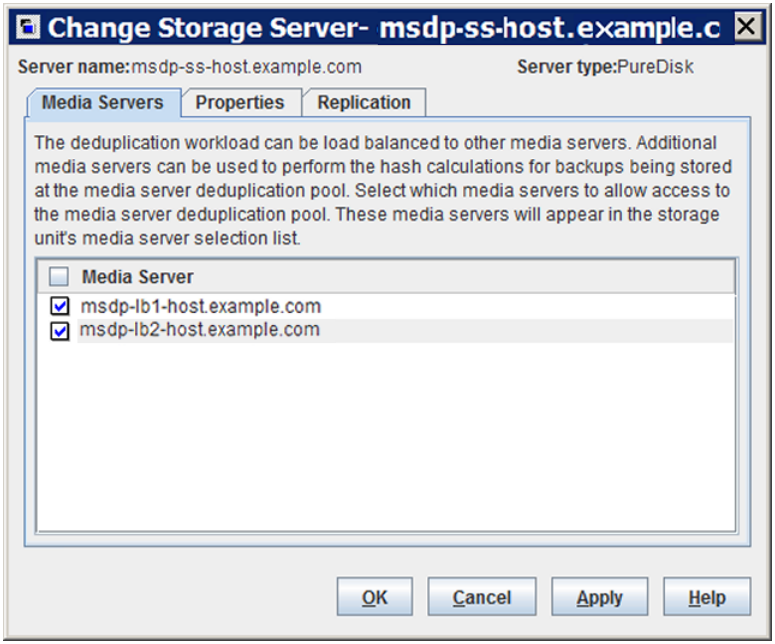
You can add a load balancing server to an existing media server deduplication node.

See "About MSDP storage servers" on page 24.

To add a load balancing server

1. In the NetBackup Administration Console, expand **Media and Device Management > Credentials > Storage Server**
2. Select the deduplication storage server.

3 On the **Edit**, select **Change**.



4 In the **Change Storage Server** dialog box, select the **Media Servers** tab

5 Select the media server or servers that you want to use as a load balancing server. It must be a supported host.

The media servers that are checked are configured as load balancing servers.

6 Click **OK**.

7 For all storage units in which **Only use the following media servers** is configured, ensure that the new load balancing server is selected.

About variable-length deduplication on NetBackup clients

Currently, NetBackup deduplication follows a fixed-length deduplication method where the data streams are chunked into fixed-length segments (128 KB) and then processed for deduplication. Fixed-length deduplication has the advantage of being a swift method and it consumes less computing resources. Fixed-length deduplication handles most kinds of data streams efficiently. However, there can be cases where fixed-length deduplication might result in low deduplication ratios.

If your data was modified in a shifting mode, that is, if some data was inserted in the middle of a file, then variable-length deduplication enables you to get higher deduplication ratios when you back up the data. Variable-length deduplication reduces backup storage, improves the backup performance, and lowers the overall cost that is spent on data protection.

Note: Use variable-length deduplication for data types that do not show a good deduplication ratio with the current MSDP intelligent deduplication algorithm and affiliated streamers. Enabling Variable-length deduplication might improve the deduplication ratio, but consider that the CPU performance might get affected.

In variable-length deduplication, every segment has a variable size with configurable size boundaries. The NetBackup client examines and applies a secure hash algorithm (SHA-2) to the variable-length segments of the data. Each data segment is assigned a unique ID and NetBackup evaluates if any data segment with the same ID exists in the backup. If the data segment already exists, then the segment data is not stored again.

Warning: If you enable compression for the backup policy, variable-length deduplication does not work even when you configure it.

The following table describes the effect of variable-length deduplication on the data backup:

Table 5-34 Effect of variable-length deduplication

Effect on the deduplication ratio	Variable-length deduplication is beneficial if the data file is modified in a shifting mode, that is when data is inserted, removed, or modified at a binary level. When such modified data is backed up again, variable-length deduplication achieves a higher deduplication ratio. Thus, the second or subsequent backups have higher deduplication ratios.
Effect on the CPU	Variable-length deduplication can be a bit more resource-intensive than fixed-length deduplication to achieve a better deduplication ratio. Variable-length deduplication needs more CPU cycles to compute segment boundaries and the backup time might be more than the fixed-length deduplication method.

Table 5-34 Effect of variable-length deduplication *(continued)*

Effect on data restore	Variable-length deduplication does not affect the data restore process.

Configure variable-length deduplication

By default, the variable-length deduplication is disabled on a NetBackup client. You can enable variable-length deduplication by adding parameters in the `pd.conf` file. To enable the same settings for all NetBackup clients or policies, you must specify all the clients or policies in the `pd.conf` file.

In a deduplication load balancing scenario, you must upgrade the media servers to NetBackup 8.1.1 or later and modify the `pd.conf` file on all the media servers. If a backup job selects an older media server (earlier than NetBackup 8.1.1) for the load balancing pool, fixed-length deduplication is used instead of variable-length deduplication. Avoid configuring media servers with different NetBackup versions in a load balancing scenario. The data segments generated from variable-length deduplication are different from the data segments generated from fixed-length deduplication. Therefore, load balancing media servers with different NetBackup versions results in a low deduplication ratio.

See "About the MSDP pd.conf configuration file" on page 197.

See "Editing the MSDP pd.conf file" on page 198.

See "MSDP pd.conf file parameters" on page 198.

About the MSDP pd.conf configuration file

On each NetBackup host that deduplicates data, a `pd.conf` file contains the various configuration settings that control the operation of deduplication for the host. By default, the `pd.conf` file settings on the deduplication storage server apply to all load balancing servers and all clients that deduplicate their own data.

You can edit the file to configure advanced settings for that host. If a configuration setting does not exist in a `pd.conf` file, you can add it. If you change the `pd.conf` file on a host, it changes the settings for that host only. If you want the same settings for all of the hosts that deduplicate data, you must change the `pd.conf` file on all of the hosts.

The `pd.conf` file settings may change between releases. During upgrades, NetBackup adds only the required settings to existing `pd.conf` files.

The `pd.conf` file resides in the following directories:

- (UNIX) `/usr/openv/lib/ost-plugins/`

- (Windows) *install_path*\Veritas\NetBackup\bin\ost-plugins

See "MSDP pd.conf file parameters" on page 198.

See "Editing the MSDP pd.conf file" on page 198.

Editing the MSDP pd.conf file

If you change the pd.conf file on a host, it changes the settings for that host only. If you want the same settings for all of the hosts that deduplicate data, you must change the pd.conf file on all of the hosts.

Note: Veritas recommends that you make a backup copy of the file before you edit it.

See "About the MSDP pd.conf configuration file" on page 197.

See "MSDP pd.conf file parameters" on page 198.

To edit the pd.conf file

1. Use a text editor to open the pd.conf file.

   The pd.conf file resides in the following directories:

   - (UNIX) /usr/openv/lib/ost-plugins/
   - (Windows) *install_path*\Veritas\NetBackup\bin\ost-plugins

2. To activate a setting, remove the pound character (#) in column 1 from each line that you want to edit.
3. To change a setting, specify a new value.

   Note: The spaces to the left and right of the equal sign (=) in the file are significant. Ensure that the space characters appear in the file after you edit the file.

4. Save and close the file.
5. Restart the NetBackup Remote Manager and Monitor Service (nbrmms) on the host.

MSDP pd.conf file parameters

Table 5-35 describes the deduplication parameters that you can configure for a NetBackup **Media Server Deduplication Pool** environment.

The parameters in this table are in alphabetical order; the parameters in a `pd.conf` file may not be in alphabetical order.

The parameters in the file in your release may differ from those that are described in this topic.

You can edit the file to configure advanced settings for a host. If a parameter does not exist in a `pd.conf` file, you can add it. During upgrades, NetBackup adds only required parameters to existing `pd.conf` files.

The `pd.conf` file resides in the following directories:

- (Windows) *`install_path`*`\Veritas\NetBackup\bin\ost-plugins`
- (UNIX) `/usr/openv/lib/ost-plugins/`

Table 5-35 pd.conf file parameters

Parameter	Description

`BACKUPRESTORERANGE`	On a client, specifies the IP address or range of addresses that the local network interface card (NIC) should use for backups and restores.
	Specify the value in one of two ways, as follows:
	■ Classless Inter-Domain Routing (CIDR) format. For example, the following notation specifies 192.168.10.0 and 192.168.10.1 for traffic:
	`BACKUPRESTORERANGE = 192.168.10.1/31`
	■ Comma-separated list of IP addresses. For example, the following notation specifies 192.168.10.1 and 192.168.10.2 for traffic:
	`BACKUPRESTORERANGE = 192.168.10.1, 192.168.10.2`
	Default value: `BACKUPRESTORERANGE=` (no default value)
	Possible values: Classless Inter-Domain Routing format notation or comma-separated list of IP addresses

`BANDWIDTH_LIMIT`	Determines the maximum bandwidth that is allowed when backing up or restoring data between the deduplication host and the deduplication pool. The value is specified in KBytes/second. The default is no limit. Default value: `BANDWIDTH_LIMIT = 0` Possible values: `0` (no limit) to the practical system limit, in KBs/sec
`COMPRESSION`	Specifies whether to compress the data during backups. By default, the data is compressed. Default value: `COMPRESSION = 1` Possible values: `0` (off) or `1` (on) See "About MSDP compression" on page 121.

Table 5-35 pd.conf file parameters *(continued)*

Parameter	Description
CR_STATS_TIMER	Specifies a time interval in seconds for retrieving statistics from the storage server host. The default value of 0 disables caching and retrieves statistics on demand. Consider the following information before you change this setting: ■ If disabled (set to 0), a request for the latest storage capacity information occurs whenever NetBackup requests it. ■ If you specify a value, a request occurs only after the specified number of seconds since the last request. Otherwise, a cached value from the previous request is used. ■ Enabling this setting may reduce the queries to the storage server. The drawback is the capacity information reported by NetBackup becomes stale. Therefore, if storage capacity is close to full, Veritas recommends that you do not enable this option. ■ On high load systems, the load may delay the capacity information reporting. If so, NetBackup may mark the storage unit as down. Default value: `CR_STATS_TIMER = 0` Possible values: `0` or greater, in seconds
DEBUGLOG	Specifies the file to which NetBackup writes the deduplication plug-in log information. NetBackup prepends a date stamp to each day's log file. On Windows, a partition identifier and slash must precede the file name. On UNIX, a slash must precede the file name. **Note:** This parameter does not apply for NDMP backups from a NetApp appliance. Default value: ■ UNIX: `DEBUGLOG = /var/log/puredisk/pdplugin.log` ■ Windows: `DEBUGLOG = C:\pdplugin.log` Possible values: Any path

Table 5-35 pd.conf file parameters *(continued)*

Parameter	Description
DISABLE_BACKLEVEL_TLS	When secure communication is established between the client and the server, this parameter specifies whether or not to disable older TLS versions. NetBackup version 8.0 and earlier use older TLS versions such as SSLV2, SSLV3, TLS 1.0, and TLS 1.1. To enable TLS 1.2, change the value of the DISABLE_BACKLEVEL_TLS parameter to 1 and restart the NetBackup Deduplication Engine (spoold) and the NetBackup Deduplication Manager (spad). Default value: DISABLE_BACKLEVEL_TLS = 0 Possible values: 0 (off) or 1 (on) **Note:** To enable TLS 1.2, NetBackup version must be 8.1 and later. When TLS 1.2 is enabled (DISABLE_BACKLEVEL_TLS = 1) on a machine (which can be a client or a media server or a load balance server), to establish communication, all machines connected to it must also enable TLS 1.2. For a standard backup, NetBackup client version 8.0 and earlier can communicate with NetBackup server (media server or load balance server) version 8.1 that has TLS 1.2 enabled. However, in case of optimized duplication and replication, load balance, and client direct duplication, NetBackup client versions 8.0 and earlier cannot communicate with NetBackup server (media server or load balance server) version 8.1, which has TLS 1.2 enabled. Further, NetBackup 5000 series appliance does not support TLS 1.2.
DONT_SEGMENT_TYPES	A comma-separated list of file name extensions of files not to be deduplicated. Files in the backup stream that have the specified extensions are given a single segment if smaller than 16 MB. Larger files are deduplicated using the maximum 16-MB segment size. Example: DONT_SEGMENT_TYPES = mp3,avi This setting prevents NetBackup from analyzing and managing segments within the file types that do not deduplicate globally. Note: this parameter does not apply to the NDMP backups that use the NetApp stream handler. Default value: DONT_SEGMENT_TYPES = (no default value) Possible values: comma-separated file extensions

Table 5-35 pd.conf file parameters *(continued)*

Parameter	Description
ENCRYPTION	Specifies whether to encrypt the data during backups. By default, files are not encrypted. If you set this parameter to 1 on all hosts, the data is encrypted during transfer and on the storage. Default value: `ENCRYPTION = 0` Possible values: `0` (no encryption) or `1` (encryption) See "About MSDP encryption" on page 123.
FIBRECHANNEL	Enable Fibre Channel for backup and restore traffic to and from a NetBackup series appliance. Default value: `FIBRECHANNEL = 0` Possible values: `0` (off) or `1` (on)

Table 5-35 pd.conf file parameters *(continued)*

Parameter	Description
FILE_KEEP_ALIVE_INTERVAL	The interval in seconds at which to perform keepalives on idle sockets. The following items describe the behavior based on how you configure this parameter: ■ Commented out (default) and Resilient Network connections are enabled: If the value is less than 75 seconds, the keep alive interval is 60 seconds. If the value is greater than 1800 seconds (30 minutes), the keep alive interval is 1440 seconds (80% of 30 minutes). If the value is between 75 and 1800 sections, the keep-alive interval is 80% of the parameter value. See "Resilient Network properties" on page 188. ■ Commented out (the default) and Resilient Network connections are *not* enabled: The keep-alive interval is 1440 seconds (80% of 30 minutes). ■ 0 or less: Disabled; no keepalives are sent. ■ Greater than 0: The keep-alive interval is the specified value in seconds except as follows: If less than 60 seconds or greater than 7200 seconds (two hours), the keep-alive interval is 1440 seconds (80% of 30 minutes). Default value : `FILE_KEEP_ALIVE_INTERVAL = 1440` Possible values: `0` (disabled) or `60` to `7200` seconds To determine the keep alive interval that NetBackup uses, examine the deduplication plug-in log file for a message similar to the following: `Using keepalive interval of xxxx seconds` For more information about the deduplication plug-in log file, see `DEBUGLOG` and `LOGLEVEL` in this table.

Table 5-35 pd.conf file parameters *(continued)*

Parameter	Description
FP_CACHE_CLIENT_POLICY	**Note:** Veritas recommends that you use this setting on the individual clients that back up their own data (client-side deduplication). If you use it on a storage server or load balancing server, it affects all backup jobs. Specifies the client, backup policy, and date from which to obtain the fingerprint cache for the first backup of a client. By default, the fingerprints from the previous backup are loaded. This parameter lets you load the fingerprint cache from another, similar backup. It can reduce the amount of time that is required for the first backup of a client. This parameter especially useful for remote office backups to a central datacenter in which data travels long distances over a WAN. Specify the setting in the following format: ***clienthostmachine,backuppolicy,date*** The ***date*** is the last date in mm/dd/yyyy format to use the fingerprint cache from the client you specify. Default value: `FP_CACHE_CLIENT_POLICY =` (no default value) See "Configuring MSDP fingerprint cache seeding on the client" on page 67.
FP_CACHE_INCREMENTAL	Specifies whether to use fingerprint caching for incremental backups. Because incremental backups only back up what has changed since the last backup, cache loading has little affect on backup performance for incremental backups. Default value: `FP_CACHE_INCREMENTAL = 0` Possible values: `0` (off) or `1` (on) **Note:** Change this value only when directed to do so by a Veritas representative.
FP_CACHE_LOCAL	Specifies whether or not to use the fingerprint cache for the backup jobs that are deduplicated on the storage server. This parameter does not apply to load balancing servers or to clients that deduplicate their own data. When the deduplication job is on the same host as the NetBackup Deduplication Engine, disabling the fingerprint cache improves performance. Default value: `FP_CACHE_LOCAL = 1` Possible values: `0` (off) or `1` (on)

Table 5-35 pd.conf file parameters *(continued)*

Parameter	Description
FP_CACHE_MAX_COUNT	Specifies the maximum number of images to load in the fingerprint cache. Default value: FP_CACHE_MAX_COUNT = 1024 Possible values: 0 to 4096 **Note:** Change this value only when directed to do so by a Veritas representative.
FP_CACHE_MAX_MBSIZE	Specifies the amount of memory in MBs to use for the fingerprint cache. Default value: FP_CACHE_MAX_MBSIZE = 20 Possible values: 0 to the computer limit **Note:** Change this value only when directed to do so by a Veritas representative.
FP_CACHE_PERIOD_REBASING_THRESHOLD	Specifies the threshold (MB) for periodic rebasing during backups. A container is considered for rebasing if both of the following are true: ■ The container has not been rebased within the last three months. ■ For that backup, the data segments in the container consume less space than the FP_CACHE_PERIOD_REBASING_THRESHOLD value. Default value: FP_CACHE_PERIOD_REBASING_THRESHOLD = 16 Possible values: 0 (disabled) to 256 See "About MSDP storage rebasing" on page 309.
FP_CACHE_REBASING_THRESHOLD	Specifies the threshold (MB) for normal rebasing during backups. A container is considered for rebasing if both of the following are true: ■ The container has been rebased within the last three months. ■ For that backup, the data segments in the container consume less space than the FP_CACHE_REBASING_THRESHOLD value. Default value:FP_CACHE_REBASING_THRESHOLD = 4 Possible values: 0 (disabled) to 200 If you change this value, consider the new value carefully. If you set it too large, all containers become eligible for rebasing. Deduplication rates are lower for the backup jobs that perform rebasing. See "About MSDP storage rebasing" on page 309.

Table 5-35 pd.conf file parameters *(continued)*

Parameter	Description
LOCAL_SETTINGS	Specifies whether to use the `pd.conf` settings of the local host or to allow the server to override the local settings. The following is the order of precedence for local settings: ■ Local host ■ Load balancing server ■ Storage server To use the local settings, set this value to `1`. Default value: `LOCAL_SETTINGS = 0` Possible values: `0` (allow override) or `1` (always use local settings)
LOGLEVEL	Specifies the amount of information that is written to the log file. The range is from 0 to 10, with 10 being the most logging. Default value: `LOGLEVEL = 0` Possible values: An integer, `0` to `10` inclusive **Note:** Change this value only when directed to do so by a Veritas representative.
MAX_IMG_MBSIZE	The maximum backup image fragment size in megabytes. Default value: `MAX_IMG_MBSIZE = 51200` Possible values: `0` to `51,200`, in MBs **Note:** Change this value only when directed to do so by a Veritas representative.
MAX_LOG_MBSIZE	The maximum size of the log file in megabytes. NetBackup creates a new log file when the log file reaches this limit. NetBackup prepends the date and the ordinal number beginning with 0 to each log file, such as `120131_0_pdplugin.log`, `120131_1_pdplugin.log`, and so on. Default value: `MAX_LOG_MBSIZE = 100` Possible values: `0` to `50,000`, in MBs
META_SEGKSIZE	The segment size for metadata streams Default value: `META_SEGKSIZE = 16384` Possible values: 32-16384, multiples of 32 **Note:** Change this value only when directed to do so by a Veritas representative.

Table 5-35 pd.conf file parameters *(continued)*

Parameter	Description
MTSTRM_BACKUP_CLIENTS	If set, limits the use of the Multi-Threaded Agent to the backups of the specified clients. The clients that are not specified use single-threading. This setting does not guarantee that the specified clients use the Multi-Threaded Agent. The MaxConcurrentSessions parameter in the mtstrm.conf file controls the number of backups the Multi-Threaded Agent processes concurrently. If you specify more clients than the MaxConcurrentSessions value, some of the clients may use single-threaded processing. See "MSDP mtstrm.conf file parameters" on page 56. The format is a comma-separated list of the clients, case insensitive (for example, MTSTRM_BACKUP_CLIENTS = client1,client2,client3). Default value: MTSTRM_BACKUP_CLIENTS = (no default value) Possible values: comma separated client names See "About the MSDP Deduplication Multi-Threaded Agent" on page 54.

Table 5-35 pd.conf file parameters *(continued)*

Parameter	Description
MTSTRM_BACKUP_ENABLED	Use the Multi-Threaded Agent in the backup stream between the deduplication plug-in and the NetBackup Deduplication Engine. Default value: MTSTRM_BACKUP_ENABLED = (no default value) Possible values: 1 (On) or 0 (Off) The value for this parameter is configured during installation or upgrade. If the hardware concurrency value of the host is greater than a hardware concurrency threshold value, NetBackup sets MTSTRM_BACKUP_ENABLED to 1. (For the purposes of this parameter, the *hardware concurrency* is the number of CPUs or cores or hyperthreading units.) The following items describe the values that are used for the determination algorithm: ■ The hardware concurrency value is one of the following: ■ For media servers, half of the host's hardware concurrency is used for the hardware concurrency value in the algorithm. ■ For clients, all of the host's hardware concurrency is used for the hardware concurrency value in the algorithm. ■ The hardware concurrency threshold value to enable multithreading is one of the following: ■ Windows and Linux: The threshold value is 2. ■ Solaris: The threshold value is 4. The following examples may be helpful: ■ A Linux media server that has 8 CPU cores with two hyperthreading units per core has a hardware concurrency of 16. Therefore, the hardware concurrency value for the algorithm is 8 (for media servers, half of the system's hardware concurrency). Eight is greater than two (the threshold value of Windows and Linux), so multithreading is enabled (MTSTRM_BACKUP_ENABLED = 1). ■ A Solaris client that has 2 CPU cores without hyperthreading has a hardware concurrency of 2. The hardware concurrency value for the algorithm is 2 (for clients, all of the system's hardware concurrency). Two is not greater than four (the threshold value of Solaris), so multithreading is not enabled (MTSTRM_BACKUP_ENABLED = 0). See "About the MSDP Deduplication Multi-Threaded Agent" on page 54.

Table 5-35 pd.conf file parameters *(continued)*

Parameter	Description
MTSTRM_BACKUP_POLICIES	If set, limits the use of the Multi-Threaded Agent to the backups of the specified policies. The clients in the policies that are not specified use single-threading, unless the client is specified in the MTSTRM_BACKUP_CLIENTS parameter. This setting does not guarantee that all of the clients in the specified policies use the Multi-Threaded Agent. The MaxConcurrentSessions parameter in the mtstrm.conf file controls the number of backups the Multi-Threaded Agent processes concurrently. If the policies include more clients than the MaxConcurrentSessions value, some of the clients may use single-threaded processing. See "MSDP mtstrm.conf file parameters" on page 56. The format is a comma-separated list of the policies, case sensitive (for example, MTSTRM_BACKUP_POLICIES = policy1,policy2,policy3). Default value: MTSTRM_BACKUP_POLICIES = (no default value) Possible values: comma separated backup policy names See "About the MSDP Deduplication Multi-Threaded Agent" on page 54.
MTSTRM_IPC_TIMEOUT	The number of seconds to wait for responses from the Multi-Threaded Agent before the deduplication plug-in times out with an error. Default value: MTSTRM_IPC_TIMEOUT = 1200 Possible values: 1-86400, inclusive See "About the MSDP Deduplication Multi-Threaded Agent" on page 54.
OPTDUP_BANDWIDTH	Determines the bandwidth that is allowed for each optimized duplication and Auto Image Replication stream on a deduplication server. OPTDUP_BANDWIDTH does not apply to clients. The value is specified in KBytes/second. Default value: OPTDUP_BANDWIDTH= 0 Possible values: 0 (no limit) to the practical system limit, in KBs/sec A global bandwidth parameter effects whether or not OPTDUP_BANDWIDTH applies. See "About configuring MSDP optimized duplication and replication bandwidth" on page 177.

Table 5-35 pd.conf file parameters *(continued)*

Parameter	Description
OPTDUP_COMPRESSION	Specifies whether to compress the data during optimized duplication and Auto Image Replication. By default, files are compressed. To disable compression, change the value to 0. This parameter does not apply to clients. Default value: OPTDUP_COMPRESSION = 1 Possible values: 0 (off) or 1 (on) See "About MSDP compression" on page 121.
OPTDUP_ENCRYPTION	Specifies whether to encrypt the data during optimized duplication and replication. By default, files are not encrypted. If you want encryption, change the value to 1 on the MSDP storage server and on the MSDP load balancing servers. This parameter does not apply to clients. If you set this parameter to 1 on all hosts, the data is encrypted during transfer. Default value: OPTDUP_ENCRYPTION = 0 Possible values: 0 (off) or 1 (on) See "About MSDP encryption" on page 123.
OPTDUP_TIMEOUT	Specifies the number of minutes before the optimized duplication times out. Default value: OPTDUP_TIMEOUT = 720 Possible values: The value, expressed in minutes

Table 5-35 pd.conf file parameters *(continued)*

Parameter	Description
PDDO_SSL_VERIFY	Specifies whether to perform SSL verification when communicating with the NetBackup 5000 series appliance. By default, SSL verification is not performed while communication with the NetBackup 5000 series appliance. To perform SSL verification, change the value to 1 and copy the root certificate file of NetBackup 5000 series appliance to following directory: ■ For Windows: install_path\Veritas\NetBackup\bin\ost-plugins ■ For UNIX: /usr/openv/lib/ost-plugins/ After copying the root certificate file, you must rename it to storage_server_name.pem, where *storage_server_name* is the fully qualified domain name of the NetBackup 5000 series appliance. The root certificate file on NetBackup 5000 series appliance is: ■ (1.4.4) /Storage/var/VRTSat/.VRTSat/profile/certstore/trusted/*.0 ■ (1.4.5) /Storage/var/VxAT/root/.VRTSat/profile/certstore/trusted/*.0 If there are multiple NetBackup servers and NetBackup clients that communicate with NetBackup 5000 series appliance, the root certificate file must be copied to all the media servers and NetBackup clients. Default value: PDDO_SSL_VERIFY = 0 Possible values: 0 (off) or 1 (on)
PREFERRED_EXT_SEGKSIZE	Specifies the file extensions and the preferred segment sizes in KB for specific file types. File extensions are case sensitive. The following describe the default values: edb are Exchange Server files; mdfare SQL Server master database files, ndf are SQL Server secondary data files, and segsize64k are Microsoft SQL streams. Default value: PREFERRED_EXT_SEGKSIZE = edb:32,mdf:64,ndf:64,segsize64k:64 Possible values: *file_extension*:*segment_size_in_KBs* pairs, separated by commas. See also SEGKSIZE.

Table 5-35 pd.conf file parameters *(continued)*

Parameter	Description
PREFETCH_SIZE	The size in bytes to use for the data buffer for restore operations. Default value: PREFETCH_SIZE = 33554432 Possible values: 0 to the computer's memory limit **Note:** Change this value only when directed to do so by a Veritas representative.
RESTORE_DECRYPT_LOCAL	Specifies on which host to decrypt and decompress the data during restore operations. Depending on your environment, decryption and decompression on the client may provide better performance. Default value: RESTORE_DECRYPT_LOCAL = 1 Possible values: 0 enables decryption and decompression on the media server; 1 enables decryption and decompression on the client.
SEGKSIZE	The default file segment size in kilobytes. Default value: SEGKSIZE = 128 Possible values: 32 to 16384 KBs, increments of 32 only **Warning:** Changing this value may reduce capacity and decrease performance. Change this value only when directed to do so by a Veritas representative. You can also specify the segment size for specific file types. See PREFERRED_EXT_SEGKSIZE.

Table 5-35 pd.conf file parameters *(continued)*

Parameter	Description
VLD_CLIENT_NAME	Specifies the name of the NetBackup client to enable variable-length deduplication. By default, the VLD_CLIENT_NAME parameter is not present in the pd.conf configuration file. You can also specify different maximum and minimum segment sizes with this parameter for different NetBackup clients. If you do not specify the segment sizes, then the default values are considered. The values are case-sensitive. Use in any of the following formats: ■ VLD_CLIENT_NAME = * Enables variable-length deduplication for all NetBackup clients and uses the default VLD_MIN_SEGKSIZE and VLD_MAX_SEGKSIZE values. ■ VLD_CLIENT_NAME = *clientname* Enables variable-length deduplication for NetBackup client *clientname* and uses the default VLD_MIN_SEGKSIZE and VLD_MAX_SEGKSIZE values. ■ VLD_CLIENT_NAME = *clientname (64, 256)* Enables variable-length deduplication for NetBackup client *clientname* and uses 64 KB as the VLD_MIN_SEGKSIZE and 256 KB as the VLD_MAX_SEGKSIZE value. **Note:** You can add a maximum of 50 clients in the pd.conf file.
VLD_MIN_SEGKSIZE	The minimum size of the data segment for variable-length deduplication in KB. The segment size must be in multiples of 4 and fall in between 4 KB to 16384 KB. The default value is 64 KB. The value must be smaller than VLD_MAX_SEGKSIZE. Different NetBackup clients can have different segment sizes. A larger value reduces the CPU consumption, but decreases the deduplication ratio. A smaller value increases the CPU consumption, but increases the deduplication ratio **Note:** Keeping similar or close values for VLD_MIN_SEGKSIZE and VLD_MAX_SEGKSIZE results in a performance that is similar to fixed-length deduplication.

Table 5-35 pd.conf file parameters *(continued)*

Parameter	Description
VLD_MAX_SEGKSIZE	The maximum size of the data segment for variable-length deduplication in KB. VLD_MAX_SEGKSIZE is used to set a boundary for the data segments. The segment size must be in multiples of 4 and fall in between 4 KB to 16384 KB. The default value is 128 KB. The value must be greater than VLD_MIN_SEGKSIZE. Different NetBackup clients can have different segment sizes. **Note:** Keeping similar or close values for VLD_MIN_SEGKSIZE and VLD_MAX_SEGKSIZE results in a performance that is similar to fixed-length deduplication.
VLD_POLICY_NAME	Specifies the name of the backup policy to enable variable-length deduplication. By default, the VLD_POLICY_NAME parameter is not present in the pd.conf configuration file. You can also specify different maximum and minimum segment sizes with this parameter for different NetBackup policies. If you do not specify the segment sizes, then the default values are considered. The values are case-sensitive. Use in any of the following formats: ■ VLD_POLICY_NAME = * Enables variable-length deduplication for all NetBackup policies and uses the default VLD_MIN_SEGKSIZE and VLD_MAX_SEGKSIZE values. ■ VLD_POLICY_NAME = *policyname* Enables variable-length deduplication for NetBackup policy *policyname* and uses the default VLD_MIN_SEGKSIZE and VLD_MAX_SEGKSIZE values. ■ VLD_POLICY_NAME = *policyname (64, 256)* Enables variable-length deduplication for NetBackup policy *policyname* and uses 64 KB as the VLD_MIN_SEGKSIZEand 256 KB as the VLD_MAX_SEGKSIZE value. **Note:** You can add a maximum of 50 policies in the pd.conf file.

See “About the MSDP pd.conf configuration file” on page 197.

See “Editing the MSDP pd.conf file” on page 198.

About the MSDP contentrouter.cfg file

The `contentrouter.cfg` file contains various configuration settings that control some of the operations of your deduplication environment.

Usually, you do not need to change settings in the file. However, in some cases, you may be directed to change settings by a Veritas support representative.

The NetBackup documentation exposes only some of the `contentrouter.cfg` file parameters. Those parameters appear in topics that describe a task or process to change configuration settings.

Note: Change values in the `contentrouter.cfg` only when directed to do so by the NetBackup documentation or by a Veritas representative.

The `contentrouter.cfg` file resides in the following directories:

- (UNIX) *storage_path*`/etc/puredisk`
- (Windows) *storage_path*`\etc\puredisk`

About saving the MSDP storage server configuration

You can save your storage server settings in a text file. A saved storage server configuration file contains the configuration settings for your storage server. It also contains status information about the storage. A saved configuration file may help you with recovery of your storage server. Therefore, Veritas recommends that you get the storage server configuration and save it in a file. The file does not exist unless you create it.

The following is an example of a populated configuration file:

```
V7.0 "storagepath" "D:\DedupeStorage" string
V7.0 "spalogpath" "D:\DedupeStorage\log" string
V7.0 "dbpath" "D:\DedupeStorage" string
V7.0 "required_interface" "HOSTNAME" string
V7.0 "spalogretention" "7" int
V7.0 "verboselevel" "3" int
V7.0 "replication_target(s)" "none" string
V7.0 "Storage Pool Size" "698.4GB" string
V7.0 "Storage Pool Used Space" "132.4GB" string
V7.0 "Storage Pool Available Space" "566.0GB" string
V7.0 "Catalog Logical Size" "287.3GB" string
```

```
V7.0 "Catalog files Count" "1288" string
V7.0 "Space Used Within Containers" "142.3GB" string
```

V7.0 represents the version of the I/O format not the NetBackup release level. The version may differ on your system.

If you get the storage server configuration when the server is not configured or is down and unavailable, NetBackup creates a template file. The following is an example of a template configuration file:

```
V7.0 "storagepath" " " string
V7.0 "spalogin" " " string
V7.0 "spapasswd" " " string
V7.0 "spalogretention" "7" int
V7.0 "verboselevel" "3" int
V7.0 "dbpath" " " string
V7.0 "required_interface" " " string
```

To use a storage server configuration file for recovery, you must edit the file so that it includes only the information that is required for recovery.

See “Saving the MSDP storage server configuration” on page 216.

See “Editing an MSDP storage server configuration file” on page 217.

See “Setting the MSDP storage server configuration” on page 218.

Saving the MSDP storage server configuration

Veritas recommends that you save the storage server configuration in a file. A storage server configuration file can help with recovery.

See “About saving the MSDP storage server configuration” on page 215.

See “Recovering from an MSDP storage server disk failure” on page 321.

See “Recovering from an MSDP storage server failure” on page 322.

To save the storage server configuration

- On the master server, enter the following command:

UNIX: `/usr/openv/netbackup/bin/admincmd/nbdevconfig -getconfig -storage_server` *`sshostname`* `-stype PureDisk -configlist` *`file.txt`*

Windows: *`install_path`*`\NetBackup\bin\admincmd\nbdevconfig -getconfig -storage_server` *`sshostname`* `-stype PureDisk -configlist` *`file.txt`*

For *sshostname*, use the name of the storage server. For *file.txt*, use a file name that indicates its purpose.

If you get the file when a storage server is not configured or is down and unavailable, NetBackup creates a template file.

Editing an MSDP storage server configuration file

To use a storage server configuration file for recovery, it must contain only the required information. You must remove any point–in–time status information. (Status information is only in a configuration file that was saved on an active storage server.) You also must add several configuration settings that are not included in a saved configuration file or a template configuration file.

Table 5-36 shows the configuration lines that are required.

Table 5-36 Required lines for a recovery file

Configuration setting	Description
`V7.0 "storagepath" " " string`	The value should be the same as the value that was used when you configured the storage server.
`V7.0 "spalogpath" " " string`	For the `spalogpath`, use the `storagepath` value and append `log` to the path. For example, if the `storagepath` is `D:\DedupeStorage`, enter `D:\DedupeStorage\log`.
`V7.0 "dbpath" " " string`	If the database path is the same as the `storagepath` value, enter the same value for `dbpath`. Otherwise, enter the path to the database.
`V7.0 "required_interface" " " string`	A value for `required_interface` is required only if you configured one initially; if a specific interface is not required, leave it blank. In a saved configuration file, the required interface defaults to the computer's hostname.
`V7.0 "spalogretention" "7" int`	Do not change this value.
`V7.0 "verboselevel" "3" int`	Do not change this value.
`V7.0 "replication_target(s)" "none" string`	A value for `replication_target(s)` is required only if you configured optimized duplication. Otherwise, do not edit this line.
`V7.0 "spalogin" "`*`username`*`" string`	Replace *username* with the NetBackup Deduplication Engine user ID.
`V7.0 "spapasswd" "`*`password`*`" string`	Replace *password* with the password for the NetBackup Deduplication Engine user ID.

Table 5-36 Required lines for a recovery file *(continued)*

Configuration setting	Description
`V7.0 "encryption" " " int`	The value should be the same as the value that was used when you configured the storage server.
`V7.0 "kmsenabled" " " int`	The value is used to enable or disable MSDP KMS configuration. The value should be the same as the value that was used when you configured the storage server.
`V7.0 "kmsservertype" " " int`	The value is KMS server type. This value should be 0.
`V7.0 "kmsservername" " " string`	The value is NBU Key Management Server. The value should be the same as the value that was used when you configured the storage server.
`V7.0 "keygroupname" " " string`	The value should be the same as the value that was used when you configured the storage server.

See "About saving the MSDP storage server configuration" on page 215.

See "Recovering from an MSDP storage server disk failure" on page 321.

See "Recovering from an MSDP storage server failure" on page 322.

To edit the storage server configuration

1. If you did not save a storage server configuration file, get a storage server configuration file.

   See "Saving the MSDP storage server configuration" on page 216.

2. Use a text editor to enter, change, or remove values.

   Remove lines from and add lines to your file until only the required lines (see Table 5-36) are in the configuration file. Enter or change the values between the second set of quotation marks in each line. A template configuration file has a space character (`" "`) between the second set of quotation marks.

Setting the MSDP storage server configuration

You can set the storage server configuration (that is, configure the storage server) by importing the configuration from a file. Setting the configuration can help you with recovery of your environment.

See "Recovering from an MSDP storage server disk failure" on page 321.

See "Recovering from an MSDP storage server failure" on page 322.

To set the configuration, you must have an edited storage server configuration file.

See "About saving the MSDP storage server configuration" on page 215.

See "Saving the MSDP storage server configuration" on page 216.

See "Editing an MSDP storage server configuration file" on page 217.

Note: The only time you should use the `nbdevconfig` command with the `-setconfig` option is for recovery of the host or the host disk.

To set the storage server configuration

- On the master server, run the following command:

  UNIX: `/usr/openv/netbackup/bin/admincmd/nbdevconfig -setconfig -storage_server` *`sshostname`* `-stype PureDisk -configlist` *`file.txt`*

  Windows: *`install_path`*`\NetBackup\bin\admincmd\nbdevconfig -setconfig -storage_server` *`sshostname`* `-stype PureDisk -configlist` *`file.txt`*

  For *sshostname*, use the name of the storage server. For *file.txt*, use the name of the file that contains the configuration.

About the MSDP host configuration file

Each NetBackup host that is used for deduplication has a configuration file; the file name matches the name of the storage server, as follows:

`storage_server_name``.cfg`

The *storage_server_name* is the fully qualified domain name if that was used to configure the storage server. For example, if the storage server name is `DedupeServer.example.com`, the configuration file name is `DedupeServer.example.com.cfg`.

The following is the location of the file:

Windows: *`install_path`*`\Veritas\NetBackup\bin\ost-plugins`

UNIX: `/usr/openv/lib/ost-plugins`

Deleting an MSDP host configuration file

You may need to delete the configuration file from the deduplication hosts. For example, to reconfigure your deduplication environment or disaster recovery may require that you delete the configuration file on the servers on which it exists.

See "About the MSDP host configuration file" on page 219.

To delete the host configuration file

- Delete the file on the deduplication host; its location depends on the operating system type, as follows:

  UNIX: `/usr/openv/lib/ost-plugins`

  Windows: *`install_path`*`\Veritas\NetBackup\bin\ost-plugins`

  The following is an example of the host configuration file name of a server that has a fully qualified domain name:

  `DedupeServer.example.com.cfg`

Resetting the MSDP registry

If you reconfigure your deduplication environment, one of the steps is to reset the deduplication registry.

See "Changing the MSDP storage server name or storage path" on page 284.

Warning: Only follow these procedures if you are reconfiguring your storage server and storage paths.

The procedure differs on UNIX and on Windows.

To reset the MSDP registry file on UNIX and Linux

- Enter the following commands on the storage server to reset the deduplication registry file:

```
rm /etc/pdregistry.cfg
cp -f /usr/openv/pdde/pdconfigure/cfg/userconfigs/pdregistry.cfg
 /etc/pdregistry.cfg
```

To reset the MSDP registry on Windows

- Delete the contents of the following keys in the Windows registry:
  - `HKLM\SOFTWARE\Symantec\PureDisk\Agent\ConfigFilePath`
  - `HKLM\SOFTWARE\Symantec\PureDisk\Agent\EtcPath`

Warning: Editing the Windows registry may cause unforeseen results.

About protecting the MSDP catalog

To increase availability, NetBackup provides a two-tier approach to protect the MSDP catalog, as follows:

Daily shadow copies	NetBackup automatically creates copies of the MSDP catalog. See "About the MSDP shadow catalog" on page 221.
Catalog backup policy	Veritas provides a utility that you can use to configure a NetBackup policy that backs up the MSDP catalog. See "About the MSDP catalog backup policy" on page 222.

See "About recovering the MSDP catalog" on page 318.

About the MSDP shadow catalog

The NetBackup Deduplication Manager automatically creates a *shadow copy* of the catalog daily. The Deduplication Manager also builds a transaction log for each shadow copy. If NetBackup detects corruption in the MSDP catalog, the Deduplication Manager restores the catalog automatically from the most recent shadow copy. That restore process also plays the transaction log so that the recovered MSDP catalog is current.

By default, the NetBackup Deduplication Manager stores the shadow copies on the same volume as the catalog itself. Veritas recommends that you store the shadow copies on a different volume.

Warning: You can change the path only during initial MSDP configuration only. If you change it after MSDP backups exist, data loss may occur.

See "Changing the MSDP shadow catalog path" on page 223.

The NetBackup Deduplication Manager creates a shadow copy at 0340 hours daily, host time. To change the schedule, you must change the scheduler definition file.

See "Changing the MSDP shadow catalog schedule" on page 224.

By default, the NetBackup Deduplication Manager keeps five shadow copies of the catalog. You can change the number of copies.

See "Changing the number of MSDP catalog shadow copies" on page 225.

About the MSDP catalog backup policy

Veritas recommends that you protect the MSDP catalog by backing it up. (A NetBackup catalog backup does not include the MSDP catalog.) The NetBackup Deduplication Catalog Policy Administration and Catalog Disaster Recovery utility (the `drcontrol` utility) configures a backup policy for the MSDP catalog. The policy also includes other important MSDP configuration information.

The MSDP catalog backups provide the second tier of catalog protection. The catalog backups are available if the shadow copies are not available or corrupt.

The following are the attributes for the catalog backup policy that the `drcontrol` utility creates:

Schedule	Weekly **Full Backup** and daily **Differential Incremental Backup**.
Backup window	6:00 A.M. to 6:00 P.M.
Retention	2 weeks
Backup selection	The following are the default catalog paths. UNIX: */database_path*/databases/catalogshadow */storage_path*/etc */storage_path*/var /usr/openv/lib/ost-plugins/pd.conf /usr/openv/lib/ost-plugins/mtstrm.conf */database_path*/databases/spa */database_path*/databases/datacheck Windows: *database_path*\databases\catalogshadow *storage_path*\etc *storage_path*\var *install_path*\Veritas\NetBackup\bin\ost-plugins\pd.conf *install_path*\Veritas\NetBackup\bin\ost-plugins\mtstrm.conf *database_path*\databases\spa *database_path*\databases\datacheck By default, NetBackup uses the same path for the storage and the catalog; the *database_path* and the *storage_path* are the same. If you configure a separate path for the deduplication database, the paths are different. Regardless, the `drcontrol` utility captures the correct paths for the catalog backup selections.

You should consider the following items carefully before you configure an MSDP catalog backup:

- Do not use the **Media Server Deduplication Pool** as the destination for the catalog backups. Recovery of the MSDP catalog from its **Media Server Deduplication Pool** is impossible.
- Use a storage unit that is attached to a NetBackup host other than the MSDP storage server.
- Use a separate MSDP catalog backup policy for each MSDP storage server. The `drcontrol` utility does not verify that the backup selections are the same for multiple storage servers. If the backup policy includes more than one MSDP storage server, the backup selection is the union of the backup selections for each host.
- You cannot use one policy to protect MSDP storage servers on both UNIX hosts and Windows hosts.
  UNIX MSDP storage servers require a Standard backup policy and Windows MSDP storage servers require an MS-Windows policy.

See "Configuring an MSDP catalog backup" on page 226.

See "Updating an MSDP catalog backup policy" on page 230.

Changing the MSDP shadow catalog path

You can change the location of the catalog shadow copies. Veritas recommends that you store the copies on a different volume than both the *storage_path* and the *database_path*. (If you configured a separate path for the deduplication database, the paths are different.)

NetBackup stores the MSDP catalog shadow copies in the following location:

UNIX: */database_path*/databases/catalogshadow

Windows: *database_path*\databases\catalogshadow

Warning: You can change the shadow catalog path during initial MSDP configuration only. If you change it after MSDP backups exist, data loss may occur.

See "About protecting the MSDP catalog" on page 221.

To change the MSDP catalog shadow path

1. Open the following file in a text editor:

   UNIX: `/storage_path/etc/puredisk/spa.cfg`

   Windows: `storage_path\etc\puredisk\spa.cfg`

2. Find the `CatalogShadowPath` parameter and change the value to the wanted path.

   The volume must be mounted and available.

3. After your changes, save the file.

4. Restart the NetBackup Deduplication Manager (`spad`).

5. Create the shadow catalog directories by invoking the following command on the MSDP storage server:

   UNIX: `/usr/openv/pdde/pdcr/bin/cacontrol --catalog backup all`

   Windows: `install_path\Veritas\pdde\cacontrol --catalog backup all`

6. If an MSDP catalog backup policy exists, update the policy with the new shadow catalog directories. To do so, invoke the following command on the MSDP storage server:

   UNIX: `/usr/openv/pdde/pdcr/bin/drcontrol --update_policy --policy policy_name`

   Windows: `install_path\Veritas\pdde\drcontrol --update_policy --policy policy_name`

Changing the MSDP shadow catalog schedule

NetBackup automatically creates a copy of the MSDP catalog at 0340 hours daily, host time. You can change the default schedule.

See “About protecting the MSDP catalog” on page 221.

To change the MSDP shadow catalog schedule

1. Open the following file in a text editor:

   UNIX: `/database_path/databases/spa/database/scheduler/5`

   Windows: `database_path\databases\spa\database\scheduler\5`

   By default, NetBackup uses the same path for the storage and the catalog; the *database_path* and the *storage_path* are the same. If you configure a separate path for the deduplication database, the paths are different.

   The contents of the file are similar to the following line. The second section of the line (`40 3 * * *`) configures the schedule.

   ```
   CatalogBackup|40 3 * * *|21600|32400|
   ```

2. Edit the second section of the file (`40 3 * * *`). The schedule section conforms to the UNIX `crontab` file convention, as follows:

   ```
   40 3 * * *
   ┬  ┬ ┬ ┬ ┬
   │  │ │ │ │
   │  │ │ │ │
   │  │ │ │ └──── Day of week (0 - 7, Sunday is both 0 and 7, or use
   │  │ │ │       sun, mon, tue, wed, thu, fri, sat; asterisk (*) is
   │  │ │ │       every day)
   │  │ │ └─────────── Month (1 - 12; asterisk (*) is every month)
   │  │ └──────────────── Day of month (1 - 31; asterisk (*) is every
   │  │                   day of the month)
   │  └────────────────────── Hour (0 - 23; asterisk (*) is every hour)
   └──────────────────────────── Minute (0 - 59; asterisk (*) is every
                                 minute of the hour)
   ```

3. After your changes, save the file.

4. Restart the NetBackup Deduplication Manager (`spad`).

Changing the number of MSDP catalog shadow copies

NetBackup keeps five shadow copies of the MSDP catalog. You can change the number of copies.

See "About protecting the MSDP catalog" on page 221.

To change the number of MSDP catalog shadow copies

1. Open the following file in a text editor:

   UNIX: `/storage_path/etc/puredisk/spa.cfg`

   Windows: `storage_path\etc\puredisk\spa.cfg`

2. Find the `CatalogBackupVersions` parameter and change the value to the wanted number of shadow copies. The valid values are 1 to 256, inclusive.
3. After your changes, save the file.
4. Restart the NetBackup Deduplication Manager (`spad`).

Configuring an MSDP catalog backup

Use the following procedure to configure a backup policy for the NetBackup MSDP catalog.

See "About protecting the MSDP data" on page 40.

See "Troubleshooting MSDP catalog backup" on page 369.

To configure an MSDP catalog backup

1. Verify that the MSDP storage server host (that is, the media server) is an additional server for the NetBackup master server. See **NetBackup Management > Host Properties > *masterserver_name* > Servers > Additional Servers** in the NetBackup Administration Console.

   If the storage server is not in the **Additional Servers** list, add the MSDP storage server host to the **Additional Servers** list. The host *must* be in the **Additional Servers** list and *cannot* be in the **Media Servers** list.

2. On the MSDP storage server, invoke the `drcontrol` utility and use the appropriate options for your needs. The following is the syntax for the utility:

   Windows: `install_path\Veritas\pdde\drcontrol --new_policy --residence residence [--policy policy_name] [--client host_name] [--hardware machine_type] [--OS operating_system] [--NB_install_dir install_directory]`

   UNIX: `/usr/openv/pdde/pdcr/bin/drcontrol --new_policy --residence residence [--policy policy_name] [--disk_pool disk_pool_name] [--client host_name] [--hardware machine_type] [--OS operating_system]`

   Descriptions of the options are available in another topic. Note: To ensure that NetBackup activates the policy, you must specify the `--residence residence` option.

   See "MSDP drcontrol options" on page 227.

   The utility creates a log file and displays its path in the command output.

   See "NetBackup MSDP log files" on page 347.

MSDP drcontrol options

The `drcontrol` utility resides in the following directories, depending on host type:

- UNIX: `/usr/openv/pdde/pdcr/bin`
- Windows: `install_path\Veritas\pdde`

The `drcontrol` utility creates a log file.

See "NetBackup MSDP log files" on page 347.

Table 5-37 describes the options for creating and updating an MSDP catalog backup policy.

Table 5-37 MSDP `drcontrol` options for catalog backup and recovery

Option	Description
`--auto_recover_DR`	Recover the MSDP catalog from the most recent backup image. This option automatically recovers the catalog and performs all of the actions necessary to return MSDP to full functionality. This option requires the `--policy` *`policy_name`* option. To recover the catalog from a backup other than the most recent, contact your Veritas Support representative.
`--client` *`host_name`*	The client to back up (that is, the host name of the MSDP storage server). Default: the value that `bpgetconfig CLIENT_NAME` returns.
`--cleanup`	Remove all of the old MSDP catalog directories during the catalog recovery process. Those directories are renamed during the recovery.
`--delete_old_files_for_cloud_catalyst`	Deletes the existing deduplication catalog files before restoring them from the last backup in the `recover_last_image` step. Used for a cloud media server after the file system has been recovered in the `recover_last_cloud_catalyst_image` step.
`--disk_pool`	In a NetBackup CloudCatalyst recovery scenario, you must specify the disk pool name that is configured for the cloud storage server. This option is required for `auto_recover_DR` when the disk pool name cannot be determined from the host name. For example, for a cloud storage server configured for as a CloudCatalyst.
`--hardware` *`machine_type`*	The hardware type or the computer type for the host. Spaces are not allowed. If the string contains special characters, enclose it in double quotation marks ("). Default: Unknown.
`--initialize_DR`	Performs the following actions to prepare for MSDP catalog recovery: ■ Verifies that the most recent catalog backup is valid. ■ Stops the deduplication services. ■ Moves the existing catalog files so that they are empty for the recovery.
`--list_files`	List the files in the most recent MSDP catalog backup. This option requires the `--policy` *`policy_name`* option.

Table 5-37 MSDP `drcontrol` options for catalog backup and recovery *(continued)*

Option	Description
`--log_file` *pathname*	The pathname for the log file that the `drcontrol` utility creates. By default, the utility writes log files to */storage_path*`/log/drcontrol/`.
`--NB_install_dir` *install_directory*	Windows only. Required option if NetBackup was installed in a location other than the default (`C:\Program Files\Veritas`). If the string contains spaces or special characters, enclose it in double quotation marks ("). Do not use a trailing backslash in the *install_directory* string.
`--new_policy`	Create a new policy to protect the deduplication catalog on this host. If a policy with the given name exists already, the command fails. **Note:** To ensure that NetBackup activates the policy, you must specify the `--residence` *residence* option.
`--OS` *operating_system*	The operating system for the host. Spaces are not allowed. If the string contains special characters, enclose it in double quotation marks ("). Default: `UNIX/Linux` or `MS-Windows`.
`--policy` *policy_name*	The name for the backup policy. Required with `--auto_recover_DR` and `--update_policy`; optional with `--new_policy`. Default: `Dedupe_Catalog_`*shorthostname*
`--print_space_required`	Display an estimate of the percentage of file system space that is required to recover the MSDP catalog.
`--recover_last_cloud_catalyst_image`	Use `bprestore` to restore the cloud media server-related contents of the last deduplication catalog backup. This requires that disaster recovery be initialized.
`--recover_last_image`	Restore the MSDP catalog from the last set of backup images (that is, the last full plus all subsequent incrementals). The `drcontrol` utility calls the NetBackup `bprestore` command for the restore operation.
`--refresh_shadow_catalog`	Deletes all existing shadow catalog copies and creates a new catalog shadow copy.

Table 5-37 MSDP `drcontrol` options for catalog backup and recovery *(continued)*

Option	Description
`--residence` *residence*	The name of the storage unit on which to store the MSDP catalog backups. Do not use the **Media Server Deduplication Pool** as the destination for the catalog backups. Recovery of the MSDP catalog from its **Media Server Deduplication Pool** is impossible. Veritas recommends that you use a storage unit that is attached to a NetBackup host other than the MSDP storage server.

`--update_policy`	Update a policy, as follows:
	
	■ If the client name (of this media server) is not in the policy's client list, add the client name to the policy's client list.
	■ If you specify the `--OS` or `--hardware` options, replace the values currently in the policy with the new values.
	■ Update the backup selection based on the locations of the MSDP storage directories and configuration files. Therefore, if you modify any of the following, you must use this option to update the catalog backup policy:
	  ■ Any of the following values in the `spa.cfg` file (`section:variable` pairs):
	  ■ `StorageDatabase:CatalogShadowPath`
	  ■ `StorageDatabase:Path`
	  ■ `Paths:Var`
	  ■ The `spa.cfg` or `contentrouter.cfg` locations in the `pdregistry.cfg` file.
	
	This option fails if there is no policy with the given policy name. It also fails if the existing policy type is incompatible with the operating system of the host on which you run the command.
	
	This option requires the `--policy` *policy_name* option.

`--verbose`	Echo all `drcontrol` log statements to stdout.

See "Configuring an MSDP catalog backup" on page 226.

Updating an MSDP catalog backup policy

You can use any NetBackup method to update an MSDP catalog backup policy manually. However, you should use the NetBackup Deduplication Catalog Policy

Administration and Catalog Disaster Recovery (`drcontrol`) under the following circumstances:

- To add the client name of the storage server to the policy's client list.
- To update the `--OS` value.
- To update the `--hardware` value.
- To update the backup selection if you modified any of the following configuration values:
  - Any of the following values in the `spa.cfg` file (`section:variable` pairs):
    - `StorageDatabase:CatalogShadowPath`
    - `StorageDatabase:Path`
    - `Paths:Var`
  - The `spa.cfg` or `contentrouter.cfg` locations in the `pdregistry.cfg` file.

See "About protecting the MSDP data" on page 40.

See "Troubleshooting MSDP catalog backup" on page 369.

To update an MSDP catalog backup

- On the MSDP storage server, invoke the `drcontrol` utility and use the appropriate options for your needs. The following is the syntax for an update operation:

  UNIX: `/usr/openv/pdde/pdcr/bin/drcontrol --update_policy --policy` *`policy_name`* `[--client` *`host_name`*`] [--hardware` *`machine_type`*`] [--OS` *`operating_system`*`]`

  Windows: *`install_path`*`\Veritas\pdde\drcontrol --update_policy --policy` *`policy_name`* `[--client` *`host_name`*`] [--hardware` *`machine_type`*`] [--OS` *`operating_system`*`] [--OS` *`operating_system`*`] [--NB_install_dir` *`install_directory`*`]`

  Descriptions of the options are available in another topic.

  See "MSDP drcontrol options" on page 227.

  The utility creates a log file and displays its path in the command output.

  See "NetBackup MSDP log files" on page 347.

About MSDP FIPS compliance

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 https://csrc.nist.gov/projects/cryptographic-module-validation-program.

The NetBackup MSDP is now FIPS validated and can be operated in FIPS mode.

Note: You must run FIPS mode on a new installation of NetBackup 8.1.1.

Enabling MSDP FIPS mode

Ensure that you configure the storage server before you enable the MSDP FIPS mode.

Caution: Enabling MSDP FIPS mode might affect the NetBackup performance on a server with the Solaris operating system.

Enable the FIPS mode for MSDP by running the following commands:

- For UNIX:

  `/usr/openv/pdde/pdag/scripts/set_fips_mode.sh 1`

  For Windows:

  `<install_path>\Veritas\pdde\set_fips_mode.bat 1`

- Restart the NetBackup service on the server and the client.
  - For UNIX:
    - `/usr/openv/netbackup/bin/bp.kill_all`
    - `/usr/openv/netbackup/bin/bp.start_all`
  - For Windows:
    - `<install_path>\NetBackup\bin\bpdown`
    - `<install_path>\NetBackup\bin\bpup`

Warning: Veritas recommends that you do not disable the MSDP FIPS mode once you enable it, for security reasons.

Getting the status of MSDP FIPS mode

To get status of the MSDP FIPS mode, enter the following commands:

For UNIX:

```
/usr/openv/pdde/pdcr/bin/crcontrol --getmode
```

For Windows:

```
<install_path>\Veritas\pdde\crcontrol.exe --getmode
```

Other things to note:

- FIPS must be enabled on all the NetBackup components to establish a connection. When the FIPS mode is not enabled, communication can occur between the NetBackup clients and the servers that have earlier, supported NetBackup versions.
- The MSDP FIPS mode does not support NetBackup CloudCatalyst.

Chapter 6

Configuring deduplication to the cloud with NetBackup CloudCatalyst

This chapter includes the following topics:

- Using NetBackup CloudCatalyst to upload deduplicated data to the cloud
- CloudCatalyst requirements and limitations
- Configuring a Linux media server as a CloudCatalyst storage server
- Configuring a CloudCatalyst storage server for deduplication to the cloud
- About the CloudCatalyst esfs.json configuration file
- About the CloudCatalyst cache
- Differences between KMS and MSDP encryption for CloudCatalyst configurations
- Controlling data traffic to the cloud when using CloudCatalyst
- Configuring push or pull optimized duplication for CloudCatalyst
- Decommissioning CloudCatalyst cloud storage
- NetBackup CloudCatalyst workflow processes
- Disaster Recovery for CloudCatalyst

Using NetBackup CloudCatalyst to upload deduplicated data to the cloud

NetBackup CloudCatalyst uses MSDP deduplication technology to upload deduplicated data to the cloud. The data is uploaded by a CloudCatalyst storage server, which first stores data in a local cache before uploading it to cloud storage. This cloud storage server is a dedicated host that can be either a NetBackup appliance or a media server configured for NetBackup CloudCatalyst.

The following topics describe scenarios that use NetBackup CloudCatalyst:

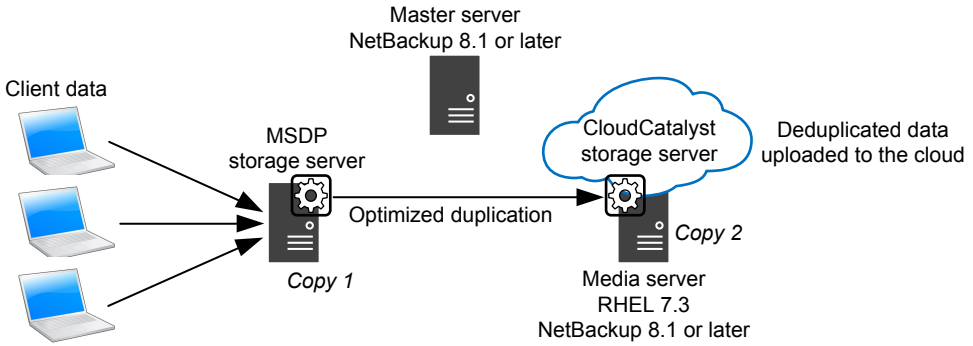
- See "Optimized duplication is used to copy data from an MSDP storage server to a CloudCatalyst storage server (preferred use case)" on page 235.
  This is the preferred use case because it uses the CloudCatalyst storage server as a target for secondary copies. These copies usually have a longer retention and are uploaded to the cloud.
- See "Backups go directly to a CloudCatalyst storage server" on page 237.
  While this configuration is supported, it is not the preferred use case. In this use case, the CloudCatalyst storage server is required to back up, deduplicate, and upload the data to cloud storage.

Optimized duplication is used to copy data from an MSDP storage server to a CloudCatalyst storage server (preferred use case)

This is the preferred CloudCatalyst use case. In this scenario, the NetBackup environment contains two media servers: one is an MSDP storage server and one is a CloudCatalyst storage server.

- First, client data is backed up to the MSDP storage server, which is used for short-term data retention. In subsequent backups, the data is deduplicated. (See Figure 6-1.)
- A storage lifecycle policy then copies the data to a CloudCatalyst storage server using optimized duplication. Data is uploaded from the CloudCatalyst local cache to the cloud when an MSDP container file is full. This occurs soon after the backup or duplication job begins, but not immediately.
  The cloud storage is used for long-term data retention. Deduplication makes it possible for subsequent jobs to transfer substantially less data to the cloud, depending on the deduplication rate.

Figure 6-1 Flow of data from an MSDP storage server to a CloudCatalyst storage server



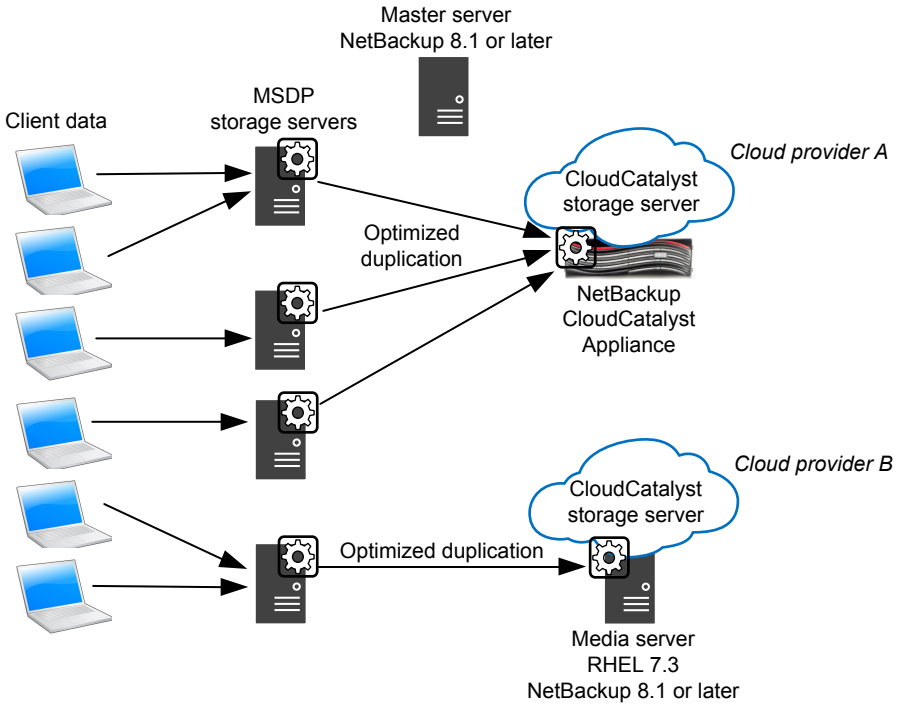
This use case is preferred to backing up directly to a CloudCatalyst storage server. (See "Backups go directly to a CloudCatalyst storage server" on page 237.)

MSDP storage servers fan-in to a single CloudCatalyst storage server

Multiple MSDP storage servers in a NetBackup domain can use a single CloudCatalyst storage server, as shown in Figure 6-2.

Figure 6-2 also shows that multiple CloudCatalyst storage servers can be included in one NetBackup domain. Separate CloudCatalyst storage servers are required for each cloud provider that is used. One CloudCatalyst storage server can write to only one cloud provider, and to only one cloud bucket.

Figure 6-2 Fan-in MSDP storage servers and multiple CloudCatalyst storage servers



Backups go directly to a CloudCatalyst storage server

In this scenario, the NetBackup environment does not use an MSDP storage server; it contains only a CloudCatalyst storage server. The CloudCatalyst storage server must back up, deduplicate, and upload the data to cloud storage.

This is not the preferred CloudCatalyst use case. This may be a good solution for some users depending on the size of the environment, the desired backup window, and other factors, but Veritas expects that most users will get better results from the preferred use case.

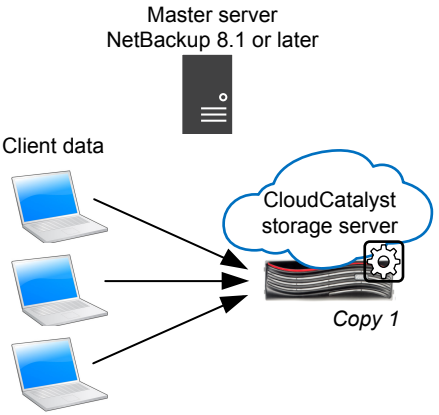
See "Optimized duplication is used to copy data from an MSDP storage server to a CloudCatalyst storage server (preferred use case)" on page 235.

Note the following disadvantages to backing up directly to the CloudCatalyst storage server:

- Since the data needs to be uploaded to the cloud before a job can be considered complete, the job may not complete within the backup window.

- If a restore is required, the data may no longer be in the local cache. If the data has been uploaded to the cloud, the restore may be slow and expensive.

Figure 6-3 Flow of data directly to a CloudCatalyst storage server



CloudCatalyst requirements and limitations

The CloudCatalyst storage server is a dedicated media server for MSDP deduplicated cloud storage. The media server must be either a NetBackup appliance or a Linux media server, as described in Table 6-1.

Table 6-1 Types of media servers that can be used as CloudCatalyst storage servers

Host	Version
NetBackup appliance	Veritas NetBackup CloudCatalyst Appliance
NetBackup media server	Red Hat Enterprise Linux, 7.3 or later NetBackup 8.1 or later See "Configuring a Linux media server as a CloudCatalyst storage server" on page 239.

Limitations

NetBackup CloudCatalyst recognizes nearly all other MSDP features and capabilities.

See the NetBackup compatibility lists for updated information on supported cloud vendors and feature support:

http://www.netbackup.com/compatibility

The following are current exclusions or limitations:

- Support limitations as listed in the *NetBackup Cloud Administrator's Guide*: http://www.veritas.com/docs/DOC5332
- The NetBackup media servers that you use as CloudCatalyst storage servers must be the same NetBackup version as the master server.
- Load balancing for CloudCatalyst storage servers or CloudCatalyst appliances is supported. See the following topic for configuration considerations.
  See "Configuring push or pull optimized duplication for CloudCatalyst" on page 256.
- OpsCenter cannot report on the data that CloudCatalyst storage servers upload to the cloud. However, if the NetBackup environment also contains a cloud storage server that is not CloudCatalyst-enabled, that storage server can be used to view the data for both storage servers.
- A single media server cannot be both an MSDP storage server and a CloudCatalyst storage server.
- A CloudCatalyst storage server is not supported for Auto Image Replication (A.I.R.) as either the source or the target.
- NetBackup Client Direct deduplication is supported in a CloudCatalyst duplication to cloud scenario. However, Client Direct deduplication is not supported in a scenario where the backup is uploaded directly to the cloud and no duplication is configured.

Configuring a Linux media server as a CloudCatalyst storage server

The CloudCatalyst storage server is a dedicated media server for MSDP deduplicated cloud storage.

The media server that is configured as the CloudCatalyst storage server must be one of the following host types:

- NetBackup CloudCatalyst Appliance
  Documentation for the CloudCatalyst Appliance can be found at the following website:
  https://www.veritas.com/content/support/en_US/Appliances.html
- A Linux media server with specifications similar to the NetBackup CloudCatalyst Appliance. The following section lists the software and hardware requirements for this media server.

Specifications for a Linux media server

The dedicated media server that will be configured as a CloudCatalyst storage server should meet or exceed the specifications of the NetBackup 5240 Appliance, configuration G. The requirements for this MSDP media server are greater than the minimum MSDP server requirements:

See "About MSDP server requirements" on page 25.

In addition to the technical requirements that are listed in Table 6-2, the media server must also contain the following:

- Red Hat Enterprise Linux 7.3 or later.
- NetBackup 8.1 or later.
- A minimum of 4 TB available for the CloudCatalyst local cache directory.
  See "About the CloudCatalyst cache" on page 252.

The technical specifications for the NetBackup 5240 Appliance are listed in the appendix of the *NetBackup 5240 Appliance Product Description*. Table 6-2 lists a subset of minimum requirements for the media server.

Table 6-2 NetBackup 5240 Appliance technical specifications

Technical Specification	NetBackup 5240 Appliance
Processor	Two Intel® Xenon® E5-2630 v3 2.40 GHz processors
CPU speed	2.40 GHz
Cores	16 (8 per processor)
System memory	192 GB DDR4 RDIMM
Usable MSDP storage capacity	14 TB with 1 GB RAID 6 cache **Note:** If a Linux media server (non-appliance) is used, it must have a minimum of 4 TB available for the CloudCatalyst local cache directory. See "About the CloudCatalyst cache" on page 252.
10 Gb Ethernet ports	5

Configuring a CloudCatalyst storage server for deduplication to the cloud

The configuration of deduplication to the cloud differs, depending on the type of host that is used for the CloudCatalyst storage server.

- See the following procedure if you are using a NetBackup CloudCatalyst Appliance:
  See "How to configure a NetBackup CloudCatalyst Appliance" on page 241.
- See the following procedure if you are using a Linux media server (non-appliance):
  See "How to configure a Linux media server as a CloudCatalyst storage server" on page 244.

How to configure a NetBackup CloudCatalyst Appliance

Use the following procedure to configure a NetBackup CloudCatalyst Appliance as a CloudCatalyst storage server.

This procedure assumes that the preferred use case is being configured. The preferred use case is described in the following topic:

See "Optimized duplication is used to copy data from an MSDP storage server to a CloudCatalyst storage server (preferred use case)" on page 235.

Table 6-3 Configuration steps for a NetBackup CloudCatalyst Appliance

Step	Task	Where to configure	Procedure
Step 1	Configure an MSDP storage server (source)	One or more media servers	A NetBackup environment may contain one or more media servers that serve as source MSDP storage servers for one or more CloudCatalyst appliances. See "About MSDP optimized duplication within the same domain" on page 135. See "About the media servers for MSDP optimized duplication within the same domain" on page 138.
Step 2	Create an account with a cloud service provider	Cloud service provider	Make sure that you have an account with a cloud service provider and that you know the user name and password.

Table 6-3 Configuration steps for a NetBackup CloudCatalyst Appliance *(continued)*

Step	Task	Where to configure	Procedure

Step 3	Configure KMS (optional)	Master server	NetBackup CloudCatalyst supports NetBackup Key Management Service (KMS) encryption.
			
			To encrypt backups, configure and start the Key Management Service (KMS).
			
			Run the following command on the master server to configure KMS:
			
			`/usr/openv/netbackup/bin/nbkms -createemptydb`
			
			As part of the setup, enter:
			
			■ A passphrase and an ID for the host master key (HMK).
			■ A passphrase and ID for the key protection key (KPK).
			
			Run the following command on the master server to start KMS:
			
			`/usr/openv/netbackup/bin/nbkms`
			
			Note: MSDP encryption may be used instead of KMS. (Do not use KMS and MSDP encryption together.)
			
			See "Configuring encryption for MSDP backups" on page 126.
			
			See "Differences between KMS and MSDP encryption for CloudCatalyst configurations" on page 254.

Step 4	Add the appliance name to the master server	Master server	Generate a set of credentials for the appliance. You must know the proposed host name of the appliance. The same name is used in the NetBackup Appliance Shell Menu during the initial configuration wizard. `/usr/openv/netbackup/bin/bpnbat -addmachine` *`appliance_name admin_password`* See the *NetBackup 52xx Appliance Initial Configuration Guide* for appliance setup information.
Step 5	Configure the appliance	Appliance	Perform the initial configuration on the appliance. When the script calls for a host name, use the host name for which credentials were generated.

Table 6-3 Configuration steps for a NetBackup CloudCatalyst Appliance *(continued)*

Step	Task	Where to configure	Procedure
Step 6	Configure an appliance as a CloudCatalyst storage server (target)	Appliance	A CloudCatalyst Appliance is the target for the optimized duplication. It is a dedicated appliance for cloud storage. A NetBackup environment may contain one or more CloudCatalyst appliances that serve as MSDP cloud storage servers. There should be one appliance for each different cloud service provider that is used in the environment. From the main shell menu, launch the Appliance Cloud Storage Server Configuration Wizard. In this wizard, select whether KMS is used to encrypt backups. As part of this wizard, a disk pool and a storage unit are configured. Documentation for the CloudCatalyst Appliance can be found at the following website: https://www.veritas.com/content/support/en_US/Appliances.html
Step 7	Configure the target to allow load balancing for push optimized duplications (optional)	Appliance	To configure load balancing for push optimized duplications, the CloudCatalyst Appliance must allow access from the source media server. **Note:** The push configuration is recommended if using load balancing for CloudCatalyst. See the following topic for configuration considerations. See "Configuring push or pull optimized duplication for CloudCatalyst" on page 256.
Step 8	Configure a storage lifecycle policy	Master server	See "Configuring a storage lifecycle policy for NetBackup CloudCatalyst" on page 247. **Note:** The backup and duplication jobs can also be run manually from the **NetBackup Administration Console** or by using the `bpduplicate` command.
Step 9	Configure a backup policy	Master server	Create a backup policy that uses the SLP. In the **Policy storage** field of the policy **Attributes** tab, select the SLP. See "About MSDP backup policy configuration" on page 186. See "Creating a backup policy" on page 187.

Table 6-3 Configuration steps for a NetBackup CloudCatalyst Appliance *(continued)*

Step	Task	Where to configure	Procedure
Step 10	Protect the MSDP data and catalog	Media server	■ Create an MSDP catalog backup policy for every MSDP storage server and CloudCatalyst storage server in the environment. See "About protecting the MSDP catalog" on page 221. See "Configuring an MSDP catalog backup" on page 226. **Note:** After the MSDP catalog backup policy is created, it is inactive. Assign a storage unit to it and then make it active by setting the **Go into effect at** option on the Attributes tab. ■ Save a configuration file for every MSDP storage server and CloudCatalyst storage server in the environment. See "About saving the MSDP storage server configuration" on page 215.

How to configure a Linux media server as a CloudCatalyst storage server

Use the following procedure if you are using a Linux media server (non-appliance) as a CloudCatalyst storage server.

This procedure assumes that the preferred use case is being configured. The preferred use case is described in the following topic:

See "Optimized duplication is used to copy data from an MSDP storage server to a CloudCatalyst storage server (preferred use case)" on page 235.

Table 6-4 Configuration steps for a media server (non-appliance)

Step	Task	Where to configure	Procedure
Step 1	Configure an MSDP storage server (source)	One or more media servers	A NetBackup environment may contain one or more media servers that serve as source MSDP storage servers for CloudCatalyst storage servers. See "About MSDP optimized duplication within the same domain" on page 135. See "About the media servers for MSDP optimized duplication within the same domain" on page 138.

Table 6-4 Configuration steps for a media server (non-appliance) *(continued)*

Step	Task	Where to configure	Procedure
Step 2	Create an account with a cloud service provider	Cloud service provider	Make sure that you have an account with a cloud service provider and that you know the user name and password.
Step 3	Deploy host name-based certificates	Master server	Deploy a host name-based security certificate for the media server that will be configured as the CloudCatalyst storage server. **1** `/usr/openv/netbackup/bin/admincmd/bpnbaz -ProvisionCert host_name` **2** Restart the services on the media server after generating a certificate.
Step 4	Configure a CloudCatalyst storage server (target)	Media server	A CloudCatalyst storage server is the target for the optimized duplication. It is a dedicated media server for cloud storage. ■ The administrator configures a local cache directory as part of configuring a CloudCatalyst storage server. The minimum size for this directory is 4 TB, however, an environment may see benefits from a larger local cache directory. See "About the CloudCatalyst cache" on page 252. ■ NetBackup Key Management Service (KMS) encryption can be set up as part of the wizard. See "Configuring a CloudCatalyst storage server as the target for the deduplications from MSDP storage servers" on page 246. See "Differences between KMS and MSDP encryption for CloudCatalyst configurations" on page 254. ■ A NetBackup environment may contain one or more media servers that serve as CloudCatalyst storage servers. There should be one CloudCatalyst storage server for each different cloud service provider that is used in the environment.
Step 5	Ensure that a common media server is configured to allow optimized duplication	Media server	If the CloudCatalyst media server was added as a load balancing media server during the MSDP storage server wizard (Step 1), pull optimized duplication is configured. See the following topic for configuration considerations: See "Configuring push or pull optimized duplication for CloudCatalyst" on page 256.

Table 6-4 Configuration steps for a media server (non-appliance) *(continued)*

Step	Task	Where to configure	Procedure
Step 6	Protect the MSDP data and catalog	Media server	■ Create an MSDP catalog backup policy for every MSDP storage server and CloudCatalyst storage server in the environment. See "About protecting the MSDP catalog" on page 221. See "Configuring an MSDP catalog backup" on page 226. **Note:** After the MSDP catalog backup policy is created, it is inactive. Assign a storage unit to it and then make it active by setting the **Go into effect at** option on the **Attributes** tab. ■ Save a configuration file for every MSDP storage server and CloudCatalyst storage server in the environment. See "About saving the MSDP storage server configuration" on page 215.
Step 7	Configure a storage lifecycle policy	Master server	See "Configuring a storage lifecycle policy for NetBackup CloudCatalyst" on page 247. The backup and duplication jobs can also be run manually from the **NetBackup Administration Console** or by using the `bpduplicate` command.
Step 8	Configure a backup policy	Master server	Create a backup policy that uses the SLP. In the **Policy storage** field of the policy **Attributes** tab, select the SLP. See "About MSDP backup policy configuration" on page 186. See "Creating a backup policy" on page 187.

Configuring a CloudCatalyst storage server as the target for the deduplications from MSDP storage servers

This media server is the target for the backups from the MSDP storage server. After configuration, this is the CloudCatalyst storage server that uploads the deduplicated data to the cloud.

Configuring a CloudCatalyst storage server as the target for the MSDP storage servers

1. On the master server, in the **NetBackup Administration Console,** click **Configure Cloud Storage Servers** to launch the Cloud Storage Server Configuration Wizard.
2. In the wizard, enable the option: **Enable NetBackup CloudCatalyst**.

3 Enter a path to use as the **Local cache directory**. Deduplicated data is written to this directory on the cloud storage server before it is uploaded to the cloud.

Notes:

- The minimum size for the local cache directory is 4 TB, however, an environment may see benefits from a larger local cache directory.
  See "About the CloudCatalyst cache" on page 252.
- This path should be to a file system which is dedicated for CloudCatalyst cache use. Inaccurate cache eviction occurs if the path shares any storage with other data or applications.
- NetBackup manages the files in the local cache directory. Users should not manually delete files in this directory.

4 Choose whether to use NetBackup KMS encryption. To use KMS encryption, it must be configured and enabled.

The *NetBackup Cloud Administrator's Guide* contains information about all of the available options and switches which are common to non-CloudCatalyst and CloudCatalyst environments.

http://www.veritas.com/docs/DOC5332

5 As part of the storage server wizard, a disk pool and a storage unit are configured.

When creating the storage lifecycle policy, this storage unit name is used in the **Storage unit** field for the **Duplication** operation.

See "Configuring a storage lifecycle policy for NetBackup CloudCatalyst" on page 247.

Configuring a storage lifecycle policy for NetBackup CloudCatalyst

A storage lifecycle policy (SLP) manages the backup jobs and the duplication jobs from a MSDP storage server to a MSDP cloud storage server. The backup and duplication jobs can also be run manually from the **NetBackup Administration Console** or by using the `bpduplicate` command.

This procedure assumes that the preferred use case is being configured. The preferred use case is described in the following topic:

See "Optimized duplication is used to copy data from an MSDP storage server to a CloudCatalyst storage server (preferred use case)" on page 235.

If an SLP is used, it must contain a **Backup** operation and a child **Duplication** operation.

Configuring a storage lifecycle policy for deduplication to the cloud

1. The first operation must be a **Backup** operation. In the **Storage unit** field, select the storage unit that was created for the MSDP storage server.
2. Create a second operation that is a child of the **Backup** operation. The second operation must be a **Duplication** operation. In the **Storage unit** field, select the storage unit that was created for the CloudCatalyst storage server.

   See "Configuring a CloudCatalyst storage server as the target for the deduplications from MSDP storage servers" on page 246.

About the CloudCatalyst esfs.json configuration file

The NetBackup CloudCatalyst uses the configuration options that are included in the `esfs.json` file for many operations, including options that determine when data is uploaded to cloud storage or when it is evicted from the local cache. Some of the options are configurable by the NetBackup administrator. The location of the `esfs.json` file depends on the location of the local cache directory.

As part of the Cloud Storage Server Configuration Wizard, the administrator configures a local cache directory. The local cache directory (*`local_cache_dir`* in the following topic) determines the location of other directories which are installed automatically and are critical to CloudCatalyst operations:

- A mount path (`/storage`): *`local_cache_dir`*`/storage`
  The Veritas NetBackup Extendable Storage File System process (`vxesfsd`) runs on the mount path.
- A cache path (`/cache`): *`local_cache_dir`*`/cache/etc/esfs.json`
  This is the location of the `esfs.json` file.

Configuring the options in the esfs.json file

The NetBackup CloudCatalyst configuration options are listed in Table 6-5.

To change the configuration items in the esfs.json configuration

1. Change one or more of the configuration items in the `esfs.json` file. The file is found in the following location:

   `local_cache_dir``/cache/etc/esfs.json`
2. Save and close the file.

3 If `vxesfsd` is running, run the `esfs_reconfig` command, indicating the mount path, as follows:

`/usr/openv/esfs/bin/esfs_reconfig` *`local_cache_dir`*`/storage`

If `esfs.json` is changed while `vxesfsd` is stopped, the changes take effect the next time `vxesfsd` starts.

4 Some items require that you restart `vxesfsd` before the new configuration can take effect.

These items are indicated in Table 6-5.

- Before stopping `vxesfsd`, make sure that no processes are using `vxesfsd`, including the current working directory of any user.
  The NetBackup Deduplication Manager (`spad`) and the NetBackup Deduplication Engine (`spoold`) use `vxesfsd`, so they need to be stopped if either is running.
- Before starting `vxesfsd`, make sure that no data exists in the mount point. If data exists in the mount point, `vxesfsd` fails to restart.

The following topic contains additional information about restarting `vxesfsd`:

See "Restarting the vxesfsd process" on page 381.

Table 6-5 Configuration items in the esfs.json file

Configuration item	Default setting	Description	vxesfsd restart required?
Log			
Path	`\/usr\/openv\/netbackup\/logs`	This setting indicates the directory where logs for the `vxesfsd` process are created. The logs include the following: ■ `esfs_database` ■ `esfs_filesystem` ■ `esfs_monitor` ■ `esfs_storage` ■ `esfs_storagemanager`	Yes
	`\/usr\/openv\/esfs\/logs\/ops`	■ `esfs-config.*` ■ `esfs-run.*`	

Table 6-5 Configuration items in the esfs.json file *(continued)*

Configuration item	Default setting	Description	vxesfsd restart required?
Size	10485760	This value (in kilobytes) controls the maximum size that a single log file is allowed to grow. Once the file reaches that approximate size, the log file is closed and another log file is opened.	No
Level	1	This value determines the logging level and what information is included in the logs: ■ 1: Errors only ■ 2: Warnings and errors ■ 3: All log entries **Note:** The **Global logging level** in the **Host Properties** has no effect on this setting.	Yes
Monitor			
DACDays	30	The Delete After Close Days value determines how long a container file remains in the cache after it is last accessed and then closed. After the specified number of days, `vxesfsd` removes the file from the cache directory only if it has been successfully uploaded to the cloud. This commonly occurs shortly after midnight where the CloudCatalyst storage server is located. Files which have not been successfully uploaded to the cloud are not removed from the cache directory.	No

Table 6-5 Configuration items in the esfs.json file *(continued)*

Configuration item	Default setting	Description	vxesfsd restart required?
HighWatermark	80	This value determines how full the cache partition is allowed to grow before `vxesfsd` begins to evict container files. The value represents the percentage of used space on the cache partition. The oldest files are evicted until the LowWatermark is met. Files that have not been successfully uploaded to the cloud are not removed from the cache directory by the eviction process. If the HighWatermark value is set very low, the cache is nearly cleared. That is, nearly all of the eligible files are evicted. **Note:** The file system on which the cache resides must not contain data from any other applications.	No
LowWatermark	70	This value determines at what point `vxesfsd` stops evicting container files after the HighWatermark triggers eviction. The value represents the percentage of used space on the cache partition.	No
BackupDBTime	12	This value determines how frequently (in hours) the database is backed up. This value is unrelated to the drcontrol policy, if one exists. Veritas recommends that a drcontrol policy is created and used to protect your cloud storage server. Veritas recommends that this value is not changed. **Note:** This is a special database for the cloud storage server, not the NetBackup or MSDP catalog.	No
StorageManager			
IOSize	1048576	This value (in bytes) has been used for internal testing. Veritas recommends that this value is not changed.	No

Table 6-5 Configuration items in the esfs.json file *(continued)*

Configuration item	Default setting	Description	vxesfsd restart required?
UploadThreads	20	This value determines the number of threads available for uploading data to the cloud.	Yes
DownloadThreads	20	This value determines the number of threads available for downloading data from the cloud.	Yes
BackupDBCopies	14	This value determines the maximum number of saved copies of the database that will be created for backup. Veritas recommends that this value is not changed. This value is unrelated to the drcontrol policy, if one exists. Veritas recommends that a drcontrol policy is created and used to protect your cloud storage server. **Note:** This is a special database for the cloud storage server, not the NetBackup or MSDP catalog.	No
FileSystem			
MaxOpenFile	192114	This value determines the maximum number of files that can be open at one time. Veritas recommends that this value is not changed.	Yes
ReadOnly	0	This value indicates whether the files currently stored in the cloud can be modified: ■ 0: The files can be modified. (Default.) ■ 1: The files are read only. This setting is used for disaster recovery and should not be changed under normal usage.	Yes

About the CloudCatalyst cache

The administrator configures a local cache directory as part of configuring a CloudCatalyst storage server. The primary function of the local cache directory (or CloudCatalyst cache) is to allow the CloudCatalyst to continue to deduplicate data,

even if the ingest rate from targeted backup and duplication jobs exceeds the available upload throughput to the destination cloud storage.

For example, if backup and duplication jobs transfer 10 TB of data per hour to the CloudCatalyst storage server, and the CloudCatalyst deduplicates the data at a ratio of 10:1, the 1 TB of deduplicated data may exceed the upload capacity of .7 TB per hour of writes to cloud storage. The cache allows the jobs to continue to send and process the data, assuming that at some point the incoming data rate slows. The CloudCatalyst cache only stores the deduplicated data. Jobs are not marked as complete until all data is uploaded to the cloud.

While a CloudCatalyst cache of 4 TB is recommended, a larger cache has the following benefits:

- For restores:
  If the data exists in the CloudCatalyst cache, it is restored from the cache instead of the cloud. The larger the cache, the more deduplicated objects can reside in the cache.
- For data with poor deduplication rates:
  A larger cache may be required since the poor deduplication ratios require that larger amounts of data be uploaded to the cloud.
- For job windows that experience bursts of activity:
  A larger cache can be helpful if frequent jobs are targeted to the CloudCatalyst storage server within a narrow window of time.

While a larger cache can be beneficial, jobs are not marked as complete until all data is uploaded to the cloud. Data is uploaded from the cache to the cloud when an MSDP container file is full. This occurs soon after the backup or duplication job begins, but not immediately. Deduplication makes it possible for second and subsequent backup jobs to transfer substantially less data to the cloud, depending on the deduplication rate.

See “Optimized duplication is used to copy data from an MSDP storage server to a CloudCatalyst storage server (preferred use case)” on page 235.

For example, 4 TB of cache is expected to manage 1 PB of data in the cloud without issue.

How CloudCatalyst manages the cache

The CloudCatalyst manages the cache based on the configuration settings in the `esfs.json` file. Once the high watermark is reached, data is purged according to the oldest accessed time (the Delete After Close Days setting) to the low watermark level. If the rate of incoming data exceeds the rate where the watermark can be maintained, the jobs begin to fail. Administrators should not manually delete or

purge the managed data in the cache storage unless directed to do so by NetBackup Technical Support.

Differences between KMS and MSDP encryption for CloudCatalyst configurations

If Key Management Service (KMS) encryption is used in a CloudCatalyst configuration, the cloud plug-in encrypts the data before it uploads the data to the cloud. The result is that the file is encrypted over the wire and in the cloud, but not in the local cache.

If MSDP encryption is used, the files are stored in the cache as encrypted, and then uploaded to the cloud in that state. The result is that the file is encrypted in the local cache, over the wire, and in the cloud.

Table 6-6 Where data is encrypted per encryption type

Encryption type	Encrypted in local cache?	Encrypted over the wire to cloud?	Encrypted in cloud?
KMS	No	Yes	Yes
MSDP	Yes	Yes	Yes

If both encryption methods are in use, the already-encrypted file from the cache is encrypted again by the cloud plug-in. This double-encryption can result in a larger file being uploaded to the cloud so using both encryption methods is generally not recommended.

Controlling data traffic to the cloud when using CloudCatalyst

CloudCatalyst offers configuration options to control the transfer rates for uploading and downloading cloud data. Use this topic to enable throttling and/or to change the CloudCatalyst default throttling values.

Note: By default, throttling is not enabled for NetBackup storage servers.

Several settings must be changed in the **NetBackup Administration Console** to configure throttling. Before changing these settings, you must know the values of the throttling-related configuration items in the `esfs.json` file on the CloudCatalyst storage server.

Table 6-7 shows the throttling configuration items and their defaults. The table also shows the value to enter in the **NetBackup Administration Console**, as described in the following procedure.

Table 6-7 Value to use in console when using esfs.json throttling defaults

esfs.json configuration item	Default	Use this value in the NetBackup Administration Console
`UploadThreads`	20	160
`DownloadThreads`	20	

If you change either throttling configuration item, apply the formula shown in Table 6-8 to determine which value to enter in the **NetBackup Administration Console**.

Table 6-8 Value to use in console if changing the esfs.json throttling defaults

esfs.json configuration item	Non-default	Formula to determine the value to use in the NetBackup Administration Console
`UploadThreads`	x	Multiply the sum of the two items by four. x + y = z x 4 = *value for console* For example, if `UploadThreads` is 50 and `DownloadThreads` is 30, use 320 in the console: 50 + 30 = 80 x 4 = 320
`DownloadThreads`	y	

To configure throttling for a CloudCatalyst storage server

1. Determine whether you want to change the throttling configuration items in the `esfs.json` file.

   The remaining steps in this procedure use a throttling value that is based on the `UploadThreads` and `DownloadThreads` configuration items.

   - If you use the defaults for both of these items, enter a value of 160 in the following steps.
   - If you change the default for either of these items, see Table 6-8 to determine the value to enter in the following steps.

2. If you changed the default for either `UploadThreads` or `DownloadThreads`, restart the NetBackup Extendable Storage File System Service (`vxesfsd`).

   See "Restarting the vxesfsd process" on page 381.

3. Change the **Scalable Storage** media server host properties:
   - In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Media Servers**.
   - In the details pane, select the media server that is the CloudCatalyst storage server.
   - On the **Actions** menu, select **Properties**.
   - Select the **Scalable Storage** properties.
   - Set the **Sampling interval** to one or more to enable throttling.
   - Set **Maximum concurrent jobs** to the value as determined in Step 1.
   - Click **Apply** and **OK** to close the dialog.
4. Change the cloud storage server properties:
   - Expand **NetBackup Management > Media and Device Management > Credentials > Storage Servers**.
   - In the details pane, select the CloudCatalyst storage server.
   - On the **Edit** menu, select **Change**.
   - Select the **Properties** tab.
   - Locate the `THR:storage_server` property in the **Property** column.
   - Select the setting in the **Value** column and change it to the value as determined in Step 1.
5. Restart the NetBackup services.

Configuring push or pull optimized duplication for CloudCatalyst

Optimized duplication requires the source storage server and the destination storage server to have at least one media server in common. For example, in a NetBackup CloudCatalyst environment that includes an MSDP media server (the source storage server) and one CloudCatalyst storage server (destination/target), either of these hosts could be the shared media server to perform optimized duplication.

The shared media server requires credentials for both the source storage server and the target storage server. (Credentials are granted in the **Media Servers** tab of the storage server properties for each storage server.) This point is important in determining whether your environment can support a push or a pull operation.

The media server which manages the duplication operation determines whether the operation is a push or a pull operation, as follows:

- If the MSDP media server manages the duplication operation, it is push duplication. The CloudCatalyst storage server must allow access from the MSDP media server. (See Example push configuration: Source media server must be RHEL and NetBackup 8.1 or later.)
  - The CloudCatalyst can allow access only if the MSDP media server is RHEL (any version) and NetBackup 8.1 or later.
    - If the MSDP media server is non-RHEL, it appears as a selection, but upon applying the credential, it fails with an **Add credentials failed** message.
    - If the MSDP media server is non-8.1, it does not appear in the **Media Servers** tab.
  - If the MSDP media server is not RHEL or is not at NetBackup 8.1 or later, a pull operation must be used instead.
- If the CloudCatalyst media server manages the duplication operation, it is pull duplication. The MSDP media server must allow access from the CloudCatalyst media server. (See Example pull configuration: Source media storage server is not RHEL or is pre-8.1.)
  The MSDP media server can be of any supported platform or NetBackup version.

See the considerations that are listed in Table 6-9.

Table 6-9 Considerations for using push or pull optimized duplication for CloudCatalyst

Type of optimized duplication	Advantages and disadvantages
Push	**Advantage:** The NetBackup Disk Manager (`bpdm`) runs on the source media server, which prevents overloading the CloudCatalyst storage server during duplication jobs. The overhead of optimized duplication does not compete with the ESFS resources. This is especially important where multiple MSDP storage servers fan-in to one CloudCatalyst storage server. **Disadvantage:** Requires that the MSDP storage server be of a specific platform and NetBackup version.
Pull	**Advantage:** The MSDP media server can be of any supported platform or NetBackup version. **Disadvantage:** The NetBackup tape manager (`bptm`) may run on the CloudCatalyst media server during backups. NetBackup may inadvertently use the CloudCatalyst storage server for load balancing during backups.

Note about credentials on media servers

There must be at least one media server which has credentials to both the MSDP storage server and the CloudCatalyst storage server for jobs to be successful.

- If there is no media server which has credentials to both storage servers, jobs fail.
- If the common media server is the same host as the source MSDP storage server, it's a push operation. (Example push configuration: Source media server must be RHEL and NetBackup 8.1 or later)
- If the common media server is the same host as the CloudCatalyst storage server, it's a pull operation. (Example pull configuration: Source media storage server is not RHEL or is pre-8.1)
- If the media servers for both have credentials in common, the NetBackup Resource Broker (NBRB) chooses a media server at job time. Some jobs will be push operations and some will be pull operations.

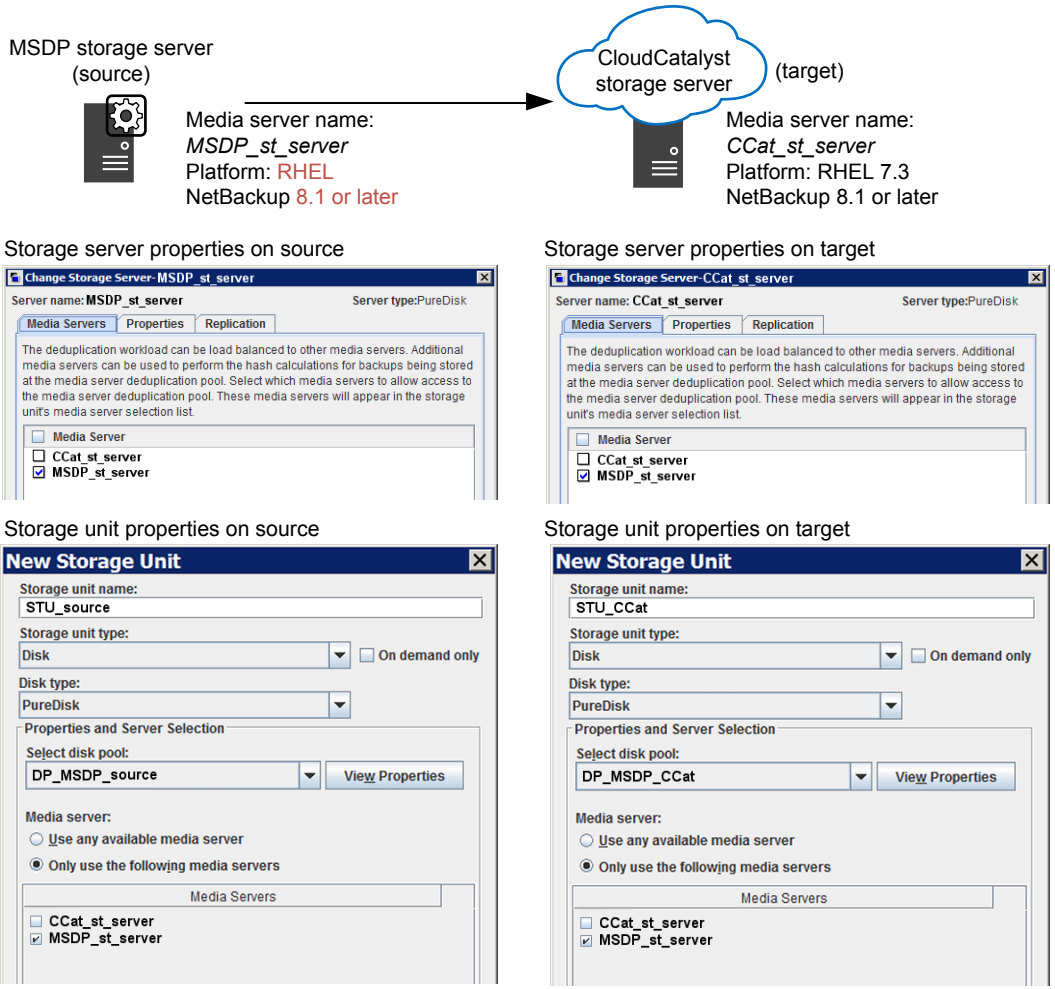
Example push configuration: Source media server must be RHEL and NetBackup 8.1 or later

In Figure 6-4, the source media server (the MSDP storage server) is configured for push duplication to the target. Note that the source is Red Hat Enterprise Linux and has NetBackup 8.1 installed.

Two configuration items allow for push duplication:

- The target (the CloudCatalyst storage server) allows access from the source media server. The credential is granted in the storage server properties of each.
- The storage unit settings on the source and the target specifically point to the source media server. (Enable **Only use the following media servers** and select the source media server.)

Figure 6-4 Push configuration



See the section called “Note about credentials on media servers” on page 258.

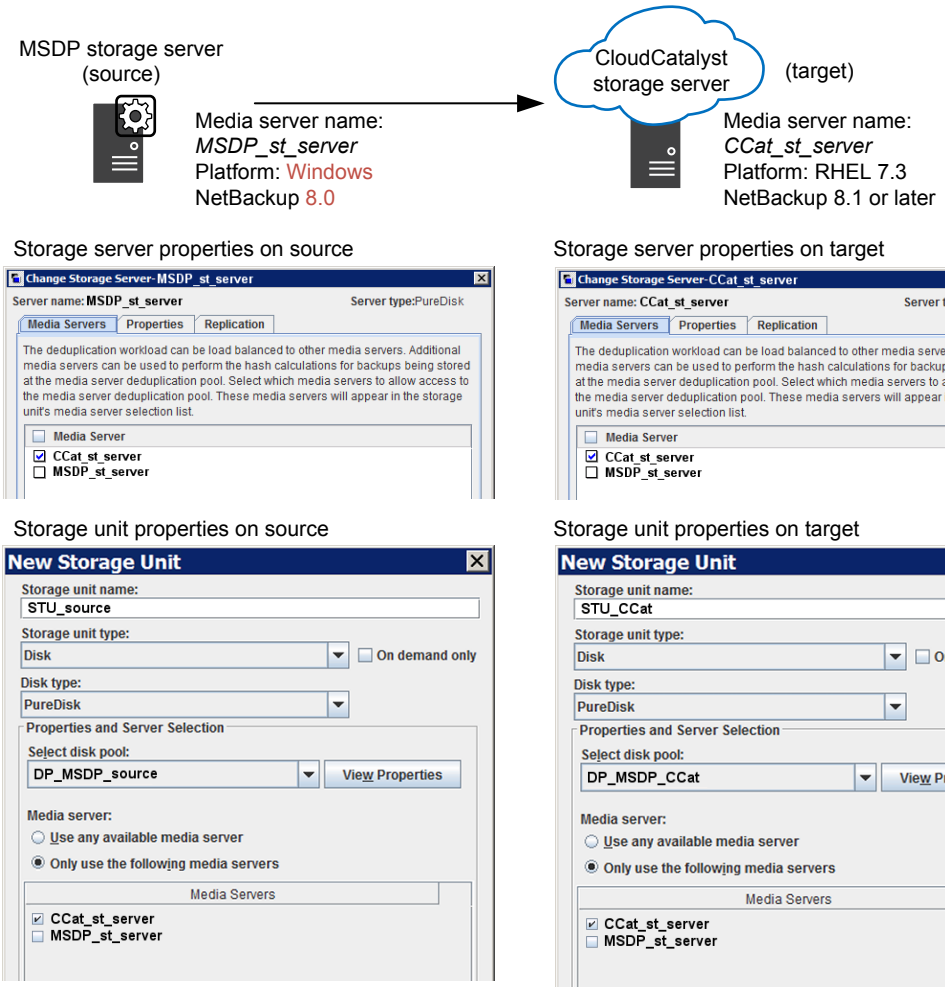
Example pull configuration: Source media storage server is not RHEL or is pre-8.1

In Figure 6-5, the target media server is configured for pull duplication. Note that the source is Windows and has NetBackup 8.0 installed.

Two configuration items allow for pull duplication:

- The source (the MSDP storage server) allows access from the target media server. This is configured in the storage server properties of each.
- The storage unit settings on the source and the target specifically point to the target media server. (Enable **Only use the following media servers** and select the target media server.)

Figure 6-5 Pull configuration



See the section called “Note about credentials on media servers” on page 258.

Decommissioning CloudCatalyst cloud storage

Perform the following procedure before manually deleting any data from the cloud.

To decommission CloudCatalyst cloud storage

1. Delete the storage unit that uses the disk pool.
2. Delete the disk pool.

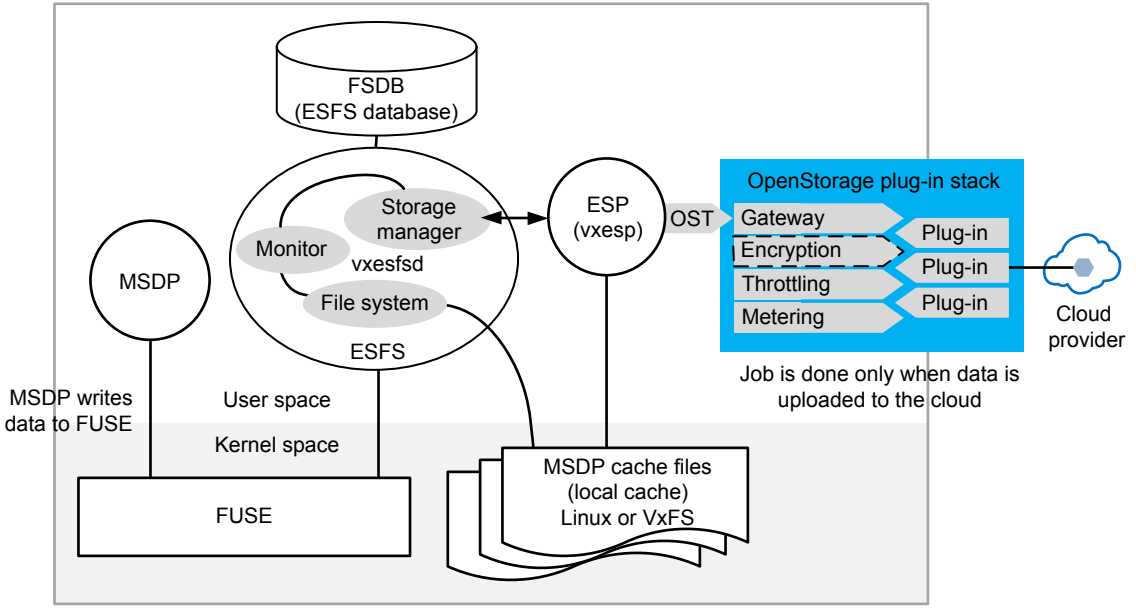
   See "Deleting a Media Server Deduplication Pool" on page 302.
3. Run the `esfs_cleanup.sh` script on the media server to remove all CloudCatalyst-related information from the server.

   `usr/openv/esfs/scripts/esfs_cleanup.sh`
4. Any remaining data on the cloud storage may now be manually removed.

NetBackup CloudCatalyst workflow processes

Figure 6-6 shows the workflow on a CloudCatalyst storage server for uploading data to the cloud.

Figure 6-6 Workflow on a CloudCatalyst storage server



Note that a single CloudCatalyst storage server can only write to one cloud provider and to one bucket within that cloud provider.

Filesystem in Userspace (FUSE)

The Filesystem in Userspace (FUSE) forwards data from MSDP to the File System Database (FSDB).

File System Database (FSDB)

The File System Database (FSDB) tracks and stores metadata about all of the files written to the NetBackup Extendable Storage File System (ESFS).

NetBackup Extendable Storage File System (ESFS)

NetBackup CloudCatalyst uses the NetBackup Extendable Storage File System Service (`vxesfsd`) and its subcomponents to move and manage files in the local cache directory and the cloud.

ESFS uses daemons to perform the following functions in its database:

- Veritas NetBackup Extendable Storage File System Service daemon (`vxesfsd`): This is the primary file system daemon. It is responsible for writing data into the MSDP cache files.
- Veritas NetBackup Extendable Storage Proxy (`vxesp`) daemons: These daemons are responsible for interacting with the cloud. Under normal operations, there are always two `vxesp` processes: one is the master and one is the worker.

  The `vxesp` daemon produces the following log:

  `/usr/openv/netbackup/logs/esfs_storage`

`vxesfsd` includes three subcomponents that perform various tasks as part of ESFS:

- File system component: Interacts with the ESFS database.
- Monitor component: The monitor component checks the file queue for files to be uploaded and checks the local cache directory for cache eviction purposes, among other activities.
- Storage manager component: Notifies `vxesp` processes when there's work to be done, manages synchronous (downloads from the cloud) and asynchronous (uploads to and deletions in the cloud), and shared memory, among other activities.

The `vxesfsd` daemon produces the following logs in `/usr/openv/netbackup/logs/`:

`esfs_filesystem`	Logs FUSE operations.
`esfs_storagemanager`	Logs the interactions of the ESFS storage manager with `vxesp`.

`esfs_monitor`	Logs job status updates and periodic tasks such as cache eviction and FSDB backups.
`esfs_database`	Logs FSDB actions that are specific to the ESFS database.

MSDP cache files

As part of the Cloud Storage Server Configuration Wizard, the administrator configures a local cache directory (*`local_cache_dir`*). The directory must be on either a Linux file system or, in the case of an appliance, a VxFS file system.

The directory is then split into two:

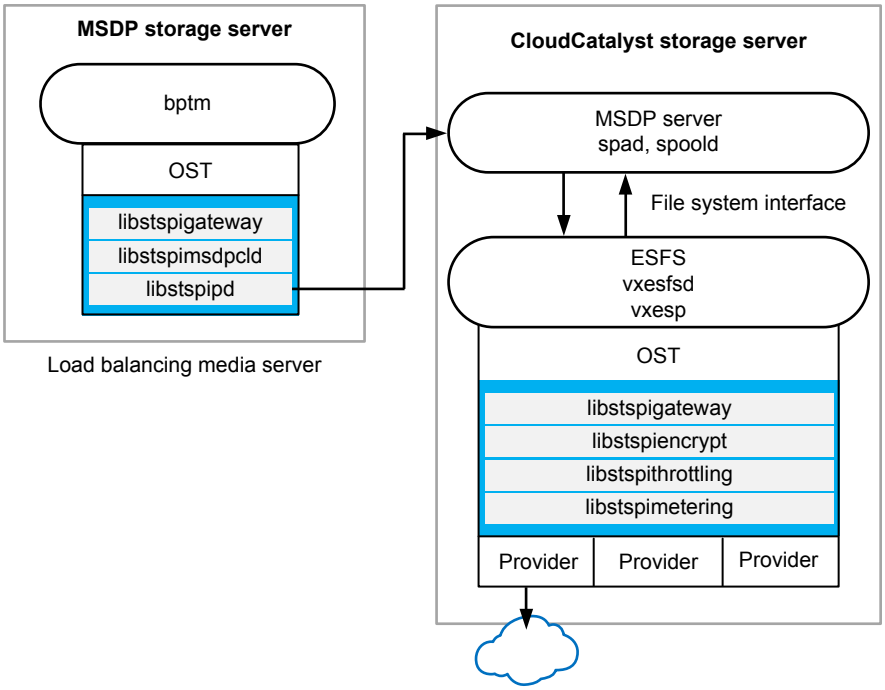
- A cache directory: *`local_cache_dir`*`/cache/userdata`
  ESFS writes out the data and the metadata in this location. This directory is mapped directly to the storage directory (*`local_cache_dir`*`/storage`). There are not two copies of each file on this media server.
- A storage directory: *`local_cache_dir`*`/storage`
  This path is the mount point to the ESFS file system. This is what MSDP knows as its storage directory.

NetBackup periodically performs data eviction tasks in the cache directory to create space for new backups. If necessary, the administrator can change when or how often data eviction occurs. For example, by default, if a file is not accessed in 30 days, and it has been uploaded to the cloud successfully, it is removed from the cache directory. These options are configured in the esfs.json file.

See "About the CloudCatalyst esfs.json configuration file" on page 248.

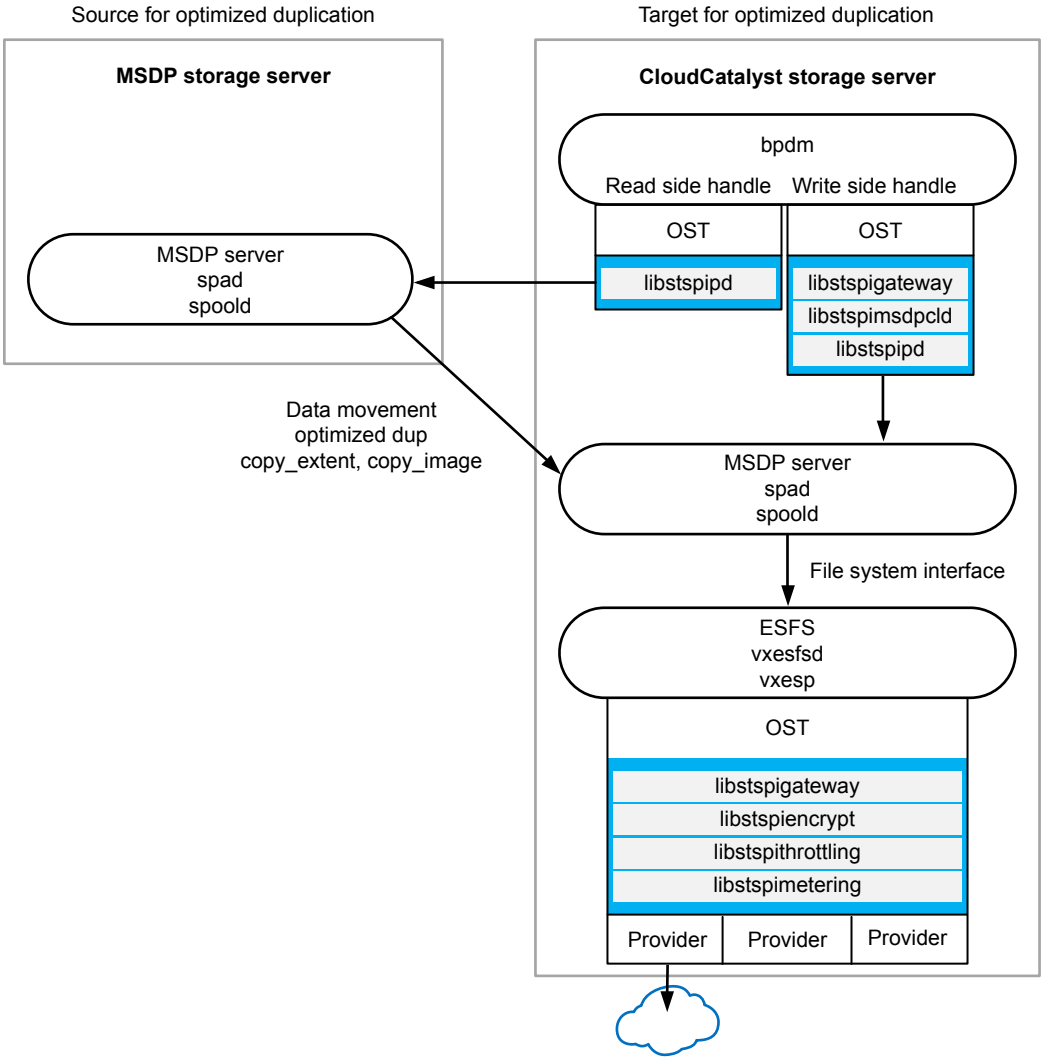
Backup workflow

Figure 6-7 Backup data workflow for a CloudCatalyst storage server



Optimized duplication workflow

Figure 6-8 Optimized duplication workflow with target as a CloudCatalyst storage server



Disaster Recovery for CloudCatalyst

Veritas recommends that you contact your Veritas Support representative to guide you through disaster recovery procedures in a CloudCatalyst environment.

You can refer the Support representative to the following Knowledge Base Article, which contains the recovery instructions:

https://www.veritas.com/support/en_US/article.100039183.html

Chapter 7

Monitoring deduplication activity

This chapter includes the following topics:

- Monitoring the MSDP deduplication rate
- Viewing MSDP job details
- About MSDP storage capacity and usage reporting
- About MSDP container files
- Viewing storage usage within MSDP container files
- Viewing MSDP disk reports
- About monitoring MSDP processes
- Reporting on Auto Image Replication jobs

Monitoring the MSDP deduplication rate

The deduplication rate is the percentage of data that was stored already. That data is not stored again.

The following methods show the MSDP deduplication rate:

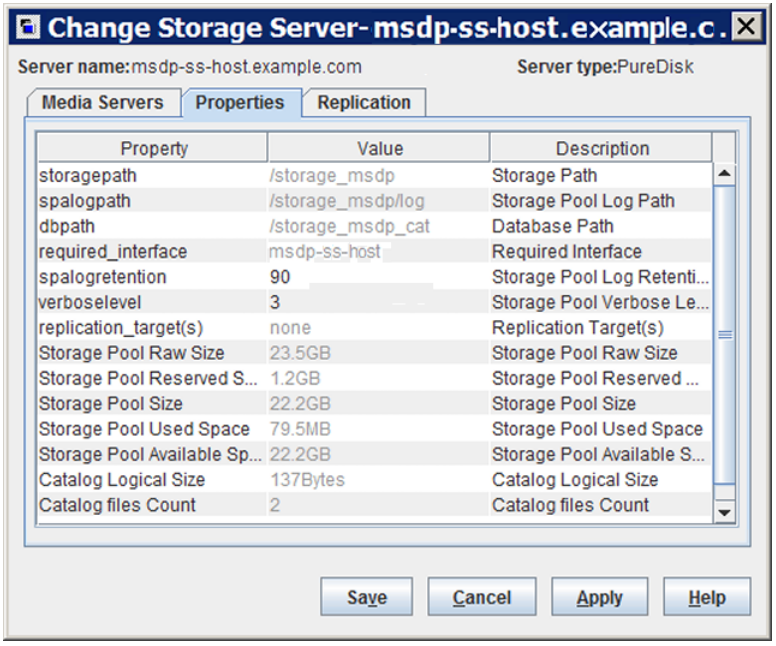
- To view the global MSDP deduplication ratio
- To view the MSDP deduplication rate for a backup job in the Activity Monitor

On UNIX and Linux, you can use the NetBackup `bpdbjobs` command to display the deduplication rate. However, you must configure it to do so.

See "To configure the bpdbjobs command to display the MSDP deduplication rate" on page 269.

To view the global MSDP deduplication ratio

1. In the NetBackup Administration Console, expand **Media and Device Management > Credentials > Storage Server**
2. Select the deduplication storage server.
3. On the **Edit** menu, select **Change**.
4. In the **Change Storage Server** dialog box, select the **Properties** tab. The **Deduplication Ratio** field displays the ratio.



To view the MSDP deduplication rate for a backup job in the Activity Monitor

1. In the **NetBackup Administration Console**, click **Activity Monitor**.
2. Click the **Jobs** tab.

   The **Deduplication Rate** column shows the rate for each job.

To configure the bpdbjobs command to display the MSDP deduplication rate

- Add a `DEDUPRATIO BPDBJOBS_COLDEFS` entry in the `bp.conf` file on the media server on which you run the command.

  The `bpdbjobs` command then shows the deduplication rate in its output.

Many factors affect deduplication performance.

See "About MSDP performance" on page 34.

Viewing MSDP job details

Use the NetBackup Activity Monitor to view deduplication job details.

To view MSDP job details

1. In the **NetBackup Administration Console**, click **Activity Monitor**.
2. Click the **Jobs** tab.
3. To view the details for a specific job, double-click on the job that is displayed in the **Jobs** tab pane.
4. In the **Job Details** dialog box, click the **Detailed Status** tab.

   The deduplication job details are described in a different topic.

   See "MSDP job details" on page 269.

MSDP job details

The **NetBackup Administration Console Job Details** dialog box shows the details of a deduplication job. The details depend on whether the job is media server deduplication or client-side deduplication job.

Media server deduplication job details

For media server deduplication, the **Detailed Status** tab shows the deduplication rate on the server that performed the deduplication. The following job details excerpt shows details for a client for which MSDP_Server.example.com deduplicated the data (the **dedup** field shows the deduplication rate):

```
03/05/2013 10:37:06 - Info MSDP_Server.example.com (pid=17498)
StorageServer=PureDisk:MSDP_Server.example.com; Report=PDDO Stats
(multi-threaded stream used) for (MSDP_Server.example.com):
scanned: 8930 KB, CR sent: 4363 KB, CR sent over FC: 0 KB, dedup: 51.1%,
cache hits: 36 (50.7%), rebased: 35 (49.3%)
```

Client-side deduplication job details

For client-side deduplication jobs, the **Detailed Status** tab shows two deduplication rates. The first deduplication rate is always for the client data. The second deduplication rate is for the metadata (disk image header and **True Image Restore** information (if applicable)). That information is always deduplicated on a server; typically, deduplication rates for that information are zero or very low. The following job details example excerpt shows the two rates. The **1/8/2013 11:58:09 PM** entry is for the client data; the **1/8/2013 11:58:19 PM** entry is for the metadata.

```
1/8/2013 11:54:21 PM - Info MSDP_Server.example.com(pid=2220)
  Using OpenStorage client direct to backup from client
  Client_B.example.com to MSDP_Server.example.com
1/8/2013 11:58:09 PM - Info MSDP_Server.example.com(pid=2220)
  StorageServer=PureDisk:MSDP_Server.example.com; Report=PDDO
  Stats for (MSDP_Server.example.com: scanned: 3423425 KB,
  CR sent: 122280 KB, dedup: 96.4%, cache hits: 49672 (98.2%)
1/8/2013 11:58:09 PM - Info MSDP_Server.example.com(pid=2220)
  Using the media server to write NBU data for backup
  Client_B_1254987197.example.com to MSDP_Server.example.com
1/8/2013 11:58:19 PM - Info MSDP_Server.example.com(pid=2220)
  StorageServer=PureDisk:MSDP_Server.example.com; Report=PDDO
  Stats for (MSDP_Server.example.com: scanned: 17161 KB,
  CR sent: 17170 KB, dedup: 0.0%, cache hits: 0 (0.0%)
```

Field descriptions

Table 7-1 describes the deduplication activity fields.

Table 7-1 MSDP activity field descriptions

Field	Description
cache hits	The percentage of data segments in the backup that is represented in the local fingerprint cache. The deduplication plug-in did not have to query the database about those segments If the `pd.conf` file `FP_CACHE_LOCAL` parameter is set to `0` on the storage, the **cache hits** output is not included for the jobs that run on the storage server. See "MSDP pd.conf file parameters" on page 198.

Table 7-1 MSDP activity field descriptions *(continued)*

Field	Description
CR sent	The amount of data that is sent from the deduplication plug-in to the component that stores the data. In NetBackup, the NetBackup Deduplication Engine stores the data. If the storage server deduplicates the data, it does not travel over the network. The deduplicated data travels over the network when the deduplication plug-in runs on a computer other than the storage server, as follows: ■ On a NetBackup client that deduplicates its own data (client-side deduplication). ■ On a fingerprinting media server that deduplicates the data. The deduplication plug-in on the fingerprinting server sends the data to the storage server, which writes it to a **Media Server Deduplication Pool**. ■ On a media server that then sends the data to a NetBackup 5000 series appliance for storage. (In NetBackup, a **PureDisk Storage Pool** represents the storage on a NetBackup 5000 series appliance.)
CR sent over FC	The amount of data that is sent from the deduplication plug-in over Fibre Channel to the component that stores the data. In NetBackup, the NetBackup Deduplication Engine stores the data.
dedup	The percentage of data that was stored already. That data is not stored again.
multi-threaded stream used	Indicates that the Deduplication Multi-Threaded Agent processed the backup. See "About the MSDP Deduplication Multi-Threaded Agent" on page 54.
PDDO stats	Indicates that the job details are for storage on the following destinations: ■ **Media Server Deduplication Pool** ■ A NetBackup 5000 series appliance, exposed to NetBackup through a **PureDisk Deduplication Pool**.
rebased	The percentage of segments that were rebased (that is, defragmented) during the backup. Those segments had poor data locality. NetBackup reports back up job completion only after backup rebasing is completed. See "About MSDP storage rebasing" on page 309.
scanned	The amount of data that the deduplication plug-in scanned.
Using OpenStorage client direct to restore...	Indicates that the restore travels over the client-direct data path and does not use NetBackup media server components to process the data.

About MSDP storage capacity and usage reporting

Several factors affect the expected NetBackup deduplication capacity and usage results, as follows:

- Expired backups may not change the available size and the used size. An expired backup may have no unique data segments. Therefore, the segments remain valid for other backups.
- NetBackup Deduplication Manager clean-up may not have run yet. The Deduplication Manager performs clean up twice a day. Until it performs clean-up, deleted image fragments remain on disk.

If you use operating system tools to examine storage space usage, their results may differ from the usage reported by NetBackup, as follows:

- NetBackup usage data includes the reserved space that the operating system tools do not include.
- If other applications use the storage, NetBackup cannot report usage accurately. NetBackup requires exclusive use of the storage.

Table 7-2 describes the options for monitoring capacity and usage.

Table 7-2 Capacity and usage reporting

Option	Description
Change Storage Server dialog box	The **Change Storage Server** dialog box **Properties** tab displays storage capacity and usage. It also displays the global deduplication ratio. This dialog box displays the most current capacity usage that is available in the NetBackup Administration Console. You can see an example of the dialog box in a different topic. See "Monitoring the MSDP deduplication rate" on page 267.
Disk Pools window	The **Disk Pools** window of the Administration Console displays the values that were stored when NetBackup polled the disk pools. NetBackup polls every 5 minutes; therefore, the value may not be as current as the value that is displayed in the **Change Storage Server** dialog box. To display the window, expand **Media and Device Management > Devices > Disk Pools**.

Table 7-2 Capacity and usage reporting *(continued)*

Option	Description
View container command	A command that is installed with NetBackup provides a view of storage capacity and usage within the deduplication container files. See "About MSDP container files" on page 273. See "Viewing storage usage within MSDP container files" on page 274.
Disk Pool Status report	The **Disk Pool Status** report displays the state of the disk pool and usage information. See "Viewing MSDP disk reports" on page 275.
Disk Logs report	The **Disk Logs** report displays event and message information. A useful event for monitoring capacity is event 1044; the following is the description of the event in the **Disk Logs** report: `The usage of one or more system resources has exceeded a warning level.` By default, the threshold (high-water mark) for this message is at 98% capacity. No more data can be stored. See "Viewing MSDP disk reports" on page 275. See "MSDP event codes and messages" on page 370.
The `nbdevquery` command	The `nbdevquery` command shows the state of the disk volume and its properties and attributes. It also shows capacity, usage, and percent used. See "Determining the MSDP disk volume state" on page 300.
NetBackup OpsCenter	The NetBackup OpsCenter also provides information about storage capacity and usage. See *NetBackup OpsCenter Administrator's Guide*: http://www.veritas.com/docs/DOC5332

About MSDP container files

The deduplication storage implementation allocates container files to hold backup data. Deleted segments can leave free space in containers files, but the container file sizes do not change. Segments are deleted from containers when backup images expire and the NetBackup Deduplication Manager performs clean-up.

The NetBackup Deduplication Manager checks the storage space every 20 seconds. It then periodically compacts the space available inside the container files. Therefore, space within a container is not available as soon as it is free. Various internal parameters control whether a container file is compacted. Although space may be available within a container file, the file may not be eligible for compaction.

Viewing storage usage within MSDP container files

The NetBackup `crcontrol` command reports on storage usage within containers.

To view storage usage within MSDP container files

- Use the `crcontrol` command and the `--dsstat` option on the deduplication storage server. (For help with the command options, use the `--help` option.)

  The following is an example of the command usage:

  - UNIX and Linux: `/usr/openv/pdde/pdcr/bin/crcontrol --dsstat`
  - Windows: *`install_path`*`\Veritas\pdde\Crcontrol.exe --dsstat`

  The following is an example of the output:

```
************ Data Store statistics ************
Data storage      Raw    Size   Used   Avail  Use%
                  1.0T  988.9G 666.0G  322.9G  68%

Number of containers             : 2981
Average container size           : 219740494 bytes (209.56MB)
Space allocated for containers   : 655046415189 bytes (610.06GB)
Reserved space                   : 45360705536 bytes (42.25GB)
Reserved space percentage        : 4.1%
```

  For systems that host a 96-TB **Media Server Deduplication Pool**, you can use the following `crcontrol` command to show information about each partition:

```
/usr/openv/pdde/pdcr/bin/crcontrol --dsstat 3
```

  From the command output, you can determine the following:

  `Raw` The raw size of the storage.

`Size`	The size of the storage that NetBackup can use: the `Raw` size of the storage minus the file system `Reserved space`. If the file system has a concept of root reserved space (such as EXT3 or VxFS), that space cannot be used for storage. The `crcontrol` command does not include reserved space in the available space. Unlike the `crcontrol` command, some operating system tools report root reserved space as usable space.
`Used`	The amount of deduplicated data that is stored on the file system. NetBackup obtains the file system used space from the operating system.
`Avail`	The `Size` minus the `Used` space.
`Use%`	The `Used` space divided by the `Size`.

Viewing MSDP disk reports

The NetBackup disk reports include information about the disk pools, disk storage units, disk logs, images that are stored on disk media, and storage capacity.

Table 7-3 describes the disk reports available.

Table 7-3 Disk reports

Report	Description
Images on Disk	The Images on Disk report generates the image list present on the disk storage units that are connected to the media server. The report is a subset of the Images on Media report; it shows only disk-specific columns. The report provides a summary of the storage unit contents. If a disk becomes bad or if a media server crashes, this report can let you know what data is lost.

Table 7-3 Disk reports *(continued)*

Report	Description
Disk Logs	The Disk Logs report displays the media errors or the informational messages that are recorded in the NetBackup error catalog. The report is a subset of the Media Logs report; it shows only disk-specific columns. The report also includes information about deduplicated data integrity checking. See "About MSDP data integrity checking" on page 304. Either `PureDisk` or `Veritas Deduplication Engine` in the description identifies a deduplication message. The identifiers are generic because the deduplication engine does not know which application consumes its resources. NetBackup and Veritas Backup Exec are Veritas applications that use deduplication.
Disk Storage Unit Status	The Disk Storage Unit Status report displays the state of disk storage units in the current NetBackup configuration. For disk pool capacity, see the disk pools window in **Media and Device Management > Devices > Disk Pools**. Multiple storage units can point to the same disk pool. When the report query is by storage unit, the report counts the capacity of disk pool storage multiple times.
Disk Pool Status	The **Disk Pool Status** report displays the state of disk pool and usage information. This report displays only when a license that enables NetBackup disk features is installed.

To view disk reports

1. In the NetBackup Administration Console, expand **NetBackup Management > Reports > Disk Reports**.
2. Select the name of a disk report.
3. In the right pane, select the report settings.
4. Click **Run Report**.

About monitoring MSDP processes

The following table shows the deduplication processes about which NetBackup reports:

See "MSDP server components" on page 331.

Table 7-4 Where to monitor the main MSDP processes

What	Where to monitor it
NetBackup Deduplication Engine	In the **NetBackup Administration Console**, the NetBackup Deduplication Engine appears as `spoold` on the **Daemons** tab of the **Activity Monitor**. The NetBackup `bpps` command also shows the `spoold` process.
NetBackup Deduplication Manager	In the **NetBackup Administration Console**, the NetBackup Deduplication Manager appears as `spad` on the **Daemons** tab of the **Activity Monitor**. The NetBackup `bpps` command also shows the `spad` process.

Reporting on Auto Image Replication jobs

The Activity Monitor displays both the **Replication** job and the **Import** job in a configuration that replicates to a target master server domain.

Table 7-5 Auto Image Replication jobs in the Activity Monitor

Job type	Description
Replication	The job that replicates a backup image to a target master displays in the Activity Monitor as a **Replication** job. The **Target Master** label displays in the **Storage Unit** column for this type of job. Similar to other **Replication** jobs, the job that replicates images to a target master can work on multiple backup images in one instance. The detailed status for this job contains a list of the backup IDs that were replicated.
Import	The job that imports a backup copy into the target master domain displays in the Activity Monitor as an **Import** job. An **Import** job can import multiple copies in one instance. The detailed status for an **Import** job contains a list of processed backup IDs and a list of failed backup IDs. Note that a successful replication does not confirm that the image was imported at the target master. If the data classifications are not the same in both domains, the **Import** job fails and NetBackup does not attempt to import the image again. Failed **Import** jobs fail with a status 191 and appear in the **Problems** report when run on the target master server. The image is expired and deleted during an **Image Cleanup** job. Note that the originating domain (Domain 1) does not track failed imports.

Chapter 8

Managing deduplication

This chapter includes the following topics:

- Managing MSDP servers
- Managing NetBackup Deduplication Engine credentials
- Managing Media Server Deduplication Pools
- Deleting backup images
- About MSDP queue processing
- Processing the MSDP transaction queue manually
- About MSDP data integrity checking
- Configuring MSDP data integrity checking behavior
- About managing MSDP storage read performance
- About MSDP storage rebasing
- About the MSDP data removal process
- Resizing the MSDP storage partition
- How MSDP restores work
- Configuring MSDP restores directly to a client
- About restoring files at a remote site
- About restoring from a backup at a target master domain
- Specifying the restore server

Managing MSDP servers

After you configure deduplication, you can perform various tasks to manage deduplication servers.

See "Viewing MSDP storage servers" on page 279.

See "Determining the MSDP storage server state" on page 279.

See "Viewing MSDP storage server attributes" on page 280.

See "Setting MSDP storage server attributes" on page 281.

See "Changing MSDP storage server properties" on page 282.

See "Clearing MSDP storage server attributes" on page 283.

See "About changing the MSDP storage server name or storage path" on page 284.

See "Changing the MSDP storage server name or storage path" on page 284.

See "Removing an MSDP load balancing server" on page 286.

See "Deleting an MSDP storage server" on page 287.

See "Deleting the MSDP storage server configuration" on page 288.

Viewing MSDP storage servers

Use the NetBackup Administration Console to view a list of deduplication storage servers already configured.

To view MSDP storage servers

- In the NetBackup Administration Console, expand **Media and Device Management > Credentials > Storage Server**.

  The **All Storage Servers** pane shows all configured deduplication storage servers. Deduplication storage servers show **PureDisk** in the **Server Type** column.

Determining the MSDP storage server state

Use the NetBackup `nbdevquery` command to determine the state of a deduplication storage server. The state is either UP or DOWN.

To determine MSDP storage server state

- Run the following command on the NetBackup master server or a deduplication storage server:

  UNIX: `/usr/openv/netbackup/bin/admincmd/nbdevquery -liststs -storage_server server_name -stype PureDisk –U`

  Windows: `install_path\NetBackup\bin\admincmd\nbdevquery -liststs -storage_server server_name -stype PureDisk –U`

  The following is example output:

  ```
  Storage Server      : bit.example.com
  Storage Server Type : PureDisk
  Storage Type        : Formatted Disk, Network Attached
  State               : UP
  ```

  This example output is shortened; more flags may appear in actual output.

Viewing MSDP storage server attributes

Use the NetBackup `nbdevquery` command to view the deduplication storage server attributes.

The *server_name* you use in the `nbdevquery` command must match the configured name of the storage server. If the storage server name is its fully-qualified domain name, you must use that for *server_name*.

To view MSDP storage server attributes

- The following is the command syntax to set a storage server attribute. Run the command on the NetBackup master server or on the deduplication storage server:

  UNIX: `/usr/openv/netbackup/bin/admincmd/nbdevquery -liststs -storage_server server_name -stype PureDisk -U`

  Windows: `install_path\NetBackup\bin\admincmd\nbdevquery -liststs -storage_server server_name -stype PureDisk -U`

  The following is example output:

```
Storage Server      : bit
Storage Server Type : PureDisk
Storage Type        : Formatted Disk, Network Attached
State               : UP
Flag                : OpenStorage
Flag                : CopyExtents
Flag                : AdminUp
Flag                : InternalUp
Flag                : LifeCycle
Flag                : CapacityMgmt
Flag                : OptimizedImage
Flag                : FT-Transfer
```

  This example output is shortened; more flags may appear in actual output.

Setting MSDP storage server attributes

You may have to set storage server attributes to enable new functionality.

If you set an attribute on the storage server, you may have to set the same attribute on existing deduplication pools. The overview or configuration procedure for the new functionality describes the requirements.

See "Setting a Media Server Deduplication Pool attribute" on page 293.

To set a MSDP storage server attribute

1. The following is the command syntax to set a storage server attribute. Run the command on the master server or on the storage server.

   `nbdevconfig -changests -storage_server storage_server -stype PureDisk -setattribute attribute`

   The following describes the options that require the arguments that are specific to your domain:

`-storage_server` *storage_server*	The name of the storage server.
`-setattribute` *attribute*	The *attribute* is the name of the argument that represents the new functionality. For example, **OptimizedImage** specifies that the environment supports the optimized synthetic backup method.

The following is the path to the `nbdevconfig` command:

- UNIX: /usr/openv/netbackup/bin/admincmd
- Windows: *install_path*\NetBackup\bin\admincmd

2 To verify, view the storage server attributes.

See "Viewing MSDP storage server attributes" on page 280.

See "About MSDP optimized synthetic backups" on page 33.

Changing MSDP storage server properties

You can change the retention period and logging level for the NetBackup Deduplication Manager.

To change MSDP storage server properties

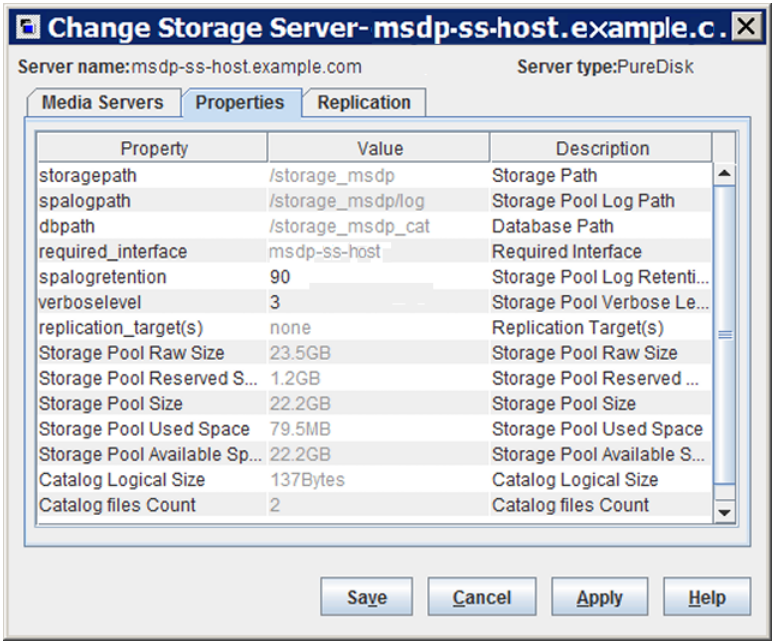
1 In the **NetBackup Administration Console**, expand **Media and Device Management > Credentials > Storage Servers**.

2 Select the deduplication storage server.

Warning: If you have load balancing servers, do not select any or all of them in the **Media Servers** pane of the **NetBackup Administration Console**. If you do, the change operation fails.

3 On the **Edit** menu, select **Change**.

4 In the **Change Storage Server** dialog box, select the **Properties** tab.



5 For the property to change, select the value in the **Value** column.

6 Change the value.

7 Click **OK**.

Clearing MSDP storage server attributes

Use the `nbdevconfig` command to remove storage server attributes.

To clear MSDP storage server attributes

- Run the following command on the NetBackup master server or on a storage server:

```
nbdevconfig -changests -storage_server storage_server -stype
PureDisk -clearattribute attribute
```

`-storage_server` *`storage_server`*	The name of the storage server.
`-setattribute` *`attribute`*	The *attribute* is the name of the argument that represents the functionality.

The following is the path to the `nbdevconfig` command:

- UNIX: `/usr/openv/netbackup/bin/admincmd`
- Windows: *`install_path`*`\NetBackup\bin\admincmd`

About changing the MSDP storage server name or storage path

You can change the storage server host name and the storage path of an existing NetBackup deduplication environment.

The following are several use cases that require changing an existing deduplication environment:

- You want to change the host name. For example, the name of host A was changed to B or a new network card was installed with a private interface C. To use the host name B or the private interface C, you must reconfigure the storage server.
  See "Changing the MSDP storage server name or storage path" on page 284.
- You want to change the storage path. To do so, you must reconfigure the storage server with the new path.
  See "Changing the MSDP storage server name or storage path" on page 284.
- You need to reuse the storage for disaster recovery. The storage is intact, but the storage server was destroyed. To recover, you must configure a new storage server.
  In this scenario, you can use the same host name and storage path or use different ones.
  See "Recovering from an MSDP storage server failure" on page 322.

Changing the MSDP storage server name or storage path

Two aspects of a NetBackup deduplication configuration exist: the record of the deduplication storage in the EMM database and the physical presence of the storage on disk (the populated storage directory).

Warning: Deleting valid backup images may cause data loss.

See "About changing the MSDP storage server name or storage path" on page 284.

Table 8-1 Changing the storage server name or storage path

Step	Task	Procedure
Step 1	Ensure that no deduplication activity occurs	Deactivate all backup policies that use deduplication storage. See the *NetBackup Administrator's Guide, Volume I*: http://www.veritas.com/docs/DOC5332
Step 2	Expire the backup images	Expire all backup images that reside on the deduplication disk storage. **Warning:** Do not delete the images. They are imported back into NetBackup later in this process. If you use the `bpexpdate` command to expire the backup images, use the `-nodelete` parameter. See the *NetBackup Administrator's Guide, Volume I*: http://www.veritas.com/docs/DOC5332
Step 3	Delete the storage units that use the disk pool	See the *NetBackup Administrator's Guide, Volume I*: http://www.veritas.com/docs/DOC5332
Step 4	Delete the disk pool	See "Deleting a Media Server Deduplication Pool" on page 302.
Step 5	Delete the deduplication storage server	See "Deleting an MSDP storage server" on page 287.
Step 6	Delete the configuration	Delete the deduplication configuration. See "Deleting the MSDP storage server configuration" on page 288.
Step 7	Delete the deduplication host configuration file	Each load balancing server contains a deduplication host configuration file. If you use load balancing servers, delete the deduplication host configuration file from those servers. See "Deleting an MSDP host configuration file" on page 219.

Step 8	Delete the identity file and the file system table file	Delete the following files from the MSDP storage server, depending on operating system:
		UNIX:
		`/storage_path/data/.identity`
		`/storage_path/etc/puredisk/fstab.cfg`
		Windows:
		`storage_path\data\.identity`
		`storage_path\etc\puredisk\fstab.cfg`

Table 8-1 Changing the storage server name or storage path *(continued)*

Step	Task	Procedure
Step 9	Change the storage server name or the storage location	See the computer or the storage vendor's documentation. See "Use fully qualified domain names" on page 36. See "MSDP storage path properties" on page 88.
Step 10	Reconfigure the storage server	When you configure deduplication, select the host by the new name and enter the new storage path (if you changed the path). You can also use a new network interface. See "Configuring MSDP server-side deduplication" on page 50.
Step 11	Import the backup images	See the *NetBackup Administrator's Guide, Volume I*: http://www.veritas.com/docs/DOC5332

Removing an MSDP load balancing server

You can remove a load balancing server from a deduplication node. The media server no longer deduplicates client data.

See "About MSDP storage servers" on page 24.

After you remove the load balancing server, restart the NetBackup Enterprise Media Manager service. The NetBackup disk polling service may try to use the removed server to query for disk status. Because the server is no longer a load balancing server, it cannot query the disk storage. Consequently, NetBackup may mark the disk volume as DOWN. When the EMM service restarts, it chooses a different deduplication server to monitor the disk storage.

If the host failed and is unavailable, you can use the `tpconfig` device configuration utility in menu mode to delete the server. However, you must run the `tpconfig` utility on a UNIX or Linux NetBackup server.

For procedures, see *NetBackup Administrator's Guide, Volume II*:

http://www.veritas.com/docs/DOC5332

To remove a media server from a MSDP node

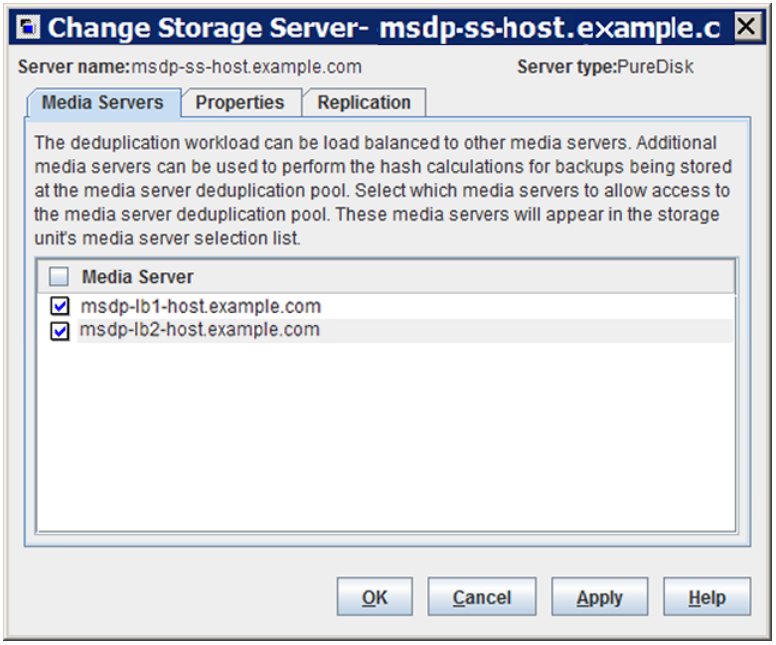
1. For every storage unit that specifies the media server in **Use one of the following media servers**, clear the check box that specifies the media server.

   This step is not required if the storage unit is configured to use any available media server.

2. In the NetBackup Administration Console, expand **Media and Device Management > Credentials > Storage Server**.

3 Select the deduplication storage server, and then select **Edit > Change**.

4 In the **Change Storage Server** dialog box, select the **Media Servers** tab.



5 Clear the check box of the media server you want to remove.

6 Click **OK**.

Deleting an MSDP storage server

If you delete a deduplication storage server, NetBackup deletes the host as a storage server and disables the deduplication storage server functionality on that media server.

NetBackup does not delete the media server from your configuration. To delete the media server, use the NetBackup `nbemmcmd` command.

Deleting the deduplication storage server does not alter the contents of the storage on physical disk. To protect against inadvertent data loss, NetBackup does not automatically delete the storage when you delete the storage server.

If a disk pool is configured from the disk volume that the deduplication storage server manages, you cannot delete the deduplication storage server.

Warning: Do not delete a deduplication storage server if its storage contains unexpired NetBackup images; if you do, data loss may occur.

To delete an MSDP storage server

1. In the **NetBackup Administration Console**, expand **Media and Device Management > Credentials > Storage Server**
2. On the **Edit** menu, select **Delete**.
3. Click **Yes** in the confirmation dialog box.

See "Changing the MSDP storage server name or storage path" on page 284.

Deleting the MSDP storage server configuration

Use this procedure to delete a deduplication storage server configuration. The script that is used in this procedure deletes the active configuration and returns the configuration files to their installed, preconfigured state.

Only use this procedure when directed to from a process topic. A process topic is a high-level user task made up of a series of separate procedures.

See "Changing the MSDP storage server name or storage path" on page 284.

See "Deactivating MSDP" on page 329.

To delete the MSDP storage server configuration

1. Use the NetBackup Administration Console to stop the NetBackup Deduplication Engine (`spoold`) and the NetBackup Deduplication Manager (`spad`).
2. On the storage server, run one of the following scripts, depending on your operating system:

   UNIX:
   `/usr/openv/pdde/pdconfigure/scripts/installers/PDDE_deleteConfig.sh`

   Windows: `install_path\Program Files\Veritas\pdde\PDDE_deleteConfig.bat`

   The command output includes the following:

   ```
   **** Starting PDDE_deleteConfig.sh ***
   You need to stop the spad and spoold daemons to proceed
   This script will delete the PDDE configuration on this system
   Would you want to continue? [ y | n ]
   ```

3. Type **y** and then press Enter.

Managing NetBackup Deduplication Engine credentials

You can manage existing credentials in NetBackup.

See "Determining which media servers have deduplication credentials" on page 289.

See "Adding NetBackup Deduplication Engine credentials" on page 289.

See "Changing NetBackup Deduplication Engine credentials" on page 290.

See "Deleting credentials from a load balancing server" on page 290.

Determining which media servers have deduplication credentials

You can determine which media servers have credentials configured for the NetBackup Deduplication Engine. The servers with credentials are load balancing servers.

To determine if NetBackup Deduplication Engine credentials exist

1. In the **NetBackup Administration Console**, expand **Media and Device Management > Credentials > Storage Server**.
2. Select the storage server, and then select **Edit > Change**.
3. In the **Change Storage Server** dialog box, select the **Media Servers** tab.

   The media servers for which credentials are configured are checked.

Adding NetBackup Deduplication Engine credentials

You may need to add the NetBackup Deduplication Engine credentials to an existing storage server or load balancing server. For example, disaster recovery may require that you add the credentials.

Add the same credentials that you already use in your environment.

Another procedure exists to add a load balancing server to your configuration.

See "Adding an MSDP load balancing server" on page 194.

To add NetBackup Deduplication Engine credentials by using the tpconfig command

- On the host to which you want to add credentials, run the following command:

  On Windows:

  ```
  install_path\Veritas\NetBackup\Volmgr\bin\tpconfig -add
  -storage_server sshostname -stype PureDisk -sts_user_id UserID
  -password PassWord
  ```

  On UNIX/Linux:

  ```
  /usr/openv/volmgr/bin/tpconfig -add -storage_server sshostname
  -stype PureDisk -sts_user_id UserID -password PassWord
  ```

  For *sshostname*, use the name of the storage server.

Changing NetBackup Deduplication Engine credentials

You cannot change the NetBackup Deduplication Engine credentials after you enter them. If you must change the credentials, contact your Veritas support representative.

See "About the NetBackup Deduplication Engine credentials" on page 30.

Deleting credentials from a load balancing server

You may need to delete the NetBackup Deduplication Engine credentials from a load balancing server. For example, disaster recovery may require that you delete the credentials on a load balancing server.

Another procedure exists to remove a load balancing server from a deduplication node.

See "Removing an MSDP load balancing server" on page 286.

To delete credentials from a load balancing server

- On the load balancing server, run the following command:

  On Windows:

  ```
  install_path\Veritas\NetBackup\Volmgr\bin\tpconfig -delete
  -storage_server sshostname -stype PureDisk -sts_user_id UserID
  ```

  On UNIX/Linux:

  ```
  /usr/openv/volmgr/bin/tpconfig -delete -storage_server sshostname
  -stype PureDisk -sts_user_id UserID
  ```

  For *sshostname*, use the name of the storage server.

Managing Media Server Deduplication Pools

After you configure NetBackup deduplication, you can perform various tasks to manage your deduplication disk pools.

See "Viewing Media Server Deduplication Pools" on page 291.

See "Changing a Media Server Deduplication Pool properties" on page 294.

See "Determining the Media Server Deduplication Pool state" on page 291.

See "Changing Media Server Deduplication Pool state" on page 292.

See "Determining the MSDP disk volume state" on page 300.

See "Changing the MSDP disk volume state" on page 300.

See "Viewing Media Server Deduplication Pool attributes" on page 292.

See "Setting a Media Server Deduplication Pool attribute" on page 293.

See "Clearing a Media Server Deduplication Pool attribute" on page 299.

See "Resizing the MSDP storage partition" on page 313.

See "Inventorying a NetBackup disk pool" on page 301.

See "Deleting a Media Server Deduplication Pool" on page 302.

Viewing Media Server Deduplication Pools

Use the NetBackup Administration Console to view configured disk pools.

To view disk pools

- In the NetBackup Administration Console, expand **Media and Device Management > Devices > Disk Pools**.

Determining the Media Server Deduplication Pool state

The disk pool state is UP or DOWN.

To determine disk pool state

1. In the **NetBackup Administration Console**, expand **Media and Device Management > Device Monitor**.
2. Select the **Disk Pools** tab.
3. The state is displayed in the **Status** column.

Changing Media Server Deduplication Pool state

You can change the state of a NetBackup disk pool. Pool states are UP or DOWN.

To change the state to DOWN, the disk pool must not be busy. If backup jobs are assigned to the disk pool, the state change fails. Cancel the backup jobs or wait until the jobs complete.

To change Media Server Deduplication Pool state

1. In the **NetBackup Administration Console**, in the left pane, select **Media and Device Management > Device Monitor**.
2. Select the **Disk Pools** tab.
3. Select the disk pool.
4. Select either **Actions > Up** or **Actions > Down**.

Viewing Media Server Deduplication Pool attributes

Use the NetBackup `nbdevquery` command to view deduplication pool attributes.

To view MSDP pool attributes

- The following is the command syntax to view the attributes of a deduplication pool. Run the command on the NetBackup master server or on the deduplication storage server:

  UNIX: `/usr/openv/netbackup/bin/admincmd/nbdevquery -listdp -dp pool_name -stype PureDisk -U`

  Windows: `install_path\NetBackup\bin\admincmd\nbdevquery -listdp -dp pool_name -stype PureDisk -U`

  The following is example output:

```
Disk Pool Name   : MediaServerDeduplicationPool
Disk Pool Id     : MediaServerDeduplicationPool
Disk Type        : PureDisk
Status           : UP
Flag             : OpenStorage
Flag             : AdminUp
Flag             : InternalUp
Flag             : LifeCycle
Flag             : CapacityMgmt
Flag             : OptimizedImage
Raw Size (GB)    : 235.76
Usable Size (GB) : 235.76
Num Volumes      : 1
High Watermark   : 98
Low Watermark    : 80
Max IO Streams   : -1
Storage Server   : DedupeServer.example.com (UP)
```

  This example output is shortened; more flags may appear in actual output.

Setting a Media Server Deduplication Pool attribute

You may have to set attributes on your existing media server deduplication pools. For example, if you set an attribute on the storage server, you may have to set the same attribute on your existing deduplication disk pools.

See "Setting MSDP storage server attributes" on page 281.

To set a MSDP disk pool attribute

1. The following is the command syntax to set a deduplication pool attribute. Run the command on the master server or on the storage server.

```
nbdevconfig -changedp -dp pool_name -stype PureDisk -setattribute
attribute
```

The following describes the options that require the arguments that are specific to your domain:

`-changedp pool_name`	The name of the disk pool.
`-setattribute attribute`	The *attribute* is the name of the argument that represents the new functionality. For example, **OptimizedImage** specifies that the environment supports the optimized synthetic backup method.

The following is the path to the `nbdevconfig` command:

- UNIX: /usr/openv/netbackup/bin/admincmd
- Windows: *install_path*\NetBackup\bin\admincmd

2 To verify, view the disk pool attributes.

See "Viewing Media Server Deduplication Pool attributes" on page 292.

Changing a Media Server Deduplication Pool properties

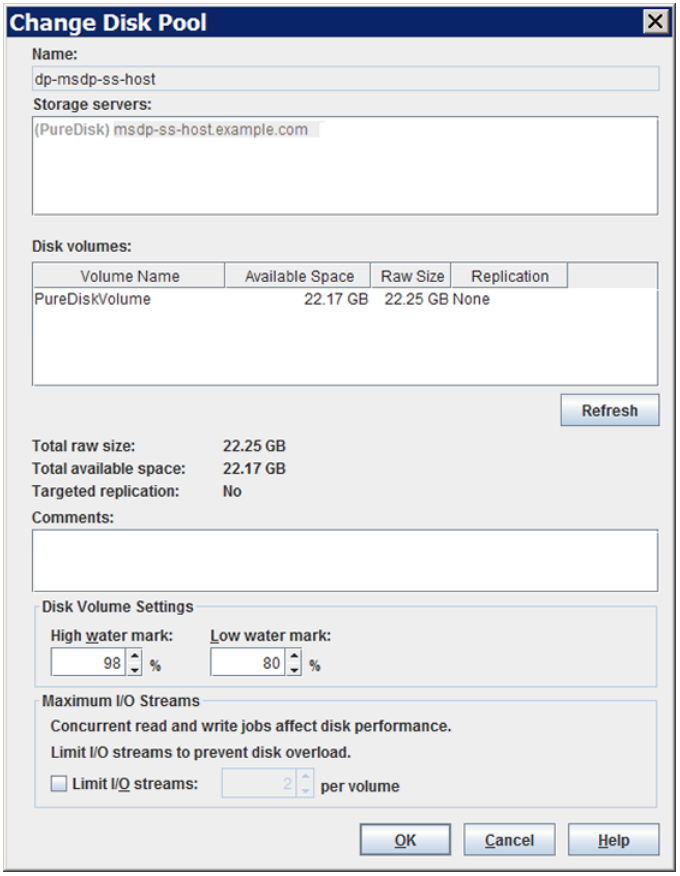
You can change the properties of a deduplication disk pool.

To change disk pool properties

1 In the NetBackup Administration Console, expand **Media and Device Management > Devices > Disk Pools**.

2 Select the disk pool you want to change in the details pane.

3 On the **Edit** menu, select **Change**.



4 In the **Change Disk Pool** dialog box, click **Refresh** to update the disk pool replication properties.

If NetBackup discovers changes, your actions depend on the changes discovered.

See "How to resolve volume changes for Auto Image Replication" on page 296.

5 Change the other properties as necessary.

See "Media Server Deduplication Pool properties" on page 110.

6 Click **OK**.

7 If you clicked **Refresh** and the **Replication** value for the **PureDiskVolume** changed, refresh the view in the **Administration Console**.

How to resolve volume changes for Auto Image Replication

When you open the **Change Disk Pool** dialog box, NetBackup loads the disk pool properties from the catalog. NetBackup queries the storage server for changes when you either click the **Refresh** button in the **Change Disk Pool** dialog box or when you configure a new disk pool for the storage server.

Veritas recommends that you take the following actions when the volume topology changes:

- Discuss the changes with the storage administrator. You need to understand the changes so you can change your disk pools (if required) so that NetBackup can continue to use them.
- If the changes were not planned for NetBackup, ask your storage administrator to revert the changes so that NetBackup functions correctly again.

NetBackup can process changes to the following volume properties:

- Replication Source
- Replication Target
- None

If these volume properties change, NetBackup can update the disk pool to match the changes. NetBackup can continue to use the disk pool, although the disk pool may no longer match the storage unit or storage lifecycle purpose.

The following table describes the possible outcomes and how to resolve them.

Table 8-2 Refresh outcomes

Outcome	Description
No changes are discovered.	No changes are required.
NetBackup discovers the new volumes that you can add to the disk pool.	The new volumes appear in the **Change Disk Pool** dialog box. Text in the dialog box changes to indicate that you can add the new volumes to the disk pool.

Table 8-2 Refresh outcomes *(continued)*

Outcome	Description
The replication properties of all of the volumes changed, but they are still consistent.	A **Disk Pool Configuration Alert** pop-up box notifies you that the properties of all of the volumes in the disk pool changed, but they are all the same (homogeneous). You must click **OK** in the alert box, after which the disk pool properties in the **Change Disk Pool** dialog box are updated to match the new volume properties If new volumes are available that match the new properties, NetBackup displays those volumes in the **Change Disk Pool** dialog box. You can add those new volumes to the disk pool. In the **Change Disk Pool** dialog box, select one of the following two choices: ■ **OK**. To accept the disk pool changes, click **OK** in the **Change Disk Pool** dialog box. NetBackup saves the new properties of the disk pool. NetBackup can use the disk pool, but it may no longer match the intended purpose of the storage unit or storage lifecycle policy. Change the storage lifecycle policy definitions to ensure that the replication operations use the correct source and target disk pools, storage units, and storage unit groups. Alternatively, work with your storage administrator to change the volume properties back to their original values. ■ **Cancel**. To discard the changes, click **Cancel** in the **Change Disk Pool** dialog box. NetBackup does not save the new disk pool properties. NetBackup can use the disk pool, but it may no longer match the intended use of the storage unit or storage lifecycle policy.

Table 8-2 Refresh outcomes *(continued)*

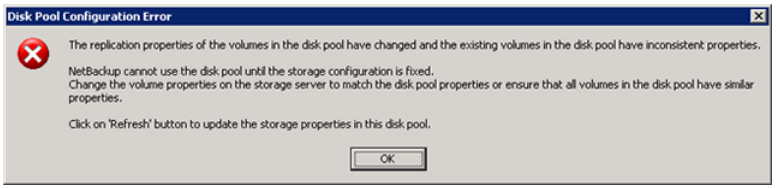
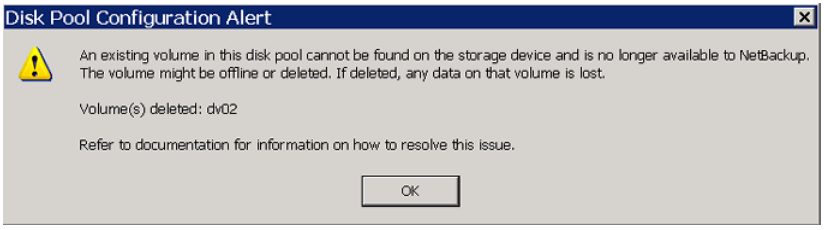
Outcome	Description
The replication properties of the volumes changed, and they are now inconsistent.	A **Disk Pool Configuration Error** pop-up box notifies you that the replication properties of some of the volumes in the disk pool changed. The properties of the volumes in the disk pool are not homogeneous.  You must click **OK** in the alert box. In the **Change Disk Pool** dialog box, the properties of the disk pool are unchanged, and you cannot select them (that is, they are dimmed). However, the properties of the individual volumes are updated. Because the volume properties are not homogeneous, NetBackup cannot use the disk pool until the storage configuration is fixed. NetBackup does not display new volumes (if available) because the volumes already in the disk pool are not homogeneous. To determine what has changed, compare the disk pool properties to the volume properties. See "Viewing the replication topology for Auto Image Replication" on page 159. Work with your storage administrator to understand the changes and why they were made. The replication relationships may or may not have to be re-established. If the relationship was removed in error, re-establishing the relationships seem justified. If you are retiring or replacing the target replication device, you probably do not want to re-establish the relationships. The disk pool remains unusable until the properties of the volumes in the disk pool are homogenous. In the **Change Disk Pool** dialog box, click **OK** or **Cancel** to exit the **Change Disk Pool** dialog box.

Table 8-2 Refresh outcomes *(continued)*

Outcome	Description
NetBackup cannot find a volume or volumes that were in the disk pool.	A **Disk Pool Configuration Alert** pop-up box notifies you that an existing volume or volumes was deleted from the storage device:  NetBackup can use the disk pool, but data may be lost. To protect against accidental data loss, NetBackup does not allow volumes to be deleted from a disk pool. To continue to use the disk pool, do the following: ■ Use the `bpimmedia` command or the Images on Disk report to display the images on the specific volume. ■ Expire the images on the volume. ■ Use the `nbdevconfig` command to set the volume state to DOWN so NetBackup does not try to use it.

Clearing a Media Server Deduplication Pool attribute

You may have to clear attributes on your existing media server deduplication pools.

To clear a Media Server Deduplication Pool attribute

◆ The following is the command syntax to clear a deduplication pool attribute. Run the command on the master server or on the storage server.

```
nbdevconfig -changedp -dp pool_name -stype PureDisk
-clearattribute attribute
```

The following describe the options that require your input:

`-changedp` *`pool_name`*	The name of the disk pool.
`-setattribute` *`attribute`*	The *attribute* is the name of the argument that represents the new functionality.

The following is the path to the `nbdevconfig` command:

- UNIX: `/usr/openv/netbackup/bin/admincmd`
- Windows: *`install_path`*`\NetBackup\bin\admincmd`

Determining the MSDP disk volume state

Use the NetBackup `nbdevquery` command to determine the state of the volume in a deduplication disk pool. NetBackup exposes all of the storage for MSDP as a single volume, **PureDiskVolume**. The command shows the properties and attributes of the **PureDiskVolume**.

To determine MSDP disk volume state

- Display the volume state by using the following command:

  UNIX: `/usr/openv/netbackup/bin/admincmd/nbdevquery -listdv -stype PureDisk -U -dp` *`disk_pool_name`*

  Windows: *`install_path`*`\NetBackup\bin\admincmd\nbdevquery -listdv -stype PureDisk -U -dp` *`disk_pool_name`*

  The *state* is either UP or DOWN.

  The following is example output

```
Disk Pool Name      : MSDP_Disk_Pool
Disk Type           : PureDisk
Disk Volume Name    : PureDiskVolume
Disk Media ID       : @aaaab
Total Capacity (GB) : 49.98
Free Space (GB)     : 43.66
Use%                : 12
Status              : UP
Flag                : ReadOnWrite
Flag                : AdminUp
Flag                : InternalUp
Num Read Mounts     : 0
Num Write Mounts    : 1
Cur Read Streams    : 0
Cur Write Streams   : 0
```

Changing the MSDP disk volume state

The disk volume state is **UP** or **DOWN**. NetBackup exposes all of the storage for MSDP as a single volume, **PureDiskVolume**.

To change the state to **DOWN**, the disk pool in which the volume resides must not be busy. If backup jobs are assigned to the disk pool, the state change fails. Cancel the backup jobs or wait until the jobs complete.

To change the MSDP disk volume state

- Change the disk volume state; the following is the command syntax:

  UNIX: `/usr/openv/netbackup/bin/admincmd/nbdevconfig -changestate -stype PureDisk -dp disk_pool_name -dv PureDiskVolume -state state`

  Windows: `install_path\NetBackup\bin\admincmd\nbdevconfig -changestate -stype PureDisk -dp disk_pool_name -dv PureDiskVolume -state state`

  For the `-state`, specify either **UP** or **DOWN**.

Inventorying a NetBackup disk pool

An inventory of a NetBackup disk pool reads the capacity of the disk volumes in the pool. An inventory operation lets you update NetBackup with the new capacity values if you do the following:

- Increase or decrease the size of the disk volumes in a disk pool.
- Add volumes to or remove volumes from a disk pool.

How you increase or decrease the underlying storage capacity depends on your storage implementation. You must complete that process before you inventory the disk pool.

To inventory a NetBackup disk pool

1. in the **NetBackup Administration Console**, select **Media and Device Management** > **Devices** > **Disk Pools**.
2. On the **Actions** menu, select **Inventory Disk Pools**.
3. In the **Inventory Disk Pool** dialog box, select the disk pool to inventory and then click **Start Inventory.**
4. To update the NetBackup catalog with the capacity values returned by the inventory, click **Update Configuration**.
5. To inventory another disk pool, go to step 3.
6. To exit, click **Close**.

Deleting a Media Server Deduplication Pool

You can delete a disk pool if it does not contain valid NetBackup backup images or image fragments. If it does, you must first expire and delete those images or fragments. If expired image fragments remain on disk, you must remove those also.

See "Cannot delete an MSDP disk pool" on page 362.

If you delete a disk pool, NetBackup removes it from your configuration.

If a disk pool is the storage destination of a storage unit, you must first delete the storage unit.

To delete an MSDP disk pool

1. In the **NetBackup Administration Console**, expand **Media and Device Management > Devices > Disk Pools**.
2. Select a disk pool
3. On the **Edit** menu, select **Delete**.
4. In the **Delete Disk Pool** dialog box, verify that the disk pool is the one you want to delete and then click **OK**.

Deleting backup images

Image deletion may be time consuming. Therefore, if you delete images manually, Veritas recommends the following approach.

See "About the MSDP data removal process" on page 312.

To delete backup images manually

1. Expire all of the images by using the `bpexpdate` command and the `-notimmediate` option. The `-notimmediate` option prevents `bpexpdate` from calling the `nbdelete` command, which deletes the image.

   Without this option, `bpexpdate` calls `nbdelete` to delete images. Each call to `nbdelete` creates a job in the Activity Monitor, allocates resources, and launches processes on the media server.

2. After you expire the last image, delete all of the images by using the `nbdelete` command with the `-allvolumes` option.

   Only one job is created in the Activity Monitor, fewer resources are allocated, and fewer processes are started on the media servers. The entire process of expiring images and deleting images takes less time.

About MSDP queue processing

Operations that require database updates accumulate in a transaction queue. Twice a day, the NetBackup Deduplication Manager directs the Deduplication Engine to process the queue as one batch. By default, queue processing occurs every 12 hours, 20 minutes past the hour.

Primarily, the transaction queue contains clean-up and integrity checking transactions. These transactions update the reference database.

Queue processing writes status information to the deduplication engine `storaged.log` file.

See "NetBackup MSDP log files" on page 347.

Because queue processing does not block any other deduplication process, rescheduling should not be necessary. Users cannot change the maintenance process schedules. However, if you must reschedule these processes, contact your Veritas support representative.

Because queue processing occurs automatically, you should not need to invoke it manually. However, you may do so.

See "Processing the MSDP transaction queue manually" on page 303.

See "About MSDP server requirements" on page 25.

Processing the MSDP transaction queue manually

NetBackup maintains a queue for MSDP database transactions.

See "About MSDP queue processing" on page 303.

Usually, you should not need to run the deduplication database transaction queue processes manually. However, when you recover the MSDP catalog from a backup, you must process the MSDP transaction queue. Processing the transaction queue is part of a larger process.

To process the MSDP transaction queue manually

1. On the MSDP storage server, run the following command:

   UNIX: `/usr/openv/pdde/pdcr/bin/crcontrol --processqueue`

   Windows: *`install_path`*`\Veritas\pdde\Crcontrol.exe --processqueue`

2. To determine if the queue processing is still active, run the following command:

   UNIX: `/usr/openv/pdde/pdcr/bin/crcontrol --processqueueinfo`

   Windows: *`install_path`*`\Veritas\pdde\Crcontrol.exe --processqueueinfo`

   If the output shows `Busy : yes`, the queue is still active.

3. To examine the results, run the following command (number 1 not lowercase letter l):

   UNIX: `/usr/openv/pdde/pdcr/bin/crcontrol --dsstat 1`

   Windows: *`install_path`*`\Veritas\pdde\Crcontrol.exe --dsstat 1`

   The command may run for a long time; if you omit the `1`, results return more quickly but they are not as accurate.

About MSDP data integrity checking

Deduplication metadata and data may become inconsistent or corrupted because of disk failures, I/O errors, database corruption, and operational errors. NetBackup checks the integrity of the deduplicated data on a regular basis. NetBackup performs some of the integrity checking when the storage server is idle. Other integrity checking is designed to use few storage server resources so as not to interfere with operations.

The data integrity checking process includes the following checks and actions:

- Automatically constrains data loss or corruption to ensure that new backups are intact.
- Automatically runs a cyclic redundancy check (CRC) for the data containers.
- Automatically collects and cleans up storage garbage.
- Automatically recovers the container-based reference database (or parts of the database) if it is corrupt or missing.
- Automatically finds storage leaks and fixes them.

NetBackup resolves many integrity issues without user intervention, and some issues are fixed when the next backup runs. However, a severe issue may require

intervention by Veritas Support. In such cases, NetBackup writes a message to the NetBackup Disk Logs report.

See "Viewing MSDP disk reports" on page 275.

The data integrity message code is 1057.

See "MSDP event codes and messages" on page 370.

NetBackup writes the integrity checking activity messages to the NetBackup Deduplication Engine `storaged.log` file.

See "NetBackup MSDP log files" on page 347.

You can configure some of the data integrity checking behaviors.

See "Configuring MSDP data integrity checking behavior" on page 305.

Configuring MSDP data integrity checking behavior

NetBackup performs several data integrity checks. You can configure the behavior of the integrity checks.

Two methods exist to configure MSDP data integrity checking behavior, as follows:

- Run a command.
  See "To configure data integrity checking behavior by using a command" on page 305.
- Edit configuration file parameters.
  See "To configure data integrity checking behavior by editing the configuration files" on page 307.

Warning: Veritas recommends that you do not disable the data integrity checking. If you do so, NetBackup cannot find and repair or report data corruption.

See "About MSDP data integrity checking" on page 304.

See "MSDP data integrity checking configuration parameters" on page 307.

To configure data integrity checking behavior by using a command

- To configure behavior, specify a value for each of the data integrity checks, as follows:
  - Data consistency checking. Use the following commands to configure behavior:

Enable	UNIX: `/usr/openv/pdde/pdcr/bin/pddecfg -a enabledataintegritycheck` Windows: *`install_path`*`\Veritas\pdde\pddecfg -a enabledataintegritycheck`
Disable	UNIX: `/usr/openv/pdde/pdcr/bin/pddecfg -a disabledataintegritycheck` Windows: *`install_path`*`\Veritas\pdde\pddecfg -a disabledataintegritycheck`
Get the status	UNIX: `/usr/openv/pdde/pdcr/bin/pddecfg -a getdataintegritycheck` Windows: *`install_path`*`\Veritas\pdde\pddecfg -a getdataintegritycheck`

- Cyclic redundancy checking. Use the following commands to configure behavior:

Enable	CRC does not run if queue processing is active or during disk read or write operations. UNIX: `/usr/openv/pdde/pdcr/bin/crcontrol --crccheckon` Windows: *`install_path`*`\Veritas\pdde\Crcontrol.exe --crccheckon`
Disable	UNIX: `/usr/openv/pdde/pdcr/bin/crcontrol --crccheckoff` Windows: *`install_path`*`\Veritas\pdde\Crcontrol.exe --crccheckoff`
Enable fast checking	Fast check CRC mode begins the check from container 64 and does not sleep between checking containers. When the fast CRC ends, CRC behavior reverts to the behavior before fast checking was invoked. UNIX: `/usr/openv/pdde/pdcr/bin/crcontrol --crccheckrestart` Windows: *`install_path`*`\Veritas\pdde\Crcontrol.exe --crccheckrestart`

Get the status	UNIX: `/usr/openv/pdde/pdcr/bin/crcontrol --crccheckstate` Windows: *install_path*`\Veritas\pdde\Crcontrol.exe --crccheckstate`

To configure data integrity checking behavior by editing the configuration files

1. Use a text editor to open the `contentrouter.cfg` file or the `spa.cfg` file, which control the data integrity checking behavior.

   The files reside in the following directories:

   - UNIX: *storage_path*`/etc/puredisk`
   - Windows: *storage_path*`\etc\puredisk`

2. To change a parameter, specify a new value.

   See "MSDP data integrity checking configuration parameters" on page 307.

3. Save and close the file.

4. Restart the NetBackup Deduplication Engine and the NetBackup Deduplication Manager.

   You can do this from the **Daemons** tab in the **Activity Monitor**.

MSDP data integrity checking configuration parameters

The configuration file parameters that control the deduplication data integrity checking are in two different configuration files, as follows:

- The `contentrouter.cfg` file.
  The parameters are described in Table 8-3.
  See "About the MSDP contentrouter.cfg file" on page 215.
- The `spa.cfg` file.
  The parameters are described in Table 8-3.

Those files reside in the following directories:

- UNIX: *storage_path*`/etc/puredisk`
- Windows: *storage_path*`\etc\puredisk`

Warning: Veritas recommends that you do not disable the data integrity checking. If you do so, NetBackup cannot find and repair or report data corruption.

See “About MSDP data integrity checking” on page 304.

Table 8-3 The contentrouter.cfg file parameters for data integrity checking

Setting	Default	Description
EnableCRCCheck	true	Enable or disable cyclic redundancy checking (CRC) of the data container files. The possible values are true or false. CRC occurs only when no backup, restore, or queue processing jobs are running.
CRCCheckSleepSeconds	5	The time in seconds to sleep between checking containers. The longer the sleep interval, the more time it takes to check containers.
CRCCheckBatchNum	40	The number of containers to check each time. The greater the number of containers, the less time it takes to check all containers, but the more system resources it takes.
ShutdownCRWhenError	false	Stops the NetBackup Deduplication Manager when a data loss is discovered. This parameter is reserved for debugging purposes by Veritas Support Representatives. The possible values are true or false.
GarbageCheckRemainDCCount	100	The number of containers from failed jobs not to check for garbage. A failed backup or replication job still produces data containers. Because failed jobs are retried, retaining those containers means NetBackup does not have to send the fingerprint information again. As a result, retried jobs consume less time and fewer system resources than when first run.

Table 8-4 spa.cfg file parameters for data integrity checking

Setting	Default	Description
EnableDataCheck	true	Enable or disable data consistency checking. The possible values are True or False.
DataCheckDays	14	The number of days to check the data for consistency. The greater the number of days, the fewer the objects that are checked each day. The greater the number of days equals fewer storage server resources consumed each day.

Table 8-4 spa.cfg file parameters for data integrity checking *(continued)*

Setting	Default	Description
`EnableDataCheckAlert`	`true`	Enable or disable alerts. If `true`, NetBackup writes a message to the Disk Logs report when it detects a lost data segment. See "NetBackup MSDP log files" on page 347.

About managing MSDP storage read performance

NetBackup provides some control over the processes that are used for read operations. The read operation controls can improve performance for the jobs that read from the storage. Such jobs include restore jobs, duplication jobs, and replication jobs.

In most cases, you should change configuration file options only when directed to do so by a Veritas support representative.

Defragment the storage

NetBackup includes a process, called *rebasing*, which defragments the backup images in a deduplication pool. Read performance improves when the file segments from a client backup are close to each other on deduplication storage.

See "About MSDP storage rebasing" on page 309.

Decrypt the data on the client rather than the server

The `RESTORE_DECRYPT_LOCAL` parameter in the `pd.conf` file specifies on which host to decrypt and decompress the data during restore operations.

See "About the MSDP pd.conf configuration file" on page 197.

See "MSDP pd.conf file parameters" on page 198.

About MSDP storage rebasing

During an initial backup, NetBackup writes the data segments from a backup to as few container files as possible. Read performance is best when the data segments from a client backup are close to each other on deduplication storage. NetBackup consumes less time finding and reassembling backed up files when their segments are near each other.

However, the data segments in a backup may become scattered across the disk storage each time the client is backed up. Such scattering is a normal consequence of deduplication.

NetBackup includes a process, called *rebasing*, that helps to maintain the data segments in as few container files as possible. Rebasing improves performance for the operations that read from the storage, such as restores and duplications. NetBackup writes all of the data segments from a backup into new container files even though the segments exist on storage already. Future backups then refer to the new copies of those segments rather than the old copies until any changes because of future rebasing. Deduplication rates for the backup jobs that perform rebasing are lower than for the jobs that do not rebase the data.

After the rebasing, NetBackup reclaims the storage space that the rebased data segments used.

Table 8-5 describes the rebasing operations.

Table 8-5 Types of rebasing

Type	Description
Normal backup rebasing	The rebasing that occurs during a backup if the normal rebasing criteria are met, as follows: ■ The container has been rebased within the last 3 months. ■ For that backup, the data segments in the container consume less space than the `FP_CACHE_PERIOD_REBASING_THRESHOLD` value. The `FP_CACHE_PERIOD_REBASING_THRESHOLD` parameter is in the `pd.conf` file. See "MSDP pd.conf file parameters" on page 198. Backup rebasing occurs only for the full backups that pass through the normal MSDP backup process. For example, the NetBackup Accelerator backups do not pass through the MSDP backup process. NetBackup reports backup job completion after the rebasing is completed.

Table 8-5 Types of rebasing *(continued)*

Type	Description
Periodic backup rebasing	The rebasing that occurs during a backup if the periodic rebasing criteria are met, as follows: ■ The container has not been rebased within the last 3 months. ■ For that backup, the data segments in the container consume less space than the `FP_CACHE_REBASING_THRESHOLD` value. The `FP_CACHE_REBASING_THRESHOLD` parameter is in the `pd.conf` file. See "MSDP pd.conf file parameters" on page 198. Backup rebasing occurs only for the full backups that pass through the normal MSDP backup process. For example, the NetBackup Accelerator backups do not pass through the MSDP backup process. NetBackup reports backup job completion after the rebasing is completed.
Server-side rebasing	The storage rebasing that occurs on the server if the rebasing criteria are met. Server-side rebasing includes the deduplicated data that does not pass through the normal MSDP backup process. For example, the NetBackup Accelerator backups do not pass through the MSDP backup process. Some parameters in the `contentrouter.cfg` file control the server-side rebasing behavior. See "MSDP server-side rebasing parameters" on page 311.

MSDP server-side rebasing parameters

Table 8-6 describes the parameters that control server-side rebasing.

See "About MSDP storage rebasing" on page 309.

Usually, you do not need to change parameter values. However, in some cases, you may be directed to change settings by a Veritas support representative.

The parameters are stored in the `contentrouter.cfg` file.

See "About the MSDP contentrouter.cfg file" on page 215.

Table 8-6 The server-side rebasing parameters

Parameter	Description
`RebaseMaxPercentage`	The maximum percentage of the data segments to be rebased in a file. For any file, if the percentage of the data segments reaches this threshold, the remainder of the data segments are not rebased. By default, this parameter is `RebaseMaxPercentage=5`.
`RebaseMaxTime`	The maximum time span in seconds of data segments to be rebased in a file. If this threshold is reached, NetBackup does not rebase the remainder of the data segments. By default, this parameter is `RebaseMaxTime=150`.
`RebaseMinContainers`	The minimum number of containers in which a file's data segments are stored for the file to be eligible for rebasing. If the number of containers in which a file's data segments are stored is less than `RebaseMinContainers`, NetBackup does not rebase the data segments. By default, this parameter is `RebaseMinContainers=4`.
`RebaseScatterThreshold`	The data locality threshold for a container. If the total size of a file's data segments in a container is less than `RebaseScatterThreshold`, NetBackup rebases all of the file's data segments. By default, this parameter is `RebaseScatterThreshold=64MB`.

About the MSDP data removal process

The data removal process removes the data segments that comprise a NetBackup backup image. Only those segments that are not referred to by a backup image are removed.

The following list describes the data removal process for expired backup images:

- NetBackup removes the image record from the NetBackup catalog.
  NetBackup directs the NetBackup Deduplication Manager to remove the image.
- The deduplication manager immediately removes the image entry in the deduplication catalog and adds a removal request to the NetBackup Deduplication Engine's transaction queue.
  From this point on, the expired backup image is no longer accessible.
- When the NetBackup Deduplication Engine processes the queue, all of the removal requests are processed. A removal request for the image is not generated again.

During the queue processing, the Deduplication Engine reclaims some of the storage space on which the data segments reside. Some is reclaimed during data compaction. If a different backup image requires a data segment, the segment is not removed.

Various internal parameters control whether a container file is compacted.

See "About MSDP container files" on page 273.

If you manually delete an image that has expired within the previous 24 hours, the data becomes garbage. It remains on disk until removed by the next garbage collection process. Garbage collection occurs during data integrity checking.

See "About MSDP data integrity checking" on page 304.

See "Deleting backup images" on page 302.

Resizing the MSDP storage partition

If the volume that contains the deduplication storage is resized dynamically, restart the NetBackup services on the storage server. You must restart the services so that NetBackup can use the resized partition correctly. If you do not restart the services, NetBackup reports the capacity as full prematurely.

To resize the MSDP storage

1. Stop all NetBackup jobs on the storage on which you want to change the disk partition sizes and wait for the jobs to end.
2. Deactivate the media server that hosts the storage server.

   See the *NetBackup Administrator's Guide, Volume I*:

   http://www.veritas.com/docs/DOC5332
3. Stop the NetBackup services on the storage server.

   Be sure to wait for all services to stop.
4. Use the operating system or disk manager tools to dynamically increase or decrease the deduplication storage area.
5. Restart the NetBackup services.
6. Activate the media server that hosts the storage server.

   See the *NetBackup Administrator's Guide, Volume I*:

   http://www.veritas.com/docs/DOC5332
7. Restart the deduplication jobs.

See "About adding additional MSDP storage" on page 44.

How MSDP restores work

The following two methods exist to for MSDP restore operations:

Table 8-7 MSDP restore types

Type	Description
Normal restore	The MSDP storage server first *rehydrates* (that is, reassembles) the data. NetBackup then chooses the least busy media server to move the data to the client. (NetBackup chooses the least busy media server from those that have credentials for the NetBackup Deduplication Engine.) The media server `bptm` process moves the data to the client. The following media servers have credentials for the NetBackup Deduplication Engine: ■ The media server that hosts the storage server. Although the media server and the storage server share a host, the storage server sends the data through the media server `bptm` process on that host. ■ A load balancing server in the same deduplication node. See "About MSDP load balancing servers" on page 25. ■ A deduplication server in a different deduplication node that is the target of optimized duplication. See "About the media servers for MSDP optimized duplication within the same domain" on page 138. You can specify the server to use for restores. See "Specifying the restore server" on page 316.
Restore directly to the client	The storage server can bypass the media server and move the data directly to the client. NetBackup does not choose a media server for the restore, and the restore does not use the media server `bptm` process. You must configure NetBackup to bypass a media server and receive the restore data directly from the storage server. See "Configuring MSDP restores directly to a client" on page 315. By default, NetBackup rehydrates the data on the storage server except for client-side deduplication clients. Those clients rehydrate the data. You can configure NetBackup so that the data is rehydrated on the storage server rather than the client. See the `RESTORE_DECRYPT_LOCAL` parameter in the MSDP `pd.conf` file. See "MSDP pd.conf file parameters" on page 198. See "Editing the MSDP pd.conf file" on page 198.

Configuring MSDP restores directly to a client

The NetBackup MSDP storage server can move restore data directly to an MSDP client, bypassing the media server components.

See "How MSDP restores work" on page 314.

To enable restores directly to a client

1. Set the `OLD_VNETD_CALLBACK` option to `YES` on the client. The `OLD_VNETD_CALLBACK` option is stored in the `bp.conf` file on UNIX systems and the registry on Windows systems.

   See "Setting NetBackup configuration options by using the command line" on page 149.

2. On the master server, run the following command to configure NetBackup to use client-direct restores for the client:

   UNIX: `/usr/openv/netbackup/bin/admincmd/bpclient -client` *`client_name`* `-update -client_direct_restore 2`

   Windows: *`install_path`*`\NetBackup\bin\admincmd\bpclient -client` *`client_name`* `-update -client_direct_restore 2`

About restoring files at a remote site

If you use optimized duplication to copy images from a local site to a remote site, you can restore from the copies at the remote site to clients at the remote site. To do so, use a server-directed restore or a client-redirected restore, which restores files to a client other than the original client.

Information about how to redirect restores is in a different guide.

See "Managing client restores" in the *NetBackup Administrator's Guide, Volume I*:

http://www.veritas.com/docs/DOC5332

You may have to configure which media server performs the restore. In optimized duplication, the media server that initiates the duplication operation becomes the write host for the new image copies. The write host restores from those image copies. If the write host is at the local site, it restores from those images at the remote site to the alternate client at the remote site. That host reads the image across the WAN and then writes the image back across the WAN to the alternate client. In this case, you can specify that the media server at the remote site as the restore server.

About restoring from a backup at a target master domain

While it is possible to restore a client directly by using the images in the target master domain, do so only in a disaster recovery situation. In this discussion, a disaster recovery situation is one in which the originating domain no longer exists and clients must be recovered from the target domain

Table 8-8 Client restores in disaster recovery scenarios

Disaster recovery scenario	Does client exist?	Description
Scenario 1	Yes	Configure the client in another domain and restore directly to the client.
Scenario 2	No	Create the client in the recovery domain and restore directly to the client. This is the most likely scenario.
Scenario 3	No	Perform an alternate client restore in the recovery domain.

The steps to recover the client are the same as any other client recovery. The actual steps depend on the client type, the storage type, and whether the recovery is an alternate client restore.

For restores that use Granular Recovery Technology (GRT), an application instance must exist in the recovery domain. The application instance is required so that NetBackup has something to recover to.

Specifying the restore server

NetBackup may not use the backup server as the restore server for deduplicated data.

See “How MSDP restores work” on page 314.

You can specify the server to use for restores. The following are the methods that specify the restore server:

- Always use the backup server. Two methods exist, as follows:
  - Use NetBackup **Host Properties** to specify a **Media host override** server. All restore jobs for any storage unit on the original backup server use the media server you specify. Specify the same server for the **Restore server** as for the **Original backup server**.
    See “Forcing restores to use a specific server” in the *NetBackup Administrator's Guide, Volume I*:

http://www.veritas.com/docs/DOC5332

This procedure sets the `FORCE_RESTORE_MEDIA_SERVER` option. Configuration options are stored in the `bp.conf` file on UNIX systems and the registry on Windows systems.

- Create the touch file `USE_BACKUP_MEDIA_SERVER_FOR_RESTORE` on the NetBackup master server in the following directory:

  UNIX: `usr/openv/netbackup/db/config`

  Windows: *`install_path`*`\veritas\netbackup\db\config`

  This global setting always forces restores to the server that did the backup. It applies to all NetBackup restore jobs, not just deduplication restore jobs. If this touch file exists, NetBackup ignores the `FORCE_RESTORE_MEDIA_SERVER` and `FAILOVER_RESTORE_MEDIA_SERVER` settings.

- Always use a different server.

  Use NetBackup **Host Properties** to specify a **Media host override** server. See the previous explanation about **Media host override**, except: Specify the different server for the **Restore server**.

- A single restore instance. Use the `bprestore` command with the `-disk_media_server` option.

  Restore jobs for each instance of the command use the media server you specify. See the *NetBackup Commands Reference Guide*:

  http://www.veritas.com/docs/DOC5332

Chapter 9

Recovering MSDP

This chapter includes the following topics:

- About recovering the MSDP catalog
- Restoring the MSDP catalog from a shadow copy
- Recovering from an MSDP storage server disk failure
- Recovering from an MSDP storage server failure
- Recovering the MSDP storage server after NetBackup catalog recovery

About recovering the MSDP catalog

The following are the recovery options for the NetBackup MSDP catalog:

Table 9-1 MSDP catalog backup recovery options

Recovery option	Description
Restore from a shadow copy	If NetBackup detects corruption in the MSDP catalog, the Deduplication Manager restores the catalog automatically from the most recent shadow copy. The automatic restore process also plays a transaction log so that the recovered MSDP catalog is current. Although the shadow copy restore process is automatic, a restore procedure is available if you need to recover from a shadow copy manually. See "About the MSDP shadow catalog" on page 221. See "Restoring the MSDP catalog from a shadow copy" on page 319.

Table 9-1 MSDP catalog backup recovery options *(continued)*

Recovery option	Description
Recover from a backup	If you configured an MSDP catalog backup policy and a valid backup exists, you can recover the catalog from a backup. As a general rule, you should only attempt to recover the MSDP catalog from a backup if you have no alternatives. As an example: A hardware problem or a software problem results in the complete loss of the MSDP catalog and the shadow copies. The greatest chance for a successful outcome when you recover the MSDP catalog from a backup is when the recovery is guided. An unsuccessful outcome may cause data loss. For the customers who need to recover the MSDP catalog, Veritas wants to guide them through the process. Therefore, to recover the MSDP catalog from a backup, contact your Veritas support representative. You can refer the support representative to Knowledge Base Article 000047346, which contains the recovery instructions.

Caution: You must determine if your situation is severe enough to recover the catalog. Veritas recommends that you contact your Veritas Support representative before you restore or recover the MSDP catalog. The Support representative can help you determine if you need to recover the catalog or if other solutions are available.

See "About protecting the MSDP catalog" on page 221.

Restoring the MSDP catalog from a shadow copy

NetBackup automatically restores the necessary parts of the MSDP catalog if corruption is detected. However, you can restore the MSDP catalog from a shadow copy manually, although in normal circumstances it is not necessary. Veritas recommends that you contact your Veritas Support representative before you restore all or part of the MSDP catalog from a shadow copy.

The procedure that you use depends on the restore scenario, as follows:

Restore the entire MSDP catalog from a shadow copy	In this scenario, you want to restore the entire catalog from one of the shadow copies. See "To restore the entire MSDP catalog from a shadow copy" on page 320.

Restore a specific MSDP database file	The MSDP catalog is composed of multiple small database files. Those files are organized in the file system by the client name and policy name, as follows: UNIX: */database_path*/databases/catalogshadow/2/*ClientName*/*PolicyName* Windows: *database_path*\databases\catalogshadow\2*ClientName**PolicyName* You can restore the database files for a client and a policy combination. The restore of a specific client's and policy's database files is always from the most recent shadow copy. See "To restore a specific MSDP database file from a shadow copy" on page 320.

See "About recovering the MSDP catalog" on page 318.

To restore the entire MSDP catalog from a shadow copy

1. If any MSDP jobs are active, either cancel them or wait until they complete.
2. Disable all policies and storage lifecycle policies that back up to the **Media Server Deduplication Pool**.
3. On the MSDP storage server, run the following command, depending on host type:
   - UNIX: `/usr/openv/pdde/pdcr/bin/cacontrol --catalog recover all`
   - Windows: *install_path*`\Veritas\pdde\cacontrol --catalog recover all`
4. Enable all policies and storage lifecycle policies that back up to the **Media Server Deduplication Pool**.
5. Restart the jobs that were canceled before the recovery.

To restore a specific MSDP database file from a shadow copy

1. If any MSDP jobs are active for the client and the backup policy combination, either cancel them or wait until they complete.
2. Disable the policies and storage lifecycle policies for the client and the backup policy combination that back up to the **Media Server Deduplication Pool**.

3 Change to the shadow directory for the client and policy from which you want to recover that database file. That directory contains the database files from which to recover. The following are the pathname formats:

UNIX:
`/database_path/databases/catalogshadow/2/ClientName/PolicyName`

Windows:
`database_path\databases\catalogshadow\2\ClientName\PolicyName`

4 Run the following command, depending on host type:

- UNIX: `/usr/openv/pdde/pdcr/bin/cacontrol --catalog recover 2 "/ClientName/PolicyName"`
- Windows: `install_path\Veritas\pdde\cacontrol --catalog recover 2 "\ClientName\PolicyName"`

5 Enable all policies and storage lifecycle policies that back up to the **Media Server Deduplication Pool**.

6 If you canceled jobs before you recovered the database files, restart them.

Recovering from an MSDP storage server disk failure

If recovery mechanisms do not protect the disk on which the NetBackup software resides, the deduplication storage server configuration is lost if the disk fails. This topic describes how to recover from a system disk or program disk failure where the disk was not backed up.

Note: This procedure describes recovery of the disk on which the NetBackup media server software resides not the disk on which the deduplicated data resides. The disk may or may not be the system boot disk.

After recovery, your NetBackup deduplication environment should function normally. Any valid backup images on the deduplication storage should be available for restores.

Veritas recommends that you use NetBackup to protect the deduplication storage server system or program disks. You then can use NetBackup to restore that media server if the disk on which NetBackup resides fails and you have to replace it.

Table 9-2 Process to recover from media server disk failure

Step	Task	Procedure
Step 1	Replace the disk.	If the disk is a system boot disk, also install the operating system. See the hardware vendor and operating system documentation.
Step 2	Mount the storage.	Ensure that the storage and database are mounted at the same locations. See the storage vendor's documentation.
Step 3	Install and license the NetBackup media server software.	See *NetBackup Installation Guide for UNIX and Windows*: http://www.veritas.com/docs/DOC5332 See "About the MSDP license" on page 46.
Step 4	Delete the deduplication host configuration file	Each load balancing server contains a deduplication host configuration file. If you use load balancing servers, delete the deduplication host configuration file from those servers. See "Deleting an MSDP host configuration file" on page 219.
Step 5	Delete the credentials on deduplication servers	If you have load balancing servers, delete the NetBackup Deduplication Engine credentials on those media servers. See "Deleting credentials from a load balancing server" on page 290.
Step 6	Add the credentials to the storage server	Add the NetBackup Deduplication Engine credentials to the storage server. See "Adding NetBackup Deduplication Engine credentials" on page 289.
Step 7	Get a configuration file template	If you did not save a storage server configuration file before the disk failure, get a template configuration file. See "Saving the MSDP storage server configuration" on page 216.
Step 8	Edit the configuration file	See "Editing an MSDP storage server configuration file" on page 217.
Step 9	Configure the storage server	Configure the storage server by uploading the configuration from the file you edited. See "Setting the MSDP storage server configuration" on page 218.
Step 10	Add load balancing servers	If you use load balancing servers in your environment, add them to your configuration. See "Adding an MSDP load balancing server" on page 194.

Recovering from an MSDP storage server failure

To recover from a permanent failure of the storage server host computer, use the process that is described in this topic.

NetBackup recommends that you consider the following items before you recover:

- The new computer must use the same byte order as the old computer.

  Warning: If the new computer does not use the same byte order as the old computer, you cannot access the deduplicated data. In computing, endianness describes the byte order that represents data: big endian and little endian. For example, SPARC processors and Intel processors use different byte orders. Therefore, you cannot replace an Oracle Solaris SPARC host with an Oracle Solaris host that has an Intel processor.

- Veritas recommends that the new computer use the same operating system as the old computer.
- Veritas recommends that the new computer use the same version of NetBackup as the old computer.
  If you use a newer version of NetBackup on the new computer, ensure that you perform any data conversions that may be required for the newer release.
  If you want to use an older version of NetBackup on the replacement host, contact your Veritas support representative.

Table 9-3 Recover from an MSDP storage server failure

Step	Task	Procedure
Step 1	Expire the backup images	Expire all backup images that reside on the deduplication disk storage. **Warning:** Do not delete the images. They are imported back into NetBackup later in this process. If you use the `bpexpdate` command to expire the backup images, use the `-nodelete` parameter. See the *NetBackup Administrator's Guide, Volume I*: http://www.veritas.com/docs/DOC5332
Step 2	Delete the storage units that use the disk pool	See the *NetBackup Administrator's Guide, Volume I*: http://www.veritas.com/docs/DOC5332
Step 3	Delete the disk pool	See "Deleting a Media Server Deduplication Pool" on page 302.
Step 4	Delete the deduplication storage server	See "Deleting an MSDP storage server" on page 287.

Table 9-3 Recover from an MSDP storage server failure *(continued)*

Step	Task	Procedure
Step 5	Delete the deduplication host configuration file	Each load balancing server contains a deduplication host configuration file. If you use load balancing servers, delete the deduplication host configuration file from those servers. See "Deleting an MSDP host configuration file" on page 219.
Step 6	Delete the credentials on deduplication servers	If you have load balancing servers, delete the NetBackup Deduplication Engine credentials on those media servers. See "Deleting credentials from a load balancing server" on page 290.

Step 7	Configure the new host so it meets deduplication requirements	When you configure the new host, consider the following:
		■ You can use the same host name or a different name.
		■ You can use the same **Storage Path** or a different **Storage Path**. If you use a different **Storage Path**, you must move the deduplication storage to that new location.
		■ If the **Database Path** on the original host is different that the **Storage Path**, you can do one of the following:
		  ■ You can use the same **Database Path**.
		  ■ You can use a different **Database Path**. If you do, you must move the deduplication database to the new location.
		  ■ You do not have to continue to use a different **Database Path**. You can move the `databases` directory into the **Storage Path** and then specify only the **Storage Path** when you configure the storage server.
		■ You can use the host's default network interface or specify a network interface.
		If the original host used a specific network interface, you do not have to use the same interface name.
		■ If you had configured the previous MSDP storage server to use MSDP Encryption using KMS service, you must use the same configuration for the new MSDP storage server.
		
		See "About MSDP storage servers" on page 24.
		
		See "About MSDP server requirements" on page 25.

Step 8	Connect the storage to the host	Use the storage path that you configured for this replacement host. See the computer or the storage vendor's documentation.
Step 9	Install the NetBackup media server software on the new host	See the *NetBackup Installation Guide for UNIX and Windows*: http://www.veritas.com/docs/DOC5332

Table 9-3 Recover from an MSDP storage server failure *(continued)*

Step	Task	Procedure
Step 10	Reconfigure deduplication	You must use the same credentials for the NetBackup Deduplication Engine. See "Configuring MSDP server-side deduplication" on page 50.
Step 11	Import the backup images	See the *NetBackup Administrator's Guide, Volume I*: http://www.veritas.com/docs/DOC5332

Recovering the MSDP storage server after NetBackup catalog recovery

If a disaster requires a recovery of the NetBackup catalog, you must set the storage server configuration after the NetBackup catalog is recovered.

See "Setting the MSDP storage server configuration" on page 218.

Veritas recommends that you save your storage server configuration.

See "Save the MSDP storage server configuration" on page 40.

Information about recovering the master server is available.

See *NetBackup Troubleshooting Guide*:

http://www.veritas.com/docs/DOC5332

Chapter 10

Replacing MSDP hosts

This chapter includes the following topics:

- Replacing the MSDP storage server host computer

Replacing the MSDP storage server host computer

If you replace the deduplication storage server host computer, use these instructions to install NetBackup and reconfigure the deduplication storage server. The new host cannot host a deduplication storage server already.

Reasons to replace the computer include a lease swap or perhaps the current deduplication storage server computer does not meet your performance requirements.

NetBackup recommends that you consider the following items before you recover:

- The new computer must use the same byte order as the old computer.

  Warning: If the new computer does not use the same byte order as the old computer, you cannot access the deduplicated data. In computing, endianness describes the byte order that represents data: Big endian and little endian. For example, SPARC processors and Intel processors use different byte orders. Therefore, you cannot replace an Oracle Solaris SPARC host with an Oracle Solaris host that has an Intel processor.

- Veritas recommends that the new computer use the same operating system as the old computer.
- Veritas recommends that the new computer use the same version of NetBackup as the old computer.
  If you use a newer version of NetBackup on the new computer, ensure that you perform any data conversions that may be required for the newer release.

If you want to use an older version of NetBackup on the replacement host, contact your Veritas support representative.

Table 10-1 Replacing an MSDP storage server host computer

Step	Task	Procedure
Step 1	Expire the backup images	Expire all backup images that reside on the deduplication disk storage. **Warning:** Do not delete the images. They are imported back into NetBackup later in this process. If you use the `bpexpdate` command to expire the backup images, use the `-nodelete` parameter. See the *NetBackup Administrator's Guide, Volume I*: http://www.veritas.com/docs/DOC5332
Step 2	Delete the storage units that use the disk pool	See the *NetBackup Administrator's Guide, Volume I*: http://www.veritas.com/docs/DOC5332
Step 3	Delete the disk pool	See "Deleting a Media Server Deduplication Pool" on page 302.
Step 4	Delete the deduplication storage server	See "Deleting an MSDP storage server" on page 287.
Step 5	Delete the deduplication host configuration file	Each load balancing server contains a deduplication host configuration file. If you use load balancing servers, delete the deduplication host configuration file from those servers. See "Deleting an MSDP host configuration file" on page 219.
Step 6	Delete the credentials on deduplication servers	If you have load balancing servers, delete the NetBackup Deduplication Engine credentials on those media servers. See "Deleting credentials from a load balancing server" on page 290.

Table 10-1 Replacing an MSDP storage server host computer *(continued)*

Step	Task	Procedure

Step 7	Configure the new host so it meets deduplication requirements	When you configure the new host, consider the following:
		■ You can use the same host name or a different name.
		■ You can use the same **Storage Path** or a different **Storage Path**. If you use a different **Storage Path**, you must move the deduplication storage to that new location.
		■ If the **Database Path** on the original host is different that the **Storage Path**, you can do one of the following:
		  ■ You can use the same **Database Path**.
		  ■ You can use a different **Database Path**. If you do, you must move the deduplication database to the new location.
		  ■ You do not have to continue to use a different **Database Path**. You can move the `databases` directory into the **Storage Path** and then specify only the **Storage Path** when you configure the storage server.
		■ You can use the host's default network interface or specify a network interface.
		If the original host used a specific network interface, you do not have to use the same interface name.
		■ If you had configured the previous MSDP storage server to use MSDP Encryption using KMS service, you must use the same configuration for the new MSDP storage server.
		See "About MSDP storage servers" on page 24.
		See "About MSDP server requirements" on page 25.

Step 8	Connect the storage to the host	Use the storage path that you configured for this replacement host. See the computer or the storage vendor's documentation.
Step 9	Install the NetBackup media server software on the new host	See the *NetBackup Installation Guide for UNIX and Windows*: http://www.veritas.com/docs/DOC5332
Step 10	Reconfigure deduplication	See "Configuring MSDP server-side deduplication" on page 50.
Step 11	Import the backup images	See the *NetBackup Administrator's Guide, Volume I*: http://www.veritas.com/docs/DOC5332

Chapter 11

Uninstalling MSDP

This chapter includes the following topics:

- About uninstalling MSDP
- Deactivating MSDP

About uninstalling MSDP

You cannot uninstall media server deduplication components separately from NetBackup. The deduplication components are installed when you install NetBackup software, and they are uninstalled when you uninstall NetBackup software.

Other topics describe related procedures, as follow:

- Reconfigure an existing deduplication environment.
  See "Changing the MSDP storage server name or storage path" on page 284.
- Deactivate deduplication and remove the configuration files and the storage files.
  See "Deactivating MSDP" on page 329.

Deactivating MSDP

You cannot remove the deduplication components from a NetBackup media server. You can disable the components and remove the deduplication storage files and the catalog files. The host remains a NetBackup media server.

This process assumes that all backup images that reside on the deduplication disk storage have expired.

Warning: If you remove deduplication and valid NetBackup images reside on the deduplication storage, data loss may occur.

Table 11-1 Remove MSDP

Step	Task	Procedure
Step 1	Remove client deduplication	Remove the clients that deduplicate their own data from the client deduplication list. See "Disabling MSDP client-side deduplication for a client" on page 121.
Step 2	Delete the storage units that use the disk pool	See the *NetBackup Administrator's Guide, Volume I*: http://www.veritas.com/docs/DOC5332
Step 3	Delete the disk pool	See "Deleting a Media Server Deduplication Pool" on page 302.
Step 4	Delete the deduplication storage server	See "Deleting an MSDP storage server" on page 287. Deleting the deduplication storage server does not alter the contents of the storage on physical disk. To protect against inadvertent data loss, NetBackup does not automatically delete the storage when you delete the storage server.
Step 5	Delete the configuration	Delete the deduplication configuration. See "Deleting the MSDP storage server configuration" on page 288.
Step 6	Delete the deduplication host configuration file	Each load balancing server contains a deduplication host configuration file. If you use load balancing servers, delete the deduplication host configuration file from those servers. See "Deleting an MSDP host configuration file" on page 219.
Step 7	Delete the storage directory and the database directory	Delete the storage directory and database directory. (Using a separate database directory was an option when you configured deduplication.) **Warning:** If you delete the storage directory and valid NetBackup images reside on the deduplication storage, data loss may occur. See the operating system documentation.

Chapter 12

Deduplication architecture

This chapter includes the following topics:

- MSDP server components
- Media server deduplication backup process
- MSDP client components
- MSDP client–side deduplication backup process

MSDP server components

Figure 12-1 is a diagram of the storage server components.

Figure 12-1 MSDP server components

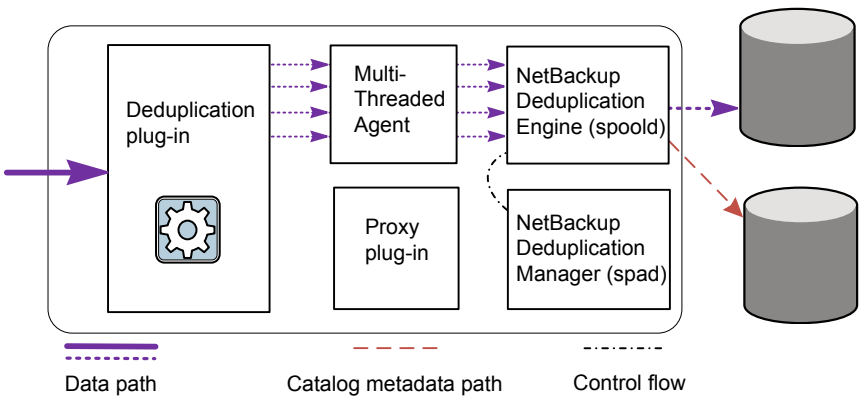


Table 12-1 describes the MSDP server components.

Table 12-1 NetBackup MSDP server components

Component	Description
Deduplication plug-in	The deduplication plug-in does the following: ■ Separates the file's metadata from the file's content. ■ Deduplicates the content (separates files into segments). ■ If required, compresses the data for backups and decompresses the backups for restores. ■ If required, encrypts the data for backups and decrypts the backups for restores. ■ If required, compresses the data for duplication and replication transfer. ■ If required, encrypts the data for duplication and replication transfer. The plug-in runs on the deduplication storage server and on load balancing servers.
Multi-Threaded Agent	The NetBackup Deduplication Multi-Threaded Agent uses multiple threads for asynchronous network I/O and CPU core calculations. The agent runs on the storage server, load balancing servers, and clients that deduplication their own data. See "About the MSDP Deduplication Multi-Threaded Agent" on page 54.
NetBackup Deduplication Engine	The NetBackup Deduplication Engine is one of the storage server core components. It provides many of the deduplication functions, which are described in Table 12-2. The binary file name is `spoold`, which is short for storage pool daemon; do not confuse it with a print spooler daemon. The `spoold` process appears as the NetBackup Deduplication Engine in the NetBackup Administration Console.
NetBackup Deduplication Manager	The deduplication manager is one of the storage server core components. The deduplication manager maintains the configuration and controls internal processes, optimized duplication, security, and event escalation. The deduplication manager binary file name is `spad`. The `spad` process appears as the NetBackup Deduplication Manager in the NetBackup Administration Console.
Proxy plug-in	The proxy plug-in manages control communication with the clients that back up their own data. It communicates with the OpenStorage proxy server (`nbostpxy`) on the client.
Reference database	The reference database stores the references that point to every data segment of which a file is composed. Unique fingerprints identify data segments. The reference database is partitioned into multiple small reference database files to improve scalability and performance. The reference database is separate from the NetBackup catalog. The NetBackup catalog maintains the usual NetBackup backup image information.

Table 12-2 describes the components and functions within the NetBackup Deduplication Engine.

Table 12-2 NetBackup Deduplication Engine components and functions

Component	Description
Connection and Task Manager	The Connection and Task Manager manages all of the connections from the load balancing servers and the clients that deduplicate their own data. The Connection and Task Manager is a set of functions and threads that does the following: ■ Provides a thread pool to serve all clients. ■ Maintains a task for each client connection. ■ Manages the mode of the Deduplication Engine based on the operation. Operations are backups, restores, queue processing, and so on.
Data integrity checking	The NetBackup Deduplication Engine checks the integrity of the data and resolves integrity problems. See "About MSDP data integrity checking" on page 304.
Data Store Manager	The Data Store Manager manages all of the data container files. The datastore Manager is a set of functions and threads that provides the following: ■ A transaction mechanism to back up data into the datastore. ■ A mechanism to read data from the datastore. ■ A transaction mechanism to reclaim space in the datastore (that is, compact containers and remove containers). Container IDs are unique. The Data Store Manager increments the container number with each new container created. The data in a container is never overwritten, and a container ID is never reused. See "About MSDP container files" on page 273.
Index Cache Manager	The Index Cache Manager manages the fingerprint cache. The cache improves fingerprint lookup speed. See "About the MSDP fingerprint cache" on page 63.
Queue processing	The NetBackup Deduplication Engine processes the transaction queue. See "About MSDP queue processing" on page 303.
Reference Database Engine	The Reference Database Engine stores the references that point to the data segments, such as read-from or write-to references. It manipulates a single database file at a time.

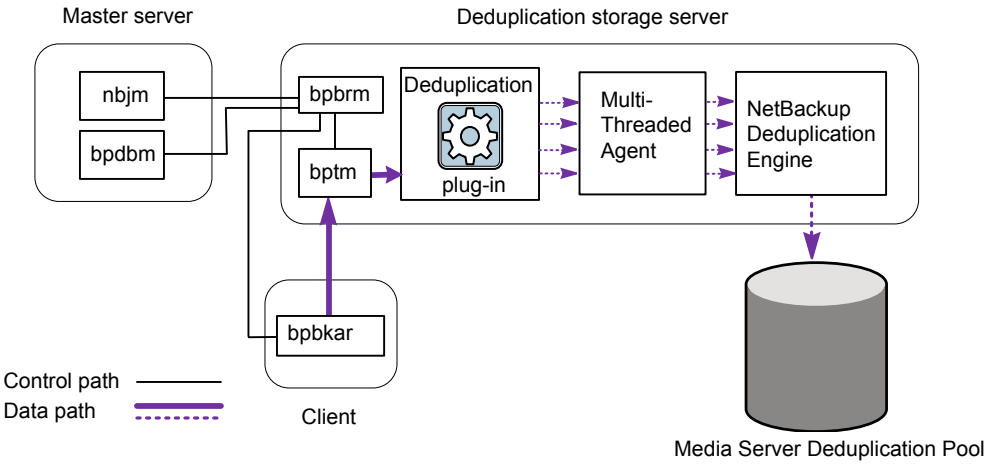
Table 12-2 NetBackup Deduplication Engine components and functions *(continued)*

Component	Description
Reference Database Manager	The Reference Database Manager manages all of the container references. It provides a transaction mechanism to manipulate a single database file.

Media server deduplication backup process

The Figure 12-2 diagram shows the backup process when a media server deduplicates the backups. The destination is a **Media Server Deduplication Pool**. A description follows.

Figure 12-2 Media server deduplication process



The following list describes the backup process when a media server deduplicates the backups and the destination is a **Media Server Deduplication Pool**:

- The NetBackup Job Manager (`nbjm`) starts the Backup/Restore Manager (`bpbrm`) on a media server.
- The Backup/Restore Manager starts the `bptm` process on the media server and the `bpbkar` process on the client.
- The Backup/Archive Manager (`bpbkar`) on the client generates the backup images and moves them to the media server `bptm` process.

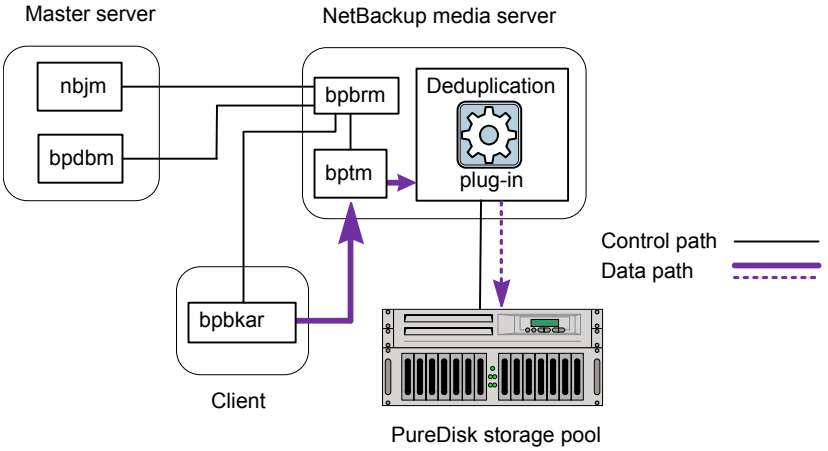
The Backup/Archive Manager also sends the information about files within the image to the Backup/Restore Manager (`bpbrm`). The Backup/Restore Manager sends the file information to the `bpdbm` process on the master server for the NetBackup database.

- The `bptm` process moves the data to the deduplication plug-in.
- The deduplication plug-in retrieves a list of IDs of the container files from the NetBackup Deduplication Engine. Those container files contain the fingerprints from the last full backup for the client. The list is used as a cache so the plug-in does not have to request each fingerprint from the engine.
- The deduplication plug-in separates the files in the backup image into segments.
- The deduplication plug-in buffers the segments and then sends batches of them to the Deduplication Multi-Threaded Agent. Multiple threads and shared memory are used for the data transfer.
- The NetBackup Deduplication Multi-Threaded Agent processes the data segments in parallel using multiple threads to improve throughput performance. The agent then sends only the unique data segments to the NetBackup Deduplication Engine.
  If the host is a load balancing server, the Deduplication Engine is on a different host, the storage server.
- The NetBackup Deduplication Engine writes the data to the **Media Server Deduplication Pool**.
  The first backup may have a 0% deduplication rate, although a 0% rate is unlikely. Zero percent means that all file segments in the backup data are unique.

The Figure 12-3 diagram shows the backup process when a media server deduplicates the backups. The destination is a **PureDisk Deduplication Pool**. A description follows.

Note: NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only.

Figure 12-3 Media server deduplication process to a PureDisk storage pool



The following list describes the backup process when a media server deduplicates the backups and the destination is a **PureDisk Deduplication Pool**:

- The NetBackup Job Manager (`nbjm`) starts the Backup/Restore Manager (`bpbrm`) on a media server.
- The Backup/Restore Manager starts the `bptm` process on the media server and the `bpbkar` process on the client).
- The Backup/Archive Manager (`bpbkar`) generates the backup images and moves them to the media server `bptm` process.

  The Backup/Archive Manager also sends the information about files within the image to the Backup/Restore Manager (`bpbrm`). The Backup/Restore Manager sends the file information to the `bpdbm` process on the master server for the NetBackup database.
- The `bptm` process moves the data to the deduplication plug-in.
- The deduplication plug-in retrieves a list of IDs of the container files from the NetBackup Deduplication Engine. Those container files contain the fingerprints from the last full backup for the client. The list is used as a cache so the plug-in does not have to request each fingerprint from the engine.
- The deduplication plug-in compares the file fingerprints and the segment fingerprints against the fingerprint list in its cache.
- The deduplication plug-in performs file fingerprinting calculations.
- The deduplication plug-in sends only unique data segments to the **PureDisk Deduplication Pool**.

MSDP client components

Table 12-3 describes the client deduplication components.

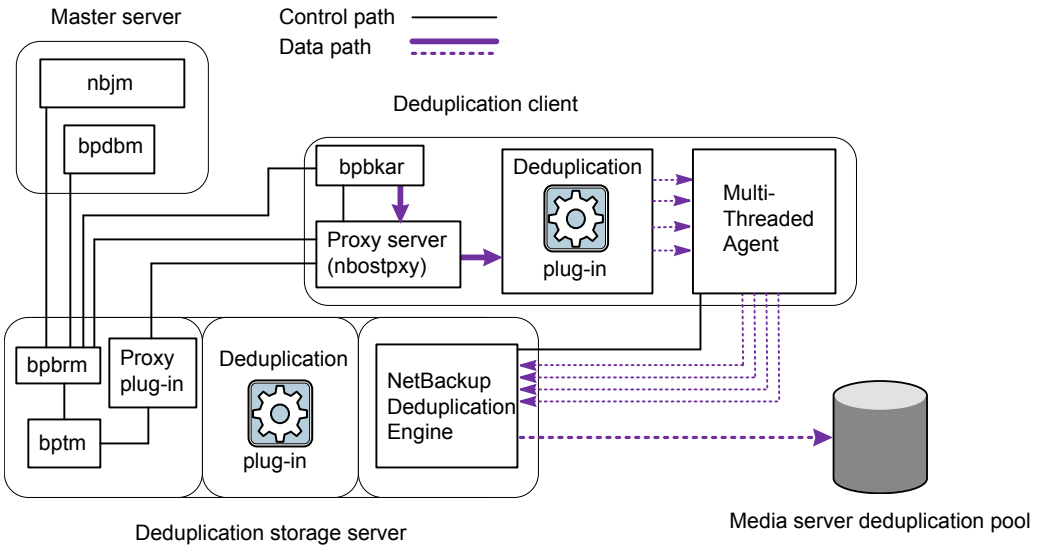
Table 12-3 Client MSDP components

Component	Description
Deduplication plug-in	The deduplication plug-in does the following: ■ Separates the file's metadata from the file's content. ■ Deduplicates the content (separates files into segments). ■ If required, compresses the data for backups and decompresses the backups for restores. ■ If required, encrypts the data for backups and decrypts the backups for restores.
Multi-Threaded Agent	The NetBackup Deduplication Multi-Threaded Agent uses multiple threads for asynchronous network I/O and CPU core calculations. The agent runs on the storage server, load balancing servers, and clients that deduplication their own data. See "About the MSDP Deduplication Multi-Threaded Agent" on page 54.
Proxy server	The OpenStorage proxy server (`nbostpxy`) manages control communication with the proxy plug-in on the storage server.

MSDP client–side deduplication backup process

The Figure 12-4 diagram shows the backup process of a client that deduplicates its own data. The destination is a media server deduplication pool. A description follows.

Figure 12-4 MSDP client backup to a deduplication pool



The following list describes the backup process for an MSDP client to a Media Server Deduplication Pool:

- The NetBackup Job Manager (`nbjm`) starts the Backup/Restore Manager (`bpbrm`) on a media server.
- The Backup/Restore Manager probes the client to determine if it is configured and ready for deduplication.
- If the client is ready, the Backup/Restore Manager starts the following processes: The OpenStorage proxy server (`nbostpxy`) on the client and the data moving processes (`bpbkar`) on the client and `bptm` on the media server).
  NetBackup uses the proxy plug-in on the media server to route control information from `bptm` to `nbostpxy`.
- The Backup/Archive Manager (`bpbkar`) generates the backup images and moves them to the client `nbostpxy` process by shared memory.
  The Backup/Archive Manager also sends the information about files within the image to the Backup/Restore Manager (`bpbrm`). The Backup/Restore Manager sends the file information to the `bpdbm` process on the master server for the NetBackup database.
- The client `nbostpxy` process moves the data to the deduplication plug-in.

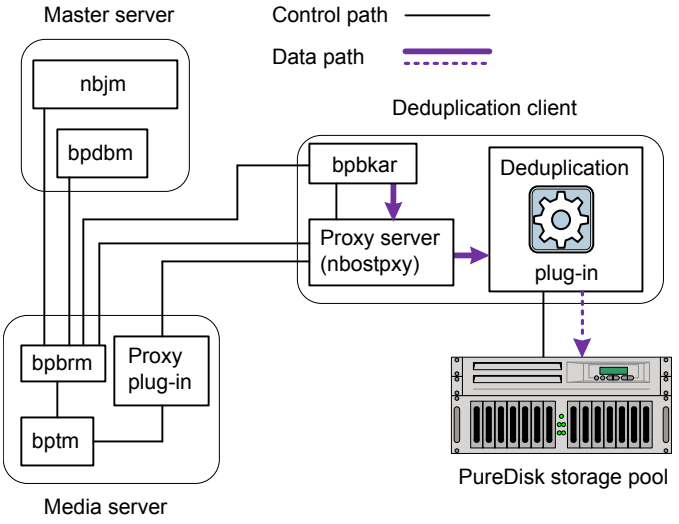
- The deduplication plug-in on the client tries to retrieve a list of fingerprints, in the following order:
  - From a client and a policy that is configured in the client's `pd.conf` file. The `FP_CACHE_CLIENT_POLICY` entry defines the client and policy to use for the fingerprint cache. The entry must be valid (that is, not expired).
    See "About seeding the MSDP fingerprint cache for remote client deduplication" on page 65.
  - From the previous backup for the client and policy.
  - From the special seeding directory on the storage server.
    See "About seeding the MSDP fingerprint cache for remote client deduplication" on page 65.

  The list of fingerprints is used as a cache so the plug-in does not have to request each fingerprint from the engine.
  If no fingerprints are loaded into the cache, the deduplication rate may be very low for the backup.
- The deduplication plug-in separates the files in the backup image into segments.
- The deduplication plug-in buffers the segments and then sends batches of them to the Deduplication Multi-Threaded Agent. Multiple threads and shared memory are used for the data transfer.
- The NetBackup Deduplication Multi-Threaded Agent processes the data segments in parallel using multiple threads to improve throughput performance. The agent then sends only the unique data segments to the NetBackupDeduplication Engine.
- The NetBackup Deduplication Engine writes the data to the **Media Server Deduplication Pool**.
  The first backup may have a 0% deduplication rate, although a 0% deduplication rate is unlikely. Zero percent means that all file segments in the backup data are unique.

The Figure 12-5 diagram shows the backup process of a client that deduplicates its own data. The destination is a PureDisk storage pool. A description follows.

Note: NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only.

Figure 12-5 MSDP deduplication client backup to a PureDisk storage pool



The following list describes the backup process for an MSDP client to a PureDisk storage pool:

- The NetBackup Job Manager (`nbjm`) starts the Backup/Restore Manager (`bpbrm`) on a media server.
- The Backup / Restore Manager probes the client to determine if it is configured and ready for deduplication.
- If the client is ready, the Backup/Restore Manager starts the following processes: The OpenStorage proxy server (`nbostpxy`) on the client and the data moving processes (`bpbkar` on the client and `bptm` on the media server).
  NetBackup uses the proxy plug-in on the media server to route control information from `bptm` to `nbostpxy`.
- The Backup/Archive Manager (`bpbkar`) generates the backup images and moves them to the client `nbostpxy` process by shared memory.
  The Backup/Archive Manager also sends the information about files within the image to the Backup/Restore Manager (`bpbrm`). The Backup/Restore Manager sends the file information to the `bpdbm` process on the master server for the NetBackup database.
- The client `nbostpxy` process moves the data to the deduplication plug-in.

- The deduplication plug-in retrieves a list of fingerprints from the last full backup of the client. The list is used as a cache so the plug-in does not have to request each fingerprint from the engine.
- The deduplication plug-in performs file fingerprint calculations.
- The deduplication plug-in sends only unique data segments to the PureDisk storage pool.

Chapter 13

Troubleshooting

This chapter includes the following topics:

- About unified logging
- About legacy logging
- NetBackup MSDP log files
- Troubleshooting MSDP installation issues
- Troubleshooting MSDP configuration issues
- Troubleshooting MSDP operational issues
- Viewing MSDP disk errors and events
- MSDP event codes and messages
- Troubleshooting CloudCatalyst issues

About unified logging

Unified logging and legacy logging are the two forms of debug logging used in NetBackup. All NetBackup processes use one of these forms of logging. Server processes and client processes use unified logging.

Unified logging creates log file names and messages in a standardized format. These logging files cannot be easily viewed with a text editor. They are in binary format and some of the information is contained in an associated resource file. Only the `vxlogview` command can assemble and display the log information correctly.

Unlike legacy logging, unified logging does not require that you create logging subdirectories. Log files for originator IDs are written to a subdirectory with the name specified in the log configuration file. All unified logs are written to subdirectories in the following directory:

Windows	*install_path*\NetBackup\logs
UNIX	/usr/openv/logs

You can access logging controls in the **NetBackup Administration Console**. In the left pane, expand **NetBackup Management > Host Properties > Master Servers** or **Media Servers**. Double-click the server you want to change. In the left pane of the dialog box, click **Logging**.

You can also manage unified logging by using the following commands:

vxlogcfg	Modifies the unified logging configuration settings. for more information about the vxlogcfg command.
vxlogmgr	Manages the log files that the products that support unified logging generate. for more information about the vxlogmgr command.
vxlogview	Displays the logs that unified logging generates. See "Examples of using vxlogview to view unified logs" on page 344. for more information about the vxlogview command.

These commands are located in the following directory:

Windows	*install_path*\NetBackup\bin
UNIX	/usr/openv/netbackup/bin

See the NetBackup Commands Reference Guide for a complete description about these commands.

More information about legacy logging is available.

See "About legacy logging" on page 345.

About using the vxlogview command to view unified logs

Use the vxlogview command to view the logs that unified logging creates. These logs are stored in the following directory.

UNIX	/usr/openv/logs
Windows	*install_path*\NetBackup\logs

Unlike the files that are written in legacy logging, unified logging files cannot be easily viewed with a text editor. The unified logging files are in binary format, and some of the information is contained in an associated resource file. Only the `vxlogview` command can assemble and display the log information correctly.

You can use `vxlogview` to view NetBackup log files as well as PBX log files.

To view PBX logs using the `vxlogview` command, do the following:

- Ensure that you are an authorized user. For UNIX and Linux, you must have root privileges. For Windows, you must have administrator privileges.
- To specify the PBX product ID, enter `-p 50936` as a parameter on the `vxlogview` command line.

`vxlogview` searches all the files, which can be a slow process. Refer to the following topic for an example of how to display results faster by restricting the search to the files of a specific process.

Examples of using vxlogview to view unified logs

The following examples demonstrate how to use the `vxlogview` command to view unified logs.

Table 13-1 Example uses of the vxlogview command

Item	Example
Display all the attributes of the log messages	`vxlogview -p 51216 -d all`
Display specific attributes of the log messages	Display the log messages for NetBackup (51216) that show only the date, time, message type, and message text: `vxlogview --prodid 51216 --display D,T,m,x`
Display the latest log messages	Display the log messages for originator 116 (`nbpem`) that were issued during the last 20 minutes. Note that you can specify `-o nbpem` instead of `-o 116`: `# vxlogview -o 116 -t 00:20:00`
Display the log messages from a specific time period	Display the log messages for `nbpem` that were issued during the specified time period: `# vxlogview -o nbpem -b "05/03/15 06:51:48 AM" -e "05/03/15 06:52:48 AM"`

Table 13-1 Example uses of the vxlogview command *(continued)*

Item	Example
Display results faster	You can use the `-i` option to specify an originator for a process: `# vxlogview -i nbpem` The `vxlogview -i` option searches only the log files that the specified process (`nbpem`) creates. By limiting the log files that it has to search, `vxlogview` returns a result faster. By comparison, the `vxlogview -o` option searches all unified log files for the messages that the specified process has logged. **Note:** If you use the `-i` option with a process that is not a service, `vxlogview` returns the message "No log files found." A process that is not a service has no originator ID in the file name. In this case, use the `-o` option instead of the `-i` option. The -i option displays entries for all OIDs that are part of that process including libraries (137, 156, 309, etc.).
Search for a job ID	You can search the logs for a particular job ID: `# vxlogview -i nbpem | grep "jobid=`*`job_ID`*`"` The `jobid=` search key should contain no spaces and must be lowercase. When searching for a job ID, you can use any `vxlogview` command option. This example uses the `-i` option with the name of the process (`nbpem`). The command returns only the log entries that contain the job ID. It misses related entries for the job that do not explicitly contain the jobid=*job_ID*.

See the *NetBackup Commands Reference Guide* for a complete description of the `vxlogview` command. The guide is available through the following URL:

http://www.veritas.com/docs/DOC5332

About legacy logging

Legacy logging and unified logging are the two forms of debug logging used in NetBackup. All NetBackup processes use either unified logging or legacy logging.

See “About unified logging” on page 342.

In legacy debug logging, each process creates log files of debug activity in its own logging directory. The NetBackup legacy debug log directories are located in the following directories:

Windows	*install_path*\NetBackup\logs *install_path*\Volmgr\debug
UNIX	/usr/openv/netbackup/logs /usr/openv/volmgr/debug

These top-level directories can contain a directory for each NetBackup process that uses legacy logging. By default, NetBackup creates only a subset of all of the possible log directories. For example, the following directories are created by default on UNIX servers:

- nbfp
- nbliveup
- nblogadm
- user_ops

To enable logging for all of the NetBackup processes that use legacy logging, you must create the log file directories that do not already exist, unless you use the Logging Assistant. For more information about the Logging Assistant, see the *NetBackup Administrator's Guide, Volume I*. The guide is available at the following location:

http://www.veritas.com/docs/DOC5332

You can use the following batch files to create all of the debug log directories at once:

- Windows: *install_path*\NetBackup\Logs\mklogdir.bat
- UNIX: usr/openv/netbackup/logs/mklogdir

See the *NetBackup Commands Reference Guide* for a complete description about the mklogdir command. The guide is available at the following location:

http://www.veritas.com/docs/DOC5332

After the directories are created, NetBackup creates log files in the directory that is associated with each process. A debug log file is created when the process begins. Each log file grows to a certain size before the NetBackup process closes it and creates a new log file.

To enable debug logging for the NetBackup Status Collection Daemon (vmscd), create the following directory before you start nbemm.

Windows	*install_path*\Volmgr\debug\vmscd\
UNIX	/usr/openv/volmgr/debug/vmscd

As an alternative, you can restart vmscd after creating the directory.

Creating NetBackup log file directories for MSDP

Before you configure your NetBackup feature, create the directories into which the NetBackup commands write log files. Create the directories on the master server and on each media server that you use for your feature. The log files reside in the following directories:

- UNIX: /usr/openv/netbackup/logs/
- Windows:*install_path*\NetBackup\logs\

More information about NetBackup logging is available in the *NetBackup Logging Reference Guide*, available through the following URL:

http://www.veritas.com/docs/DOC5332

To create log directories for NetBackup commands

- Depending on the operating system, run one of the following scripts:

  UNIX: /usr/openv/netbackup/logs/mklogdir

  Windows: *install_path*\NetBackup\logs\mklogdir.bat

To create the tpconfig command log directory

- Depending on the operating system, create the debug directory and the tpcommand directory (by default, the debug directory and the tpcommand directory do not exist). The pathnames of the directories are as follows:

  UNIX: /usr/openv/volmgr/debug/tpcommand

  Windows: *install_path*\Veritas\Volmgr\debug\tpcommand

NetBackup MSDP log files

The NetBackup deduplication components write information to various log files. Some NetBackup commands or processes write messages to their own log files. Other processes use the Veritas unified log (VxUL) files. VxUL uses a standardized

name and file format for log files. An originator ID (OID) identifies the process that writes the log messages.

See "About legacy logging" on page 345.

See "About unified logging" on page 342.

In VxUL logs, the messages that begin with an `sts` prefix relate to the interaction with the deduplication plug-in. Most interaction occurs on the NetBackup media servers. To view and manage VxUL log files, you must use NetBackup log commands. For information about how to use and manage logs on NetBackup servers, see the *NetBackup Logging Reference Guide*. The guide is available through the following URL:

http://www.veritas.com/docs/DOC5332

Most interaction occurs on the NetBackup media servers. Therefore, the log files on the media servers that you use for disk operations are of most interest.

Warning: The higher the log level, the greater the affect on NetBackup performance. Use a log level of 5 (the highest) only when directed to do so by a Veritas representative. A log level of 5 is for troubleshooting only.

Specify the NetBackup log levels in the **Logging** host properties on the NetBackup master server. The log levels for some processes specific to certain options are set in configuration files as described in Table 13-2.

Table 13-2 describes the log files for each component.

Table 13-2 Logs for NetBackup MSDP activity

Component	VxUL OID	Description
Backups and restores	117	The `nbjm` Job Manager.

Table 13-2 Logs for NetBackup MSDP activity *(continued)*

Component	VxUL OID	Description
Backups and restores	N/A	Messages appear in the log files for the following processes: ■ The `bpbrm` backup and restore manager. The following is the path to the log files: UNIX: `/usr/openv/netbackup/logs/bpbrm` Windows: *`install_path`*`\Veritas\NetBackup\logs\bpbrm` ■ The `bpdbm` database manager. The following is the path to the log files: UNIX: `/usr/openv/netbackup/logs/bpdbm` Windows: *`install_path`*`\Veritas\NetBackup\logs\bpdbm` ■ The `bptm` tape manager for I/O operations. The following is the path to the log files: UNIX: `/usr/openv/netbackup/logs/bptm` Windows: *`install_path`*`\Veritas\NetBackup\logs\bptm`
Catalog shadow copies	N/A	The MSDP catalog shadow copy process writes messages to the following log files and directories: UNIX: *`/storage_path`*`/log/spad/spad.log` *`/storage_path`*`/log/spad/sched_CatalogBackup.log` *`/storage_path`*`/log/spad/`*`client_name`*`/` Windows: *`storage_path`*`\log\spad\spad.log` *`storage_path`*`\log\spad\sched_CatalogBackup.log` *`storage_path`*`\log\spad\`*`client_name`*`\`

Table 13-2 Logs for NetBackup MSDP activity *(continued)*

Component	VxUL OID	Description
Client deduplication proxy plug-in	N/A	The client deduplication proxy plug-in on the media server runs under `bptm`, `bpstsinfo`, and `bpbrm` processes. Examine the log files for those processes for proxy plug-in activity. The strings `proxy` or `ProxyServer` embedded in the log messages identify proxy server activity. They write log files to the following directories: ■ For `bptm`: UNIX: `/usr/openv/netbackup/logs/bptm` Windows: *`install_path`*`\Veritas\NetBackup\logs\bptm` ■ For `bpstsinfo`: Windows: `/usr/openv/netbackup/logs/admin` UNIX: `/usr/openv/netbackup/logs/bpstsinfo` Windows: *`install_path`*`\Veritas\NetBackup\logs\admin` Windows: *`install_path`*`\Veritas\NetBackup\logs\stsinfo` ■ For `bpbrm`: UNIX: `/usr/openv/netbackup/logs/bpbrm` Windows: *`install_path`*`\Veritas\NetBackup\logs\bpbrm`
Client deduplication proxy server	N/A	The deduplication proxy server `nbostpxy` on the client writes messages to files in the following directory, as follows: UNIX: `/usr/openv/netbackup/logs/nbostpxy` Windows: *`install_path`*`\Veritas\NetBackup\logs\nbostpxy`.
Deduplication configuration script	N/A	The following is the path name of the log file for the deduplication configuration script: ■ UNIX: *`storage_path`*`/log/pdde-config.log` ■ Windows: *`storage_path`*`\log\pdde-config.log` NetBackup creates this log file during the configuration process. If your configuration succeeded, you do not need to examine the log file. The only reason to look at the log file is if the configuration failed. If the configuration process fails after it creates and populates the storage directory, this log file identifies when the configuration failed.

Table 13-2 Logs for NetBackup MSDP activity *(continued)*

Component	VxUL OID	Description
Deduplication plug-in	N/A	The `DEBUGLOG` entry and the `LOGLEVEL` in the `pd.conf` file determine the log location and level for the deduplication plug-in. The following are the default locations for log files: ■ UNIX: `/var/log/puredisk/pdplugin.log` ■ Windows: `C:\pdplugin.log` You can configure the location and name of the log file and the logging level. To do so, edit the `DEBUGLOG` entry and the `LOGLEVEL` entry in the `pd.conf` file. See "About the MSDP pd.conf configuration file" on page 197. See "Editing the MSDP pd.conf file" on page 198.
Device configuration and monitoring	111	The `nbemm` process.
Device configuration and monitoring	178	The Disk Service Manager process that runs in the Enterprise Media Manager (EMM) process.
Device configuration and monitoring	202	The storage server interface process that runs in the Remote Manager and Monitor Service. RMMS runs on media servers.
Device configuration and monitoring	230	The Remote Disk Service Manager interface (RDSM) that runs in the Remote Manager and Monitor Service. RMMS runs on media servers.

`drcontrol` utility	N/A	You must run the `drcontrol` utility on the MSDP storage server host. The command requires administrator privileges.
		The utility creates a log file and displays its pathname in the command output. The utility writes log files to the following directory, depending on the operating system:
		UNIX:
		`/[storage_path]/log/drcontrol/policy_admin`
		`/storage_path/log/drcontrol/dedupe_catalog_DR`
		Windows:
		`storage_path\log\drcontrol\policy_admin`
		`storage_path\log\drcontrol\dedupe_catalog_DR`
		See "About protecting the MSDP catalog" on page 221.
		See "About recovering the MSDP catalog" on page 318.

Table 13-2 Logs for NetBackup MSDP activity *(continued)*

Component	VxUL OID	Description
Installation	N/A	The NetBackup installation process writes information about the installation of the deduplication components to a log file in the following directory: ■ UNIX: `/var/log/puredisk` ■ Windows: `%ALLUSERSPROFILE%\Symantec\NetBackup\InstallLogs`
NetBackup Deduplication Engine	N/A	The NetBackup Deduplication Engine writes several log files, as follows: ■ Log files in the *`storage_path`*`/log/spoold` directory, as follows: ■ The `spoold.log` file is the main log file ■ The `storaged.log` file is for queue processing. ■ A log file for each connection to the engine is stored in a directory in the storage path `spoold` directory. The following describes the pathname to a log file for a connection: *hostname/application/TaskName/MMDDYY*.log For example, the following is an example of a `crcontrol` connection log pathname on a Linux system: *`/storage_path`*`/log/spoold/server.example.com/crcontrol/Control/010112.log` Usually, the only reason to examine these connection log files is if a Veritas support representative asks you to. ■ A VxUL log file for the events and errors that NetBackup receives from polling. The originator ID for the deduplication engine is 364.
NetBackup Deduplication Engine	364	The NetBackup Deduplication Engine that runs on the deduplication storage server.

Table 13-2 Logs for NetBackup MSDP activity *(continued)*

Component	VxUL OID	Description
NetBackup Deduplication Manager	N/A	The log files are in the `/storage_path/log/spad` directory, as follows: ■ `spad.log` ■ `sched_QueueProcess.log` ■ `SchedClass.log` ■ A log file for each connection to the manager is stored in a directory in the storage path `spad` directory. The following describes the pathname to a log file for a connection: *hostname/application/TaskName/MMDDYY*.log For example, the following is an example of a `bpstsinfo` connection log pathname on a Linux system: `/storage_path/log/spoold/server.example.com/bpstsinfo/spad/010112.log` Usually, the only reason to examine these connection log files is if a Veritas support representative asks you to. You can set the log level and retention period in the **Change Storage Server** dialog box **Properties** tab. See "Changing MSDP storage server properties" on page 282.
Optimized duplication and replication	N/A	For optimized duplication and Auto Image Replication, The following are the log files that provide information: ■ The NetBackup `bptm` tape manager for I/O operations. The following is the path to the log files: UNIX: `/usr/openv/netbackup/logs/bptm` Windows: `install_path\Veritas\NetBackup\logs\bptm` ■ The following is the path name of MSDP replication log file: `/storage_path/log/spad/replication.log`
Resilient network connections	387	The Remote Network Transport Service (`nbrntd`) manages resilient network connection sockets. It runs on the master server, on media servers, and on clients. Use the VxUL originator ID 387 to view information about the socket connections that NetBackup uses. **Note:** If multiple backup streams run concurrently, the Remote Network Transport Service writes a large amount of information to the log files. In such a scenario, Veritas recommends that you set the logging level for OID 387 to 2 or less. To configure unified logs, see the following guide: The *NetBackup Logging Reference Guide*: http://www.veritas.com/docs/DOC5332

Table 13-2 Logs for NetBackup MSDP activity *(continued)*

Component	VxUL OID	Description
Resilient network connections	N/A	The deduplication plug-in logs information about keeping the connection alive. For more information about the deduplication plug-in log file, see “Deduplication plug-in” in this table. The `pd.conf` file `FILE_KEEP_ALIVE_INTERVAL` parameter controls the connection keep alive interval. See “About the MSDP pd.conf configuration file” on page 197. See “Editing the MSDP pd.conf file” on page 198.

Troubleshooting MSDP installation issues

The following sections may help you troubleshoot installation issues.

See “MSDP installation on SUSE Linux fails” on page 354.

MSDP installation on SUSE Linux fails

The installation trace log shows an error when you install on SUSE Linux:

```
....NetBackup and Media Manager are normally installed in /usr/openv.
Is it OK to install in /usr/openv? [y,n] (y)

Reading NetBackup files from /net/nbstore/vol/test_data/PDDE_packages/
suse/NB_FID2740_LinuxS_x86_20090713_6.6.0.27209/linuxS_x86/anb

/net/nbstore/vol/test_data/PDDE_packages/suse/NB_FID2740_LinuxS_x86_
20090713_6.6.0.27209/linuxS_x86/catalog/anb/NB.file_trans: symbol
lookup error: /net/nbstore/vol/test_data/PDDE_packages/suse/
NB_FID2740_LinuxS_x86_20090713_6.6.0.27209/linuxS_x86/catalog/anb/
NB.file_trans: undefined symbol: head /net/nbstore/vol/test_data/
PDDE_packages/suse/NB_FID2740_LinuxS_x86_20090713_6.6.0.27209/
linuxS_x86/catalog/anb/NB.file_trans failed. Aborting ...
```

Verify that your system is at patch level 2 or later, as follows:

```
cat /etc/SuSE-release
SUSE Linux Enterprise Server 10 (x86_64)
VERSION = 10
PATCHLEVEL = 2
```

Troubleshooting MSDP configuration issues

The following sections may help you troubleshoot configuration issues.

See "NetBackup MSDP log files" on page 347.

See "MSDP storage server configuration fails" on page 355.

See "MSDP database system error (220)" on page 355.

See "MSDP server not found error" on page 356.

See "License information failure during MSDP configuration" on page 356.

See "The disk pool wizard does not display an MSDP volume" on page 357.

MSDP storage server configuration fails

If storage server configuration fails, first resolve the issue that the **Storage Server Configuration Wizard** reports. Then, delete the deduplication host configuration file before you try to configure the storage server again.

NetBackup cannot configure a storage server on a host on which a storage server already exists. One indicator of a configured storage server is the deduplication host configuration file. Therefore, it must be deleted before you try to configure a storage server after a failed attempt.

See "Deleting an MSDP host configuration file" on page 219.

MSDP database system error (220)

A database system error indicates that an error occurred in the storage initialization.

Error message `ioctl() error, Database system error (220)`

Example

```
RDSM has encountered an STS error:

  Failed to update storage server ssname, database
  system error
```

Diagnosis

The `PDDE_initConfig` script was invoked, but errors occurred during the storage initialization.

First, examine the deduplication configuration script log file for references to the server name.

See "NetBackup MSDP log files" on page 347.

Second, examine the `tpconfig` command log file errors about creating the credentials for the server name. The `tpconfig` command writes to the standard NetBackup administrative commands log directory.

MSDP server not found error

The following information may help you resolve a server not found error message that may occur during configuration.

Error message

```
Server not found, invalid command parameter
```

Example

```
RDSM has encountered an issue with STS where
  the server was not found:  getStorageServerInfo

   Failed to create storage server ssname, invalid
   command parameter
```

Diagnosis

Possible root causes:

- When you configured the storage server, you selected a media server that runs an unsupported operating system. All media servers in your environment appear in the **Storage Server Configuration Wizard**; be sure to select only a media server that runs a supported operating system.
- If you used the `nbdevconfig` command to configure the storage server, you may have typed the host name incorrectly. Also, case matters for the storage server type, so ensure that you use **PureDisk** for the storage server type.

License information failure during MSDP configuration

A configuration error message about license information failure indicates that the NetBackup servers cannot communicate with each other.

If you cannot configure a deduplication storage server or load balancing servers, your network environment may not be configured for DNS reverse name lookup.

You can edit the hosts file on the media servers that you use for deduplication. Alternatively, you can configure NetBackup so it does not use reverse name lookup.

To prohibit reverse host name lookup by using the Administration Console

1. In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Master Servers**.
2. In the details pane, select the master server.
3. On the **Actions** menu, select **Properties**.
4. In the **Master Server Properties** dialog box, select the **Network Settings** properties.
5. Select one of the following options:
   - **Allowed**
   - **Restricted**
   - **Prohibited**

   For a description of these options, see the NetBackup online Help or the administrator's guide.

To prohibit reverse host name lookup by using the `bpsetconfig` command

- Enter the following command on each media server that you use for deduplication:

  ```
  echo REVERSE_NAME_LOOKUP = PROHIBITED | bpsetconfig -h host_name
  ```

  The `bpsetconfig` command resides in the following directories:

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

  Windows: *`install_path`*`\Veritas\NetBackup\bin\admincmd`

The disk pool wizard does not display an MSDP volume

The **Disk Pool Configuration Wizard** does not display a disk volume for the deduplication storage server.

First, restart all of the NetBackup daemons or services. The step ensures that the NetBackup Deduplication Engine is up and ready to respond to requests.

Second, restart the **NetBackup Administration Console**. This step clears cached information from the failed attempt to display the disk volume.

Troubleshooting MSDP operational issues

The following sections may help you troubleshoot operational issues.

See "Verify that the MSDP server has sufficient memory" on page 358.

See “MSDP backup or duplication job fails” on page 358.

See “MSDP client deduplication fails” on page 360.

See “MSDP volume state changes to DOWN when volume is unmounted” on page 361.

See “MSDP errors, delayed response, hangs” on page 362.

See “Cannot delete an MSDP disk pool” on page 362.

See “MSDP media open error (83)” on page 363.

See “MSDP media write error (84)” on page 365.

See “MSDP no images successfully processed (191)” on page 368.

See “MSDP storage full conditions” on page 368.

See “Troubleshooting MSDP catalog backup” on page 369.

Verify that the MSDP server has sufficient memory

Insufficient memory on the storage server can cause operation problems. If you have operation issues, you should verify that your storage server has sufficient memory.

See “About MSDP server requirements” on page 25.

If the NetBackup deduplication processes do no start on Red Hat Linux, configure shared memory to be at least 128 MB (`SHMMAX=128MB`).

MSDP backup or duplication job fails

The following subsections describe some potential failures for backup or deduplication jobs and how to resolve them.

- Disk volume is down
- Storage server is down or unavailable
- Backup job: System error occurred (174)
- Failure to open storage path or to prepare CRQP transaction

Disk volume is down

A message similar to the following appears in the job details:

```
Error 800: Disk Volume is Down
```

Examine the disk error logs to determine why the volume was marked DOWN.

If the storage server is busy with jobs, it may not respond to master server disk polling requests in a timely manner. A busy load balancing server also may cause this error. Consequently, the query times out and the master server marks the volume DOWN.

If the error occurs for an optimized duplication job: verify that source storage server is configured as a load balancing server for the target storage server. Also verify that the target storage server is configured as a load balancing server for the source storage server.

See "Viewing MSDP disk errors and events" on page 370.

Storage server is down or unavailable

Windows servers only.

A message similar to the following appears in the job details:

```
Error nbjm(pid=6384) NBU status: 2106, EMM status: Storage Server is
down or unavailable Disk storage server is down(2106)
```

The NetBackup Deduplication Manager (`spad.exe`) and the NetBackup Deduplication Engine (`spoold.exe`) have different shared memory configuration values. This problem can occur when you use a command to change the shared memory value of only one of these two components.

To resolve the issue, specify the following shared memory value in the configuration file:

```
SharedMemoryEnabled=1
```

Then, restart both components. Do not change the values of the other two shared memory parameters.

The `SharedMemoryEnabled` parameter is stored in the following file:

storage_path`\etc\puredisk\agent.cfg`

Backup job: System error occurred (174)

A message similar to the following appears in the job details:

```
media manager - system error occurred (174)
```

If the job details also include errors similar to the following, it indicates that an image clean-up job failed:

```
Critical bpdm (pid=610364) sts_delete_image
 failed: error 2060018 file not found
Critical bpdm (pid=610364) image delete
 failed: error 2060018: file not found
```

This error occurs if a deduplication backup job fails after the job writes part of the backup to the **Media Server Deduplication Pool**. NetBackup starts an image cleanup job, but that job fails because the data necessary to complete the image clean-up was not written to the **Media Server Deduplication Pool**.

Deduplication queue processing cleans up the image objects, so you do not need to take corrective action. However, examine the job logs and the deduplication logs to determine why the backup job failed.

See "About MSDP queue processing" on page 303.

See "NetBackup MSDP log files" on page 347.

Failure to open storage path or to prepare CRQP transaction

Error messages similar to the following appear in one of the NetBackup Deduplication Engine (`spoold`) log files.

```
RefDBEngine::write_prepare fail to open
/storage_path/databases/refdb/prepare/64.ref.prepare
```

```
RefDBManager::write_prepare fail to prepare CRQP transaction for
refdb 64
```

See "NetBackup MSDP log files" on page 347.

This error occurs if the `/storage_path/databases/refdb/prepare` directory is deleted.

To fix this problem, do one of the following:

- Create the missing directory manually.
- Restart the NetBackup Deduplication Engine (`spoold`). First ensure that no backups are running on the storage unit on that media server.

Note: `RefDBEngine` and `refdb` do not refer to nor are they related to the open source RefDB reference database and bibliography tool.

MSDP client deduplication fails

NetBackup client-side agents (including client deduplication) depend on reverse host name look up of NetBackup server names. Conversely, regular backups depend on forward host name resolution. Therefore, the backup of a client that deduplicates it's own data may fail, while a normal backup of the client may succeed.

If a client-side deduplication backup fails, verify that your Domain Name Server includes all permutations of the storage server name.

Also, Veritas recommends that you use fully-qualified domain names for your NetBackup environment.

See "Use fully qualified domain names" on page 36.

MSDP volume state changes to DOWN when volume is unmounted

If a volume becomes unmounted, NetBackup changes the volume state to DOWN. NetBackup jobs that require that volume fail.

To determine the volume state

- Invoke the following command on the master server or the media server that functions as the deduplication storage server:

  UNIX: `/usr/openv/netbackup/bin/admincmd/nbdevquery -listdv -stype PureDisk -U`

  Windows: *`install_path`*`\NetBackup\bin\admincmd\nbdevquery -listdv -stype PureDisk -U`

  The following example output shows that the `DiskPoolVolume` is UP:

```
Disk Pool Name      : PD_Disk_Pool
Disk Type           : PureDisk
Disk Volume Name    : PureDiskVolume
Disk Media ID       : @aaaab
Total Capacity (GB) : 49.98
Free Space (GB)     : 43.66
Use%                : 12
Status              : UP
Flag                : ReadOnWrite
Flag                : AdminUp
Flag                : InternalUp
Num Read Mounts     : 0
Num Write Mounts    : 1
Cur Read Streams    : 0
Cur Write Streams   : 0
```

To change the volume state to UP

1. Mount the file system

   After a brief period of time, the volume state changes to UP. No further action is required.

2. If the volume state does not change, change it manually.

   See "Changing the MSDP disk volume state" on page 300.

MSDP errors, delayed response, hangs

Insufficient memory or inadequate host capabilities may cause multiple errors, delayed response, and hangs.

See "About MSDP server requirements" on page 25.

For virtual machines, Veritas recommends that you do the following:

- Set the memory size of each virtual machine to double the physical memory of the host.
- Set the minimum and the maximum values of each virtual machine to the same value (double the physical memory of the host). These memory settings prevent the virtual memory from becoming fragmented on the disk because it does not grow or shrink.

These recommendations may not be the best configuration for every virtual machine. However, Veritas recommends that you try this solution first when troubleshooting performance issues.

Cannot delete an MSDP disk pool

If you cannot delete a disk pool that you believe contains no valid backup images, the following information may help you troubleshoot the problem.

- Expired fragments remain on MSDP disk
- Incomplete SLP duplication jobs

Expired fragments remain on MSDP disk

Under some circumstances, the fragments that compose an expired backup image may remain on disk even though the images have expired. For example, if the storage server crashes, normal clean-up processes may not run. In those circumstances, you cannot delete a disk pool because image fragment records still exist. The error message may be similar to the following:

```
DSM has found that one or more volumes in the disk pool diskpoolname
has image fragments.
```

To delete the disk pool, you must first delete the image fragments. The `nbdelete` command deletes expired image fragments from disk volumes.

To delete the fragments of expired images

- Run the following command on the master server:

UNIX: `/usr/openv/netbackup/bin/admincmd/nbdelete -allvolumes -force`

Windows: `install_path\NetBackup\bin\admincmd\nbdelete -allvolumes -force`

The `-allvolumes` option deletes expired image fragments from all volumes that contain them.

The `-force` option removes the database entries of the image fragments even if fragment deletion fails.

Incomplete SLP duplication jobs

Incomplete storage lifecycle policy duplication jobs may prevent disk pool deletion. You can determine if incomplete jobs exist and then cancel them.

To cancel storage lifecycle policy duplication jobs

1. Determine if incomplete SLP duplication jobs exist by running the following command on the master server:

   UNIX: `/usr/openv/netbackup/bin/admincmd/nbstlutil stlilist -image_incomplete`

   Windows: *`install_path`*`\NetBackup\bin\admincmd\nbstlutil stlilist -image_incomplete`

2. Cancel the incomplete jobs by running the following command for each backup ID returned by the previous command (*xxxxx* represents the backup ID):

   UNIX: `/usr/openv/netbackup/bin/admincmd/nbstlutil cancel -backupid` *`xxxxx`*

   Windows: *`install_path`*`\NetBackup\bin\admincmd\nbstlutil cancel -backupid` *`xxxxx`*

MSDP media open error (83)

The `media open error (83)` message is a generic error for the duplication. The error appears in the **NetBackup Administration Console Activity Monitor**.

Often, the NetBackup Deduplication Engine (`spoold`) or the NetBackup Deduplication Manager (`spad`) were too busy to respond to the deduplication process in a timely manner. External factors may cause the Deduplication Engine or the Deduplication Manager to be unresponsive. Were they temporarily busy (such as queue processing in progress)? Do too many jobs run concurrently?

See "About MSDP performance" on page 34.

Usually but not always the NetBackup `bpdm` log provides additional information about status 83.

The following subsections describe use cases that generated an error 83.

SQL Server client-side backups fail

Client-side backups of a SQL Server database may fail in the following circumstances:

- The **Both IPv4 and IPv6** option is enabled for the master server, the media server that hosts the NetBackup Deduplication Engine, and the client. The **Both IPv4 and IPv6** option is configured in the **Network Settings** host properties.
- The IPv6 network is configured as a preferred network for the master server, the media server that hosts the NetBackup Deduplication Engine, and the client. The preferred network **Match (Above network will be preferred for communication)** property also is enabled. Preferred networks are configured in the **Preferred Networks** host properties.
- The IPv6 network is chosen for the backup.

Examine the `bpbrm` log file for an error similar to the following:

```
probe_ost_plugin: sts_get_server_prop_byname failed: error 2060057
```

If the error message appears, the NetBackup host name cache may not contain the correct host name mapping information. The cache may be out of sync if DNS changes in your network environment were not fully propagated throughout your environment. It takes some amount of time for DNS changes to propagate throughout a network environment.

To resolve the problem, do the following on the NetBackup master server and on the MSDP storage server:

1. Stop the NetBackup services.
2. Run the following command:

   UNIX: `/usr/openv/netbackup/bin/bpclntcmd -clearhostcache`

   Windows: *`install_path`*`\NetBackup\bin\bpclntcmd.exe -clearhostcache`
3. Start the NetBackup services.

For more information about client deduplication logging, see the description of “Client deduplication proxy plug-in” in the “MSDP log files” topic.

See “NetBackup MSDP log files” on page 347.

Restore or duplication fails

The `media open error (83)` message appears in the **NetBackup Administration Console Activity Monitor**.

Table 13-3 describes other messages that may appear.

Table 13-3 Case sensitivity error messages

Operation	Activity Monitor job details	Status in `bpdm` and `bptm` log files
Restore	`Image open failed: error 2060018: file not found`	`sts_open_image failed: error 2060018`
Duplication (MSDP source)	`Image open failed: error 2060018: file not found`	`sts_open_image failed: error 2060018`
Replication (MSDP source)	`get image properties failed: error 2060013: no more entries`	`rpl_add_image_set: rpl_get_image_info() failed, error 2060013`
Duplication (NetBackup 5000 series appliance source)	`Image open failed: error 2060018: file not found`	`sts_open_image failed: error 2060018`
Replication (NetBackup 5000 series appliance source)	`get image properties failed: error 2060013: no more entries`	`rpl_add_image_set: rpl_get_image_info() failed, error 2060013`

The messages may indicate a client name case sensitivity issue in your MSDP environment. For a description of the problem and the procedures to resolve it, see the following Veritas tech note:

http://www.veritas.com/docs/TECH207194

MSDP media write error (84)

Table 13-4 describes solutions to the media write errors that may occur during **Media Server Deduplication Pool** backups, duplication, or replication.

Also see the following subsections for descriptions of more complicated solutions:

- Host name resolution problems

Table 13-4 Media write error causes

The NetBackup Deduplication Engine (`spoold`) was too busy to respond.	Examine the Disk Logs report for errors that include the name PureDisk. Examine the disk monitoring services log files for details from the deduplication plug-in. See "Viewing MSDP disk reports" on page 275.
Data removal is running.	Data cannot be backed up at the same time as it is removed. See "About MSDP queue processing" on page 303.
A user tampered with the storage.	Users must not add files to, change files on, delete files from, or change file permissions on the storage. If a file was added, remove it.
Storage capacity was increased.	If you grew the storage, you must restart the NetBackup services on the storage server so the new capacity is recognized.
The storage is full.	If possible, increase the storage capacity. See "About adding additional MSDP storage" on page 44.
The deduplication pool is down.	Change the state to up. See "Changing Media Server Deduplication Pool state" on page 292.
Firewall ports are not open.	Ensure that ports 10082 and 10102 are open in any firewalls between the deduplication hosts.

Host name resolution problems

Client-side deduplication can fail if the client cannot resolve the host name of the server. More specifically, the error can occur if the storage server was configured with a short name and the client tries to resolve a fully qualified domain name

To determine which name the client uses for the storage server, examine the deduplication host configuration file on the client.

See "About the MSDP host configuration file" on page 219.

To fix this problem, configure your network environment so that all permutations of the storage server name resolve.

Veritas recommends that you use fully qualified domain names.

See "Use fully qualified domain names" on page 36.

Duplication job to PureDisk storage fails

Note: NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only.

A duplication job to PureDisk storage may fail for a large number of small files. This failure may occur if the storage unit maximum fragment is at the default setting.

Messages similar to the following may appear in the NetBackup job details:

```
2/12/2013 2:33:20 AM - Critical bpdm(pid=25204) Storage Server Error:
 (Storage server: PureDisk: msdp.example.com) async_get_job_status:
 Replication started but failed to complete successfully:  __process_batch:
 CRStoreDO failed: broken pipe, DO fingerprint d6f2521a5c66c54225ecd6a4c92.
 Look at the replication logs on the source storage server for more
 information. V-454-105
2/12/2013 2:33:22 AM - Critical bpdm(pid=25204) sts_copy_extent failed:
 error 2060014 operation aborted
2/12/2013 2:33:22 AM - end writing; write time: 3:39:53
2/12/2013 2:33:39 AM - Error bpduplicate(pid=5300) host
 msdp.example.com backup id msdp.example.com_1360303271 optimized
 duplication failed, media write error (84).
2/12/2013 2:33:39 AM - Info msdp.example.com(pid=25204)
 StorageServer=PureDisk:msdp.example.com; Report=PDDO Stats for
 (msdp.example.com): scanned: 0 KB, CR sent: 0 KB, CR sent over FC:
 0 KB, dedup: 0.0%, cache disabled
2/12/2013 2:33:40 AM - Error bpduplicate(pid=5300) Duplicate of backupid
 msdp.example.com_1360303271 failed, media write error (84).
2/12/2013 2:33:40 AM - Error bpduplicate(pid=5300) Status = no images
 were successfully processed.
2/12/2013 2:33:40 AM - end Duplicate; elapsed time: 3:41:03 media write
 error(84)
```

Messages similar to the following also may appear in a log file on the PureDisk content router that processed the duplication operation. The log file resides in a directory that corresponds to the connection to the content router for the duplication operation. The name of the directory is the NetBackup storage server IP address, and it resides in the `/Storage/log/spoold` directory on the content router.

```
spad/Store/2/266020624-1360833685.log:July 14 04:12:03 ERR [1081665856]:
25112: DO: DO 065ab494d80277148c559071d007bde1: DO record size of
378652257 bytes is larger than the maximum allowed size of 335544320
```

```
bytes: DO has too many segments
spad/Store/2/266020624-1360833685.log:February 14 04:12:03 ERR
[1081665856]: 8413608: Store terminated due to a local processing
error at: Sun Jul 14 04:12:03 2013
```

To resolve this problem, reduce the fragment size of the NetBackup storage unit that represents the PureDisk storage. Depending on the source storage content, you may have to reduce the fragment size significantly.

MSDP no images successfully processed (191)

The `no images successfully processed (191)` message appears in the **NetBackup Administration Console Activity Monitor**.

Table 13-5 describes other messages that may appear.

Table 13-5 Case sensitivity error messages

Operation	Activity Monitor job details	Status in `bpdm` and `bptm` log files
Verify	`image open failed: error 2060018: file not found`	`sts_open_image failed: error 2060018`

The message may indicate a client name case sensitivity issue in your MSDP environment. For a description of the problem and the procedures to resolve it, see the following Veritas tech note:

http://www.veritas.com/docs/TECH207194

MSDP storage full conditions

Operating system tools such as the UNIX `df` command do not report deduplication disk usage accurately. The operating system commands may report that the storage is full when it is not. NetBackup tools let you monitor storage capacity and usage more accurately.

Note: In a CloudCatalyst environment, however, the UNIX `df` command can be used to determine the disk space in the local cache directory.

See "About MSDP storage capacity and usage reporting" on page 272.

See "About MSDP container files" on page 273.

See "Viewing storage usage within MSDP container files" on page 274.

Examining the disk log reports for threshold warnings can give you an idea of when a storage full condition may occur.

How NetBackup performs maintenance can affect when storage is freed up for use.

See "About MSDP queue processing" on page 303.

See "About the MSDP data removal process" on page 312.

Although not advised, you can reclaim free space manually.

See "Processing the MSDP transaction queue manually" on page 303.

Troubleshooting MSDP catalog backup

The following subsections provide information about MSDP catalog backup and recovery.

Catalog backup

Table 13-6 describes error messages that may occur when you create or update a catalog backup policy. The messages are displayed in the shell window in which you ran the `drcontrol` utility. The utility also writes the messages to its log file.

Table 13-6 MSDP drcontrol codes and messages

Code or message	Description
1	Fatal error in an operating system or deduplication command that the `drcontrol` utility calls.
110	The command cannot find the necessary NetBackup configuration information.
140	The user who invoked the command does not have administrator privileges.
144	A command option or argument is required.
226	The policy name that you specified already exists.
227	This error code is passed from the NetBackup `bplist` command. The MSDP catalog backup policy you specified does not exist or no backups exist for the given policy name.
255	Fatal error in the `drcontrol` utility.

For more information about status codes and error messages, see the following:

- The Troubleshooter in the NetBackup Administration Console.
- The *NetBackup Status Codes Reference Guide* available through the following webpage:
  http://www.veritas.com/docs/DOC5332

Catalog recovery from a shadow copy

If NetBackup detects corruption in the MSDP catalog, the Deduplication Manager recovers the catalog automatically from the most recent shadow copy. That recovery process also plays a transaction log so that the recovered MSDP catalog is current.

Although the shadow copy recovery process is automatic, a recovery procedure is available if you need to recover from a shadow copy manually.

See "Restoring the MSDP catalog from a shadow copy" on page 319.

Viewing MSDP disk errors and events

You can view disk errors and events in several ways, as follows:

- The Disk Logs report.
  See "Viewing MSDP disk reports" on page 275.
- The NetBackup `bperror` command with the `-disk` option reports on disk errors. The command resides in the following directories:
  UNIX: `/usr/openv/netbackup/bin/admincmd`
  Windows: *`install_path`*`\Veritas\NetBackup\bin\admincmd`

MSDP event codes and messages

The following table shows the deduplication event codes and their messages. Event codes appear in the `bperror` command `-disk` output and in the disk reports in the NetBackup Administration Console.

Table 13-7 MSDP event codes and messages

Event #	Event Severity	NetBackup Severity	Message example
1000	2	Error	`Operation configload/reload failed on server PureDisk:server1.example.com on host server1.example.com.`
1001	2	Error	`Operation configload/reload failed on server PureDisk:server1.example.com on host server1.example.com.`
1002	4	Warning	`The open file limit exceeded in server PureDisk:server1.example.com on host server1.example.com. Will attempt to continue further.`
1003	2	Error	`A connection request was denied on the server PureDisk:server1.example.com on host server1.example.com.`

Table 13-7 MSDP event codes and messages *(continued)*

Event #	Event Severity	NetBackup Severity	Message example
1004	1	Critical	`Network failure occurred in server PureDisk:server1.example.com on host server1.example.com.`
1008	2	Error	`Task Aborted; An unexpected error occurred during communication with remote system in server PureDisk:server1.example.com on host server1.example.com.`
1009	8	Authorization	`Authorization request from <IP> for user <USER> denied (<REASON>).`
1010	2	Error	`Task initialization on server PureDisk:server1.example.com on host server1.example.com got an unexpected error.`
1011	16	Info	`Task ended on server PureDisk:server1.example.com on host server1.example.com.`
1013	1	Critical	`Task session start request on server PureDisk:server1.example.com on host server1.example.com got an unexpected error.`
1012	2	Error	`A request for agent task was denied on server PureDisk:server1.example.com on host server1.example.com.`
1014	1	Critical	`Task session start request on server PureDisk:server1.example.com on host server1.example.com got an unexpected error.`
1015	1	Critical	`Task creation failed, could not initialize task class on server PureDisk:server1.example.com on host server1.example.com.`
1017	1	Critical	`Service Veritas DeduplicationEngine exit on server PureDisk:server1.example.com on host server1.example.com. Please check the server log for the probable cause of this error. The application has terminated.`
1018	16	Info	`Startup of Veritas Deduplication Engine completed successfully on server1.example.com.`
1019	1	Critical	`Service Veritas DeduplicationEngine restart on server PureDisk:server1.example.com on host server1.example.com. Please check the server log for the probable cause of this error. The application has restarted.`

Table 13-7 MSDP event codes and messages *(continued)*

Event #	Event Severity	NetBackup Severity	Message example
1020	1	Critical	Service Veritas Deduplication Engine connection manager restart failed on server PureDisk:server1.example.com on host server1.example.com. Please check the server log for the probable cause of this error.The application has failed to restart.
1028	1	Critical	Service Veritas DeduplicationEngine abort on server PureDisk:server1.example.com on host server1.example.com. Please check the server log for the probable cause of this error.The application has caught an unexpected signal.
1029	1	Critical	Double backend initialization failure; Could not initialize storage backend or cache failure detected on host PureDisk:server1.example.com in server server1.example.com.
1030	1	Critical	Operation Storage Database Initialization failed on server PureDisk:server1.example.com on host server1.example.com.
1031	1	Critical	Operation Content router context initialization failed on server PureDisk:server1.example.com on host server1.example.com.
1032	1	Critical	Operation log path creation/print failed on server PureDisk:server1.example.com on host server1.example.com.
1036	4	Warning	Operation a transaction failed on server PureDisk:server1.example.com on host server1.example.com.
1037	4	Warning	Transaction failed on server PureDisk:server1.example.com on host server1.example.com. Transaction will be retried.
1040	2	Error	Operation Database recovery failed on server PureDisk:server1.example.com on host server1.example.com.
1043	2	Error	Operation Storage recovery failed on server PureDisk:server1.example.com on host server1.example.com.
1044	multiple	multiple	The usage of one or more system resources has exceeded a warning level. Operations will or could be suspended. Please take action immediately to remedy this situation.

Table 13-7 MSDP event codes and messages *(continued)*

Event #	Event Severity	NetBackup Severity	Message example
1057			`A data corruption has been detected.` The data consistency check detected a data loss or data corruption in the Media Server Deduplication Pool (MSDP) and reported the affected backups. The backup ID and policy name appear in the NetBackup Disk Logs report and the *`storage_path`*`/log/spoold/storaged.log` file on the storage server.
2000		Error	`Low space threshold exceeded on the partition containing the storage database on server PureDisk:server1.example.com on host server1.example.com.`

Troubleshooting CloudCatalyst issues

The following sections may help you troubleshoot issues that involve NetBackup CloudCatalyst.

See "CloudCatalyst logs" on page 373.

See "Problems encountered while using the Cloud Storage Server Configuration Wizard" on page 375.

See "Disk pool problems" on page 377.

See "Problems during cloud storage server configuration" on page 378.

See "Status 191: No images were successfully processed" on page 380.

See "Media write error (84) if due to a full local cache directory" on page 380.

See "Restarting the vxesfsd process" on page 381.

See "Problems restarting vxesfsd" on page 382.

See "CloudCatalyst troubleshooting tools" on page 383.

CloudCatalyst logs

In addition to the MSDP logs, NetBackup CloudCatalyst creates additional logs.

The logs for the `vxesfsd` process are located in the following directory:

- `/usr/openv/netbackup/logs/esfs_database`
- `/usr/openv/netbackup/logs/esfs_filesystem`
- `/usr/openv/netbackup/logs/esfs_monitor`

- /usr/openv/netbackup/logs/esfs_storage
- /usr/openv/netbackup/logs/esfs_storagemanager

The logs generated by the ESFS file system are located in the following directory:

- /usr/openv/esfs/log/ops/esfs-config.*
- /usr/openv/esfs/log/ops/esfs-run.*

The location of the logs is configurable in the esfs.json file.

See "About the CloudCatalyst esfs.json configuration file" on page 248.

Error messages in esfs_storage

The following error message may be found in the esfs_storage log:

/usr/openv/netbackup/logs/esfs_storage:

Error message	DEBUG - "ESP ERROR [create_or_open_image_v10]exceed max connections."
Diagnosis	One possible cause is that throttling has been set up incorrectly or incompletely on the CloudCatalyst storage server. The correct values must be set in the following locations: ■ The **Scalable Storage** media server host properties. ■ The cloud storage server properties. The values that are entered in the **NetBackup Administration Console** depend on the UploadThreads and DownloadThreads values that are set in the esfs.json file on the CloudCatalyst storage server. See the following topic for CloudCatalyst throttling configuration information: See "Controlling data traffic to the cloud when using CloudCatalyst" on page 254.

Error messages in esfs_filesystem

The following error message may be found in the esfs_filesystem log:

/usr/openv/netbackup/logs/esfs_filesystem:

Error message	ERROR - "Failed to write /data/521/534297.bhd allow_write F skip_write_fail F"

Diagnosis	One possible cause is that cache eviction cannot clean up any data from the local cache directory for non-MSDP system file writes. The cache eviction is triggered when the high watermark setting (`HighWatermark`) for the directory is reached. Files that have not yet been uploaded to the cloud cannot be deleted. This error occurs if files pending upload are also targeted for cache eviction. In this situation, if the cache eviction can't delete enough files to satisfy the high watermark, the write operation will fail. Since the upload speed to the cloud is slower than the hard disk drive write speed, this situation can arise when the partition for the local cache directory is small. Increase the space that is allowed for the local cache directory.

Problems encountered while using the Cloud Storage Server Configuration Wizard

The following topics are problems that a user might encounter while using the Cloud Storage Server Configuration Wizard to configure a CloudCatalyst storage server.

Unable to select the desired media server

In the **Add Storage Server** wizard screen, the user selects a media server in the drop-down menu that will become the CloudCatalyst storage server.

If the media server that you want to use does not appear in the drop-down menu, check the following:

Media server version

The NetBackup media servers that you use as CloudCatalyst storage servers must be the same NetBackup version as the master server.

Host name-based security certificate

If the media server that you want to use does not appear in the drop-down menu, make sure that a host name-based security certificate has been deployed for that media server. Use the following procedure to deploy a certificate if needed.

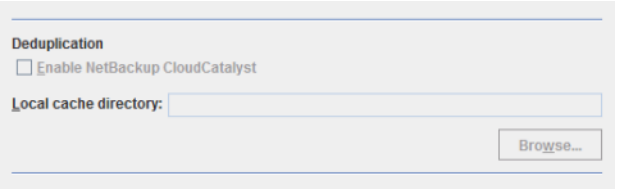
1. `/usr/openv/netbackup/bin/admincmd/bpnbaz -ProvisionCert` *`host_name`*
2. Restart the services on the media server after generating a certificate.

Unable to select the Deduplication option

To create a CloudCatalyst storage server, the **Enable NetBackup CloudCatalyst** option must be selected in the Cloud Storage Server Configuration Wizard. Also, a directory must be indicated as the **Local cache directory**.

These options are grayed out if any of the following cases are true:

- The selected media server does not have NetBackup 8.1 or later installed.
- CloudCatalyst does not support the media server operating system.
- CloudCatalyst does not support the cloud vendor.



See the NetBackup compatibility lists for support information:

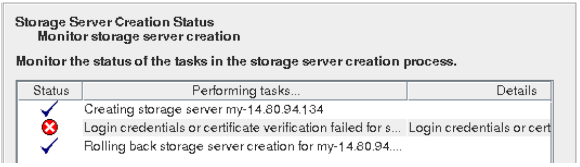
http://www.netbackup.com/compatibility

Storage Server Creation Status errors

The following errors may appear in the Storage Server Creation Status wizard screen.

Login credentials or certificate failed message

The following error may appear in the Storage Server Creation Status wizard screen if CloudCatalyst is being configured for use with a private cloud.



The full error is as follows:

`Login credentials or certificate verification failed for server` *`media_server`*

Logs that are related to this error can be found in the `/usr/openv/volmgr/debug/tpconfig` logs.

Make sure the SSL (Secure Sockets Layer) is configured properly on the private cloud server.

NetBackup supports only Certificate Authority (CA)-signed certificates while it communicates with cloud storage in the SSL mode. Ensure that the cloud server has CA-signed certificate. If it does not have the CA-signed certificate, data transfer between NetBackup and the cloud provider fails in the SSL mode.

The *NetBackup Cloud Administrator's Guide* contains information about SSL mode in private clouds:

http://www.veritas.com/docs/DOC5332

Failure to add credentials

The wizard may display a failure to add credentials if the media server had previously been configured as a CloudCatalyst storage server. It also fails if the media server is currently configured as a CloudCatalyst storage server.

Run the `esfs_cleanup.sh` script on the media server to remove all CloudCatalyst-related information from the server.

The script is located in the following directory:

`usr/openv/esfs/scripts/esfs_cleanup.sh`

Disk pool problems

The following topics present issues concerning disk pools and CloudCatalyst storage servers.

See "Disk pool creation problem due to timeout issue" on page 377.

See "One disk pool for each CloudCatalyst storage server" on page 378.

Disk pool creation problem due to timeout issue

For disk pool failures while creating a disk pool for a CloudCatalyst storage server, search for an error message that is similar to the following:

```
Cannot upload MSDP system files, done 5 error code 0, tried 300 times
```

The log is located in `usr/openv/netbackup/logs/esfs_filesystem`.

If the error shows that 300 attempts were made, the failure was due to a timeout issue. A slow network connection to the cloud is often the cause. Check network connections before contacting Veritas Support.

One disk pool for each CloudCatalyst storage server

Each CloudCatalyst storage server may have only one disk pool.

The following error message appears if the user attempts to create a second disk pool for the cloud storage server:

```
The CloudCatalyst disk volume cannot be reconfigured for this storage server.
```

Problems during cloud storage server configuration

The following errors may appear during configuration of a CloudCatalyst storage server.

Table 13-8 Cloud storage server configuration errors

Error	Reason
An unknown error occurred in the CloudCatalyst subsystem	This is a general configuration error. Check the following log for more specific information: `/usr/openv/esfs/log/ops/esfs-config.log.*` Contact Veritas Support to determine a corrective action.
An error occurred in ESFS initialization	This error may occur if the `esfs_init.sh` script is run without all of the required parameters. Check the following log for more specific information: `/usr/openv/esfs/log/ops/esfs-config.log.*`
FUSE not installed	NetBackup installs the Filesystem in Userspace (FUSE) upon installation. If the FUSE version is too old, this message appears. Contact Veritas Support to determine the correct version of FUSE to install it.
Unsupported ESFS operating system	A CloudCatalyst storage server can be configured on a media server only if the host is running Red Hat Enterprise Linux 7.3 or later. See the NetBackup compatibility lists for support information: http://www.netbackup.com/compatibility
The CloudCatalyst service could not be started	Check that the `vxesfsd` daemon has sufficient memory to run. Check the following log for more specific information: `/usr/openv/esfs/log/ops/esfs-config.log. *`

Table 13-8 Cloud storage server configuration errors *(continued)*

Error	Reason
An ESFS mount could not be found	This error indicates that something is preventing the NetBackup Extendable Storage File System (ESFS) from starting properly. There may also be a problem with the `vxesfsd` process. Check the following log for more specific information: `/usr/openv/esfs/log/ops/esfs-config.log. *` Contact Veritas Support to determine a corrective action.

Media server not available in Media Servers tab to add credentials

The CloudCatalyst storage server can allow access to media servers only if they are Red Hat Enterprise Linux (any version) and have NetBackup 8.1 or later installed. Access is given to media servers by granting them credentials in the **Media Servers** tab of the CloudCatalyst storage server properties.

If the media server does not have NetBackup 8.1 or later installed, it does not appear in the **Media Servers** tab, so it cannot be selected.

See "Configuring push or pull optimized duplication for CloudCatalyst" on page 256.

Add credentials failed message for media server

The CloudCatalyst storage server can allow access to media servers only if they are Red Hat Enterprise Linux (any version) and have NetBackup 8.1 or later installed. Access is given to media servers by granting them credentials in the **Media Servers** tab of the CloudCatalyst storage server properties.

If the media server is non-RHEL, it appears in the **Media Servers** tab. However, if it is selected to have access to the CloudCatalyst storage server, the operation fails with an **Add credentials failed** message.

See “Configuring push or pull optimized duplication for CloudCatalyst” on page 256.

Status 191: No images were successfully processed

The `no images were successfully processed (191)` message can appear for a duplication job in the **Detailed Status** tab of the **Activity Monitor**.

Storage unit configuration for selecting media servers

Part of creating a cloud storage server includes creating a disk pool and storage unit. When creating the storage unit, you must indicate whether NetBackup can use any available media server or whether NetBackup should use only specific media servers. To configure load balancing for push optimized duplications, select **Only use the following media servers** and then specify the media server that hosts the MSDP storage server.

See “Configuring push or pull optimized duplication for CloudCatalyst” on page 256.

Media write error (84) if due to a full local cache directory

One possible cause for a `media write error (84)` in a CloudCatalyst environment is described in the following topic.

The administrator configures a local cache directory as part of configuring a CloudCatalyst storage server. Cache eviction is triggered when data causes this directory to reach the high watermark setting (`HighWatermark`). If files in the local cache directory have not been uploaded to the cloud, the files cannot be evicted (deleted) from the directory. In this situation, the directory does not have enough space for new files and the MSDP write operation fails with a `media write error (84)`.

This error is more likely to occur when a relatively small disk is used for demonstration or proof-of-concept testing. To prevent this error in a production environment, make sure that there is at least 4 TB of disk space available for the cache. Make sure that the cache is located on a dedicated file system that is used only for the CloudCatalyst local cache.

After receiving a `media write error (84)` and addressing the cause, restart all NetBackup services to avoid a `media open error (83)`.

The UNIX `df` command can be used to determine the disk space in the local cache directory. For example:

```
df /esfs
Filesystem     1K-blocks  Used       Available  Use%  Mounted on
/dev/loop0     1007896    1007896    0          100%  /esfs
```

See the following topic for more information about CloudCatalyst local cache considerations:

See “About the CloudCatalyst cache” on page 252.

Trouble restarting ESFS after the CloudCatalyst storage server is down

If the CloudCatalyst storage server goes down abnormally, ESFS (`vxesfsd`) may not restart when NetBackup is restarted.

To allow `vxesfsd` to start, check the following location to see if a `rocksdb.log` file was created:

```
/cache/fsdb/log
```

Remove the `rocksdb.log` file and restart the NetBackup services.

Restarting the vxesfsd process

To restart the Veritas NetBackup Extendable Storage File System Service (`vxesfsd`), the process must first be stopped.

- Before stopping `vxesfsd`, make sure that no processes are using `vxesfsd`, including the current working directory of any user.
  The NetBackup Deduplication Manager (`spad`) and the NetBackup Deduplication Engine (`spoold`) use `vxesfsd`, so they need to be stopped if either is running.
- Before starting `vxesfsd`, make sure that no data exists in the mount point. If data exists in the mount point, `vxesfsd` fails to restart.

The following methods assume that no jobs are running.

Using the Activity Monitor to stop and start processes specific to vxesfsd

Using the Activity Monitor to stop the processes specific to vxesfsd

1. In the **NetBackup Administration Console**, click **Activity Monitor**.
2. On the **Daemons** tab, select the `spoold`.
3. On the **Actions** menu, select **Stop Daemon**.
4. Stop `spad`.
5. Stop `vxesfsd`.

Using the Activity Monitor to start the processes specific to vxesfsd

1. In the **NetBackup Administration Console**, click **Activity Monitor**.
2. On the **Daemons** tab, select `vxesfsd`.
3. On the **Actions** menu, select **Start Daemon**.
4. Start `spoold`.
5. Start `spad`.

Using the command line to stop and start processes specific to vxesfsd

To stop and start processes that are specific to `vxesfsd` (and to avoid stopping all NetBackup processes), run:

```
/usr/openv/netbackup/bin/nbsvcmon -terminate
/usr/openv/pdde/pdconfigure/pdde stop
/usr/openv/netbackup/bin/vxesfsd stop
```

To start these processes:

- To start `vxesfsd`, run:

  ```
  /usr/openv/esfs/bin/vxesfsd start
  /usr/openv/pdde/pdconfigure/pdde start
  ```

- To start `nbsvcmon`, run:

  ```
  /usr/openv/netbackup/bin/nbsvcmon &
  ```

Stopping and starting all NetBackup processes

To stop and start all processes, run the following command on the CloudCatalyst storage server:

```
/etc/init.d/NetBackup stop
/etc/init.d/NetBackup start
```

Problems restarting vxesfsd

Restarting `vxesfsd` fails if processes are accessing the ESFS mount point when NetBackup is attempting to shut it down.

See the following log to determine if this is the problem:

`/usr/openv/esfs/log/ops/esfs-run.`*`process_id`*

In the following example, the mount point directory is `/space/d2c/storage`.

```
Wed Jul 5 15:44:34 CDT 2017 Calling "umount /space/CC/storage"
to stop vxesfsd gracefully
umount: /space/d2c/storage: target is busy.
        (In some cases useful info about processes that use
         the device is found by lsof(8) or fuser(1))
Wed Jul 5 15:44:45 CDT 2017 Sending SIGKILL to vxesfsd
Wed Jul 5 15:44:45 CDT 2017 Calling "umount /space/CC/storage"
after hard kill of vxesfsd
umount: /space/CC/storage: target is busy.
        (In some cases useful info about processes that use
         the device is found by lsof(8) or fuser(1))
Wed Jul 5 15:44:45 CDT 2017 Sending SIGKILL to vxesp
```

Note that after the hard kill of `vxesfsd`, the target remains busy.

To check if any processes are using the ESFS mount point

1. Unmount the mount directory:

   `umount mount_dir`

   or

   `lsof mount_dir`

2. Verify that the directory is not mounted:

   `mount | grep mount_dir`

   or

   `lsof | grep mount_dir`

3. Restart `vxesfsd`:

   ```
   /usr/openv/esfs/bin/vxesfsd start
   /usr/openv/pdde/pdconfigure/pdde start
   ```

CloudCatalyst troubleshooting tools

NetBackup offers several tools that can help to troubleshoot CloudCatalyst problems.

See “esfs_cleanup.sh script” on page 384.

See “esfs_check consistency checking tool” on page 384.

See “setlsu_ioctl tool” on page 385.

esfs_cleanup.sh script

In certain conditions, use the `esfs_cleanup.sh` script on the CloudCatalyst storage server to remove all CloudCatalyst-related information from the host.

For example, when decommissioning CloudCatalyst cloud storage. (See "Decommissioning CloudCatalyst cloud storage" on page 261.)

The script is located in the following directory:

`usr/openv/esfs/scripts/esfs_cleanup.sh`

esfs_check consistency checking tool

The `esfs_check` tool determines whether the data that is stored in the cloud and the data in the ESFS database are consistent, and then reports any inconsistencies between the two.

Note: Since the tool reads data from the cloud, it is likely that the NetBackup customer will incur a financial cost by the cloud vendor. Consider contacting Veritas Support before running the tool.

The `esfs_check` tool is located in the following directory: `/usr/openv/esfs/bin`

It uses the following syntax:

`esfs_check -cachedir` *`path_to_local_cache`* `[-strict] [-verbose]`

Where:

- *`path_to_local_cache`* is the path to the local cache directory.
- The `-strict` option provides an additional check to compare the file size in the local cache with the file size in the ESFS database.
- The `-verbose` option enables logging to the following directory: `/usr/openv/esfs/log/ops/esfs_check`

Before running the `esfs_check` tool:

- To ensure accurate results, the system should not have any active backup or duplication jobs to the cloud.
- Shut down NetBackup services except for the ESFS daemons. Only `vxesfsd` and `vxesp` should be running.

Example where the data is consistent

The following example output shows that the data that is stored in the cloud is consistent with the ESFS database.

```
esfs_check -cachedir /root/cache/msdp/ -verbose
consistency check successful
```

Example where the data is inconsistent

The following example output shows that there are inconsistencies between the cloud and the ESFS database.

```
esfs_check -cachedir /root/cache/msdp/ -verbose
File /data/2/97.bin not exist in cloud, expect in cloud
File /data/2/97.bin not exist in cache/cloud
```

Output line 1 means that file `/data/2/97.bin` appears in the ESFS database and should also be in the cloud, but it is not.

Output line 2 means that file `/data/2/97.bin` appears in the ESFS database, but is neither in the cloud nor the local cache.

If the `esfs_check` tool finds an inconsistency, contact Veritas Support.

setlsu_ioctl tool

This tool is used in a disaster recovery scenario to set the cloud bucket name.

The `setlsu_ioctl` tool is located in the following directory: `/usr/openv/esfs/bin`

It uses the following syntax:

`./setlsu_ioctl /`*`cache_directory`*`/storage/proc/cloud.lsu `*`name_of bucket`*

Appendix A

Migrating to MSDP storage

This appendix includes the following topics:

- Migrating from PureDisk to the NetBackup MSDP
- Migrating from another storage type to MSDP

Migrating from PureDisk to the NetBackup MSDP

Note: NetBackup supports **PureDisk Deduplication Pool** storage on NetBackup 5000 series appliances only.

NetBackup cannot use the storage hardware while PureDisk uses it for storage. The structure of the PureDisk storage is different than the structure of the storage for integrated NetBackup deduplication. The disk systems cannot be used simultaneously by both NetBackup and PureDisk. The PureDisk images on the storage cannot be transferred to the deduplication storage server storage.

Therefore, to replace a NetBackup 5000 series appliance with the NetBackup Media Server Deduplication Option, migrate the storage to a NetBackup **Media Server Deduplication Pool**.

Table A-1 To migrate from PureDisk to NetBackup MSDP

Step	Task	Procedure
Step 1	Install and configure NetBackup	See the *NetBackup Installation Guide for UNIX and Windows*: http://www.veritas.com/docs/DOC5332

Table A-1 To migrate from PureDisk to NetBackup MSDP *(continued)*

Step	Task	Procedure
Step 2	Configure NetBackup deduplication	See "Configuring MSDP server-side deduplication" on page 50.
Step 3	Redirect your backup jobs	Redirect your backup jobs to the NetBackup **Media Server Deduplication Pool**. See the *NetBackup Administrator's Guide, Volume I*: http://www.veritas.com/docs/DOC5332
Step 4	Decommission your appliance	Optionally, after the backup images expire on your NetBackup 5000 series appliance, decommission your NetBackup 5000 series appliance. See your NetBackup PureDisk documentation.

See "Migrating from another storage type to MSDP" on page 387.

Migrating from another storage type to MSDP

To migrate from another NetBackup storage type to deduplication storage, Veritas recommends that you age the backup images on the other storage until they expire. Veritas recommends that you age the backup images if you migrate from disk storage or tape storage.

You should not use the same disk storage for NetBackup deduplication while you use it for other storage such as AdvancedDisk. Each type manages the storage differently and each requires exclusive use of the storage. Also, the NetBackup Deduplication Engine cannot read the backup images that another NetBackup storage type created. Therefore, you should age the data so it expires before you repurpose the storage hardware. Until that data expires, two storage destinations exist: the media server deduplication pool and the other storage. After the images on the other storage expire and are deleted, you can repurpose it for other storage needs.

Table A-2 Migrating to NetBackup MSDP

Step	Task	Procedure
Step 1	Configure NetBackup deduplication	See "Configuring MSDP server-side deduplication" on page 50.

Table A-2 Migrating to NetBackup MSDP *(continued)*

Step	Task	Procedure
Step 2	Redirect your backup jobs	Redirect your backup jobs to the media server deduplication pool storage unit. To do so, change the backup policy storage destination to the storage unit for the deduplication pool. See the *NetBackup Administrator's Guide, Volume I*: http://www.veritas.com/docs/DOC5332
Step 3	Repurpose the storage	After all of the backup images that are associated with the storage expire, repurpose that storage. If it is disk storage, you cannot add it to an existing media server deduplication pool. You can use it as storage for another, new deduplication node.

See “Migrating from PureDisk to the NetBackup MSDP” on page 386.

Index

A

Active secondary operations 186
Add at least one index marker 113
Add credentials failed 257, 379
Advanced Encryption Standard (AES) encryption 124
AES encryption
    Blowfish encryption 131
AES-256 128–129
appliance deduplication 13
attributes
    clearing deduplication pool 299
    clearing deduplication storage server 283
    OptimizedImage 33
    setting deduplication pool 293
    setting deduplication storage server 281
    viewing deduplication pool 292
    viewing deduplication storage server 280
Auto Image Replication
    about 153
    and trusted master servers 161
    Backup operation in source domain 151, 154
    configuring MSDP replication to a different domain 152
    for MSDP 172
    no disk spanning support 154
    overview 153
    synchronizing clocks of master servers 154
    Targeted 162, 171
    topology of storage 158

B

Backup
    operation 185
backup
    client deduplication process 337
big endian 323, 326
bpstsinfo command 159
byte order 323, 326

C

cache hits field of the job details 270
Cannot upload MSDP system files error 377
capacity
    adding storage 44
capacity and usage reporting for deduplication 272
case sensitivity
    in NetBackup names 16
catalog, MSDP. *See* about recovering the MSDP catalog. *See* MSDP catalog
certificate, generating for CloudCatalyst storage server 245
changing deduplication server hostname 284
changing the deduplication storage server name and path 284
CIFS 20
clearing deduplication pool attributes 299
client deduplication
    components 337
    disabling for a specific client 121
    host requirements 29
Client Direct deduplication
    where not supported 120, 239
CloudCatalyst
    additional drcontrol option 228
    Appliance
        configuring 241
        documentation 239
        for deduplication to the cloud 235
        technical specifications 240
    Client Direct deduplication 120
    direct to cloud (not the preferred use case) 235, 237
    disaster recovery 266
    limitations 238
    load balancing 25, 79, 239
    Local cache directory 248
    local cache directory 247, 253–254
    logs
        esfs_filesystem 374
        esfs_storage 374

CloudCatalyst *(continued)*
logs *(continued)*
location 373
media server version 239, 375
overview 235
preferred use case 235, 241, 244, 247
pull optimized duplication 256
push optimized duplication 256
vxesfsd process 255, 262
clustering
master server inter-node authentication 171
Common Internet File System 20
compacting container files 274
compression
for MSDP backups 122
for MSDP optimized duplication and replication 122
pd.conf file setting 199
configuring a deduplication pool 103
configuring a deduplication storage server 73, 91
configuring a deduplication storage unit 115
configuring deduplication 50, 53, 247
container files
about 273
compaction 274
viewing capacity within 274
contentrouter.cfg file
about 215
parameters for data integrity checking 308
ServerOptions for encryption 127
Coordinated Universal Time (UTC) 154
CR sent field of the job details 271
crcontrol 130
credentials 30
adding NetBackup Deduplication Engine 289
changing NetBackup Deduplication Engine 290
on media servers in CloudCatalyst configuration 256, 258–259

D

DACDays (Delete After Close Days) CloudCatalyst setting 250
data classifications
in storage lifecycle policies 179, 185
data conversion
encryption 129
data integrity checking
about deduplication 304
configuration settings for deduplication 307
data integrity checking *(continued)*
configuring behavior for deduplication 305
data removal process
for deduplication 312
database system error 355
deactivating media server deduplication 329
dedup field of the job details 271
deduplication
about credentials 30
about fingerprinting 62
about the license 46
adding credentials 289
and Fibre Channel 21
and iSCSI 21
cache hits field of the job details 270
capacity and usage reporting 272
changing credentials 290
client backup process 337
configuration file 197
configuring 50, 53, 247
configuring optimized synthetic backups 132
container files 273
CR sent field of the job details 271
data removal process 312
dedup field of the job details 271
event codes 370
license for 46
licensing 47
limitations 27
media server process 334
network interface 31
node 17
performance 34
planning deployment 15
requirements for optimized within the same domain 136
scaling 36
scanned field of the job details 271
storage capacity 18
storage destination 17
storage management 45
storage requirements 19
storage unit properties 117
to the cloud 235
deduplication configuration file
editing 61, 198
parameters 199
deduplication data integrity checking
about 304

deduplication data integrity checking *(continued)*
configuring behavior for 305
settings 307
deduplication deduplication pool. *See* deduplication pool
deduplication disk volume
changing the state 300
determining the state 300
deduplication encryption
enabling for MSDP backups 126
deduplication host configuration file 219
deleting 219
deduplication hosts
and firewalls 32
client requirements 29
load balancing server 25
server requirements 25
storage server 24
deduplication installation
log file 352
deduplication logs
about 348
client deduplication proxy plug-in log 350
client deduplication proxy server log 350
configuration script 350
deduplication plug-in log 351
NetBackup Deduplication Engine 352
NetBackup Deduplication Manager 353
VxUL deduplication logs 348
deduplication node
about 17
adding a load balancing server 194
removing a load balancing server 286
deduplication optimized synthetic backups
about 33
deduplication plug-in
about 332
log file 351
deduplication plug-in configuration file
configuring 56
deduplication pool. *See* deduplication pool
about 101
changing properties 294
clearing attributes 299
configuring 103
deleting 302
determining the state 291
properties 110
setting attributes 293
deduplication pool *(continued)*
viewing 291
viewing attributes 292
deduplication port usage
about 32
troubleshooting 366
deduplication processes do not start 358
deduplication rate
how file size affects 35
monitoring 267
deduplication reference database
about 332
deduplication registry
resetting 220
deduplication servers
components 331
host requirements 25
deduplication storage capacity
about 18
viewing capacity in container files 274
deduplication storage destination 17
deduplication storage requirements 19
deduplication storage server
about 24
change the name 284
changing properties 282
clearing attributes 283
components 331
configuration failure 356
configuring 73, 91
defining target for Auto Image Replication 158
deleting 287
deleting the configuration 288
determining the state 279
editing configuration file 217
getting the configuration 216
recovery 322
replacing the host 326
setting attributes 281
setting the configuration 218
viewing 279
viewing attributes 280
deduplication storage server configuration file
about 215
deduplication storage server name
changing 284
deduplication storage type 17
Deduplication storage unit
Only use the following media servers 117

Deduplication storage unit *(continued)*
Use any available media server 117
deduplication to the cloud
direct to cloud 237
deleting backup images 302
deleting CloudCatalyst cloud storage 261
deleting deduplication host configuration file 219
df command 368, 380
disaster recovery
for CloudCatalyst 266
protecting the data 40
recovering the storage server after catalog recovery 325
disk failure
deduplication storage server 321
disk logs 276
disk logs report 273
disk pool status report 273, 276
disk pools
cannot delete 362
changing the state 292
creation failure for CloudCatalyst 377
failure for CloudCatalyst 378
disk storage unit report 276
Disk type 117
disk volume
changing the state 300
determining the state of a deduplication 300
volume state changes to down 361
domains
replicating backups to another. *See* Auto Image Replication
DownloadThreads CloudCatalyst setting 252, 374
Duplication
optimized 186
duplication jobs, cancelling 363
Duplication to remote master. *See* Auto Image Replication

E

Enable file recovery from VM backup 187
encryption
enabling for MSDP backups 126
pd.conf file setting 202
SHA-2 62, 128–129
endian
big 323, 326
little 323, 326
ESFS database 374, 384
esfs.json configuration file 248, 252, 254–255, 374
esfs_check tool 384
esfs_cleanup.sh script 261, 377, 384
event codes
deduplication 370

F

Fibre Channel
and iSCSI comparison 21
support for 20
Fibre Channel and iSCSI comparison for MSDP 21
file system
CIFS 20
NFS 20
Veritas File System for deduplication storage 45
ZFS 20
File System Database (FSDB) 262
Filesystem in Userspace (FUSE) 262, 378
fingerprinting
about deduplication 62
firewalls and deduplication hosts 32
FlashBackup policy
Maximum fragment size (storage unit setting) 117
FQDN or IP Address property in Resilient Network host properties 190
FSDB (File System Database) 262
FUSE (Filesystem in Userspace) 262, 378

G

garbage collection. *See* queue processing
Global logging level property 250

H

HighWatermark CloudCatalyst setting 251, 375, 380
host requirements 25

I

images on disk report 275
Import
operation 180
iSCSI
and Fibre Channel comparison 21
support for 20

J

job ID search in unified logs 345

K

KMS encryption 242, 245, 247, 254

L

legacy logging 346
    directories 346
    locations 346
Level (logging) CloudCatalyst setting 250
license
    for deduplication 46
license information failure
    for deduplication 356
licensing deduplication 47
limitations
    media server deduplication 27
little endian 323, 326
load balancing server
    about 25
    adding to a deduplication node 194
    for deduplication 25
    removing from deduplication node 286
Local cache directory for CloudCatalyst 245, 247–248, 368
logging
    legacy 346
    level default for CloudCatalyst 250
logs
    about deduplication 348
    Auto Image Replication 353
    client deduplication proxy plug-in log 350
    client deduplication proxy server log 350
    deduplication configuration script log 350
    deduplication installation 352
    deduplication plug-in log 351
    disk 276
    NetBackup Deduplication Engine log 352
    NetBackup Deduplication Manager log 353
    optimized duplication 353
    VxUL deduplication logs 348
LowWatermark CloudCatalyst setting 251

M

maintenance processing. *See* queue processing
master servers
    inter-node authentication for clustering 171
Maximum concurrent jobs 118
Maximum concurrent jobs host property 256
Maximum fragment size 117
Media open error (83) 380
media server deduplication
    process 334
Media Server Deduplication Pool 101, 172
    changing the state 292
    creating directories for 96-TB support 112
    enable 96-TB support 71
media server deduplication pool. *See* deduplication pool
Media write error (84) 380
migrating from PureDisk to NetBackup deduplication 386
migrating to NetBackup deduplication 387
mklogdir.bat 346
MSDP
    replication 150
    replication target, configuring 172
MSDP catalog 221, 318
    See also MSDP catalog backup
    See also MSDP catalog recovery
    about the catalog backup policy 222
    about the shadow catalog 221
    changing the number of shadow copies 225
    changing the shadow catalog path 223
    changing the shadow catalog schedule 224
    shadow copy log files 349
MSDP catalog backup
    about protecting the MSDP catalog 222
    configuring 226, 231
MSDP catalog recovery
    about 318
    error codes 369
    process the transation queue. 303
    recover from a shadow copy 319
MSDP drcontrol utility
    options 227
MSDP encryption 242, 254
MSDP replication
    about 34
MSDP storage rebasing. *See* rebasing
mtstrm.conf file
    configuring 56

N

nbstserv process 181
NDMP
    storage units 186
NetBackup
    naming conventions 16

NetBackup 5200 series appliance
as a storage destination 18
NetBackup 5300 series appliance
as a storage destination 18
NetBackup appliance deduplication 13
NetBackup Appliance Shell Menu 242–243
NetBackup CloudCatalyst 235
See also CloudCatalyst
NetBackup deduplication
about 12
license for 46
NetBackup Deduplication Engine
about 332
about credentials 30
adding credentials 289
changing credentials 290
logs 352
NetBackup Deduplication Manager
about 332
logs 353
NetBackup deduplication options 12
NetBackup Service Monitor (nbsvcmon) 382
network interface
for deduplication 31
NFS 20
node
deduplication 17

O

OpenStorage
optimized duplication 186
OpenStorage Disk Option 178
OpsCenter 239
optimized deduplication
configuring bandwidth 177
configuring for MSDP 143
limitations 136
logs 353
pull configuration within the same domain 141
separate network for 134
optimized deduplication copy
guidance for 138
optimized duplication
about 34
about the media server in common within the same domain 138
load balancing for 243, 245
push and pull considerations for CloudCatalyst 256
optimized duplication *(continued)*
push configuration within the same domain 138
optimized duplication encryption
configuring for MSDP 127
optimized MSDP deduplication
requirements 136
within the same domain 135
optimized synthetic backups
configuring for deduplication 132
deduplication 33
OptimizedImage attribute 33

P

pd.conf file
about 197
editing 61, 198
parameters 199
pdde-config.log 350
performance
deduplication 34
monitoring deduplication rate 267
policies
changing properties 187
creating 187
port usage
and deduplication 32
troubleshooting 366
Postponed secondary operations 186
Priority for secondary operations 185
provisioning the deduplication storage 42
pull optimized duplication for CloudCatalyst 256
PureDisk Deduplication Pool 101
push optimized duplication for CloudCatalyst 256

Q

queue processing 303
invoke manually 303

R

ReadOnly CloudCatalyst setting 252
rebasing
about 309
FP_CACHE_PERIOD_REBASING_THRESHOLD parameter 205
FP_CACHE_REBASING_THRESHOLD parameter 205
RebaseMaxPercentage parameter 312
RebaseMaxTime parameter 312

rebasing *(continued)*
RebaseMinContainers parameter 312
RebaseScatterThreshold parameter 312
server-side rebasing parameters 311
recovery
deduplication storage server 322
from deduplication storage server disk failure 321
Red Hat Linux
deduplication processes do not start 358
replacing the deduplication storage server 326
replication
between NetBackup domains. *See* Auto Image Replication
configuring MSDP replication to a different domain 152
for MSDP 34, 150
to an alternate NetBackup domain. *See* Auto Image Replication
Replication Director
Policy Configuration Wizard, unsupported 187
replication encryption
configuring for MSDP 127
reports
disk logs 273, 276
disk pool status 273, 276
disk storage unit 276
resetting the deduplication registry 220
Resiliency property in Resilient Network host properties 190
Resilient connection
Resilient Network host properties 188
resilient network connection
log file 353
Resilient Network host properties 188
FQDN or IP Address property in 190
Resiliency property in 190
restores
at a remote site 315
how deduplication restores work 314
specifying the restore server 316
reverse host name lookup
prohibiting 356
reverse name lookup 356
rolling conversion
AES encryption 128

S

Sampling interval host property 256
Scalable Storage host properties 256, 374
scaling deduplication 36
scanned field of the job details 271
Secure Hash Algorithm 62, 128
server
NetBackupdebug logs 346
server not found error 356
setlsu_ioctl tool 385
setting deduplication pool attributes 293
SHA-2 62, 128–129
SHA-512/256 128–129
SLP Parameters 149
snapshots
operation type 185
spa.cfg file
parameters for data integrity checking 309
status code 191 (no images were successfully processed) 380
Status Collection Daemon 347
storage capacity
about 18
adding 44
for deduplicaton 18
viewing capacity in container files 274
Storage Lifecycle Manager service (nbstserv) 181
storage lifecycle policies
Active secondary operations 186
best practices document 179
cancelling duplication jobs 363
Data classification setting 185
hierarchy 183
operations 181
Postponed secondary operations 186
Priority for secondary operations 185
Storage lifecycle policy name 185
utility 178
Validate Across Backup Policies button 186
storage paths
about reconfiguring 284
changing 284
storage rebasing. *See* rebasing
storage requirements
for deduplication 19
storage server
about the configuration file 215
change the name 284
changing properties for deduplication 282
changing the name 284
components for deduplication 331
configuring for deduplication 73, 91

storage server *(continued)*
deduplication 24
define target for Auto Image Replication 158
deleting a deduplication 287
deleting the deduplication configuration 288
determining the state of a deduplication 279
editing deduplication configuration file 217
getting deduplication configuration 216
recovery 322
replacing the deduplication host 326
setting the deduplication configuration 218
viewing 279
viewing attributes 280
storage server configuration
getting 216
setting 218
storage server configuration file
editing 217
storage type
for deduplication 17
storage unit
configuring for deduplication 115
properties for deduplication 117
recommendations for deduplication 118
storage unit groups
and storage lifecycle polices 186
not supported for Auto Image Replication source 151, 154
Storage unit name 117
Storage unit type 117
stream handlers
NetBackup 35
synthetic backups
no Auto Image Replication support 154

T

Targeted A.I.R. 171
throttling, configuring for CloudCatalyst 254, 256, 374–375
topology of storage 158–159
troubleshooting
database system error 355
deduplication backup jobs fail 358
deduplication processes do not start 358
general operational problems 362
host name lookup 356
installation fails on Linux 354
no volume appears in disk pool wizard 357
server not found error 356
trusted master servers
adding 164
for Auto Image Replication 161
removing 169

U

unified logging 342
format of files 344
location 342
uninstalling media server deduplication 329
UploadThreads CloudCatalyst setting 252, 374
UTC (Coordinated Universal Time) 154

V

Validate Across Backup Policies button in SLP 186
Validation Report tab 186
Veritas NetBackup Extendable Storage File System Service (vxesfsd) 248, 255, 262, 381–382, 384
Veritas NetBackup Extendable Storage Proxy (vxesp) 384
viewing deduplication pool attributes 292
viewing storage server attributes 280
VM backup 187
vmscd 347
vmscd directory 347
volume manager
Veritas Volume Manager for deduplication storage 45
VxESFS (Veritas NetBackup Extendable Storage File System) 248, 255
vxesfsd (Veritas NetBackup Extendable Storage File System Service) 262, 381–382, 384
vxlogview command 343
with job ID option 345

W

wizards
Policy Configuration 187

Z

ZFS 20