

Symantec NetBackup™ Search Administrator's Guide

Release 7.6



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

Documentation version: 7.6

Legal Notice

Copyright © 2013 Symantec Corporation. All rights reserved.

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

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

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

| | |
|------------------------|--|
| Asia-Pacific and Japan | customercare_apac@symantec.com |
|------------------------|--|

| | |
|---------------------------------|--|
| Europe, Middle-East, and Africa | semea@symantec.com |
|---------------------------------|--|

| | |
|---------------------------------|--|
| North America and Latin America | supportsolutions@symantec.com |
|---------------------------------|--|

Contents

| | |
|-------------------------|--|
| Technical Support | 4 |
| Chapter 1 | About NetBackup Search 10 |
| | About NetBackup Search 10 |
| | Components of NetBackup Search 11 |
| | What you can do with NetBackup Search 13 |
| | How NetBackup Search works 15 |
| | About snapshots and NetBackup Search 16 |
| Chapter 2 | Installation and Configuration 17 |
| | Overview of installing the NetBackup Search components 17 |
| | Requirements and capabilities 18 |
| | Supported deployment scenarios 20 |
| | Installing an indexing server 20 |
| | Installing NetBackup Search in a clustered environment 22 |
| | Upgrading a previous release of NetBackup Search 22 |
| | Configuring an indexing server 27 |
| | Changing the staging directory for NetBackup Search 27 |
| | Changing the port specification for NetBackup Search 28 |
| Chapter 3 | Indexing Management 30 |
| | Indexing backup images 30 |
| | Adding historical backup images to the indexing queue 32 |
| | Removing backup images from the indexing queue 33 |
| | Removing references of the backup images from the index 33 |
| | Viewing the list of backup images based on the indexing state 33 |
| | Marking an index as invalid 35 |
| | Re-indexing backup images 35 |
| | About indexing jobs 36 |
| | Adding indexing servers 39 |
| | Decommissioning an indexing server 40 |
| | Migrating an indexing server to another indexing server 41 |
| | Suspending and resuming indexing jobs 45 |

| | | |
|-----------|--|----|
| | Adding or modifying indexing server schedules | 45 |
| | Configuring an indexing server in a backup policy | 48 |
| | Protecting indexing servers | 49 |
| | Configuring a backup policy that protects the indexing server | 50 |
| | Running indexing server backups | 51 |
| | Restoring the indexing database from a backup image | 53 |
| | Best practices for protecting indexing servers | 55 |
| | Starting and stopping indexing engine services | 56 |
| Chapter 4 | Search Queries | 57 |
| | About searches queries | 57 |
| | Search criteria | 58 |
| | Searching files and folders in indexed backup images | 59 |
| | Working with Image Search | 62 |
| | Searching backup images within a date range | 62 |
| | Exporting details of backup images | 65 |
| | About using wildcard characters in a search | 66 |
| | Search terms | 67 |
| | Managing saved search queries | 70 |
| | Editing a saved search query | 70 |
| | Running a saved search | 71 |
| | Deleting a saved search | 72 |
| | Managing search results | 72 |
| | Viewing search results | 73 |
| | Deleting search results | 76 |
| | Finding the search ID | 77 |
| Chapter 5 | Holds Management | 78 |
| | Placing a hold on a backup image | 78 |
| | Viewing holds details | 83 |
| | Search & Hold > Holds view | 85 |
| | Search & Hold > Holds > Hold Details view | 86 |
| | Releasing a hold | 87 |
| | About Hold reports in Symantec NetBackup OpsCenter | 90 |
| | Viewing hold reports | 91 |
| | Hold Reports > Image Retention Summary | 91 |
| | Hold Reports > Top Holds by Size | 91 |
| | Hold Reports > Top Holds by Age | 91 |
| | How to find the status of backup images on hold | 92 |
| | Finding the media information of backup images on hold | 95 |

| | | |
|-------------|--|-----|
| Chapter 6 | Mass Restore | 96 |
| | About mass restore | 96 |
| | Preparing for mass restore | 96 |
| | Sharing the staging directory | 97 |
| | Updating the RestoreConfig.ini file | 98 |
| | Submitting mass restore requests | 98 |
| | About restoring the data on hold and ingesting it into Enterprise Vault | 101 |
| | Prerequisites for ingesting the restored data into Enterprise Vault | 101 |
| | Ingesting the restored data into Enterprise Vault | 102 |
| | Mass restore error messages | 103 |
| Chapter 7 | Troubleshooting | 107 |
| | About NetBackup Search status codes and log files | 108 |
| | Enabling debug logging for NetBackup Search functions by using the Setup Debug Logging Wizard | 112 |
| | Unable to save the search criteria | 118 |
| | Resolving excessive log generation and memory usage | 119 |
| | Resolving conflicting failed and indexed log entries for the same backup image | 119 |
| | Resolving indexing job errors while sending data to the master server | 120 |
| | Re-initiating indexing jobs that have failed | 120 |
| | Fixing indexing jobs that fail with error code 5027 after an upgrade | 122 |
| | Fixing indexing jobs that fail with status code 25 (cannot connect on socket) | 123 |
| | Fixing indexing jobs that fail with status code 50 (client process aborted) when NBAC is enabled | 124 |
| | Recovering from disk-full situations | 125 |
| | Recovering from disk-error situations | 126 |
| | Resolving begin_restore operation failures | 127 |
| | Resolving nbholdrestorehelper operation failures | 127 |
| | About Java and MFC UI differences | 127 |
| | About obsolete search criteria and results for Files & Folder searches | 128 |
| | Fixing collection-service issues | 129 |
| Index | | 130 |

About NetBackup Search

This chapter includes the following topics:

- [About NetBackup Search](#)
- [Components of NetBackup Search](#)
- [What you can do with NetBackup Search](#)
- [How NetBackup Search works](#)
- [About snapshots and NetBackup Search](#)

About NetBackup Search

NetBackup Search provides a mechanism to index the file system metadata that is associated with NetBackup backup images. With indexed backup images, searching for relevant information is simple, powerful, and fast.

NetBackup Search also provides a robust legal hold function. You can search through the metadata in the catalog at file level and locate any file or folder from the repository. Then you can select the specific files or folders in backup images and retain them by placing them on hold. These files or folders expire only after you release the hold. This function ensures that images relevant to a legal case are not inadvertently deleted or allowed to expire based on retention levels.

Note: NetBackup Search is a licensed feature.

The following capabilities are provided with this feature:

- Advanced search capabilities enable you to find relevant information faster.
 - Search across multiple domains.
 - Save and edit search queries for legal traceability.

- Robust solution for legal hold management.
 - Legal holds let you retain backup images regardless of existing retention levels. Legal holds ensure that backup images and associated media are not expired until the legal proceeding completes.
 - Hold reports in Symantec NetBackup OpsCenter provide insight into size and age of legal hold and length of time of the associated holds.

Components of NetBackup Search

The components of NetBackup Search and their descriptions are as follows:

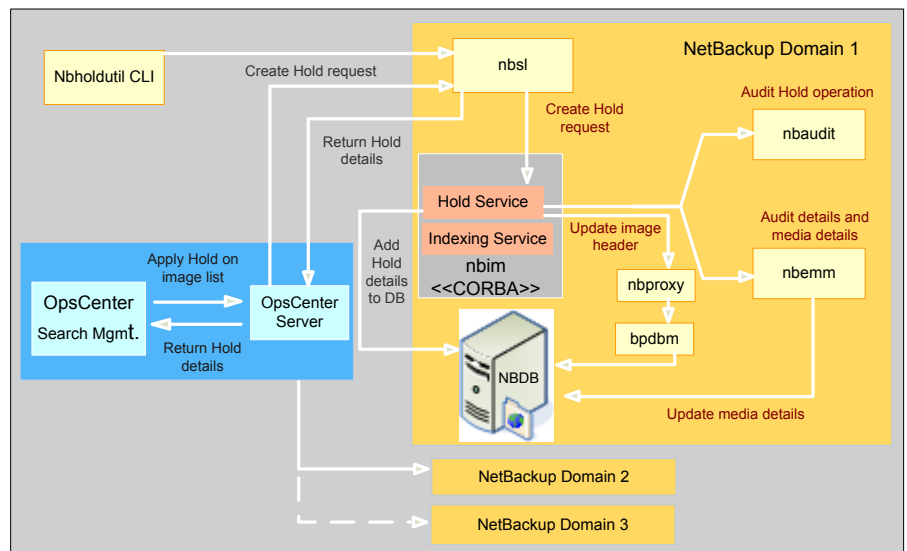
Table 1-1 NetBackup Search components

| Component | Description |
|--|--|
| Search services on the NetBackup master server and media server | |
| Indexing manager (NBIM) | This service manages the Indexing and Hold functionality. NBIM runs on the NetBackup master server. |
| Indexing server | The indexing server is installed on a standalone server that runs a NetBackup 7.6 client or on a NetBackup media server |
| Search executor | The Search executor runs the catalog search query on the indexing server. |
| Indexing engine | The indexing engine is a web server service that runs on the indexing server. |
| Symantec NetBackup OpsCenter components | |
| Search UI | The NetBackup Search user interface is available on the Symantec NetBackup OpsCenter UI. NetBackup Search options are visible to security administrators in OpsCenter only if you have added a valid NetBackup Search license key in Symantec NetBackup OpsCenter. |
| Search Broker | The Search Broker allows search requests to search across multiple NetBackup domains. |
| Reports | From the Symantec NetBackup OpsCenter Reports tab, you can view hold reports. The Hold reports are visible to security administrators in OpsCenter only if you have added a valid NetBackup Search license key in Symantec NetBackup OpsCenter. |
| Commands that you enter from the command line interface (CLI) of the NetBackup master server | |

Table 1-1 NetBackup Search components (*continued*)

| Component | Description |
|--------------------------|--|
| <code>nbholdutil</code> | The command <code>nbholdutil</code> helps to place a local hold on backup images. |
| <code>nbindexutil</code> | The command <code>nbindexutil</code> helps to index backup images or delete indexed backup images. |
| <code>nbsl</code> | The NetBackup Service Layer service facilitates communication between the Symantec NetBackup OpsCenter interface and the core NetBackup components. |
| <code>nbaudit</code> | The NetBackup Audit Manager service records the audit events in the Enterprise Media Manager (EMM) database. It runs on the NetBackup master server. |
| <code>nbproxy</code> | This service allows the multi-threaded NetBackup processes to use existing multi-threaded unsafe libraries. |
| <code>bpdbm</code> | The NetBackup Database Manager service manages the internal databases and catalogs of NetBackup. It runs on the master server. |

Figure 1-1 NetBackup Search components



What you can do with NetBackup Search

NetBackup Search helps you to locate any specific file or folder. You can then place it on hold, and release the hold when the hold is no longer required. The following scenario explains how it can help you to overcome the tedious process of responding to eDiscovery requests.

Earlier, to perform eDiscovery searches in the backup environment you had to keep a track of the following:

- The master server that took the backups.
- The host name of the server that stored the original data.
- The locations where pertinent information is stored.
- The type of backup taken, full or incremental.

Searching for files was laborious and not completely exhaustive. Backup administrators had to guess which file servers to search and which keyword to search for. It would take hours as there was no centralized search mechanism that spanned the entire backup environment for searching.

You had to browse for long hours for the file and then restore it. There may be cases where you would not be able to locate that file. However, the real scenario is as follows:

You lose the file system on one of the volumes and contact the NetBackup administrator to help you retrieve it. But it becomes difficult for you to provide details like the server name, the backup method used, and which NetBackup server protected it.

Managing legal holds was difficult and led to increased storage requirements. This situation also led to increased risk of legal sanctions due to an incomplete system. To hold certain legal files for a specified duration (for instance, for the last year), you had to access numerous logs to specify the server names or end up holding all the data from the last year.

The data includes personal files, legal files, administration files, and much more. To remove the legal files, you may have to look through numerous NetBackup storage servers to find the files on which you applied the hold. This leads to another problem; are you sure that there are no other holds applied to the images? The process may get tedious and prompt you to buy more storage. It may also lead you to leave the previously held tapes to gather dust in the storage vault with infinite retentions.

Through NetBackup Search you can find the backup data based on the following criteria:

- File name

- User name
- File Path
- Date Range

In NetBackup Search you can create search queries, to search for files or folder and then place holds on the files or folders. It also provides you an option to search and hold backup images within a date range. NetBackup Search also provides you with an automatic email notification on the completion of every search.

Figure 1-2 Search and Hold tab on Symantec NetBackup OpsCenter user interface

Symantec OpsCenter Analytics Logged in as: [admin] [About](#) [Logout](#)

Home Monitor Manage Reports **Search & Hold** Settings

New Saved Holds

This Will Search

Masters 1
Clients 1
Users and 3
Groups

New Search

Search For: Files & Folder Search ⓘ

Search Terms

Enter the terms below to begin a search for backups.
Separate multiple terms with a semicolon.

User and Group: All ... Backups Taken in: Last Month ▼

Files and Folders: *

▶ **Advanced**

Save Clear

Symantec

When you no longer need the backup image, you can release the hold that you placed on the files through the Symantec NetBackup OpsCenter user interface. NetBackup Search options are visible in Symantec NetBackup OpsCenter only if you have added a valid NetBackup Search license key in OpsCenter and you log on as a Security Administrator.

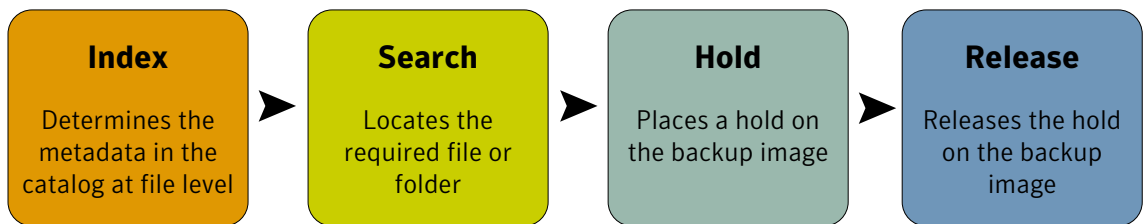
NetBackup Search helps you to:

- Reduce the time and the effort that is required for locating and preserving required backup images.
- Reduce the cost of storage to 'hold everything'.
- Maintain only the required data in the Catalog.
- Efficiently recover the backup files.
- Maintain confidentiality of user data.

How NetBackup Search works

NetBackup Search consists of a number of components that help you to locate backup files, hold them and then release them. The following diagram provides an overview of the operational workflow of NetBackup Search.

Figure 1-3 NetBackup Search workflow overview



- **Index**
A backup of the data from the NetBackup Client is taken on the NetBackup media server. A catalog of the metadata is created on the NetBackup master server.
The master server comprises of the services `NBIM` and `bpdbm`. `NBIM` initiates the indexing jobs. The indexing jobs run on the indexing server. Indexing jobs perform searches of complex and high-volume data. These jobs locate the data from the `bpdbm` service running on the master server.
The NetBackup indexing server indexes the metadata in the catalog on the NetBackup master server.
To retain a file or folder for the required duration, you must find and select it from the Symantec NetBackup OpsCenter interface. You can then place a hold on it.
- **Search**

From the Symantec NetBackup OpsCenter interface, you create a search query to find the file or folder on which you want to hold. The search query is sent to the indexing server, and the requested file or folder is retrieved.

- **Hold**
From the Symantec NetBackup OpsCenter interface, you can place a hold on the backup image that contains the file or folder.
- **Release**
When you no longer need to retain the backup image, you can release the hold that you placed on the file or folder. If the original retention period has expired and there are no other holds on the backup images being released, they are deleted immediately.

About snapshots and NetBackup Search

Files belonging to snapshot images can be included in search results depending upon your search criteria. NetBackup Search does not check on the storage unit type or the backup method that is used for individual images. You can place a snapshot image on hold. However, only the tar ball copies of the selected snapshot image are placed on hold. You cannot expire the tar ball copies of the snapshot image if they are on hold. However, you can delete or change the expiration date of the primary copy.

Note: The primary copy and tar ball copy differ in size for the snapshot image. The hold only consists of the overall size of the tar ball copies.

Installation and Configuration

This chapter includes the following topics:

- [Overview of installing the NetBackup Search components](#)
- [Requirements and capabilities](#)
- [Supported deployment scenarios](#)
- [Installing an indexing server](#)
- [Upgrading a previous release of NetBackup Search](#)
- [Configuring an indexing server](#)
- [Changing the staging directory for NetBackup Search](#)
- [Changing the port specification for NetBackup Search](#)

Overview of installing the NetBackup Search components

The following NetBackup Search components are installed when you install NetBackup Search Software:

- Client software (if not already installed)
- Indexing server

Note: Indexing server is supported only on Windows 2008 R2 (x64) and Windows 2012 (x64) platforms.

The following NetBackup Search components are installed when you install master server from NetBackup:

- Indexing management
- Holds management

Note: The NetBackup Search user interface is installed when you install Symantec NetBackup OpsCenter. For more information about installing Symantec NetBackup OpsCenter, see *Symantec NetBackup OpsCenter Administrator's Guide*.

Table 2-1 Overview of the installation of NetBackup Search in the NetBackup 7.6 release

| Step | Description | References |
|------|--|---|
| 1 | Install Symantec NetBackup OpsCenter. | <i>Symantec NetBackup OpsCenter Administrator's Guide</i> |
| 2 | Install a NetBackup 7.6 master server. | <i>Symantec NetBackup Administrator's Guide</i> |
| 3 | Install and identify a NetBackup 7.6 media server. | <i>Symantec NetBackup Administrator's Guide</i> |
| 4 | Install the NetBackup 7.6 indexing server. | See "Installing an indexing server" on page 20. |

You can find all NetBackup-related reference guides at the following Internet location:

[NetBackup Release Notes, Administration, Installation, Troubleshooting, Getting Started, and Solutions Guides](#)

Note: After you install NetBackup Search, you are prompted to run the configuration wizard to configure the port number and the staging directory for the indexing engine. You must complete this configuration for the NetBackup Search to start functioning.

Requirements and capabilities

This topic describes hardware requirements, software requirements, licensing requirements, and compatibilities.

Hardware requirements for indexing server

Following are the minimum and the recommended hardware requirements to install indexing server:

Table 2-2 Hardware requirements

| Hardware | Minimum requirements | Recommended requirements |
|-----------|----------------------|--------------------------|
| CPU cores | 4 | 8 |
| Memory | 16 GB | 32 GB |

Note: The disk space requirement for an indexing server depends on the size of the index.

The size of the index is approximately same as the size of the catalog that was indexed. This size estimation varies based on the type of data and also the extent of the catalog that has been indexed. The storage optimization from single instancing of index entries also varies based on the type of data, data duplication, backup schedule, and so on.

If the indexing server is configured on a computer with less than the recommended hardware configuration, the RAM and core are not updated in the database after the first indexing job. After the first batch of indexing jobs runs, the subsequent indexing jobs are not triggered for the indexing server.

For more information about hardware requirements of other NetBackup components, see the [Symantec NetBackup Installation Guide](#).

Software requirements for indexing server

Indexing server is supported only on Windows 2008 R2 (x64) and Windows 2012 (x64) platforms. For more information about software requirements of other NetBackup components, see the [Symantec NetBackup Installation Guide](#).

Licensing requirements

Symantec NetBackup Search is a licensed software of NetBackup. The **Search and Holds** tab in Symantec NetBackup OpsCenter is seen only if you have added a valid NetBackup Search license key and if you log on as a Security Administrator. You can then search and hold the backup images in Symantec NetBackup OpsCenter. You can also see the Reports of all the backup images on hold.

See [“About searches queries”](#) on page 57.

See [“Placing a hold on a backup image”](#) on page 78.

See [“Viewing hold reports”](#) on page 91.

Compatibilities

For information about compatibilities, see [NetBackup Master Compatibility List](#).

Supported deployment scenarios

You can install an indexing server as a standalone entity on any computer that has a minimum of NetBackup Client software that is installed on it. The installation wizard prompts you to install or upgrade the NetBackup Client software before you proceed with the indexing server installation, if no other compatible NetBackup component is found.

Note: Symantec does not recommend installing a NetBackup indexing server on a master server.

Additionally, the following deployment scenarios are supported for NetBackup Search in the NetBackup 7.6 release:

- **Clustered environments**
You can run NetBackup Search in a NetBackup or OpsCenter clustered environment by adding the node names in `bp.conf` on UNIX or on the Windows registry.
See [“Installing NetBackup Search in a clustered environment”](#) on page 22.
- **Distributed deployment requires a minimum of three systems (hosts):**
Host 1: NetBackup master server.
Host 2: NetBackup media server or NetBackup client + NetBackup indexing server .
Host 3: Symantec NetBackup OpsCenter server.

Installing an indexing server

You can install an indexing server as a standalone entity on any computer that has a minimum of NetBackup Client software installed on it. If you install an indexing server on a computer without the NetBackup Client software installed, the installation wizard prompts you to install or upgrade the NetBackup Client software before you proceed.

Note: Symantec does not recommend installing a NetBackup indexing server on a master server.

Installing the indexing server on a virtual machine might result in performance issues.

Perform the following procedure to install the indexing server (NetBackup Search Software).

To install an indexing server

- 1 Run `Browser.exe` from the NetBackup installation files, and then select **Installation**.
- 2 From the **Installation** menu, select **Search Software Installation**.

Note: The installation wizard checks whether a NetBackup 7.6 client is installed on the computer where you install indexing server. If the installation does not find a NetBackup 7.6 client, it prompts you to install or upgrade the client. For more information about installing NetBackup Client software, see the [Symantec NetBackup Installation Guide](#).

- 3 Follow the prompts that the installer presents to install the indexing server.

Note: When specifying the install path for the indexing server, specify a location (partition) with disk space of at least 70 percent of the projected catalog size. The indexing server creates and maintains the index database in one of the directories under its installation location. This path can be different from the installation path of the NetBackup client on that host.

At the end of the installation, you are prompted to launch the NetBackup Search Configuration Wizard for configuring the indexing engine. You must complete this configuration for NetBackup Search to start functioning. If you want to launch the Configuration Wizard at another time, enter the following command on the indexing server command prompt:

```
<Install_Path>\..\Symantec\NetBackupSearch\bin\SearchConfig.exe
```

- 4 To verify whether the installation was successful, verify that the NetBackup Search Executor Service and NetBackup Indexing Engine service are installed and running.

Note: You can install an indexing server on a NetBackup Media server.

Symantec recommends that for better performance and scalability you should install multiple indexing servers per domain.

You must exclude the NetBackup Search component directory

(`<<Install_Path>\..\Symantec\NetBackupSearch\`) from the antivirus scanning list.

Information about how to upgrade a previous version of NetBackup Search to version 7.6 is available. See [“Upgrading a previous release of NetBackup Search”](#) on page 22.

Information about adding indexing servers in the domain is available. See [“Adding indexing servers”](#) on page 39.

Installing NetBackup Search in a clustered environment

You can run NetBackup Search in a clustered environment of NetBackup or Symantec NetBackup OpsCenter. You must add each node name to `bp.conf` on UNIX or on the Windows registry.

For a OpsCenter cluster mode, the NetBackup server list must contain the name of each OpsCenter node in the cluster and the virtual server of OpsCenter cluster.

- Nodes of OpsCenter: `OpsC_Node1`, `OpsC_Node2`
- Virtual Name: `OpsC_Virtual`
 You must add `OpsC_Node1`, `OpsC_Node2`, and `OpsC_Virtual` at the following location:

On Windows:

`HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\NetBackup\CurrentVersion\Config\Server`

On UNIX:

`/usr/opensv/netbackup/bp.conf`

Note: If these entries are not added, the search operations fail and display the `Communication Failed` message. In logs, the `NO PERMISSION` message appears.

Upgrading a previous release of NetBackup Search

Before you apply the version 7.6 upgrade, you must first suspend indexing activity on the indexing servers you want to upgrade. When an indexing server is suspended, new indexing jobs cannot be submitted to it. Any indexing jobs that are already

running continue until they complete. You must allow all indexing jobs to complete before you apply the upgrade.

- To upgrade only the NetBackup master server, complete the following procedure only if NetBackup Search is configured in the environment:
 See [“To upgrade a NetBackup master server if NetBackup Search is configured in the environment”](#) on page 24.
- To upgrade only a NetBackup media server that contains NetBackup Search indexing servers, complete the following procedure:
 See [“To upgrade a NetBackup media server and NetBackup Search”](#) on page 26.
- To upgrade all components, complete both of the following procedures:
 See [“To upgrade a NetBackup master server if NetBackup Search is configured in the environment”](#) on page 24.
 See [“To upgrade a NetBackup media server and NetBackup Search”](#) on page 26.
- If you are upgrading NetBackup clients, complete the appropriate procedures in the [NetBackup Upgrade Guide version 7.6](#). No additional steps are necessary because upgrades to NetBackup Search do not affect NetBackup clients.
- If you are upgrading a NetBackup media server that does not contain indexing servers, complete the appropriate procedures in the [NetBackup Version 7.6 Upgrade Guide](#). No additional steps are necessary because upgrades to NetBackup Search do not affect NetBackup media servers that do not contain indexing servers.

Upgrading a NetBackup master server if NetBackup Search is configured in the environment

If NetBackup Search is configured in the NetBackup environment, use the following instructions to upgrade a NetBackup master server from a previous release to version 7.6.

To upgrade a NetBackup master server if NetBackup Search is configured in the environment

- 1 Get a complete list of the indexing servers.

From the NetBackup Administration Console, go to **Host Properties > Indexing Servers**.

- 2 Suspend all of the indexing servers.

For each indexing server, enter the following command from a command prompt on the master server. In clustered environments, enter this command on the active master server.

```
nbindexutil -suspend -indexserver <indexing server name>
```

This command ensures that no new indexing jobs are submitted. This command does not stop the indexing jobs that are currently running. You must allow all indexing jobs to complete before you apply the upgrade. Use the **Activity Monitor** in the **NetBackup Administration Console** to check the status and progress of indexing jobs.

Note: You may create and run a script that contains all of the commands for each server.

- 3 Apply the version 7.6 upgrade to the master server.

Procedures for upgrading NetBackup master servers are available in the [NetBackup Version 7.6 Upgrade Guide](#).

Note: Remember to upgrade Symantec NetBackup OpsCenter to version 7.6 before you upgrade your NetBackup master servers to version 7.6. You must also disable OpsCenter data collection. See the [Symantec NetBackup OpsCenter Administrator's Guide](#) for complete information.

4 Verify that the version 7.6 upgrade completed successfully.

Enter the following command from a command prompt on the master server. In clustered environments, enter this command on the active master server.

```
nbermmcmd -listhosts
```

The output of the command lists the hosts that are found. In the following example, two indexing servers were found:

The following hosts were found:

```
server          Host1
master          Host1
media           Host2
media           Host3
index_server    Host2
index_server    Host3
```

Command completed successfully.

If you do not see your indexing servers in the list or if the upgrade logs include a failure entry for `nbindexutil - upgrade`, re-enter the following command from the active master server:

```
nbindexutil -upgrade
```

5 Resume indexing after the version 7.6 upgrade completes successfully.

For each indexing server, enter the following command from a command prompt on the master server. In clustered environments, enter this command on the active master server.

```
nbindexutil -resume -indexserver <indexing server name>
```

Upgrading a NetBackup media server and NetBackup Search

Use the following instructions to upgrade a NetBackup media server and NetBackup Search from previous release to version 7.6.

To upgrade a NetBackup media server and NetBackup Search

1 Suspend the indexing servers that you want to upgrade.

For each indexing server, enter the following command from a command prompt on the master server. In clustered environments, enter this command on the active master server.

```
nbindexutil -suspend -indexserver <indexing server name>
```

This command ensures that no new indexing jobs are submitted. This command does not stop the indexing jobs that are currently running. You must allow all indexing jobs to complete before you apply the upgrade. Use the **Activity Monitor** in the NetBackup Administration Console to check the status and progress of indexing jobs.

Note: You may create and run a script that contains all of the commands for each server.

2 Check the state of each indexing server to ensure that all indexing servers are suspended.

Enter the following command from a command prompt on the master server. In clustered environments, enter this command on the active master server.

```
nbindexutil -listindexservers
```

Note: You may need to wait until the suspend processes complete for all indexing servers.

For example, the following output from the command shows one indexing server that is suspended and another indexing server that is still active.

| Indexing Server | State |
|-----------------|-----------|
| IndexServer1 | Suspended |
| IndexServer2 | Active |

3 Apply the version 7.6 upgrade to the NetBackup media server and indexing servers.

Procedures for upgrading NetBackup media servers are available in the [NetBackup Version 7.6 Upgrade Guide](#).

- 4 Ensure that the NetBackup media server and NetBackup Search are running version 7.6.

When the NetBackup media server and NetBackup Search indexing servers run different versions of the software, indexing jobs fail. Therefore, it is important that you check that the NetBackup media server and NetBackup Search are running version 7.6 before you resume indexing.

- 5 Resume indexing.

For each indexing server, enter the following command from a command prompt on the master server. In clustered environments, enter this command on the active master server.

```
nbindexutil -resume -indexserver <indexing server name>
```

Configuring an indexing server

You must perform the following tasks to configure the indexing server in your NetBackup domain. This set of tasks allows NetBackup Search to start indexing the backup images during the schedule that you define.

Table 2-3 Configuring an indexing server

| Task | Reference |
|---|---|
| Add the indexing server to the NetBackup domain. | See “ Adding indexing servers” on page 39. |
| Define a schedule for indexing server. | See “Adding or modifying indexing server schedules” on page 45. |
| Configure the indexing server in a backup policy. | See “Configuring an indexing server in a backup policy” on page 48. |

Changing the staging directory for NetBackup Search

Over a period of time, if the staging directory in your NetBackup domain grows bigger in size, it may result in low performance. To resolve this situation, you must change the staging directory to another location.

Caution: The existing search results may not be displayed correctly. To overcome this issue, you can re-run the searches. However, you cannot re-run the saved searches if any of the backup images from their search result are on hold.

The search results may not be deleted correctly.

To change the staging directory

- 1 From the Activity Monitor, ensure that no indexing job or search operation is running on the indexing server.
- 2 From a command prompt on the indexing server, enter the following command to stop both the NetBackup Search Executer service and the NetBackup Indexing Engine service:

```
<Install_path>\Symantec\NetBackupSearch\bin\velocity-shutdown.exe
```

- 3 From a command prompt on the indexing server, run the following command to launch the NetBackup Search Configuration Wizard:

```
<Install_path>\Symantec\NetBackupSearch\bin\SearchConfig.exe
```

- 4 On the Configuration Wizard, enter the new staging directory path.
- 5 Click **Configure** to complete the configuration changes.

Note: The NetBackup Search Executer service and the NetBackup Indexing Engine service is automatically started.

- 6 Exit the NetBackup Search Configuration Wizard.
- 7 Move the following folders from the old staging directory to the new staging directory:
 - Data
 - Staging

Note: Do not copy the folders from the old staging directory to the new staging directory.

Note: The hold on old searches is retained.

When you perform a mass restore, you must specify the new staging location.

Changing the port specification for NetBackup Search

If the default port number is not available, you might want to change the port number for the indexing server.

To change the port specification

- 1 From the Activity Monitor, ensure that no indexing job or search operation is running on the indexing server.
- 2 From a command prompt on the indexing server, enter the following command to stop the NetBackup Search Executer and NetBackup Indexing Engine service:

```
<Install_path>\Symantec\NetBackupSearch\bin\velocity-shutdown.exe
```

- 3 From a command prompt on the indexing server, run the following command to launch the NetBackup Search Configuration Wizard:

```
<Install_path>\Symantec\NetBackupSearch\bin\SearchConfig.exe
```

- 4 On the Configuration Wizard, enter the new port number.
- 5 Click **Configure** to complete the configuration changes.
- 6 Exit the NetBackup Search Configuration Wizard.

Indexing Management

This chapter includes the following topics:

- [Indexing backup images](#)
- [About indexing jobs](#)
- [Adding indexing servers](#)
- [Decommissioning an indexing server](#)
- [Migrating an indexing server to another indexing server](#)
- [Suspending and resuming indexing jobs](#)
- [Adding or modifying indexing server schedules](#)
- [Configuring an indexing server in a backup policy](#)
- [Protecting indexing servers](#)
- [Starting and stopping indexing engine services](#)

Indexing backup images

Indexing is classified into indexing on-going backup images and indexing historical backup images. Indexing on-going backup images means indexing either scheduled or manual backup images. Whereas, indexing historical backup images means indexing images those are already backed up. Indexing in NetBackup Search is supported on the following backup policy types:

- FlashBackup
- FlashBackup-Windows
- Hyper-V

- MS- Windows
- NDMP
- Standard
- VMware

If you enable indexing with VMware and Hyper-V policy types, you must also select **Enable file recovery from VM backup** on the **VMware** or **Hyper-V** tab of the policy window.

Indexing is not supported for unmapped backup images. If a policy for which indexing and mapping are enabled specifies a virtual machine (VM) for which mapping is not supported, the indexing job fails with error code 5028. This situation may occur when the backup policy contains both mapping-supported and mapping-unsupported types of VMs. The backup job completes successfully (although mapping does not occur), but the indexing job fails.

For more information about error status 5028 ("The backup image did not have any files that can be indexed."), see the [Symantec NetBackup Commands Reference Guide](#) version 7.6.

More information is available about how to configure indexing backup images on these policies. See ["Configuring an indexing server in a backup policy"](#) on page 48.

Indexing on-going backup images

The backup policy types that are supported for indexing can be configured for indexing backup images on a particular indexing server. When the backup operation is completed, the indexing requests for these backup images are added to the indexing queue. Based on the indexing server schedule, these backup images are indexed on the associated indexing server. You can configure to index on-going backups on a particular indexing server in a backup policy. See ["Configuring an indexing server in a backup policy"](#) on page 48.

Indexing historical backup images

Old backup images or the backup images of the policies those were not configured for indexing are called historical backups. For indexing historical backup images, on a command prompt on the master server, use the `nbindexutil - add` command to add the indexing request to the indexing queue. More information about the command is available. See [Table 3-1](#) on page 32.

You can index the backup images that meet the following criteria:

- Old backup images or backup images for which the policy is not selected in NetBackup Search indexing server.

- The backup images that are already indexed, but you want to reindex them. For more information about reindexing backup images, see [Re-indexing backup images](#)

Adding historical backup images to the indexing queue

To index the historical backups, from a command prompt on the master server, run the following command:

```
nbindexutil -add
```

The `nbindexutil -add` command lets you add the backup images to the indexing queue.

Note: You can also remove the references of the backup images from the index by using the `nbindexutil -add` command. For more information, see [Removing references of the backup images from the index](#).

The following table lists the options and descriptions of the `nbindexutil -add` base command:

Table 3-1 `nbindexutil -add` options

| Option | Description |
|---|---|
| <code>-bid <Backup ID> -bid_file <name of the file that contains the backup IDs></code> | Enter the Backup ID with bid or path of the file containing Backup IDs with bid_file |
| <code>-indexserver <Indexing Server Name></code> | Enter the indexing server Name, it is required for adding the images for indexing. |
| <code>[-force]</code> | For re-indexing the indexed Backup ID(s). Note: This option is not applicable for the indexing of Backup IDs that are in waiting or in progress state. |
| <code>[-operation <Operation ID>]</code> | Select 1 for adding a new backup image to the indexing queue. Select 2 for deleting the reference of the selected backup image from the index. By default, 1 is selected. Note: The -Indexserver option is not applicable for Delete operation. |

Table 3-1 `nbindexutil -add` options (*continued*)

| Option | Description |
|---|--|
| <code>[-priority <Priority>]</code> | Set the indexing job priority to Low or High. The default value is set to Low. |

Note: You can use the `-help` command option with the command options to view help for that option. For example, enter `nbindexutil -help -add` to view help for `add`.

Removing backup images from the indexing queue

The `nbindexutil -remove` command removes the specified backup IDs from the indexing request. The following table lists the option and description of the `nbindexutil -remove` base command:

Table 3-2 `nbindexutil -remove` options

| Option | Description |
|--|---|
| <code>-bid <Backup ID> -bid_file <name of the file that contains the backup IDs></code> | Enter the Backup ID with the bid or path of the file containing Backup IDs with <code>bid_file</code> |

Removing references of the backup images from the index

When the indexed backup image expires, the references of the backup image are automatically removed from the index. Alternatively, you can also manually remove the references of the backup images from the index. To remove references of the backup images from the index, from a command prompt on the master server, run the following command:

```
nbindexutil -add -operation 2
```

See [“Adding historical backup images to the indexing queue”](#) on page 32.

Viewing the list of backup images based on the indexing state

To view the list of backup images based on the indexing state, from a command prompt on the master server, run the following command:

```
nbindexutil -list
```

You can also see the list of backup images in a particular state on a particular server. The following table lists the options and descriptions of the `nbindexutil -list` base command:

Table 3-3 `nbindexutil -list` options

| Option | Description |
|--|--|
| <code>-inprogress</code> | Lists all the images for which indexing is in progress. |
| <code>-waiting</code> | Lists all the images which are in a queued state for indexing. |
| <code>-indexed</code> | Lists the indexed images. |
| <code>-failed</code> | Lists the images for which indexing has failed. |
| <code>-indexserver <Indexing Server Name></code> | Enter the indexing server name. |
| <code>[-out <Filepath>]</code> | Enter the path of the file to redirect the output to a specified file. |

For the `-indexed` and `-failed` options, you can enter both or one of the following commands to list the images that were indexed or failed to index:

- `[-date_from mm/dd/yyyy HH:MM:SS]`
- `[-date_to mm/dd/yyyy HH:MM:SS]`

Note: You must enter the value for seconds (`SS`) while specifying the time (`HH:MM:SS`) for `-date_from` and `-date_to` options. Also, the date must be later than 1st of January, 1970.

You can enter the hours in the `[-hoursago hours] |` command to list the images that were indexed or failed to index during the last specified hours.

For example, if you enter the `[-hoursago 5] |` command, the images that were indexed or failed to index in the last five hours are provided.

More information is available about indexing backup images:

See [“Adding historical backup images to the indexing queue”](#) on page 32.

Marking an index as invalid

You can mark an index as invalid if it is corrupted or when indexing repeatedly fails on it. To mark the index as invalid, from a command prompt on the master server, run the following command:

```
nbindexutil -invalidateindices
```

The following table lists the options and descriptions of the `nbindexutil -invalidateindices` base command:

Table 3-4 `nbindexutil -invalidateindices` options

| Option | Description |
|--|---|
| <code>-indexserver <Indexing Server Name></code> | Enter the indexing server name. |
| <code>-index <Index Name> -index_file</code> | Enter the path of the file containing the index name. |

More information is available:

See [“Re-indexing backup images”](#) on page 35.

Re-indexing backup images

In case of a disaster recovery, or when you want to index backup images present in all the invalid indices you must re-index the backup images. You can also re-index the backup images that are indexed after a given time. From a command prompt on the master server, run the following command:

```
nbindexutil -reindex
```

The following table lists the options and descriptions of the `nbindexutil -reindex` base command:

Table 3-5 `nbindexutil -reindex` options

| Option | Description |
|--|---------------------------------|
| <code>-indexserver <Indexing Server Name></code> | Enter the indexing server name. |

Table 3-5 nbindexutil -reindex options (continued)

| Option | Description |
|--|--|
| <code>-invalid -indexed_after</code> <code><mm/dd/yyyy [HH:MM:SS]</code> | <p>Enter the date and time. The backup images that are indexed after this date and time are re-indexed.</p> <p>Note: The entered date must be later than 01st January, 1970.</p> <p>The hours, minutes, and seconds fields are mandatory.</p> |

More information is available:
See [“Marking an index as invalid”](#) on page 35.

About indexing jobs

The indexing jobs in NetBackup Search are of two types:

- Index for Search
- Index Cleanup for Search

An Index for Search job collects the metadata of all the files present in the backup image into the indexing engine. Based on the configuration of the backup policy, this job triggers automatically after the backup job completes. This job adds the backup images to the indexing queue for indexing. When the indexing schedule is open, these backup images are indexed. Alternatively, you can also manually add the historical backup images to the indexing queue by using the command prompt on the master server. More information is available about how to add historical backup images to an indexing queue. See [“Adding historical backup images to the indexing queue”](#) on page 32. An Index for Search job runs for each backup image. In Activity Monitor in the NetBackup Administration Console, you see an Index for Search job is created for each backup image.

An Index Cleanup for Search job performs each of the following activities:

- Removes the references of the expired backup image from the index
- Purges the index

When the indexed backup image expires, Index Cleanup for Search job is triggered automatically that adds these expired backup images to the indexing queue for removing the references from the index. When the indexing schedule is open, the indexing references of these expired backup images are removed. Alternatively, you can also manually remove the references of the backup images from the index.

More information is available about how to remove references of the expired backup images from the index:

See [“Removing references of the backup images from the index”](#) on page 33.

An Index Cleanup for Search job for removing references of the backup image from the index runs for each backup image. In Activity Monitor in the NetBackup Administration Console, when removing references of the backup images, you see an Index Cleanup for Search job is created for each backup image

After the Index Cleanup for Search job completes removing references of the backup image, an Index Cleanup for Search job starts purging the index when the following conditions are met:

- The indexing server is idle, that is, there is no indexing job running for that indexing server.
- The indexing queue does not contain a pending request of any backup image in the ‘waiting state of indexing’.
- The index being used for purging has not undergone any indexing activity (index\delete\purge) for last 12 hours (provided when the indexing schedule window is open).

An Index Cleanup for Search job for purging index runs for each index. In Activity Monitor in the NetBackup Administration Console, you see an Index Cleanup for Search job is created for each index when purging an index.

Note: To identify if the Index Cleanup for Search job is for removing references of the expired backup images or for purging an index, view **Job Details** by double-clicking the job.

NetBackup Search does not currently support indexing synthetic backups.

Indexing jobs sometimes may take a long time to complete successfully. A timeout mechanism specifies the number of hours after which the internal indexing process fails with status code 5042. The default timeout value is 4 hours. To change this value, on the indexing server, change the `AuditLogTimeoutInHours` at the `HKEY_LOCAL_MACHINE\\SOFTWARE\\Symantec\\NetBackupSearch\\CurrentVersion` registry location. For more information about status code 5042, see the [NetBackup Status Codes Reference Guide](#).

You cannot manually initiate the indexing jobs outside of a schedule. However, you can add a temporary indexing schedule and manually add the backup image to the indexing queue with high priority with the `nbindexutil` command.

About multiple indexing jobs running in parallel

You must consider the following factors when running multiple indexing jobs in parallel:

- **Indexing server configuration**
Each indexing job requires one core and 4 GB RAM. For example: On an indexing server with four cores and 16 GB, **NBIM** submits a maximum of four indexing jobs to that indexing server.
- **Number of clients that are configured for indexing**
If the indexing queue has backup images from multiple backup clients, multiple indexing jobs are submitted in parallel. Whereas, if the indexing queue has multiple backup images from one client, an indexing job is submitted only after the earlier job finishes.
For example, for a given backup client, **NBIM** submits the indexing jobs sequentially. Only one indexing job runs even if only one client is configured and when the indexing server is a high-end computer.
- **Number of indexing jobs per indexing server**
The **MAX_INDEXING_JOBS** parameter in **bp.conf** on the NetBackup master server controls the maximum number of indexing jobs that can run in parallel on an indexing server. For example, **NBIM** may submit eight indexing jobs to an indexing server. If the **MAX_INDEXING_JOBS** parameter is set to five, only five jobs can run in parallel, and the other three jobs are queued. However, if the **MAX_INDEXING_JOBS** parameter is set to eight, and **NBIM** submits five jobs, all five jobs run.

Note: Symantec recommends that you must have a robust master server. The **NBIM** and **bpdbm** services on a master server play an important role in indexing jobs and performing the search operation.

The **NBIM** service initiates the content indexer (**nbc_i**) service that indexes a high volume of data on the indexing server. The indexing jobs search the data from the **bpdbm** service that runs on the master server.

To change the number of maximum indexing jobs per indexing server

- 1 In NetBackup Administration Console, from the list of master servers, right-click the master server and select **Properties**.
- 2 On the **Properties** dialog box, select **Global Attributes** from the left pane.
- 3 Change the value of **Maximum indexing jobs per index server**, and click **Apply**.

- 4 Click **OK** to close the Properties dialog box.
- 5 Restart the NetBackup services.

Alternatively, you can also change the value of **Maximum indexing jobs per index server** by using the `bpsetconfig` command on the master server command prompt. For more information about how to use the command, see [NetBackup Commands Reference Guide](#).

Note: The NetBackup Search indexing processes crash if antivirus software scans the index location, namely - `<NetBackupSearch install location>\data` directory. To avoid this situation, exclude the `<NetBackupSearch install location>\data` directory from the antivirus scanning list.

Adding indexing servers

You can install an indexing server as a standalone entity on any computer that has a minimum of NetBackup Client software installed on it. If you install an indexing server on a computer that does not have the NetBackup Client software installed, the installation wizard prompts you to install the NetBackup Client software before you proceed with the indexing server installation.

Note: An indexing server is supported only on a Windows 2008 R2 (x64) and Windows 2012 (x64) platforms.

To add an indexing server

- 1 From the NetBackup Administration Console, select **Host Properties > Indexing Servers** from the task panel.
- 2 From the **Actions** menu, select **Configure Indexing Server**.
- 3 In the **Choose Indexing Server** window, enter the name of the client where the NetBackup Search software is installed. Click **OK**.

Note: If adding an indexing server fails with a short name for the server, try entering the fully qualified domain name of the client where the NetBackup Search software is installed. Symantec recommends that you use the same name for the indexing server and the client or the media server.

You must then create a schedule for the indexing server, which defines when to index backup images. See [“Adding or modifying indexing server schedules”](#) on page 45.

Decommissioning an indexing server

This procedure explains how to decommission an indexing server. You may need to decommission an indexing server when you no longer want to use the computer as an indexing server.

To migrate the data and software to another server before you decommission an indexing server, see the following topic:

See [“Migrating an indexing server to another indexing server”](#) on page 41.

Warning: If you recover a NetBackup master server catalog that includes backup images from the decommissioned indexing server, searches for those backup images may fail. To fix this problem, you must explicitly remove references to the decommissioned indexing server entries from the recovered master catalog.

To decommission an indexing server

- 1 Remove indexing server references from the master server. From a master server command prompt, run the following command:

```
nbindexutil -removeindexserver -indexserver <indexing server name>
```

This command removes all indexing server references and data from the master server index tables. All existing backup policies are updated by removing indexing server references and disabling the indexing option from policy attributes. This command does not have any effect on other indexing servers in the master server domain. Indexing on the other indexing servers continues.

Answer the prompt to proceed. If this command fails with an error, re-run the command to complete the removal of the indexing server references.

- 2 Ensure that all indexing server references and data have been removed:
 - From a command prompt on the master server, run the following command to ensure that no policies refer to the indexing server that you want to decommission:

```
nbindexutil -listpolicies -indexserver <indexing server name>
```

You receive the following message if no policies refer to the indexing server:

```
Failed to list policies associated with indexing server (index server name). Error: 5007 (Invalid Indexing Server) EXIT STATUS = 5007
```
 - From a command prompt on the master server, run the following command to ensure that no indexed images exist on the indexing server that you want to decommission:

```
nbindexutil -list -indexserver <indexing server name> -indexed
```


You receive the following message if no indexed images exist on the indexing server:

```
Failure in listing required information. Error: 5007 (Invalid Indexing Server) EXIT STATUS = 5007
```

- You must refresh the indexing servers list in the NetBackup Administration Console.
From the NetBackup Administration Console, select **Host Properties > Indexing Servers**.
Select **View > Refresh All**. Do not use **Refresh (F5)**.
Confirm that list of indexing servers does not include the indexing server that you decommissioned.
- 3 Uninstall the NetBackup Search software using the NetBackup Installation and Configuration Wizard.

Note: If you want to decommission the media server that has an indexing server installed on it, you must first decommission the indexing server and then follow the procedure documented in the [Symantec NetBackup Administrator's Guide, Volume I](#) to uninstall media server.

Migrating an indexing server to another indexing server

Complete this procedure to migrate an indexing server to a different indexing server.

Note: In this procedure, the source indexing server refers to the existing indexing server. The target indexing server refers to the server to which you want to migrate.

To migrate one indexing server to another indexing server

- 1 Ensure that NetBackup Search 7.6 is installed and running on the target indexing server.

NetBackup Search 7.6 is supported only on Windows 2008 R2 (x64) or Windows 2012 (x64) systems. More information about installation and configuration is available:

See [“Supported deployment scenarios”](#) on page 20.
- 2 Stop the indexing engine services. More information is available about how to start and stop the indexing engine services. See [“Starting and stopping indexing engine services”](#) on page 56.

- 3 **Note:** This step applies only to migration of a NetBackup Search 7.5 or 7.5.x.x indexing server to an NetBackup Search 7.6 indexing server. It is a required step if your source indexing server runs NetBackup Search 7.5 or 7.5.x.x and your target indexing server runs NetBackup Search 7.6.

Copy the following files and directories from the target indexing server that runs NetBackup Search 7.6 to a temporary location:

- The `key` file from `<target indexing server install path>\NetBackupSearch\data\static\key`
 - The `repository-supplements` directory from `<target indexing server install path>\NetBackupSearch\data\repository-supplements`
- These copies are required in step 11.

- 4 Ensure that no indexing jobs are presently running.
- Indexing jobs fail if you migrate the source indexing server while the jobs are running. Check the indexing server's configured schedules to see if the indexing jobs can start during the time period you want to migrate the server.
 - From the NetBackup Administration Console, select **Host Properties > Indexing Servers** from the task panel. Next, right-click the indexing server name and select **Properties**. Under **Indexing Server Properties**, select **Schedules**.
 - For each schedule that is listed, select it and click **Properties**.
 - Select the **Start Window** tab. Examine the schedule's start and end specifications to see whether indexing jobs can start during the time period you want to migrate the server.
 - If the indexing schedule window is open for jobs to start, suspend the source indexing server by running the following command on the master server:

```
nbindexutil -suspend -indexserver <source indexing server name>
```

This command ensures that no new indexing jobs are submitted. This command does not stop the indexing jobs that are currently running.

More information about suspending indexing jobs is available:
See ["Suspending and resuming indexing jobs"](#) on page 45.
- 5 Start the indexing engine services. More information is available about how to start and stop the indexing engine services. See ["Starting and stopping indexing engine services"](#) on page 56.
- 6 Copy the following folders from the source indexing server to the target indexing server:

- `<install path>\NetBackupSearch\data*`

- `<install_path>\NetBackupSearch\staging*`

The `data` folder contains indexing data. The `staging` folder contains search data. The default install path location is `C:\Program Files\Symantec`.

Note: Ensure that the `<install_path>` for the target indexing server is the same as the source indexing server. If the target indexing server `<install_path>` is different, the search results from the period before the migration cannot be accessed on the target indexing server. Symantec recommends that you do not change the default `<install_path>`.

The following options are possible for copying the folders:

- Manually copy the folders from the source server to the target server. To ensure faster copying, you can use replication methods.
- If you created a file system backup policy for the source indexing servers, restore the indexing server data to target indexing server. To account for any differences since the last source indexing server backup, you must sync the target indexing server with any changes in step 9.
More information about backing up and restoring indexing server data is available:
See [“Protecting indexing servers”](#) on page 49.

- 7 Update indexing server information for all affected policies in the master server database.

Enter the following command from a master server command prompt:

```
nbindexutil -migrateindexserver -old_indexserver  
source_indexing_server_name -new_indexserver  
target_indexing_server_name
```

This command changes the indexing server name for indexing-enabled policies to the target indexing server's name. It also updates the master server database with the new indexing server information.

If an error occurs due to an issue with updating the policies, run the following command:

```
nbindexutil -migrateindexserver -old_indexserver  
source_indexing_server_name -new_indexserver  
target_indexing_server_name -policyonly
```

Refer to the [NetBackup Commands Reference Guide](#) for more information about the `nbindexutil` utility and the `-migrateindexserver` and `-policyonly` options.

- 8 Verify that the migration completed successfully.

Enter the following command from a master server command prompt:

```
nbindexutil -listindexservers
```

Ensure that the list of indexing servers now includes the target indexing server and not the old indexing server. Also ensure that the server's state is **Active**.

- 9 If you restored indexing data from a backup to the target indexing server in step 6, run the following command on a command prompt on the master server:

```
nbindexutil -reindex -indexserver <target_indexing_server>  
-indexed_after <date>
```

This command updates the target indexing server with any indexing data created since the backup.

- 10 Refresh indexing server references in existing Symantec NetBackup OpsCenter search records with the target indexing server name.

- If Symantec NetBackup OpsCenter runs in a Windows environment, from a command prompt on the OpsCenter server, run the following command:

```
<install_path>\OpsCenter\server\bin\migrateIndexingServer.bat  
<source_indexing_server> <target_indexing_server>
```

- If Symantec NetBackup OpsCenter runs in a UNIX environment, from a command prompt on the OpsCenter server, run the following command:

```
<install  
path>\SYMCOpsCenter\server\bin\migrateIndexingServer.sh  
<source_indexing_server> <target_indexing_server>
```

Upon completion, the utility displays the number of search records updated.

- 11 **Note:** This step applies only to migration of a NetBackup Search 7.5 or 7.5.x.x indexing server to an NetBackup Search 7.6 indexing server. It is a required step if your source indexing server runs NetBackup Search 7.5 or 7.5.x.x and your target indexing server runs NetBackup Search 7.6.

Perform the following subtasks to complete the migration from a NetBackup Search 7.5 or 7.5.x.x indexing server to an NetBackup Search 7.6 indexing server:

- Copy the files and directories from the temporary location you used in step 3 to the target indexing server:
 - The key file to `<target_indexing_server install path>\NetBackupSearch\data\static\key`

- The repository-supplements directory to *<target indexing server install path>\NetBackupSearch\data\repository-supplements*
- Run the following command from a prompt on the target indexing server:
<target indexing server install path>\NetBackupSearch\bin>admin-cmd.exe unpack-repository

Suspending and resuming indexing jobs

You may need to suspend and resume an indexing server when you install software updates or when you migrate to another indexing server.

To suspend indexing jobs for an indexing server, run the following command from a master server command prompt:

```
nbindexutil -suspend -indexserver <indexing server name>
```

This command does not stop the indexing jobs that are currently running. It ensures that no new indexing jobs are submitted.

Answer the prompt to proceed.

To resume indexing jobs for an indexing server, run the following command from a master server command prompt:

```
nbindexutil -resume -indexserver <indexing server name>
```

This command allows new indexing jobs to be submitted.

Answer the prompt to proceed.

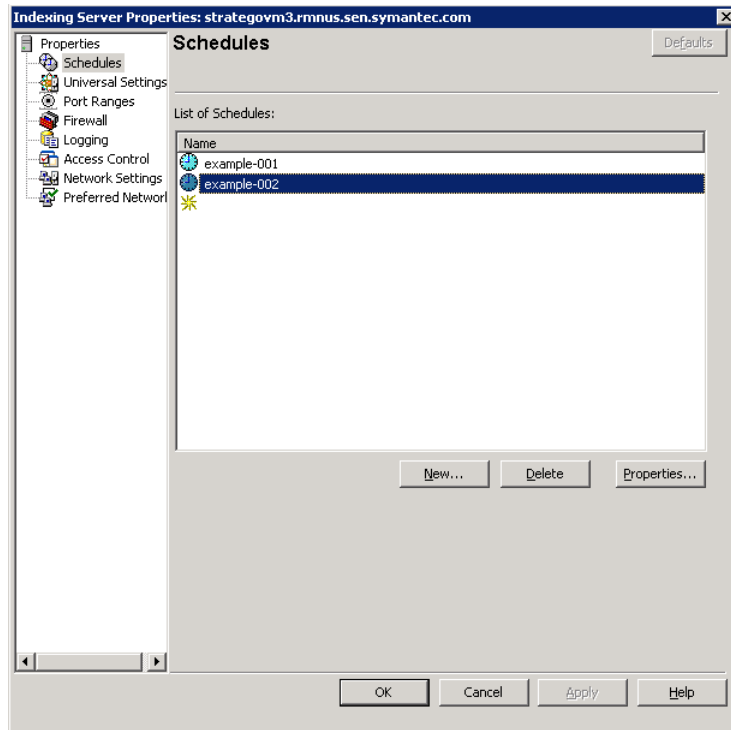
For more information about the `nbindexutil` utility and the `-suspend` and `-resume` options, see the [NetBackup Commands Reference Guide](#).

Adding or modifying indexing server schedules

You can add, view, and modify the schedules of a configured indexing server from the **Indexing Server Properties** window.

To add or modify an indexing server schedule:

- 1 In the NetBackup Administration Console, navigate to **Indexing Server Properties**.

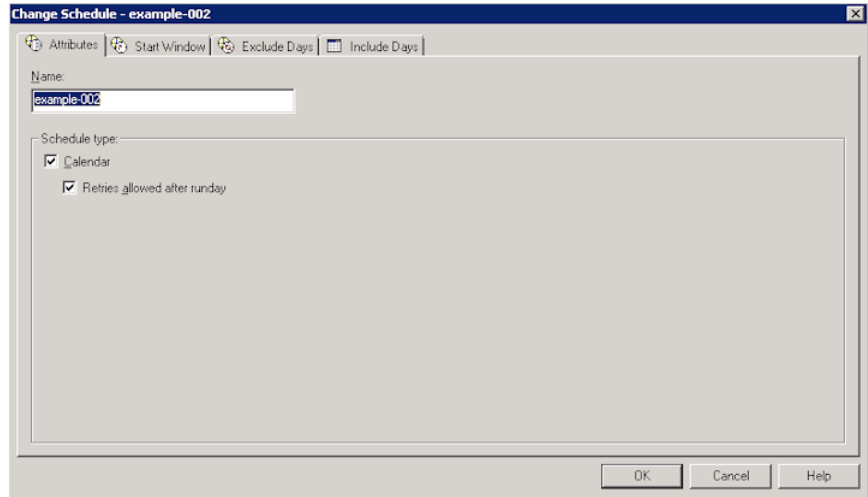


During the configuration of a new indexing server, the **Indexing Server Properties** window opens immediately after you add the indexing server.

For an existing indexing server, select **Host Properties > Indexing Servers** from the task panel. Next, right-click the indexing server name and select **Properties**.

- 2 Select **Schedules** on the **Indexing Server Properties** window. The details panel lists all existing schedules.
 - To add a new schedule, click **New**. The **Add New Schedule** dialog box opens.
 - To modify an existing schedule, select the schedule and click **Properties**. The **Change Schedule** dialog box opens.
 - To delete a schedule, select the schedule and click **Delete**. The schedule is removed without a confirmation prompt. You cannot undo this action.

- 3 Provide the schedule information in the **Add New Schedule** window or the **Change Schedule** window.



- In the **Attributes** tab, enter a unique name for the schedule.
Optionally, under **Schedule Type**, you can select **Calendar** to specify particular days to run a policy. The **Include Days** tab displays when you choose **Calendar**. On the **Include Days** tab, you can schedule to run a task by indicating specific dates, recurring weekdays, recurring days of the month.
For more information, see the **Calendar Schedule** topic in the [NetBackup Administrator's Guide, Volume I](#).
 - In the **Start Window** tab, set the time periods during which NetBackup can start indexing using a schedule.
 - In the **Exclude Dates** tab, specify any specific dates to exclude from a policy schedule. If a date is excluded from a schedule, the policy does not run on that day. The tab displays a calendar of three consecutive months. Use the lists at the top of the calendar to change the first month or year displayed.
- 4 After you complete the schedule configuration, click **OK** on the **Add New Schedule** window or the **Change Schedule** window.
 - 5 Click **OK** on the **Indexing Server Properties** window.

Configuring an indexing server in a backup policy

You must configure the indexing server in a backup policy to enable indexing of the data that is backed up by that backup policy.

You must select the **Enable indexing for search** option on the **Attribute** tab, **Schedule** tab, and **Clients** tab of the **Add New Policy** window or the **Change Policy** window.

The **Enable indexing for search** option is available for the following backup policy types:

- FlashBackup
- FlashBackup-Windows
- Hyper-V
- MS-Windows
- NDMP
- Standard
- VMware

Note: If you enable indexing with VMware and Hyper-V backup policy types, you must also select **Enable file recovery from VM backup** on the **VMware** or **Hyper-V** tab of the backup policy window.

To configure the indexing server in a backup policy:

- 1 Navigate to the backup policy's **Attributes** tab.
 - For a new backup policy, select **Policies** from the task panel.
Select **Actions > New > New Policy**.
Provide a unique name for the backup policy on the **Add a New Policy** dialog box. Do not select the **Use Policy Configuration Wizard** option.
Click **OK**.
 - For an existing backup policy, right-click the backup policy name under **Policies** in the task panel.
Select **Change**.
- 2 Select the **Enable indexing for search** option on the **Attribute** tab, **Schedule** tab, and **Clients** tab of the **Add New Policy** window or the **Change Policy** window.

- | | |
|--------------------------|---|
| Attributes | <ul style="list-style-type: none">■ Select the Enable indexing for search check box.■ From the Indexing Server drop-down list, select the indexing server on which you want to keep the index information. |
| Schedules | <ul style="list-style-type: none">■ Click New to specify a new schedule, or select an existing schedule from the list and click Properties. The Add New Schedule - Policy <backup_policy_name> or Change Schedule - Policy <backup_policy_name> window opens.■ Select Enable indexing for search on the schedule's Attributes tab.■ Click OK when you finish with the Add New Schedule - Policy <backup_policy_name> or Change Schedule - Policy <backup_policy_name> window.■ Also, select Enable indexing for search for other schedules that are defined for the backup policy. |
| Clients | <ul style="list-style-type: none">■ Click New to specify a new client, or select an existing client from the list and click Properties. The Client Hardware and Operating System window opens.■ Select the Enable indexing for search check box.■ Click OK when you finish with the Client Hardware and Operating System window. |
| Backup Selections | No specific indexing server options are available on this tab. Complete the fields that are required for the backup policy type. |

Note: You must also complete other fields that are required for the backup policy type. See **Help** for specific instructions about other options on these tabs.

NetBackup Search does not currently support synthetic backups. Therefore you should not select the **Synthetic backup** schedule attribute for indexing.

- 3 Click **OK** on the **Add New Policy** or **Change Policy** window.

Protecting indexing servers

This topic explains the following aspects of protecting your indexing servers:

- Configuring a backup policy that protects the indexing server
- Running indexing server backups
- Restoring the indexing database from a backup image

- Best practices for protecting indexing servers

Configuring a backup policy that protects the indexing server

This topic describes how to configure a backup policy for protecting your indexing servers. It is a one-time activity that helps NetBackup to protect its own index databases.

To configure a backup policy that protects the indexing server

- 1 From the NetBackup Administration Console, create a new backup policy.
- 2 Configure the new backup policy with these specific backup policy attributes:

Note: You must also complete the other fields that are required for the backup policy type. Refer to **Help** for specific instructions about the other options on these tabs.

- **Attributes** tab
Select **MS-Windows** for **Policy type**.
- **Schedules** tab
Specify a manual schedule. To avoid contention with previously configured indexing jobs, exclude any schedule periods for the indexing servers that are included in this backup policy.
- **Clients** tab
Include all configured indexing servers.
- **Backup Selections** tab
Make sure that you include the NetBackup Search `data` directory and `staging` directory in the selections.
`install_path\Symantec\NetBackupSearch\data`
`install_path\Symantec\NetBackupSearch\staging`

Note: Symantec recommends that your backup selections also include other important files and folders that reside on the indexing servers. For example, you should include any scripts that you create to start and stop indexing services.

See [“Running indexing server backups”](#) on page 51.

Running indexing server backups

This topic explains how to prepare and run indexing server backup jobs. These jobs can be either manually started or configured in the backup policy schedule. In latter case, the job starts automatically. You have to monitor the job progress and ensure that it completes successfully and in a timely manner.

Note: For more information about the scripts that this topic references, see the following publications:

[How to use bpstart and bpend notify scripts](#) and [NetBackup Administrator's Guide, Volume I](#)

To run indexing server backups with a backup policy and automated scripts

1 Create a pre-job script that contains the following commands:

```
net stop "NetBackup Search Executor Service"  
  
"install_path\bin\velocity-shutdown.exe -y"
```

The first statement stops the Search Executor service. The second command stops the indexing engine and related NetBackup Search services. Make sure that you include the double quotation marks (") where indicated.

For Windows clients, save the script as `bpstart_notify.policy_name.bat`.

`policy_name` is the name of the backup policy that was created in [Configuring a backup policy that protects the indexing server](#). The `bpbkar[32]` process runs `bpstart_notify.policy_name.bat` before the backup job starts.

2 Create a post-job script that contains the following commands:

```
"install_path\bin\velocity-startup.exe -y"
```

The command `velocity-startup` keeps the `netbackupindexingengine` service in "Manual" startup mode, to bring it back to automatic mode issue the command `sc config NetBackupIndexingEngine start= auto` and proceed with the next commands or steps.

```
net start "NetBackup Search Executor Service"
```

The first command restarts the indexing engine and related NetBackup Search services. The second command restarts the Search Executor service. Make sure that you include the double quotation marks (") where indicated.

For Windows clients, save the script as `bpend_notify.policy_name.bat`

`policy_name` is the name of the backup policy that was created in [Configuring a backup policy that protects the indexing server](#). The `bpbkar[32]` process runs `bpend_notify.policy_name.bat` after the backup job completes.

3 On each indexing server, copy both scripts to the following location:

```
install_path\bin\
```

Note: If you cannot deploy scripts on your indexing servers or if you want to perform a trial run of a backup, you can manually back up the indexing server. See the next procedure for instructions on how to manually back up an indexing server.

At this point, the configuration of your indexing server backup is complete. As the backup job starts according to the backup policy schedule, the `bpstart_notify`

script runs first. After the script finishes, the job backs up the selected files and folders. After the backup job finishes, the `bpstart_notify` runs.

Note: Symantec recommends that you add the `bpstart_notify` and `bpend_notify` scripts to the backup selections for the indexing server backup policy. This practice ensures that the scripts are automatically available and in place in the event that you restore a server after it fails.

See [“Configuring a backup policy that protects the indexing server”](#) on page 50.

To run an indexing server backup manually

For a manual backup, you must perform the following steps on each indexing server that you back up. The backup policy cannot have a schedule wherein the backup jobs are started automatically by NetBackup Scheduler.

- 1 Stop the indexing engine services. More information is available about how to start and stop the indexing engine services. See [“Starting and stopping indexing engine services”](#) on page 56.
- 2 From the NetBackup Administration Console, start a user-initiated backup job from the indexing server backup policy.

Monitor the backup job in Activity Monitor and allow the job to complete.
- 3 Start the indexing engine services. More information is available about how to start and stop the indexing engine services. See [“Starting and stopping indexing engine services”](#) on page 56.

Restoring the indexing database from a backup image

If a disaster involves failure of the indexing server or the indexing server application, you must restore the indexing server first. You may install an indexing server on the same hardware or a new hardware and configure it. This section describes how to restore a backup of an indexing server to reinstate the server and resume the indexing operation.

To restore the indexing database from a backup image

- 1 Reinstall NetBackup and NetBackup Search software (indexing server).

More information about installing NetBackup Search software is available:

See [“Installing an indexing server”](#) on page 20.

To reinstall NetBackup master servers or media servers, refer to the [NetBackup Installation Guide](#).

- 2 From a command prompt on the indexing server, stop the indexing engine and search executor services:

```
install_path\bin\velocity-shutdown.exe -y
```

- 3 Locate the backup image that contains the indexing server files that you need to restore:

```
install_path\Symantec\NetBackupSearch\data
```

```
install_path\Symantec\NetBackupSearch\staging
```

Also locate any other files such as scripts that you have backed up with indexing server files.

- 4 From the NetBackup **Backup, Restore, and Archive** interface, restore the indexing server files from the backup image.

For information about restoring files and directories from a backup, refer to the [NetBackup Backup, Archive, and Restore Getting Started Guide](#).

- 5 Start the indexing engine services. More information is available about how to start and stop the indexing engine services. See [“Starting and stopping indexing engine services”](#) on page 56.

Note: Although the indexing server is restored, the data does not include any new, indexed backup images that were created since the indexing server's last backup.

- 6 Re-index any backup images that were created since the last indexing server backup. More information is available about how to re-index backup images. See [“Re-indexing backup images”](#) on page 35.

Note: You must first convert the timestamp on the indexing server to the `mm-dd-yy-hh-mm-ss` format and then use it in the command. For more information about time conversion, see TECH138460 on the [Symantec support](#) website. You can also migrate the old indexing server to another server. More information is available about how to migrate the old indexing server to another server. See [“Migrating an indexing server to another indexing server”](#) on page 41.

- 7 To verify that the indexing data is restored successfully, create and run a set of sample search queries.

These queries should return results from the latest backup images and from earlier backup images.

Best practices for protecting indexing servers

This topic describes the best practices that Symantec recommends for most common scenarios and discusses the alternatives for non-standard scenarios

- Create a single backup policy for all the indexing servers in a domain. This practice minimizes the administration overheads and streamlines the process of protecting indexing servers. However, you may need a separate configuration for one or more indexing servers. For example, if scheduling windows for the indexing jobs and the indexing server backup jobs do not match, then the indexing servers cannot be backed up at the same time. Also, if the indexing server is co-located on a media server, their backups should be directed to a different media server.
- Schedule the indexing server backup job immediately after the backup window starts. After the indexing server backup starts, the indexing engine and the service can be stopped. Any indexing job that starts during this time fails. Stopping the indexing engine causes the least amount of disruption.
- For a standalone indexing server, pause between the indexing window and the backup window. Then back up the indexing server during this short gap. The advantage of this practice is that the indexing server protection job does not have to compete with other backup jobs. The indexing server runs faster and the indexing engine can restart sooner.

- Ensure that the NetBackup image catalog and the indexing database are in-sync with each other.
For best results, back up the catalog and the index database at the same time. If it is not feasible, then try to make the time between the two backups as short as possible.
- Back up the indexing servers before you back up your NetBackup image catalog. Usually the NetBackup image catalog should be before the indexing server backup. By design, indexing is a step that follows backup. If the image catalog and the indexing data need to be restored, it is appropriate to restore the catalog before the indexing data. Therefore, the index backup should happen before the scheduled catalog backup as far as possible.

Starting and stopping indexing engine services

This topic describes how to start and stop the indexing engine services.

To start indexing engine services

- 1 From a command prompt on the indexing server, run the following command:

```
install_path\bin\velocity-startup.exe -y
```

This command starts the NetBackup Indexing Engine service in manual startup mode.

- 2 To bring the NetBackup Indexing Engine service to automatic mode, run the following command:

```
sc config NetBackupIndexingEngine start= auto
```

This command starts the NetBackup Indexing Engine service only.

- 3 To start the NetBackup Search Executor service, from a command prompt on the indexing server, run the following command:

```
net start "NetBackup Search Executor Service"
```

To stop indexing engine services, run the following command from a command prompt on the indexing server:

```
install_path\bin\velocity-shutdown.exe -y
```

Note: This command stops both, the NetBackup Indexing Engine and NetBackup Search Executor services.

Search Queries

This chapter includes the following topics:

- [About searches queries](#)
- [Search criteria](#)
- [Searching files and folders in indexed backup images](#)
- [Working with Image Search](#)
- [About using wildcard characters in a search](#)
- [Search terms](#)
- [Managing saved search queries](#)
- [Managing search results](#)
- [Finding the search ID](#)

About searches queries

Use NetBackup Search to search for data in indexed backup images and the Symantec NetBackup OpsCenter database. The data is searched based on the criteria that you provide in the query page. You can search for backup images of the relevant data based on date range across all the NetBackup domains and all the types of backup.

More information is available:

See [“Searching files and folders in indexed backup images”](#) on page 59.

See [“Search terms”](#) on page 67.

See [“About using wildcard characters in a search”](#) on page 66.

See [“Editing a saved search query”](#) on page 70.

See [“Running a saved search”](#) on page 71.

See [“Viewing search results”](#) on page 73.

See [“Deleting search results”](#) on page 76.

See [“Deleting a saved search”](#) on page 72.

Search criteria

The Search window on the Symantec NetBackup OpsCenter UI displays various fields that let you specify the search criteria. You must separate multiple values in a multi-valued field with a semi-colon. The search criteria comprises of the following fields:

| Field name | Multi-valued field |
|-------------------|--------------------|
| User and Group | Yes |
| Backups taken in | No |
| Files and Folders | Yes |
| Master Servers | Yes |
| Clients | Yes |
| File Type | Yes |
| File Created | No |
| File Modified | No |

When you enter multiple values in a field, you must observe the following rules:

- Search results are displayed if at least one of the values match. For example, In the **Files and Folder** field, if you enter multiple values like `file1.txt;*.exe` to specify the **File Path**, the search result matches if the name of the file is `file1.txt` or if a file matches the extension `*.exe`.
- If you specify multiple values, the condition must match for every field, and the operation across fields. For example:
For the **Files and Folder** field, if you enter multiple values like `file1.txt;*.exe`, and in the **Backups Taken in** field if you select **Last Month**, then the search results will match if the name of the file is `file1.txt` or if the file matches the extension `*.exe`, and the backup was taken in the last month

Note: The **File Path** and the **File Extension** are distinct fields. If both these fields are specified, the **File Path** and **File Extension** conditions must match.

Searching files and folders in indexed backup images

To search files and folders from the backup images that are indexed, you must first create a search for data in indexed backup images with the search criteria that defines your search. You must then run that search to display the search results related to your search.

Creating a search for data in indexed backup images

Perform the following procedure to create a search for data in indexed backup images.

To create a search for data in indexed backup images

- 1 From the Symantec NetBackup OpsCenter interface, select **Search & Hold > New**.

Ensure that the index data collection has completed. If you select **Files and Folder**, the left pane of the **New Search Criteria** page displays the numbers of master servers, clients, users, and views for which index data collection has completed. However, if you select **Image Search**, the left pane of the **New Search Criteria** page displays only the number of master and client servers for which image data collection has completed. If there are two master servers for which image data is in the process of being collected, the left pane does not include those two master servers in the master count. Also, the numbers in the left pane change appropriately when you select a master server, client, user, or a view in the right pane.

To view the status of the index data collection, select **Settings > Configuration** and see the NetBackup Masters Data Collection Status.

- 2 From the **Search For:** drop-down list select **Files and Folder**.
- 3 Select the appropriate criteria for the search. To refine the search, click **Advanced** and add one or more of the criteria that is displayed.

More information is available about the search terms.

See [“Search terms”](#) on page 67.

More information is available about using wildcards in the search criteria.

See [“About using wildcard characters in a search”](#) on page 66.

- 4 Click **Save** to save the selected search criteria.
A new dialog box opens.
- 5 Provide a unique **Name** for the search. For example, you can name the search so that it corresponds with an on-going legal proceeding.
- 6 (*Optional*) Provide a description of the search criteria in **Comments**.

- 7 (Optional) Select **Send Search Completion Email Notification** to send an email when the search completes, and then select recipients.

Note: This option is available only for **File & Folder** search.

The list of recipients is defined in Symantec NetBackup OpsCenter. To add the recipients that are not in the list of recipients, enter their email addresses in the **Add Email Address** field. You must separate multiple addresses with a semicolon. For example,

john_doe@symantec.com;jane_doe@symantec.com

For more information about managing email recipients, see [Symantec NetBackup Administrator's Guide](#).

Save

Name your search and add additional comments

Name : test_1 *

Comments :

☐ ⚠ Send Search Completion Email Notification

OK Cancel

- 8 Click **OK** to save the search.

A list of saved searches is displayed. By default, the list is sorted by name. Click the plus sign next to the name of a saved search to display more information about it.

You must run the saved search to search files and folders from backup images. More information is available about how to run a saved search. See [“Running a saved search”](#) on page 71.

Working with Image Search

In the early stages of litigation, you might not know which exact backup images to search and place a hold on. You are not sure of the search criteria too to search and hold the backup images. In this case, to prevent the backup images from expiring, you can search and hold the backup images within a date range by using Image Search. This way you can hold the backup images within a date range across all policy types and of all users.

For example, in the early stages of litigation, you know that you do not want approximately last six month's backup images to expire. You can use the Image Search functionality to search and hold all the backup images for last six months.

Image Search not only lets you search the backup images within a date range, but it also lets you search the backup images within a date range of a particular backup policy type, or of a particular user.

Note: The search results include backup images that are indexed and also the ones that are not indexed.

You cannot perform a mass restore of the backup images that are searched and placed on hold by using Image Search.

You can perform the following tasks for backup images within a date range:

Search - See [“Searching backup images within a date range”](#) on page 62.

Hold - See [“Placing a hold on a backup image”](#) on page 78.

Export - See [“Exporting details of backup images”](#) on page 65.

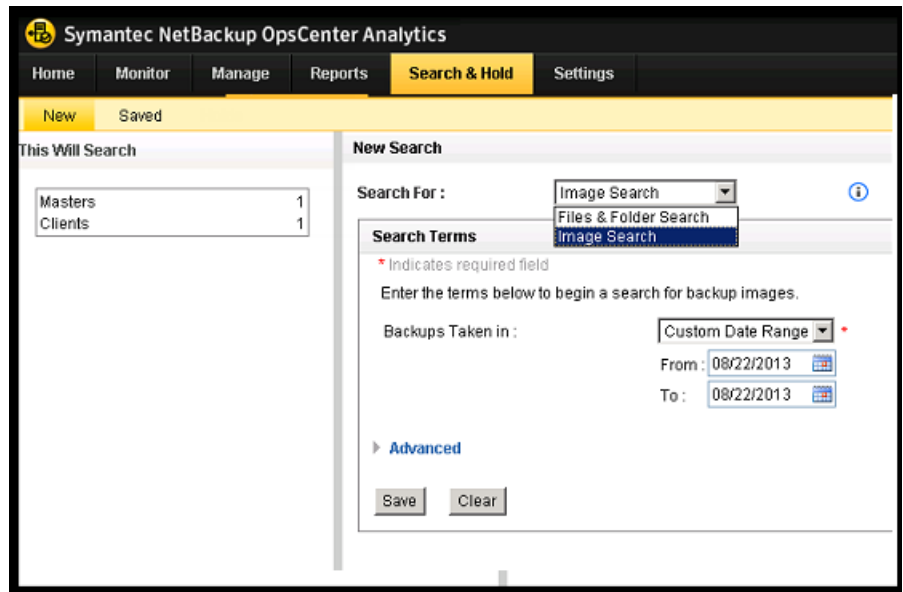
Searching backup images within a date range

Perform the following procedure to search backup images within a date range:

Note: The search results include backup images that are indexed and also the ones that are not indexed.

To search backup images within a date range

- 1 From the Symantec NetBackup OpsCenter console, select the **Search & Hold** tab.
- 2 On the **New** tab, select **Image Search** from the **Search For:** drop-down menu.



- 3 Enter the custom date range or select the predefined date range from the **Backups Taken In:** drop-down menu.
- 4 Click **Save**.
A new dialog box opens.
- 5 Enter a name for the search in the **Name** text box, and add comments, if any, in the **Comments** text box, and then click **OK**.
The **Saved** tab opens with the list of saved image searches.
- 6 Select the check-box next to the saved image search that you want to run and click the **Run** button.
The status of the image search changes to **Queued**.

- 7 Click **Refresh** to refresh the search status.

When the search is completed, the status is changed to **Completed** followed by a hyperlink to the number of hits found. For example, **Completed: (3 Hits found)**.

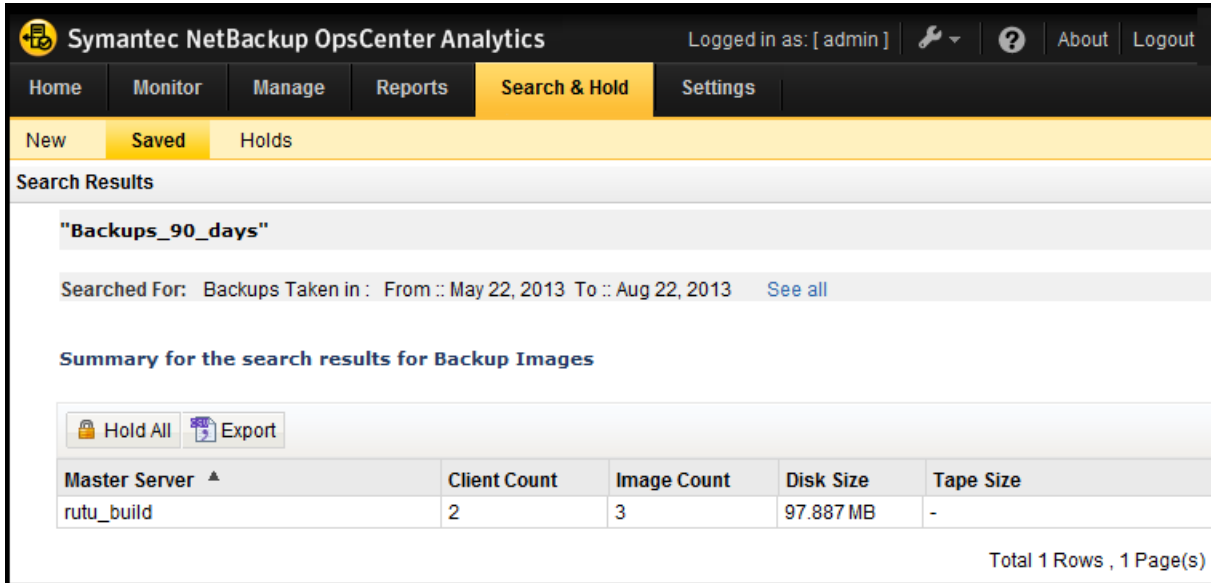
The screenshot displays the Symantec NetBackup OpsCenter Analytics web interface. The top navigation bar includes tabs for Home, Monitor, Manage, Reports, Search & Hold (active), and Settings. A user is logged in as 'admin'. Below the navigation bar, there are tabs for New, Saved, and Holds. The 'Saved Searches' section is active, showing a list of saved searches. A 'View Searches For:' dropdown is set to 'Image Search'. Below this, there are buttons for Run, Delete Search, and Refresh. A table lists the saved searches with columns for Name, Hold, Last Saved, Status, and Last Run. Two searches are listed: 'Backups_90_days' and 'Backups_one_month', both with a status of 'Completed:(3 Hits Found)'. A 'Search Overview' sidebar on the left shows counts for Saved (2), Completed (2), In Progress (0), Queued (0), and Failed (0). The bottom right corner indicates 'Total 2 Rows, 1 Page(s)'.

| Name | Hold | Last Saved | Status | Last Run |
|-------------------|------|-------------------------|--------------------------|-------------------------|
| Backups_90_days | - | Aug 22, 2013 1:57:40 PM | Completed:(3 Hits Found) | Aug 22, 2013 1:57:53 PM |
| Backups_one_month | - | Aug 22, 2013 1:57:07 PM | Completed:(3 Hits Found) | Aug 22, 2013 1:57:53 PM |

Note: The hits count displayed in the status link is the number of backup images found for the given search criteria.

- 8 Click the hyperlink of the number of hits found.

The Search Results window is displayed with the total number of images found.



Symantec NetBackup OpsCenter Analytics

Logged in as: [admin]

Home Monitor Manage Reports Search & Hold Settings

New Saved Holds

Search Results

"Backups_90_days"

Searched For: Backups Taken in : From :: May 22, 2013 To :: Aug 22, 2013 [See all](#)

Summary for the search results for Backup Images

[Hold All](#) [Export](#)

| Master Server ▲ | Client Count | Image Count | Disk Size | Tape Size |
|-----------------|--------------|-------------|-----------|-----------|
| rutu_build | 2 | 3 | 97.887 MB | - |

Total 1 Rows , 1 Page(s)

More information is available about how to place a hold on backup images. See ["Placing a hold on a backup image"](#) on page 78.

More information is available about how to export details of backup images. See ["Exporting details of backup images"](#) on page 65.

Exporting details of backup images

The search results that are displayed when you use the Image Search option includes summary of the backup images per master server, like, the master server name, client count, image count, disk size, and so on. To view more details of each backup image, like backup image ID, client name, whether expired, and so on, export the details of backup images by using the **Export** button.

To export details of backup images

Before performing this procedure, you must search backup images within a date range. More information is available about how to search backup images within date range. See ["Searching backup images within a date range"](#) on page 62.

- 1 To export the details of these backup images to a .CSV file, click the **Export** button.

A dialog box is displayed.

- 2 Perform one of the following:
 - Click **Open** to open the .CSV file.
 - Click **Save** to save the .CSV file.

The .CSV file includes the following details of backup images:

- Image ID
- Master server
- Client
- Policy type
- Media IDs
- Tape count
- Tape size
- Disk size
- Location type
- Is expired
- Number of copies

About using wildcard characters in a search

Wildcards are special characters that support a single or multi-character sequence. You can search for files or folders by using the following wildcard entries:

- ?

When you use a question mark, your entry is matched with a single character entry. For example:

The query `Ren?s` matches the terms `Renás` and `Renas`.

The query `t?ll` matches the words `tall`, `tell`, and `till`. Any three-character word that begins with `t`, followed by any other character, and ends with `ll` are matched.

Similarly for the query `??ll` any four-character word that ends with the characters `ll` are matched.
- *

When you use an asterisk, your entry is matched with any sequence of zero or more characters.

This wildcard expression can be written in phrases like `?Name LNa*`, but it does not match terms that are used in a phrase. For example:

The query `?Name LNa*` matches `FName LName`, but `F*L` does not match with `FName LName`.

Similarly, the query `??ow*ng` matches terms like `growing` and `flowing`. Any word that begins with any two characters, followed by the character sequence `ow`, followed by any number of other characters, and ending in the character sequence `ng` are matched.

Search terms

The search terms for the Files and Folder Search and Image Search selection are mentioned below:

Table 4-1 Field descriptions for Files and Folder Search and Image Search-Search Terms

| Field | Description |
|---|--|
| Users and Groups (For Files and Folder Search selection only) | <p>Click the ellipses to select the users and groups that created the files that you want to find. Selected users are searched within selected groups.</p> <p>To find users and groups in this list, enter text in Search this list. You may use wildcard characters; for example, enter Group* to include users and the groups that begin with "Group".</p> <p>To include all users and groups on the displayed page, select the check box at the top of the left-most column.</p> |
| Backups Taken in | <p>From the drop-down list, select a time period in which the backup was taken. Select Custom Date Range to specify a specific range of dates.</p> |
| Files and Folders (For Files and Folder Search selection only) | <p>Specify the names of the files and folders you want to include in the search. Separate multiple names with semicolons. You may use wildcard characters to specify patterns in file names and folder names. For entering a valid file and folder pattern imply the following:</p> <ul style="list-style-type: none">■ Enter at least one alpha or numeric character for every files and folders name. For example: /c/Group* or /c/Group2■ Enter double quotes at the beginning and at the end of files and folders name. For example: "MyQueryfiles" <p>These criteria are required for a valid search.</p> |

Table 4-1 Field descriptions for Files and Folder Search and Image Search-
Search Terms (*continued*)

| Field | Description |
|---|--|
| Advanced | Click this link to display the advanced search criteria. |
| Domain Views | <p>Choose to search Domains or Views:</p> <ul style="list-style-type: none">■ Choose Domain to search the backups that were taken for master servers and clients.■ Choose View to search the backups that were taken for master server views or client views. Only master servers of clients that are configured for indexing are listed with views. |
| Master servers Note: (Domain selection only) | <p>Click the ellipses to select the names of the NetBackup master servers you want to include in this search. Separate multiple names with semicolons.</p> <p>To find master servers in this list, enter text in the Search this list field. You may use wildcard characters; for example, enter *symantec.com to include master servers that end with "symantec.com".</p> <p>From the Version drop-down list, select a version number to find the master servers that are running a specific version of NetBackup.</p> |
| Name Note: (Views selection only) | Click the ellipses to select the names of the views you want to include in this search. |
| Clients Note: (Domain selection only) | <p>Click the ellipses to select the names of the clients you want to include in this search. Separate multiple names with semicolons.</p> <p>To find clients in this list, enter text in the Search this list field. You may use wildcard characters; for example, enter *symantec.com to include the clients that end with "symantec.com".</p> <p>To view clients on other master servers and select them if required for this search, select the Master Servers from the drop-down list.</p> |

Table 4-1 Field descriptions for Files and Folder Search and Image Search-
Search Terms (*continued*)

| Field | Description |
|---|--|
| File Type (For Files and Folder Search selection only) | Select one or more of the following file types to include in the search: <ul style="list-style-type: none">■ Excel Spreadsheets (<code>xls</code> and <code>xlsx</code>)■ PDF Documents (<code>pdf</code>)■ PowerPoint Presentation (<code>ppt</code> and <code>pptx</code>)■ Text Files (<code>txt</code> and <code>rtf</code>)■ Word Documents (<code>doc</code> and <code>docx</code>)■ (Other) / Specify . Use a semicolon to specify multiple file types; for example: <code>exe;png;mp3</code> and so on. Separate multiple values with semicolons. |
| File Created (For Files and Folder Search selection only) | From the drop-down list, select a time period in which the files for the search were created. Select Custom Date Range to specify a specific range of dates. |
| Policy Type (For Image Search selection only) | By default all the policies are selected, you can click the ellipses to select the policy you want to configure for this search. Separate multiple names with semicolons. |
| File Modified (For Files and Folder Search selection only) | From the drop-down list, select a time period in which the files for the search were most recently changed. Select Custom Date Range to specify a specific range of dates. |

For the Files and Folder Search and Image Search, the valid date options for the **Backups Taken in**, **File Created**, and **File Modified** fields are as follows:

- Today - This is the current day.
- Yesterday
- Last week - The time span consists of the last seven days. For Example: If the current day is Wednesday, then the span is calculated from last Wednesday to the current day (Wednesday).
- Last month - The time span consists of the last 31 days. For Example: If current date is 7th December, then span is calculated from 7th November to the current day (7th December).

- Last 90 days - The time span consists of the last 90 days. For Example: If the current day is 8th December, then the span is calculated from 8th September to the current day (8th December).
- Last year - The time span consists of the last year. For Example: If the current date is 7th December, 2011, then the span is calculated from 7th December, 2010 to the current day (7th December, 2011).
- Custom date range - You can select the from and to date options.

Managing saved search queries

You can perform the following tasks with the saved search queries:

- [Editing a saved search query](#)
- [Running a saved search](#)
- [Deleting a saved search](#)

Editing a saved search query

To edit a saved search for data in indexed backups

- 1 From the Symantec NetBackup OpsCenter interface, select **Search & Hold > Saved**.
- 2 Select the type of search - **Files & Folder Search** or **Image Search**.
- 3 Click the **Name** of the saved search that you want to edit.
- 4 Make the changes you want to the criteria for the search. Detailed information about the search terms is available:

See [“Search terms”](#) on page 67.

A basic search includes one or more of the following criteria:

- **Users and Groups**
- **Backups Taken in**
- **Files and Folders** (required)

Click **Advanced** to change or add one or more of the advanced criteria.

- 5 Click **Save** to save the changed search criteria.

Click **Save as** to save the changed search with another name.

- If you clicked **Save as**, provide a **Name** for the search.
- Optionally, provide a description of the search criteria in **Comments**.

- Optionally, select **Send Search Completion Email Notification** to send a message when the search completes, and then select recipients. The list of recipients is defined in Symantec NetBackup OpsCenter. To add the recipients that are not in the list of recipients, enter their email addresses in the **Add Email Address** field. Separate multiple addresses with semicolons; for example,
john_doe@symantec.com;jane_doe@symantec.com

Note: To enable email recipients through Symantec NetBackup OpsCenter, select **Settings > Recipients > Email**. See *About managing recipients in OpsCenter* for detailed information about email notifications through Symantec NetBackup OpsCenter.

- Click **OK** to complete saving the search.

Next, a list of saved searches is displayed. You can find the recently changed saved search at the top of the list. Click the plus symbol next to the name of a saved search to display information about it.

Running a saved search

To run a saved search

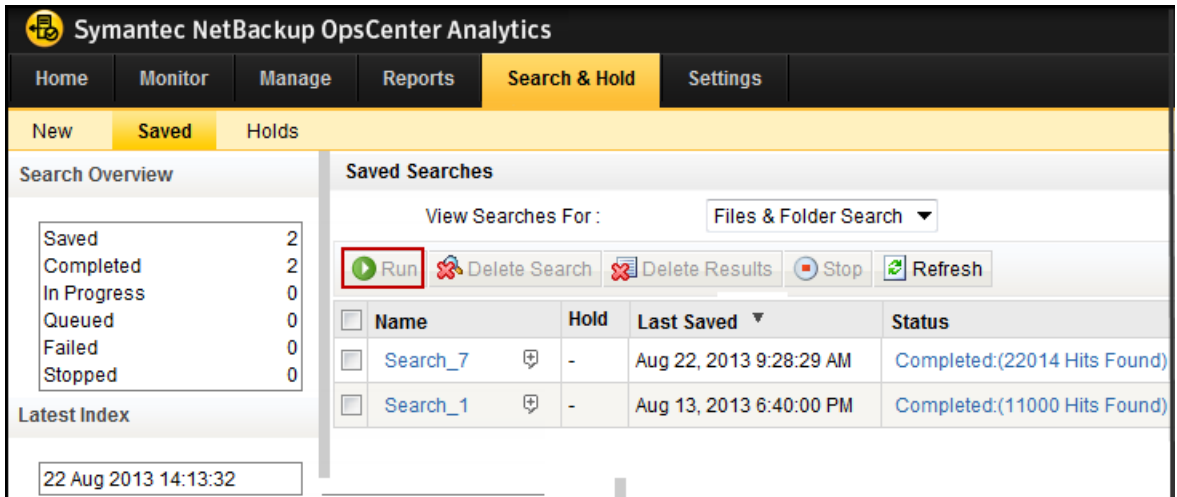
- 1 From the Symantec NetBackup OpsCenter interface, select **Search & Hold > Saved** to view the list of saved searches.
- 2 Select the type of search - **Files & Folder Search** or **Image Search**.
- 3 Select the saved search you want to run. You may select multiple searches from the list.

Note: You can run a maximum of 10 searches simultaneously. Requests for more than 10 searches are queued and run as previously submitted searches complete. You can run and save the results of a maximum of 50 searches. After this limit, you must delete the results of completed searches to run a new search.

- 4 Click **Run**.

Some searches run for a long time. Check the **Status** column to see how the search progresses.

Figure 4-1 Running a Saved Search



Deleting a saved search

Use this procedure to delete a saved search.

To delete a saved search

- 1 From the Symantec NetBackup OpsCenter interface, select **Search & Hold > Saved** to view the list of saved searches.
- 2 Select the type of search - **Files & Folder Search** or **Image Search**.
- 3 Select the saved search you want to delete. You may select multiple searches from the list.
- 4 Click **Delete Search**.
- 5 Respond to the prompt **Are you sure you want to delete the selected search criteria?**

Either click **OK** to delete the search, or click **Cancel** to keep the saved search.

Managing search results

You can perform the following tasks with the search results:

View - See [“Viewing search results”](#) on page 73.

Delete - See [“Deleting search results”](#) on page 76.

Viewing search results

This topic describes viewing search results.

Note: Before performing this procedure, you must run a saved search query. See [“Running a saved search”](#) on page 71.

To view search results

- 1 To view search results, find the saved search and select the status link in the Status column.

For example, **Completed (13 hits found)**, **In Progress**, or **Failed**.

The search results for the saved search that you selected are displayed.

Note: You can view the partial search results while the search is in progress. You do not have to wait until the search is complete to view the search results.

For **Files and Folder Search**, the hits count displayed in the status link is the number of files found for the given search criteria.

For **Image Search**, the hits count displayed in the status link is the number of backup images found for the given search criteria.

- 2 For **Files & Folder Search** - To view list of the files that matched the search criteria in that backup, select the backup from the **Backup Taken At** column, and then click the plus sign next to the date to view the corresponding backup image details.

This view displays detailed information about a backup image.

For Image Search - You can view the number of images backed up on the Master Server. You can select **Export** to generate a CSV file of the search results.

Note: If there are millions of results, and you try to view the last page by clicking the **Last Page** button, it may take a long time to view the results. The session might even time out.

For **Files & Folder Search** you can filter the backups for the search results from the left panel.

Filters are available on Master and Client only. These filters are persisted across sessions when you select **Apply**. Click **Clear** to remove the filter.

The **Last Sync Time** column on the Symantec NetBackup OpsCenter UI does not change for a considerable duration when a search operation is run.

When you run the search operation, Symantec NetBackup OpsCenter receives results for the Search and updates the **Last Sync Time** column. The **Last Sync Time** column lists the most recent time when Symantec NetBackup OpsCenter receives results for a given Search. If the **Last Sync Time** column does not change for a considerable duration, then there is a possibility of one or more Search services being down or unresponsive on related Hosts.

Workaround: Analyze the progress information on the Search Broker in `<install_path>\SearchBroker\var\progress\<search-id>.csv` to determine the status of the search on related hosts. You may have to stop and re-run the search operation.

- 3 To place a hold for **Files & Folder Search**, select the backup images that you want to hold, and then click **Hold** or **Hold All**.

More information about holds is available:

See [“Placing a hold on a backup image”](#) on page 78.

Figure 4-2 Search results for Files & Folder search

The screenshot shows the Symantec NetBackup OpsCenter Analytics interface. The top navigation bar includes Home, Monitor, Manage, Reports, Search & Hold (selected), and Settings. The left sidebar has tabs for New, Saved, and Holds. The main content area is titled 'Search Overview' and 'Saved Searches'. Under 'Saved Searches', there is a dropdown menu set to 'Files & Folder Search'. Below this are buttons for Run, Delete Search, Delete Results, Stop, and Refresh. A table lists saved searches with columns: Name, Hold, Last Saved, Status, Last Run, and Last Sync Time. The table contains two rows: 'Search_7' and 'Search_1'. The bottom right corner indicates 'Total 2 Rows, 1 Page(s)'.

| Name | Hold | Last Saved | Status | Last Run | Last Sync Time |
|----------|------|-------------------------|------------------------------|-------------------------|-------------------------|
| Search_7 | - | Aug 22, 2013 9:28:29 AM | Completed (22014 Hits Found) | Aug 22, 2013 2:15:30 PM | Aug 22, 2013 2:15:30 PM |
| Search_1 | - | Aug 13, 2013 6:40:00 PM | Completed (11000 Hits Found) | Aug 22, 2013 2:15:30 PM | Aug 22, 2013 2:15:30 PM |

For **Image Search** you can only click **Hold All** to place a hold on all backup images.

Figure 4-3 Search results for Image Search

The screenshot shows the Symantec NetBackup OpsCenter Analytics interface. The top navigation bar includes Home, Monitor, Manage, Reports, Search & Hold (selected), and Settings. The left sidebar has tabs for New, Saved, and Holds. The main content area is titled 'Search Overview' and 'Saved Searches'. Under 'Saved Searches', there is a dropdown menu set to 'Image Search'. Below this are buttons for Run, Delete Search, and Refresh. A table lists saved searches with columns: Name, Hold, Last Saved, Status, and Last Run. The table contains two rows: 'Backups_90_days' and 'Backups_one_month'. The bottom right corner indicates 'Total 2 Rows, 1 Page(s)'.

| Name | Hold | Last Saved | Status | Last Run |
|-------------------|------|-------------------------|--------------------------|-------------------------|
| Backups_90_days | - | Aug 22, 2013 1:57:40 PM | Completed (3 Hits Found) | Aug 22, 2013 1:57:53 PM |
| Backups_one_month | - | Aug 22, 2013 1:57:07 PM | Completed (3 Hits Found) | Aug 22, 2013 1:57:53 PM |

Deleting search results

Use this procedure to delete the search results from a saved search. You may want to perform this procedure in the following scenarios:

- You want to retain the saved search criteria, but you do not need the current results of the search.
- You have reached the limit of 50 completed searches, and you want to run more searches.

To delete search results

- 1 From the Symantec NetBackup OpsCenter interface, select **Search & Hold > Saved** to view the list of saved searches.
- 2 Select the type of search - **Files & Folder Search** or **Image Search**.

- 3 Select the saved search you want to delete. You may select multiple searches from the list.
- 4 Click **Delete Search Results**.
- 5 Respond to the prompt **Are you sure you want to delete the results for selected search criteria?**
Click **OK** to delete the search results. Click **Cancel** to keep the search results.

Finding the search ID

You need the search ID to perform a mass restore. Perform the following procedure to find the search ID.

To find the search ID:

- 1 From the Symantec NetBackup OpsCenter interface, select **Search & Hold > Saved**.
- 2 Select **Files & Folder Search**.
- 3 From the list of saved search, click the expand icon:



The Search Criteria details view is displayed. You can note the Search ID from the Search Criteria details view.

Holds Management

This chapter includes the following topics:

- [Placing a hold on a backup image](#)
- [Viewing holds details](#)
- [Search & Hold > Holds view](#)
- [Search & Hold > Holds > Hold Details view](#)
- [Releasing a hold](#)
- [About Hold reports in Symantec NetBackup OpsCenter](#)
- [Viewing hold reports](#)
- [Hold Reports > Image Retention Summary](#)
- [Hold Reports > Top Holds by Size](#)
- [Hold Reports > Top Holds by Age](#)
- [How to find the status of backup images on hold](#)
- [Finding the media information of backup images on hold](#)

Placing a hold on a backup image

NetBackup Search provides two methods for placing a hold on a backup image:

- **Legal hold** - You create a legal hold from Symantec NetBackup OpsCenter based on the results of a saved search.
- **Local hold** - You create a local hold from the command line interface of the NetBackup master server.

Caution: Placing a hold on backup images may disrupt new backups from completing. Storage may fill up if previous backups are not automatically expired.

When you start the Symantec NetBackup OpsCenter server, the Hold Agent initializes to perform hold operation. Ensure that the hold status is started on **Setting > Configuration > DataCollection** status page. If the Hold status is not started and you attempt to perform any hold operation, the message **Communication With Master Server Failed** is displayed.

To place a legal hold on a backup image by using Symantec NetBackup OpsCenter

- 1 From the Symantec NetBackup OpsCenter interface, select **Search & Hold > Saved**.
- 2 Select the type of search - **Files & Folder Search** or **Image Search**.
- 3 Find the saved search that contains the backup images that you want to hold.
- 4 Click the **Completed** link in the **Status** column of the saved search.

Note: You cannot place a hold if the status is **In progress**.

- 5 For **Files & Folder Search** - From the **Backup Taken At** list, select the checkboxes next to the backup images that you want to hold.

You can also select all backup images that are displayed on a page, by selecting the check box in the column heading. The check box in the column heading is only for selecting all images on a single page. Move to the next pages to select images on subsequent pages.

For **Image Search** - Click the **Hold All** button to place all the images on hold.

The screenshot shows the Symantec NetBackup OpsCenter Analytics interface. The top navigation bar includes 'Home', 'Monitor', 'Manage', 'Reports', 'Search & Hold' (active), and 'Settings'. The 'Search & Hold' section has tabs for 'New', 'Saved', and 'Holds'. The 'Search Results' section displays a search for 'Backups_90_days' with filters for 'Backups Taken in: From :: May 22, 2013 To :: Aug 22, 2013'. Below the search results, there is a 'Summary for the search results for Backup Images' section. In this section, the 'Hold All' button (with a lock icon) is highlighted with a red box, and the 'Export' button (with a document icon) is also visible. Below the buttons is a table with the following data:

| Master Server ▲ | Client Count | Image Count | Disk Size | Tape Size |
|-----------------|--------------|-------------|-----------|-----------|
| rutu_build | 2 | 3 | 97.887 MB | - |

Total 1 Rows , 1 Page(s)

- 6 (Optional) You can click the **Export** button to generate a CSV file of the search results.
- 7 Provide the following information in the **Create Hold** dialog:
 - Provide a unique **Name** for the hold. For example, you can name the hold to correspond to an ongoing legal proceeding.
 - Optionally, provide a description of the hold in **Comments**. Comments can provide the reason for the hold for audit purposes.
To include this hold in a group of holds, enable **Add to a Hold group**, and then provide the following information:
 - To add this hold to a previously defined group of holds, select **Existing Groups** and then select the existing group from the drop-down list.
 - To add this hold to a new group of holds, select **New Group**, and then provide a unique name for the new group.

- Optionally, provide a description of the group in **Comments**.

Note: Hold groups are useful in cases where multiple holds are related to a single legal case.

- Optionally, select **Hold any copies that were not selected** to hold all copies of the selected backup images. If this option is not enabled, NetBackup Search holds only the primary copy of the selected backup images.
- For snapshot images, only the tar ball copies are placed on hold. See [“About snapshots and NetBackup Search”](#) on page 16.

Create Hold

WARNING

Placing a hold on backups may disrupt new backups from completing since storage may fill up due to these previous backups not being automatically expired

Only tar ball copies of the selected snapshot image(s) will be placed on hold.

Name : testhold11 *

Comments :

☐ **Add to a Hold group**

☒ Existing Select a hold group

Group

☐ New Group

Comments :

☒ Hold any copies that were not selected

OK Cancel

- 8 Click **OK** to complete creating the hold.

Note: When you retry a failed Hold creation, an empty hold is created if the backup images have expired between the initial hold and the retry.

To place a local hold on a backup image by using the command line interface

- 1 On a command prompt on the NetBackup master server, enter `nbholdutil -create` with appropriate options and elements. For example:

```
nbholdutil.exe -create -holdname legal_case1 -backupid
win81.sky.com_1307425938 -allcopy
```

This command creates a local hold called `legal_case1`. The backup image ID is `win81.sky.com_1307425938`. The option `-allcopy` indicates that the hold includes all copies of the selected backup image. If this option is not included, NetBackup Search holds only the primary copy of the selected backup image.

For more information about related command options, see [Table 5-1](#).

- 2 To display a list of holds, enter the `nbholdutil -list` command with appropriate options and elements. For example:

```
nbholdutil.exe -list
```

For more information about related command options, see [Table 5-1](#).

To display help information about the command and its options, enter

```
nbholdutil -help [-option]
```

The `nbholdutil -create` command lets you create a local hold for a backup image. The following table lists the options and descriptions of the `nbholdutil -create` base command:

Table 5-1 Options of `nbholdutil -create`

| Option | Description |
|---|--|
| <code>-holdname <hold name></code> | Enter a unique name for the hold. |
| <code>[-reason <reason>]</code> | Enter a description of the hold . The comment provides the reason for the hold for audit purposes. This option is optional. |
| <code>-filepath <filepath> -backupid <backup ID> -primarycopy -allcopy</code> | <p>Specify the file path or the backup ID to the backup image.</p> <p>Also, include one of the following copy methods:</p> <ul style="list-style-type: none"> ■ To include only the primary copy of the specified backup image, specify <code>-primarycopy</code> or <code>-p</code>. ■ To include all copies of the specified backup image, specify <code>-allcopy</code> or <code>-a</code>. |

The `nbholdutil.exe -list` command lists the holds that have been placed on backup images. The following table lists the options and descriptions of the `nbholdutil.exe -list base` command:

Table 5-2 Options of `nbholdutil.exe -list`

| Option | Description |
|---|---|
| <code>[-holdname <hold name>]</code> | Enter the name for the hold. This option is optional. |
| <code>[-backupid <backup ID>]</code> <code>-primarycopy -allcopy]</code> | Specify the backup ID for the backup image. Also, include one of the following copy methods: <ul style="list-style-type: none">■ To include only the primary copy of the specified backup image, specify <code>-primarycopy</code> or <code>-p</code>.■ To include all copies of the specified backup image, specify <code>-allcopy</code> or <code>-a</code>. This option is optional. |
| <code>[-U]</code> | Specify this option to display detailed output for all holds. This option is optional. |

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

Viewing holds details

- You can view the details of the images that are placed on hold. The Hold view displays the following buttons:
- **Release**
See [“Releasing a hold”](#) on page 87.
 - **Export**
Click to generate the Hold traceability report in a PDF. The PDF is downloadable and lists the following:
 - Hold Name
 - Hold Description
 - Search Details
 - Search Criteria

- Image List

The Image List section lists the following details:

- Image information
- Number of copies
- Media IDs
- Tape count
- Tape size
- Disk size
- Location type

- **Refresh**

Click to update the list of images that are placed on hold.

To view hold details

- 1 From the Symantec NetBackup OpsCenter interface, select **Search & Hold > Holds**.

The list displays two types of holds:

- **Local Holds** are created using the NetBackup command line interface (CLI).
- **Legal Holds** are created using Symantec NetBackup OpsCenter

Each hold type has its own icon.

- 2 In the **Name** column, find the hold or hold group for which you want to view details.

To display the members of a hold group, click the plus sign before the hold group name.

To view the stored comments about the hold or the hold group, click the plus sign after the hold name or the hold group name.

- 3 To view the **Hold Details** page, click the **Complete/Failed** link for a specific hold. This page displays a list of images that are a part of a hold. It also displays details of any errors that occurred when this hold was in progress.

When the Symantec NetBackup OpsCenter database is crashed and restored to a stage in the past when the hold was not created, the hold becomes **Orphan**. An Orphan hold is a Legal hold present on NetBackup but Symantec NetBackup OpsCenter fails to associate it with any searches. The state of an orphan hold cannot be changed.

If a hold creation or hold deletion fails, click **Retry** after you resolve any issue that caused the failure.

For a legal hold, click **View Associated Search Results** to view the Search Results from which this hold was created. Images that are a part of this hold are shown as pre-selected on this page. Any filters that were applied when the hold was placed appear on the left portion of the page. You can change these filters and view the resulting images. However you cannot save your changes to these filters. Original filters are retained to maintain traceability between the Search Results and the Hold.

Search & Hold > Holds view

This view is displayed when you select **Search & Hold > Holds**.

This view displays a summarized information about holds that have been placed on backed up images. You can view the following tabs:

- **Release**
Click to release hold placed on the selected image.
- **Export**
Click to generate the Hold traceability report in a PDF. The PDF is downloadable and lists the following:
 - Hold Name
 - Hold Description

- Search Details
- Search Criteria
- Image List
- **Refresh**
 - Click to update the list of images that are placed on hold.

Table 5-3 Search & Holds > Holds column headings

| Field | Description |
|-------------------|--|
| Name | Lists the names of the holds or hold groups. To display the members of a hold group, click the plus sign before the hold group name. To view the stored comments about the hold or the hold group, click the plus sign after the hold name or the hold group name. |
| Media | Lists the number of media types that are included with the hold. |
| Backups | Lists the number of backup images that are included with the hold. |
| Size | Lists the total size of the images that are included with the hold. |
| Files | Lists the number of files that are included with the hold. |
| Created by | Lists the user name that is responsible for creating the hold. |
| Placed on | Lists the date and time on which the hold was placed. |
| Status | Lists the current status of the hold. Click the status to view details about the hold. |

Search & Hold > Holds > Hold Details view

This view is displayed when you select the status link for a hold in the **Search & Hold > Holds** view.

This view displays detailed information about a hold that has been placed on backed up images.

When you click **View search results that produced this hold**, the **Search > Saved > Search Results** view is displayed. Use the browser's **Back** button to return to the hold details.

Table 5-4 Search & Hold > Holds > Hold Details column headings

| Field | Description |
|--------------------------------|--|
| Total backup images (n) | Displays the number of backup images that are included with this hold. |
| Backup Taken At | Displays each backup image that contains hits (or matches) to the saved search criteria. The backups images are referenced by the date and time of the backup's completion. The number in parentheses after the date and time indicates the number of search hits in the backup image. Click the plus sign to view details about the backup image. |

Note: The remainder of this table lists search-related fields. The search-related details about holds are available only for the legal holds that were placed using Symantec NetBackup OpsCenter. If the hold was placed by `nbholdutil` from a command line, it is not associated with a saved search. Therefore, search-related details do not exist for the hold.

| | |
|------------------------------|---|
| Total search hits (n) | Displays the number of hits (or matches) in the selected backup image to the search criteria. |
| File/Folder name | Lists the file names and the folder names within the selected backup image that matched the search criteria |
| Size | Displays the size of the file or folder. |
| User | Displays the user name that created or last modified the file or folder. |
| User group | Displays the user group to which the user is a member. If the user is not a member of a user group, None is displayed. |
| File Created | Displays the date and time on which the file was created. |
| File Modified | Displays the date and time on which the file was last modified. |

Releasing a hold

You can release local holds and legal holds by using Symantec NetBackup OpsCenter. However, you can release only local holds by using the command line interface of the master server.

Figure 5-1 Releasing a hold

Symantec OpsCenter Analytics Logged in as: [admin] About Logout

Home Monitor Manage Reports **Search & Hold** Settings

New Saved **Holds**

Summary

Hold 46
Hold Group 0

Release Export Refresh

| | Name | Media Backups | Size | Files | Created By | Placed On | Status |
|-------------------------------------|------|---------------|------|----------|------------|-----------|--------------------------------|
| Total 46 Rows , 4 Pages 1 | | | | | | | |
| <input checked="" type="checkbox"/> | 12 | 0 | 0 | 0 B | 0 | admin | Aug 17, 2012 10:55 AM Complete |
| <input type="checkbox"/> | 81 | 1 | 1 | 8.817 MB | 28 | admin | Aug 14, 2012 3:23 PM Complete |

Note: To remove a backup image, you must first release all the holds that include that backup image.

To release a hold by using Symantec NetBackup OpsCenter

- 1 From the Symantec NetBackup OpsCenter interface, select **Search & Hold > Holds**.
- 2 In the **Name** column, find the hold or the hold group that you want to release.
To display the members of a hold group, click the plus sign before the hold group name.
To view the details of the hold, click the plus sign after the hold name or the hold group name.
- 3 Select the holds or the hold groups that you want to release.

Note: A hold group must include at least one hold. When you release the last hold in a hold group, the hold group is also released and therefore no longer available for use.

4 Click **Release**.

The following message appears:

Releasing selected holds may delete *nn* backup images. If the original retention period has expired and there are no other holds on the backup images being released the backup images will be immediately deleted.

A backup image is expired only after the last hold on it is released and its expiration time has passed.

5 Click **OK** to proceed with the release. Click **Cancel** to keep the hold active.

To release a local hold by using the command line interface

- 1 From the command line interface of the NetBackup master server, enter `nbholdutil -delete` with appropriate options and elements. For example:

```
nbholdutil.exe -delete -holdname legal_case1 -force -reason
Legal_Case1 resolved
```

This command releases a local hold that is called `legal_case1`. The optional option `-force` instructs the command to bypass a prompt that asks you to confirm the release of the hold. If this option is not included, NetBackup Search prompts you to confirm the release of the hold. The optional option `-reason` provides a a brief description of the release of this hold. For example, for audit purposes:

For more information about related command options, see [Table 5-5](#).

Note: After the command completes successfully, the hold status is displayed as **CLI Modified**.

- 2 To display help information about the command and its options, enter `nbholdutil -help [-option]`

The command `nbholdutil -delete` lets you release a local hold. The following table lists the options and descriptions of the `nbholdutil -delete` base command:

Table 5-5 Options of `nbholdutil -delete`

| Option | Description |
|---|--|
| <code>-holdid <holdid> -holdname <hold name></code> | Provide either the hold ID or the name for the hold. |

Table 5-5 Options of `nbholdutil -delete` (*continued*)

| Option | Description |
|---------------------------------------|---|
| <code>[-force]</code> | Bypasses a prompt to confirm the release of the local hold. This option is useful in a script because it allows the release operations to continue without waiting for a response to the prompt. This option is optional. |
| <code>[-reason <reason>]</code> | Enter a description of the release of the hold. The comment provides the reason for the release of the hold for audit purposes. This option is optional. |

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

About Hold reports in Symantec NetBackup OpsCenter

This section describes Hold reports (optional for the NetBackup Search feature). NetBackup Search provides the ability to perform a legal search and hold data that is contained in NetBackup backup images.

Note: The Hold reports is visible if you have added a valid NetBackup Search license key in Symantec NetBackup OpsCenter and when you log on as a Security Administrator.

| | |
|-------------------------|---|
| Image Retention Summary | See “Hold Reports > Image Retention Summary” on page 91. |
| Top Holds by Size | See “Hold Reports > Top Holds by Size” on page 91. |
| Top Holds by Age | See “Hold Reports > Top Holds by Age” on page 91. |

Viewing hold reports

Note: Symantec NetBackup OpsCenter Help contains information and procedures for the reports that are generated from Symantec NetBackup OpsCenter. Click **Help** at the top left corner of the Symantec NetBackup OpsCenter browser to open Help, and then go to *Reporting in OpsCenter* for complete details about reporting options.

The Hold reports is visible if you have added a valid NetBackup Search license key in Symantec NetBackup OpsCenter and when you log on as a Security Administrator.

To view a hold report

- 1 From the Symantec NetBackup OpsCenter interface, select **Reports > Report Template**.
- 2 In the left pane, expand **Hold Reports**.
- 3 Select a hold report template:
 - Image Retention Summary
 - Top Holds by Size
 - Top Holds by Age

Hold Reports > Image Retention Summary

This report provides information about status of the images that are on hold. You can select the size unit (B, KB, MB, GB, or TB) to display.

Hold Reports > Top Holds by Size

This report shows holds that are ranked by the total size of their backup images. You can select the number of holds in the display, the size unit (B, KB, MB, GB, or TB), and whether the holds should display in ascending or descending order.

Hold Reports > Top Holds by Age

This report shows holds that are ranked by the age of their backup images. You can select the number of holds in the display, the time duration, and whether the holds should display in ascending or descending order.

How to find the status of backup images on hold

You can determine the status of images on hold by issuing commands and their options from a command line.

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

Use the `bpimage` command and its options to perform the required function on the images that are stored in a database. The following table lists the options and descriptions of the base command `bpimage`:

Table 5-6 Options of `bpimage`

| Option | Description |
|--|---|
| <code>bpimage -cleanup</code> | Removes the expired images from the database. |
| <code>bpimage -deletecopy #</code> | Removes the images that the copy number (#) and the <code>backup_id</code> specify. |
| <code>bpimage -backupid backup_id</code> | Lists the details of the backup image. |

Note: More information about the `bpimage` command is available:

See [“Finding the media information of backup images on hold”](#) on page 95.

Use the `bpimagelist` command to view the status report on NetBackup images or the removable media. The following table lists the options and descriptions of the base command `bpimagelist`:

Table 5-7 Options of `bpimagelist`

| Options | Description |
|------------------------------------|---|
| <code>bpimagelist -media -L</code> | Lists the media that is used in the present day to take backup. |
| <code>bpimagelist -L</code> | Lists all the images that are written in the present day. |

Use the `bpimmedia` command to view the information about NetBackup images on media. The following table lists the options and descriptions of the base command `bpimmedia`:

Table 5-8 Options of `bpimmedia`

| Option | Description |
|--|--|
| <code>bpimmedia -disk_stu <stu label></code> | Lists all the images that are specified on the NetBackup storage unit. |
| <code>bpimmedia -disk</code> | Lists all the images from the disk. |
| <code>bpimmedia -tape</code> | Lists all the images from the tape. |

Use the `nbemmcmd` command to update and view information in the EMM database. The following table lists the options and descriptions of the base command `nbemmcmd`:

Table 5-9 Options of `nbemmcmd`

| Option | Description |
|--|---|
| <code>nbemmcmd.exe-listmedia-allrecords</code> | Lists the details of all available media. |
| | |

Use the `bpexpdate` command to change the expiration date of backups in image catalog, and media in media catalog. The following table lists the options and descriptions of the base command `bpexpdate`:

Table 5-10 Options of `bpexpdate`

| Option | Description |
|---|-------------------------------------|
| <code>bpexpdate-backupid <backupid> -d 0</code> | Expires the specified backup image. |
| <code>bpexpdate -m <media id> -d 0</code> | Expires the specified media. |

Use the `bpmedialist` command to view the status of NetBackup tape media. On the output window, you have to select the Image on Hold, and Media on Hold options. The following table lists the options and descriptions of the base command `bpmedialist`:

Table 5-11 Options of `bpmedialist`

| Option | Description |
|---|--|
| <code>bpmedialist -mcontents -m <mediaid> -l (-L, U, -o)</code> | Displays the details of all backups that are taken on the specified media. |
| <code>bpmedialist -m <mediaid> -L (-l, U, -o)</code> | Displays the detail of the specified media. |

Use the `nbauditreport` command to create and view a NetBackup audit report. You can use the command `./nbauditreport -help` with the options of `nbauditreport` to view the help of that command. For example: enter the command `./nbauditreport -help [-sdate <"MM/DD/YY [HH:[MM[:SS]]]">]` to view the help for the start date or time of the audit report. The following table lists the options and descriptions of the base command `nbauditreport`:

Table 5-12 Options of `nbauditreport`

| Option | Description |
|--|---|
| <code>[-sdate <"MM/DD/YY [HH:[MM[:SS]]]">]</code> | Displays the start date or time of the audit report. |
| <code>[-edate <"MM/DD/YY [HH:[MM[:SS]]]">]</code> | Displays the end date or time of the audit report. |
| <code>[-ctgy <POLICY JOB STU STORAGE_SRV POOL AUDITCFG AUDITSVC BPCONF HOLD>]</code> | Specifies the categories to be displayed in the audit report: POLICY, JOB, STU, STORAGE_SRV, POOL, AUDITCFG, AUDITSVC, BPCONF, and HOLD. You can view the audit messages for the hold operations: CREATE, MODIFY, and DELETE |
| <code>[-user <username[:domainname]>]</code> | Specifies the name of the user for whom you want to display the audit information |
| <code>[-fmt <SUMMARY DETAIL PARSABLE>]</code> | Specifies the out put format for the audit report in the form of Summary, Details, and Parsable. |
| <code>[-notruncate] [-pagewidth <NNN>]</code> | Displays the old and new values of a changed attribute on separate lines, and the page width for the details section of the audit report. This option is used with the DETAIL option. |
| <code>[-order <DTU DUT TDU TUD UDT UTD>]</code> | Specifies the order in which the information is to be displayed in the parsable format of the audit report. This option is used with the PARSABLE option. D, T, and U represent the following: <ul style="list-style-type: none"> ■ D - Description ■ T - Timestamp ■ U - User |

Finding the media information of backup images on hold

To find the media information of backup images that are on hold, you can issue the `bpimage` command from a command prompt on the master server. For example,

```
bpimage -backupid <image_id>
```

The variable `<image_id>` refers to the **Image ID** value for the backup image.

To determine the **Image ID**, select **Search & Hold > Saved** in the Symantec NetBackup OpsCenter UI, then select the status link for a saved search. The resulting view displays detailed information about a hold that has been placed on backed up images. Find the backup image you want in the **Backup Taken At** column, and click the plus sign on the right to view details about the backup. **Image ID** is one of the details displayed.

For example, if the **Image ID** for the backup image is `client1_1319540407`, run the following command to view detailed image information including media information:

```
bpimage -backupid client1_1319540407
```

The output of this command includes information similar to the following display:

```
...
Media Type:      Disk (0)
Density:         qscsi (0)
File Num:        0
ID:              /diskstul/clinet1_1319540407_C1_F1
Host:            reabl2.min.veritas.com
Block Size:      262144
...
```

Note: You must scroll down through the display to find these fields.

Refer to the [Symantec NetBackup Commands Reference Guide](#) for more information about the `bpimage` command.

Mass Restore

This chapter includes the following topics:

- [About mass restore](#)
- [Preparing for mass restore](#)
- [Submitting mass restore requests](#)
- [About restoring the data on hold and ingesting it into Enterprise Vault](#)
- [Mass restore error messages](#)

About mass restore

NetBackup Search helps you to restore the backup images that are placed on hold to a required location.

The restore operation supports individual holds only. It is not supported for the hold groups. You can initiate a mass restore on a hold that is in **Complete** or **Partial** state. However, the restore operation is restricted for the holds which are in **Orphan** or **Failed** state.

NetBackup Search helps you to restore data across different platforms. You can specify the restore host or restore location on a per policy type basis. If you back up the data using standard policy, the data is restored to a UNIX or a Linux host. Whereas, if you back up the data using MS-Windows policy, the data is restored to a windows host

Preparing for mass restore

You must initiate a separate mass restore operation for each master server that is a part of the hold. Before you perform a mass restore, you complete the following tasks:

| Task | Reference |
|--|---|
| On every indexing server, share the configured staging folder. | See “ Sharing the staging directory ” on page 97. |
| Create the <code>RestoreConfig.ini</code> file | See template available at http://www.symantec.com/docs/DOC5787 |
| Update the <code>RestoreConfig.ini</code> file | See “ Updating the RestoreConfig.ini file ” on page 98. |
| Provide server privileges to the processing host | See Symantec NetBackup Administrator's Guide - Volume 1 |

Note: Update the configuration when an indexing server is added or removed, or when you want to update the alternate restore clients or locations.

Providing server privileges to the processing host

To provide server privileges to the processing host (server), you must add the processing host to the servers list in NetBackup. For more information about adding servers to the server list, see [Symantec NetBackup Administrator's Guide - Volume 1](#).

Sharing the staging directory

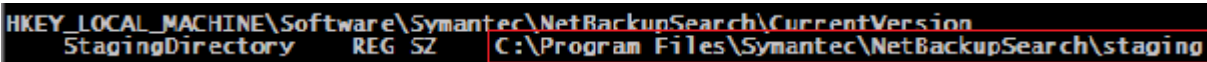
Before you perform a mass restore you must share the staging directory.

Note: A read-only permission is sufficient.

To share the staging directory

- 1 On the individual indexing server, run the following command to identify the location of the staging directory:

```
reg query HKLM\Software\Symantec\NetBackupSearch\CurrentVersion  
/v StagingDirectory
```



- 2 Right-click the directory and select **Properties**.
- 3 On the **Properties** dialog box, select the **Sharing** tab.

- 4 Share the directory and assign permissions.
- 5 Click **OK**, and then click **Close** to close the **Properties** dialog box.

Updating the RestoreConfig.ini file

After you create a RestoreConfig.ini file, update the following values:

- **General\ProcessingDir**: Specify the directory to store the processed data.
- **IndexServers\Server**: Create one entry for each indexing server in the NetBackup domain pointing to the shared staging folder location.
- **Policy_*\RestoreLocation**: On a per policy-type basis, specify the alternate restore client and location where data needs to be restored.
- **EVIngest\EVIngestDataLocation**: When you want to ingest data into Enterprise Vault, provide the location on the Enterprise Vault client where the restored data from various alternate restore clients is consolidated

Submitting mass restore requests

You can submit a mass restore request by using the `nbholdrestorehelper` command on the master server command prompt. The `nbholdrestorehelper` command processes the search results from NetBackup Search.

Note: Mass restore is supported only for **Files & Folder Searches**. It is not supported for **Image Search**.

To perform mass restore from the command line

- 1 Create the Backup ID (BID) file and enter the following command on the master server:

```
nbholdutil.exe -list -holdname <holdname> -U
-include_extended_info > bid.txt
```

Note: If a BID file already exists, it is overwritten by the newly created file.

- 2 Enter the following command on the indexing server to process the results:

```
nbholdrestorehelper process_results <-s search_id> <-b bid_file>
[-f conf_file] [-e] [-v]
```

Note: More information is available about how to find the search ID. See [“Finding the search ID”](#) on page 77.

The attribute `[-f conf_file]` is optional if the `RestoreConfig.ini` file is already present in its default location: `<NBU_Install_Path>\bin\goodies\.`

The following is a sample of the summary of the process:

| summary for process result | |
|----------------------------|-----------------------|
| Storage requirements: | |
| ----- | |
| Client Name | Storage required (MB) |
| ----- | |
| XYZ123 | 1001.543 |
| ----- | |

- 3 To start the restore of the processed results, enter the following command on the master server command prompt:

```
nbholdrestorehelper begin_restore <-s search_id> [-f conf_file]
[-v]
```

During the restore process, if you want to cancel the operation at any stage, press **Ctrl + C**.

The status of the restore is displayed after the restore is complete. For example:

| Restore Summary: | |
|------------------|-------------|
| Exit status | No. of Jobs |
| Success | 2 |

At the end of the restore operation, the `nbholdrestorehelper` utilities print a job summary that shows the number of pass or fail jobs. Additionally, a `Restore_Job_Status.csv` file containing detailed status on a per-job ID basis is also created.

The total number of restore jobs that are initiated depends on the number of backup images being restored and the value of `General\RestoreBatchSize` that you specify in the `RestoreConfig.ini` file. The value of `General\MaxConcurrentRestoreJobs` that you specify in the `RestoreConfig.ini` file governs the total number of concurrent active restore jobs.

For data traceability, the data is restored with the following folder structure:

```
<RestoreLocation>
    |__<SearchID>
        |__<MasterServer>
            |__<ClientName>
                |__<BackupID>
                    |__<Original backup location>
```

Note: For restore jobs, same troubleshooting steps apply for `bprestore` and `nbholdrestorehelper`.

About restoring the data on hold and ingesting it into Enterprise Vault

A natural progression of placing holds on backup images is the ability to ingest that data into an eDiscovery product. This ability allows data on hold to be processed further through the eDiscovery workflow and eventually presented in the context of a legal case. For NetBackup, the obvious eDiscovery product choice is Symantec's market-leading products Enterprise Vault/Discovery Accelerator.

To provide a seamless transition of data between the backup world and the eDiscovery domain, NetBackup 7.6 provides a command for ingesting the relevant data into Enterprise Vault.

The `nbholdrestorehelper` utility generates some additional metadata files that are required for the next step of ingesting the restored data into Enterprise Vault. Using the metadata and the restored data as inputs, the `nbeingest` utility ingests the files one-by-one into the Vault Store of the designated Enterprise Vault server. One important value addition this command makes is that it adds original metadata attributes to the files being ingested. This metadata makes these files searchable based on original attributes, such as NetBackup Client name, original timestamps, and so on in Enterprise Vault.

Prerequisites for ingesting the restored data into Enterprise Vault

You must have a good understanding of the NetBackup tasks and the concepts of Enterprise Vault. The following are the prerequisites for ingesting the restored data into Enterprise Vault:

- **NetBackup**

You should deploy the NetBackup Search solution and be aware of the deployed indexing servers.

The scope of the restore operation is limited to one NetBackup domain. If a specific Legal Hold spans across more than one master server, the restore and ingest procedures should be performed separately for each NetBackup domain. Sometimes the backup data may be from Windows, Linux, or UNIX or NDMP clients. Therefore, a separate host of each type must be specified as a destination client during a restore.

- **Enterprise Vault**

After you restore the data, you must consolidate it to a single windows host that acts as a client for Enterprise Vault. The host should have Enterprise Vault Content Management (ECM) SDK v9.0 or a higher version installed. Also, the host should have write permissions on shared archives into which the data is

ingested. The ECM SDK is an independent component that is shipped with Enterprise Vault.

Ingesting the restored data into Enterprise Vault

This section discusses the optional step of ingesting the restored files into Enterprise Vault by using the `nbevingest` command. The configuration parameter in `RestoreConfig.ini` governs the generation of Enterprise Vault ingest specific files. You can override it on run-time by passing the `-e` parameter during the `process_results` operation. During the processing phase, the required input xml files for the `nbevingest` command are generated.

Additionally, an `EVingest.bat` file is created to help in the ingestion process. When ingesting the files into the Archive, the `EVingest.bat/nbevingest` command sets the file's original metadata (original NetBackup client name from where it was backed up, Master server name, policy type) and related information as the custom attributes of the ingested file. By using the Discovery Accelerator product; the custom attributes are searchable from the Enterprise Vault console.

EV ingest workflow:

- 1 **Consolidate restored data** - The restored data can be present across multiple hosts or restore locations based on the inputs that are provided in the `RestoreConfig.ini` file. Once the restore is complete, the data from the alternate restore clients must be consolidated on the host that might act as the EV client. The search ID forms the basis of the copy operation. You have to consolidate the data at the folder location specified by the `EVIngestDataLocation` parameter in the `RestoreConfig.ini` file.
- 2 **Create required vault store retention policy on Enterprise Vault server** - When ingesting data into EV, you must provide the vault store information on the EV server where the relevant archives are created during the ingestion process. Additionally, a retention policy is required.
- 3 **Run `EVingest.bat` from `<Processing_Dir>/<SearchID>/EVingest.bat` to ingest data into EV with the following parameters:**

```
-V EV_vault_store
-hold custom_identifier_for_ingest_operation
-retentionpolicy an_existing_EV_retention_category
-report file_for_detailed_ingestion_report
-directoryserver hostname_of_ev_server
```

After the data is ingested into Enterprise Vault, you can use the Discovery Accelerator product to:

- Search for ingested files based on their content (items that are ingested into Enterprise Vault are content-indexed).
- Refine the searches based on the files' original metadata attributes (set as custom attributes in Enterprise Vault). For more information about the NetBackup attributes that are searchable and retrievable from data ingested into Enterprise Vault, see [Table 6-1](#).
- Put file-level legal hold from Discovery Accelerator on the final search results.

Table 6-1 Searchable and retrievable NetBackup attributes from data ingested into Enterprise Vault

| Parameter | Searchable | Retrievable |
|-------------------|------------|-------------|
| NetBackup Master | Yes | Yes |
| Backup client | Yes | Yes |
| Policy type | Yes | Yes |
| Group name | Yes | Yes |
| Hold name | Yes | Yes |
| Original location | No | Yes |
| Backup Id | No | Yes |

***Searchable** - Items that can be searched based on this attribute. If the attribute is searchable, you can query items with a specific value for this attribute.

***Retrievable** - This attribute is returned with the items that were returned in response to a search. If the attribute is retrievable, it is a part of the result set and it can be displayed in the UI that shows the search results.

Mass restore error messages

During a mass restore, sometimes you may receive an error message. The error messages and the recovery actions that you need to perform to resume the restore process are as follows:

Error message

Could not find precheck_info.txt to process.

Recovery action

Ensure that the process_results operation during the mass restore activity is performed successfully.

| Error message | Recovery action |
|--|---|
| Could not find restore_info.txt to process. | Ensure that the process_results operation during the mass restore activity is performed successfully. |
| Unable to create <file> | Ensure that sufficient disk space is available and write permissions are provided at the location. |
| Could not delete <processing_directory>\<search_id> directory | Ensure that no file is opened from <processing_directory>\<search_id > directory |
| Could not find <processing_directory>\<search_id> directory | Ensure that the process_results operation during the mass restore activity is performed successfully. |
| Unable to find <searchstates_folder> folder for <indexing_server>. | Ensure that the specified search ID and the staging path are correct. |
| Unable to find <searchresults_folder> folder for <indexing_server>. | Ensure that the specified search ID and the staging path are correct. |
| Failed to read from <searchstates_folder> folder. | Ensure that the search and the hold operations have completed successfully. |
| Backup ID list file <backup_id_list_file> does not exist. | Ensure that nbholdutil has completed successfully and that the output file contains backup IDs. |
| Backup ID file <backup_id_list_file> is either empty or incorrectly formatted. | Ensure that nbholdutil has completed successfully and that the output file contains backup IDs. |
| Specified search ID <search_id> does not have data for clients specified in <backup_id_list_file>. | This error may occur if the specified hold name does not relate to the specified search ID. Ensure that correct hold name is specified for correct search ID. |
| Warning: Could not find search results for all input BID's. | Ensure that all the indexing servers are specified in the RestoreConfig.ini file. |
| Invalid BID input file. | Ensure that the specified backup ID file exists at the specified location. |
| Unsupported policy type <policy_type> found | Ensure that the RestoreConfig.ini file contains only supported policy types. |

| Error message | Recovery action |
|--|--|
| No alternate restore client specified for NDMP host <i><client_name></i> . | Ensure that an alternate client is specified for NDMP host client in the <code>RestoreConfig.ini</code> file. |
| No alternate restore client specified for policy type <i><policy_type></i> . | Ensure that an alternate client is specified for the specified <i><policy_type></i> in the <code>RestoreConfig.ini</code> file. |
| No value specified for ProcessingDir | Ensure that appropriate value is specified for ProcessingDir in the <code>RestoreConfig.ini</code> . |
| Invalid location specified for ProcessingDir | Ensure that appropriate value is specified for ProcessingDir in the <code>RestoreConfig.ini</code> . |
| Invalid value for RestoreBatchSize | Ensure that a valid numeric value is specified for batch size in the <code>RestoreConfig.ini</code> file. |
| No value specified for EVIngestDataLocation | Ensure that an appropriate value is specified for EVIngestDataLocation in the <code>RestoreConfig.ini</code> file. |
| No index servers specified | Ensure that appropriate values are specified for indexing servers field in the <code>RestoreConfig.ini</code> file. |
| Empty server entry found | Ensure that appropriate values are specified for indexing servers field in the <code>RestoreConfig.ini</code> file. |
| Could not read <i><searchstates_folder></i> | Ensure that an appropriate value is specified for the staging path in the <code>RestoreConfig.ini</code> file. |
| Index servers from more than one index servers provided | This error can occur if invalid indexing servers are provided. Ensure that appropriate values are specified for the indexing servers field in the <code>RestoreConfig.ini</code> file. To verify the exact list of indexing servers, run <code>nbindexutil -listindexservers</code> command on the master server command prompt. |

| Error message | Recovery action |
|---|---|
| None of the specified index servers contain data corresponding to search_id | This error can occur in a situation where search results are deleted and you perform a restore or when you provide a wrong staging path. Ensure that correct staging path is provided and that the search results are present on the staging path during a restore. |
| Incomplete RestoreLocation found for policy type <policy_type> | Ensure that an appropriate value is specified for RestoreLocation in the <i>RestoreConfig.ini</i> file. |

Troubleshooting

This chapter includes the following topics:

- [About NetBackup Search status codes and log files](#)
- [Enabling debug logging for NetBackup Search functions by using the Setup Debug Logging Wizard](#)
- [Unable to save the search criteria](#)
- [Resolving excessive log generation and memory usage](#)
- [Resolving conflicting failed and indexed log entries for the same backup image](#)
- [Resolving indexing job errors while sending data to the master server](#)
- [Re-initiating indexing jobs that have failed](#)
- [Fixing indexing jobs that fail with error code 5027 after an upgrade](#)
- [Fixing indexing jobs that fail with status code 25 \(cannot connect on socket\)](#)
- [Fixing indexing jobs that fail with status code 50 \(client process aborted\) when NBAC is enabled](#)
- [Recovering from disk-full situations](#)
- [Recovering from disk-error situations](#)
- [Resolving begin_restore operation failures](#)
- [Resolving nbholdrestorehelper operation failures](#)
- [About Java and MFC UI differences](#)
- [About obsolete search criteria and results for Files & Folder searches](#)
- [Fixing collection-service issues](#)

About NetBackup Search status codes and log files

For information about status codes, see the [Symantec NetBackup Status Codes Reference Guide](#).

You may need to refer to log files to resolve issues that occur. The following tables provide the locations of the log files that are associated with NetBackup Search.

Table 7-1 Indexing Logs

| Log Folder | Resides on | UL Product ID | Originator ID |
|--|-------------------------|---------------|---------------|
| Use Case: Indexing server configuration | | | |
| <i>install_path</i> \NetBackup\logs\nbim | NetBackup master server | 51216 | 371 |
| <i>install_path</i> \NetBackup\logs\bpdbm | NetBackup master server | N/A | N/A |
| <i>install_path</i> \NetBackup\logs\nbsl | NetBackup master server | 51216 | 132 |
| <i>install_path</i> \NetBackup\logs\wingui | NetBackup master server | 51216 | 263 |
| <i>install_path</i> \NetBackup\logs\user_ops\nbjlogs | NetBackup master server | N/A | N/A |
| Use Case: Backup policy configuration | | | |
| <i>install_path</i> \NetBackup\logs\bpdbm | NetBackup master server | N/A | N/A |
| <i>install_path</i> \NetBackup\logs\wingui | NetBackup master server | 51216 | 263 |
| <i>install_path</i> \NetBackup\logs\user_ops\nbjlogs | NetBackup master server | N/A | N/A |
| Use Case: Indexing jobs | | | |
| <i>install_path</i> \NetBackup\logs\nbim | NetBackup master server | 51216 | 371, 373 |
| <i>install_path</i> \NetBackup\logs\nbjm | NetBackup master server | 51216 | 117 |
| <i>install_path</i> \NetBackup\logs\nbpem | NetBackup master server | 51216 | 116 |

Table 7-1 Indexing Logs (*continued*)

| Log Folder | Resides on | UL Product ID | Originator ID |
|---|---------------------------|---------------|---------------|
| <i>install_path</i> \NetBackup\logs\bpjobd | NetBackup master server | N/A | N/A |
| <i>install_path</i> \NetBackup\logs\bpdbm | NetBackup master server | N/A | N/A |
| <i>install_path</i> \NetBackup\logs\ncfnbci | NetBackup indexing server | 51216 | 385 |
| <i>install_path</i> \NetBackup\logs\nbci | NetBackup indexing server | 60385 | 405 |

Table 7-2 Search operations logs

| Log Folder | Resides on | UL Product ID | Originator ID |
|--|-------------------------------------|---------------|---------------|
| Use Case: Search operations (execute, stop, delete -search) | | | |
| Windows: <i>install_path</i> \OpsCenter\gui\logs UNIX: <i>install_path</i> /SYMCOpsCenterGUI/logs | Symantec NetBackup OpsCenter server | 58330 | 147 |
| Windows: <i>install_path</i> \OpsCenter\server\logs UNIX: <i>install_path</i> /SYMCOpsCenterServer/logs | Symantec NetBackup OpsCenter server | 58330 | 148, 149 |
| <i>install_path</i> \Searchbroker\logs | Symantec NetBackup OpsCenter server | 60325 | 404, 137 |
| <i>install_path</i> \NetBackup\logs\nbsl | NetBackup master server | 51216 | 132, 137 |
| <i>install_path</i> \NetBackup\logs\nbim | NetBackup master server | 51216 | 371 |
| <i>install_path</i> \NetBackupSearch\logs\nbsearch | NetBackup indexing server | 60385 | 405 |
| Use Case: Search operations (save -search) | | | |
| Windows: <i>install_path</i> \OpsCenter\gui\logs UNIX: <i>install_path</i> /SYMCOpsCenterGUI/logs | Symantec NetBackup OpsCenter server | 58330 | 147 |
| Windows: <i>install_path</i> \OpsCenter\server\logs UNIX: <i>install_path</i> /SYMCOpsCenterServer/logs | Symantec NetBackup OpsCenter server | 58330 | 148, 149 |

Table 7-3 Hold operations logs

| Log Folder | Resides on | UL Product ID | Originator ID |
|--|--|---------------|---------------|
| Use Case: Legal Hold operations (add hold, release hold) | | | |
| Windows: <i>install_path\OpsCenter\gui\logs</i> UNIX: <i>install_path/SYMCOpsCenterGUI/logs</i> | Symantec NetBackup OpsCenter server | 58330 | 147 |
| Windows: <i>install_path\OpsCenter\server\logs</i> UNIX: <i>install_path/SYMCOpsCenterServer/logs</i> | Symantec NetBackup OpsCenter server | 58330 | 148, 149 |
| <i>install_path\NetBackup\logs\admin</i> | NetBackup master server | N/A | N/A |
| <i>install_path\NetBackup\logs\nbsl</i> | NetBackup master server | 51216 | 132 |
| <i>install_path\NetBackup\logs\nbim</i> | NetBackup master server | 51216 | 371, 372 |
| <i>install_path\NetBackup\logs\bpdbm</i> | NetBackup master server | N/A | N/A |
| <i>install_path\NetBackup\logs\nbemmm</i> | NetBackup master server | 51216 | 111 |
| <i>install_path\NetBackup\logs\nbemmm</i> | NetBackup master server | N/A | N/A |
| Use Case: Local Hold operations (add hold, release hold) | | | |
| <i>install_path\NetBackup\logs\admin</i> | NetBackup master server | N/A | N/A |
| <i>install_path\NetBackup\logs\nbsl</i> | NetBackup master server | 51216 | 132 |
| <i>install_path\NetBackup\logs\nbim</i> | NetBackup master server | 51216 | 371, 372 |
| <i>install_path\NetBackup\logs\bpdbm</i> | NetBackup master server | N/A | N/A |
| <i>install_path\NetBackup\logs\nbemmm</i> | NetBackup master server | 51216 | 111 |
| <i>install_path\NetBackup\logs\nbemmm</i> | NetBackup master server | N/A | N/A |

Table 7-4 Enterprise Vault ingest logs

| Log Folder | Resides on | UL Product ID | Originator ID |
|---|-------------------------|---------------|---------------|
| Use Case: Ingest restored data into Enterprise Vault with <code>nbevingest.exe</code> | | | |
| <code>install_path\NetBackup\logs\nbevingest</code> | NetBackup client | 51216 | 398 |
| Use Case: Restore data searched using NetBackup Search <code>nbrestorehelper.exe</code> | | | |
| Windows temp directory [%TMP%] | NetBackup client | N/A | N/A |
| <code>install_path\NetBackup\logs\nbholdrestorehelper</code> | NetBackup master server | N/A | N/A |

Table 7-5 Logs for other NetBackup Search operations

| Log Folder | Resides on | UL Product ID | Originator ID |
|--|---|---------------|---------------|
| Use Case: Search Executor service-related operations | | | |
| <code>install_path\NetBackupSearch\logs</code> | NetBackup indexing server | N/A | N/A |
| Use Case: PBX operations | | | |
| Program Files\VERITAS\VxPBX\logs | Symantec NetBackup OpsCenter server NetBackup master server NetBackup indexing server | N/A | N/A |
| Use Case: Search progress (.cvs file) | | | |
| <code>install_path\SearchBroker\var\progress</code> | Symantec NetBackup OpsCenter server | N/A | N/A |
| Use Case: Search error details (.error file) | | | |
| <code>install_path\SearchBroker\var\progress</code> | Symantec NetBackup OpsCenter server | N/A | N/A |

Enabling debug logging for NetBackup Search functions by using the Setup Debug Logging Wizard

NetBackup 7.6 provides a new Logging Assistant feature. Logging Assistant is a helpful tool that can speed up the time required to gather and upload debug logs and other information to Symantec Technical Support. Because Logging Assistant automatically performs a number of functions, you can avoid the problems associated with manually logging into NetBackup hosts, creating log directories, changing logging levels, and restarting services.

Part of Logging Assistant is the **Setup Debug Logging** wizard. This wizard lets you select NetBackup Search indexing job-related debug logging from a list of problem categories. Additionally, you may want to set up debug logging for the Search, Hold, Restore, and EVIngest functions of NetBackup Search. To enable debug logging for these functions, you must follow the steps in this procedure.

More detailed information about the Logging Assistant and setting up debug logging is available in the [Symantec NetBackup Administrator's Guide, Volume I](#) and in the **Help** for **NetBackup Administration Console**.

Click **Help** on any of the **Setup Debug Logging** wizard pages for general information about using the wizard. The following procedure explains how to use the wizard specifically for NetBackup Search functions.

To enable debug logging for NetBackup Search functions using the Setup Debug Logging Wizard

- 1 Launch the **Setup Debug Logging** wizard.
 - Select the **Logging Assistant** node on the left pane of the **NetBackup Administration Console**.
 - Next, select one of the Logging Assistant records in the right pane or create a new record if none exists.
 - Then select **Setup Debug Logging** from the right-click menu.

Provide the required information as you advance through the wizard. For the NetBackup Search functions, provide the additional information as described in the following steps.

- 2 On the **Host Selection** page, select the options that are appropriate to your environment:
 - Select **Setup debug logging on Master Server** if you want to enable logging for Search or Hold functions.
 - If the indexing server is installed on either a master server or a media server, select **Setup debug logging on Media Server**. Next, select the host name

from **Available Media Servers**. Then click **Add>** to move the host name to **Selected Media Servers**.

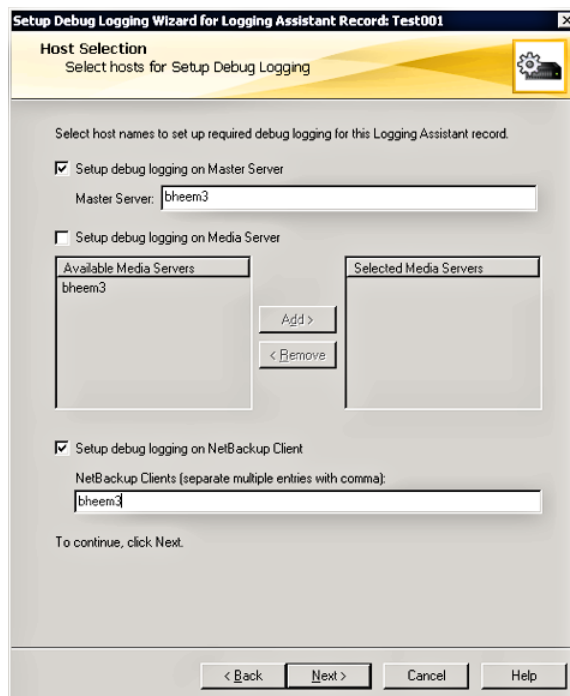
- If the indexing server is installed as a standalone server, select **Setup debug logging on NetBackup Client**. Next, enter the host name in **NetBackup Clients**.

If you also want to enable logging for Restore functions, you must select **Setup debug logging on NetBackup Client**. Then add the name of the client where data on hold will be restored.

If you also want to enable logging for EVIngest functions, you must select **Setup debug logging on NetBackup Client**. Then add the name of the client where you will run `nbevingest`.

Separate multiple client names with commas.

In the following figure, debug logging is set up for a standalone indexing server.



3 On the **Master Server Debug Logging Selection** page:

- Ensure that **Search - Index** is selected under **Problem Category**. This selection enables logging for Indexing functions. It is selected by default.

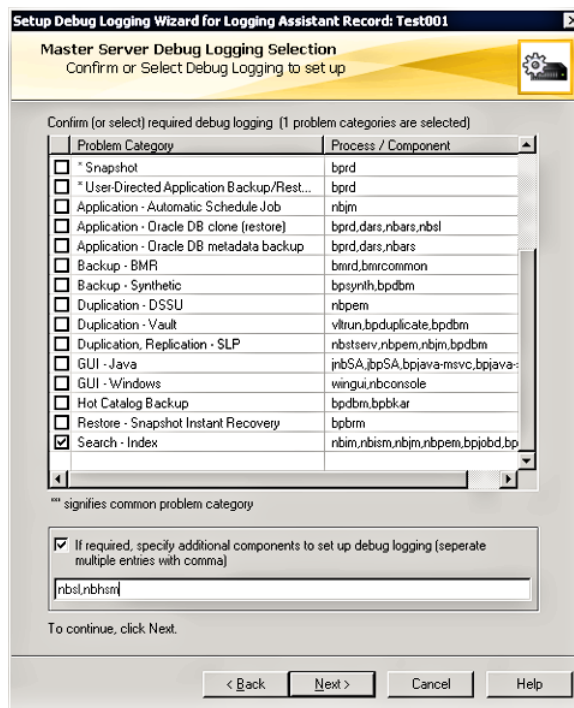
Enabling debug logging for NetBackup Search functions by using the Setup Debug Logging Wizard

- If you also want to enable logging for Search functions, you must select **If required, specify additional components to set up debug logging**. Then add `nbsl` to the text box.

If you also want to enable logging for Hold functions, you must select **If required, specify additional components to set up debug logging**. Then add `nbsl, nbhsm` to the text box.

Separate multiple component names with commas.

In the following figure, debug logging is set up for Indexing, Search, and Hold functions on the selected master server.



- 4 If your indexing server is installed on a NetBackup media server, ensure that **Search - Index** is selected under **Problem Category** on the **Media Server Debug Logging Selection** page.

Note: The wizard displays the **Media Server Debug Logging Selection** page only if you selected **Setup debug logging on Media Server** on the **Host Selection** page.

| Problem Category | Process / Component |
|---|-----------------------|
| <input type="checkbox"/> * Backup | bpbrm, bptm |
| <input type="checkbox"/> * Duplication | bptm, bpd, bpbrm |
| <input type="checkbox"/> * Network Communication | bpcd, vnetd |
| <input type="checkbox"/> * Restore | bpbrm, bptm |
| <input type="checkbox"/> * Scheduled Application Backup/Restore | bpbrm, bptm |
| <input type="checkbox"/> * Snapshot | bpbrm |
| <input type="checkbox"/> Application - MS Exchange | nbfsd |
| <input type="checkbox"/> Backup - Accelerator | nbostpy |
| <input type="checkbox"/> Backup - Synthetic | bpd, bptm, bpcd |
| <input type="checkbox"/> Duplication - DSSU | bpbrm |
| <input type="checkbox"/> Duplication - MSDP | spad, spool, pdplugin |
| <input type="checkbox"/> Duplication - Vault | bptm, bpbrm |
| <input type="checkbox"/> Hot Catalog Backup | bpbrm, bptm |
| <input checked="" type="checkbox"/> Search - Index | ncfnci, nbcij |

*** signifies common problem category

☐ If required, specify additional components to set up debug logging (separate multiple entries with comma)

To continue, click Next.

< Back Next > Cancel Help

- 5 On the **NetBackup Client Debug Logging Selection** page, provide the appropriate component names for the functions that run on the client:
 - If you also want to enable logging for Restore functions, you must select **If required, specify additional components to set up debug logging**. Then add `bprestore` to the text box.
 - If you also want to enable logging for EVIngest functions, you must select **If required, specify additional components to set up debug logging**. Then add `nbevingest` to the text box.

Separate multiple component names with commas.

Note: In your environment, you may run Restore on a different client than EVIngest. You must indicate each of these clients on the **Host Selection** page as described in step 2. Then, the wizard displays separate **NetBackup Client Debug Logging Selection** pages for each client.

In the following figure, debug logging is set up for Restore and EVIngest functions on a single NetBackup client.

Enabling debug logging for NetBackup Search functions by using the Setup Debug Logging Wizard

Setup Debug Logging Wizard for Logging Assistant Record: Test001

NetBackup Client Debug Logging Selection
Confirm or Select Debug Logging to set up

Confirm (or select) required debug logging (0 problem categories are selected)

| Problem Category | Process / Component |
|---|----------------------------------|
| <input type="checkbox"/> Application - Oracle DB, template based | bpdbsora,bpubsora,user_ops |
| <input type="checkbox"/> Application - SAP DB | backint,user_ops |
| <input type="checkbox"/> Application - Sybase DB | sybackup,bpcd,vnetd,user_ops |
| <input type="checkbox"/> Application - VMware | bpfis,bpVMutil |
| <input type="checkbox"/> Application - XBSA-Datastore | exten_client,bpcd,vnetd,user_ops |
| <input type="checkbox"/> Backup - Accelerator | bpcd,nbostpxy,acclmetadata |
| <input type="checkbox"/> Backup - BMR | bmrsavecfg,bmrcommon |
| <input type="checkbox"/> Backup - Client Encryption | bpfilter |
| <input type="checkbox"/> Backup - VMware Accelerator | bpcd,bpfis,acclmetadata |
| <input type="checkbox"/> Backup - VxMS | vms |
| <input type="checkbox"/> Backup - Windows Accelerator | bpinstd |
| <input type="checkbox"/> GUI - Java | jnbSA,jbpSA,user_ops |
| <input type="checkbox"/> GUI - Windows | wingui,nbwin |
| <input type="checkbox"/> Restore - Snapshot Instant Recovery | bpffis,bpfis,bpbkar,tar |
| <input type="checkbox"/> Snapshot - Alternate Client or Third Party ... | bpbkar,pbx |

*** signifies common problem category

☒ If required, specify additional components to set up debug logging (separate multiple entries with comma)

bprestore,nbevingest

To continue, click Next.

< Back

Next >

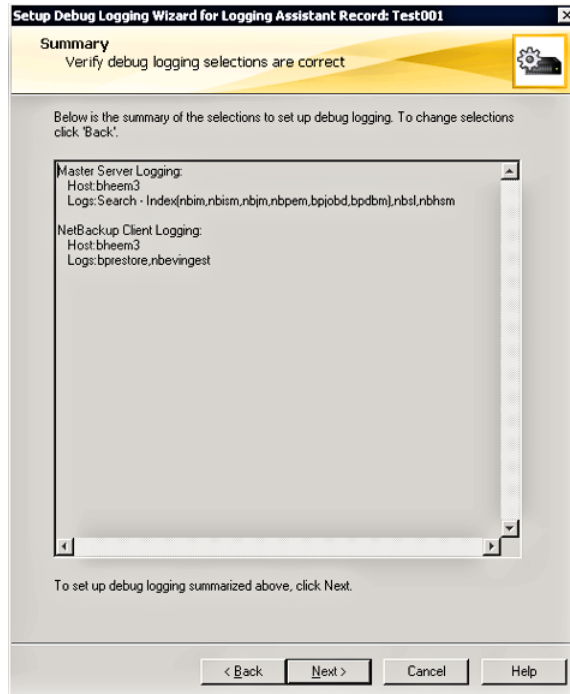
Cancel

Help

6 On the **Summary** page, review your selections.

If the selections are correct, click **Next >** to complete the wizard.

To change the selections, click **< Back** to return to a previous page.



Unable to save the search criteria

Search criteria cannot be saved when one of the following conditions exist:

- No master server (7.5 or later) is configured.
- No backup is available on the master server.
- Image Data Collection for the given master server is yet to complete.

Confirm that a master server (7.5 or later) is configured. Also, confirm that the data collection for backup images is complete before you try to save the search criteria. A master server is eligible for a backup image search only when the data collection is complete.

Resolving excessive log generation and memory usage

In some cases, the `ncfnbci` process can generate as much as 500GB of logs for each indexing server in a short period, such as two days.

If this situation happens in your environment, reduce the log levels of `ncfnbci` to 3 or less. Enter the following command from a command prompt on the indexing server:

```
vxlogcfg -a -p 51216 -o 385 -s DebugLevel=3
```

This command overrides the default logging levels for originator ID 385 and sets the logging level to 3.

The `nbci` process may also consume a large amount of memory when logging is high during indexing.

If this situation happens in your environment, reduce the log levels of `nbci` to 3 or less. Enter the following command from a command prompt on the indexing server:

```
vxlogcfg -a -p nnnnn -o nnn -s DebugLevel=3
```

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

Resolving conflicting failed and indexed log entries for the same backup image

In some cases, a backup image can be reported in NetBackup logs as both failed and indexed. This situation may occur if the indexing service is stopped and restarted.

To determine if a backup image has been reported as failed and indexed, enter the following commands from a command prompt on the master server:

```
nbindexutil -list -indexed -indexserver indexing_server_name
-date_from mm/dd/yyyy HH:MM:SS
```

```
nbindexutil -list -failed -indexserver indexing_server_name -date_from
mm/dd/yyyy HH:MM:SS
```

Note: The `-date_from mm/dd/yyyy HH:MM:SS` option and values specify that the list will include backup images from the specified date and time to the present. You must enter a value for seconds (*ss*) when you specify the time (*HH:MM:SS*). Also, the date must be later than 1st of January, 1970, for example `01/02/1970 12:00:00`.

If the same backup ID is listed in the outputs of both commands, a conflict exists.

To resolve the conflict between the entries, remove the failed entry from the NetBackup system. Enter the following command from a command prompt on the master server:

```
nbindexutil -remove -bid <backupid>
```

Note: Replace *<backupid>* with the backup ID of the image that is reported as both failed and indexed.

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

Resolving indexing job errors while sending data to the master server

Indexing jobs may hang or fail with status code 50 if the NetBackup master server cannot be reached from indexing server.

To detect any anomalies in the network configuration, run the `bptestnetconn` utility. Resolve any of the issues that are related to mismatched or failed domain name service (DNS) lookups by adding or correcting entries in the `etc/hosts` files. You can find the `etc/hosts` files on both the master server and the indexing server. Provide the IP address and the fully qualified domain name (FQDN) with the entries.

Re-initiate the indexing job after you have resolved the issues that caused the problem:

See [“Re-initiating indexing jobs that have failed”](#) on page 120.

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

Re-initiating indexing jobs that have failed

Indexing jobs may fail due to external issues such as disk space exhaustion, network outage, and so on. After the external issue is resolved, perform the following procedure on the master server.

To re-initiate indexing jobs that have failed

- 1 From a command prompt on the master server, enter the following command to list backup images for which indexing jobs have failed on a specific indexing server:

```
nbindexutil -list -failed -indexserver <index_server_name>
[-date_from mm/dd/yyyy [HH:MM:SS]] [-date_to mm/dd/yyyy
[HH:MM:SS]].
```

For example, this command lists the backup images in failed indexing jobs on the `hpindexServer` indexing server from July 6, 2011 to July 15, 2011:

```
nbindexutil -list -failed -indexserver hpindexServer -date_from
07/06/2011 -date_to 07/15/2011
```

The output from the command lists the backup IDs for all of the specified backup images. For example, the command may provide the following output:

```
Backup ID
vmevwin107x64_1322422142
vmevwin107x64_1322426378
vmevwin107x64_1322426379
vmevwin107x64_1322426558
```

- 2 Copy the backup IDs only into a text file. Separate each backup ID with a newline character. For example, you can copy the following backup IDs from the previous step into a file called `bids.txt`:

```
vmevwin107x64_1322422142
vmevwin107x64_1322426378
vmevwin107x64_1322426379
vmevwin107x64_1322426558
```

Note: The `bid_file` can contain only up to 100 images in one file. You have to divide the file into smaller files and run the command `nbindexutil` multiple times if your original `bid_file` contains more than 100 images.

- 3 If you want to index the backup images from the failed job on another indexing server, remove the failed image entries from the indexing queue of the first indexing server with the following command:

```
nbindexutil -remove -bid_file <file_path>
```

For example, this command removes indexing requests for the backup images listed in the text file `bids.txt` from the indexing queue of the first indexing server, where the indexing job failed:

```
nbindexutil -remove -bid_file E:\bids.txt
```

Note: This step is not necessary if you re-initiate the failed job on the same indexing server. This step is necessary only if you want to add the indexing requests listed in the text file to the indexing queue of a different indexing server. In step 4, you can specify the indexing server on which you want to re-initiate the indexing job.

- 4 From a command prompt on the master server, enter the following command to re-initiate an indexing job for the backup images in the text file `bids.txt`:

```
nbindexutil -add -bid_file <file_path> -indexserver  
<index_server_name> - force
```

For example, this command adds indexing requests for backup images listed in the text file `bids.txt` to the indexing queue for the `hpindexServer` indexing server. The job indexes the backup images that are listed in the text file:

```
nbindexutil -add -bid_file E:\bids.txt -indexserver hpindexServer
```

The indexing job runs per backup image (listed in text file) when the indexing schedule window is open for processing. These jobs index the backup images that are listed in the text file.

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

Fixing indexing jobs that fail with error code 5027 after an upgrade

After an upgrade of the indexing server from NetBackup 7.5, the indexing jobs may fail with the error code 5027. The `nbcij` logs on the indexing server provide the following error message for the error code:

For more information about status code 5027, see the [NetBackup Status Codes Reference Guide](#).

```
"Java.lang.IllegalArgumentException: prefix xs is not bound to a
namespace at
com.sun.xml.internal.bind.DatatypeConverterImpl._parseQName"
```

After upgrading the NetBackup Search software package from NetBackup 7.5, you can resubmit the failed indexing jobs.

To fix the failed indexing jobs after an upgrade, on the indexing server perform the following steps:

- 1 Create the directory **repository-supplements** under
`<install-path>\NetBackupSearch\data`
- 2 In the repository-supplements directory, copy the following XML files:
 - application.api-soap.xml
 - iopro.xml
 Reference files are as follows:
[Sample application api-soap.xml](#)
[Sample iopro.xml](#)

Open a command prompt

- 3 Navigate to the folder "`<install-path>\NetBackupSearch\bin\`"
 Make sure that the NetBackup Indexing Engine service is running
- 4 Run the command "`admin-cmd unpack-repository`"

For example, run the following command at command prompt:

```
c:\> cd c:\Program Files\Symantec\NetBackupSearch\bin c:\Program
Files\Symantec\NetBackupSearch\bin> admin-cmd unpack-repository
```

After you fix the indexing jobs, you have to re-initiate the indexing jobs.

See ["Re-initiating indexing jobs that have failed"](#) on page 120.

Fixing indexing jobs that fail with status code 25 (cannot connect on socket)

Indexing jobs (Index for Search or Index Cleanup for Search) may fail with status code 25 (cannot connect on socket). This issue can occur on stressed or loaded systems due to a timeout occurring during socket connection operations in indexing processes (`nbcindex` and `nbcindexdelete`).

Workaround: Reduce the maximum indexing jobs that can run in parallel on the indexing server from the host properties of the master server. From the NetBackup Administration Console, select **Host Properties > Global Attributes > Maximum indexing jobs per index server** and change the value.

You must re-submit failed indexing jobs using the `nbindexutil -add` command. More information is available:

See [“Re-initiating indexing jobs that have failed”](#) on page 120.

Fixing indexing jobs that fail with status code 50 (client process aborted) when NBAC is enabled

Indexing jobs may fail with status code 50 (client process aborted) if NetBackup Access Control (NBAC) is enabled. Follow this procedure to fix the error.

For more information about status code 50, see the [NetBackup Status Codes Reference Guide](#).

To fix indexing jobs that fail with status code 50

- 1 The NetBackup Access Control (NBAC) REQUIRED mode is not supported on the master server. Only the AUTOMATIC mode is supported. You can find NetBackup Access Control properties under the Host Properties of the NetBackup Administration Console. General information about access control is available in the [NetBackup Security and Encryption Guide](#).

Make sure that NBAC is enabled properly.

Note: In NBAC mode, the catalog node on the NetBackup Administration Console may show incorrect statuses for hold and indexing.

- 2 Restart NetBackup services on the master server and indexing server host.

To start the NetBackup indexing engine service (web server service), enter the following commands from a command prompt:

```
net start "NetBackupIndexingEngine"
net start "NetBackup Search Executor Service"
```

- 3 Re-initiate the indexing job requests for the failed jobs.

See [“Re-initiating indexing jobs that have failed”](#) on page 120.

Recovering from disk-full situations

When available disk space is exhausted, indexing jobs may fail. To recover from this situation, you must shut down the indexing engine, resolve the disk space issue, and then restart the indexing engine.

To recover from disk-full situations:

- 1 From a command prompt on the master server, enter the following command:

```
nbindexutil -suspend -indexserver <index_server_name>
```

This command suspends further initiation of indexing jobs for the indexing server.

- 2 From a command prompt on the indexing server, navigate to the NetBackup Search server folder:

```
cd <install_path>\NetBackupSearch\bin
```

- 3 From a command prompt on the indexing server, enter the following command:

```
velocity_shutdown.exe
```

This command shuts down the indexing engine.

- 4 Resolve the disk space issue.

- 5 From a command prompt on the indexing server, enter the following command:

```
velocity_startup.exe
```

The command `velocity-startup` keeps the `netbackupindexingengine` service in “Manual” startup mode, to bring it back to automatic mode issue the command `sc config NetBackupIndexingEngine start= auto` and proceed with the next commands or steps.

- 6 From a command prompt on the master server, enter the following command:

```
nbindexutil -resume -indexserver <index_server_name>
```

This command resumes the processing of indexing jobs for the indexing server.

- 7 Re-initiate any indexing jobs that have failed due to the disk full scenario.

See [“Re-initiating indexing jobs that have failed”](#) on page 120.

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

Recovering from disk-error situations

When a disk controller fails, the disk error occurs, and the indexing jobs get caught in an infinite loop.

To recover from a disk-error situation:

- 1 Cancel the hung indexing job from the NetBackup Activity Monitor.
- 2 From a command prompt on the master server, enter the following command:

```
nbindexutil -suspend -indexserver <index_server_name>
```

This command suspends further initiation of indexing jobs for the indexing server.

- 3 From a command prompt on the indexing server, navigate to the NetBackup Search server folder:

```
cd <install_path>\NetBackupSearch\bin
```

- 4 From the NetBackup Search install path on the indexing server, enter the following command:

```
velocity_shutdown.exe
```

This command shuts down the indexing engine.

- 5 Review the audit log to check if the queued jobs are not indexed.
- 6 Resolve
- 7 From a command prompt on the indexing server, enter the following command:

```
velocity_startup.exe
```

The command `velocity-startup` keeps the `netbackupindexingengine` service in “Manual” startup mode, to bring it back to automatic mode issue the command `sc config NetBackupIndexingEngine start= auto` and proceed with the next commands or steps.

- 8 Queue the entries that were not indexed when they were queued in step 2.
- 9 Re-initiate any indexing jobs that have failed due to the disk error scenario.

See [“Re-initiating indexing jobs that have failed”](#) on page 120.

You can use the `nbindexutil` command to get a list of failed indexing jobs and then resubmit those jobs for indexing.

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

Resolving begin_restore operation failures

The `begin_restore` operation uses the `bprestore` command internally. The same troubleshooting steps that apply to a restore operation apply here as well.

For failures during restore phase, check the following conditions:

- Verify the server privileges of the processing host on the master server.
- Verify the available storage on the alternate restore clients.
- Verify the restore logs on master or media servers.
- Verify the `bprestore` logs on the processing host.
- Verify the availability of the media server.

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

Resolving nbholdrestorehelper operation failures

For failures during the `process_results` phase, check the following conditions:

- Ensure that the staging folder from all indexing servers is accessible on the processing host.
- Verify the restore locations for all types of policy types.
- Ensure that the search ID and `bid_file` provided map each other.

The `nbholdrestorehelper` logs are available on the processing host at
`<install_path>/logs/nbholdrestorehelper/`

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

About Java and MFC UI differences

For certain consoles of the NetBackup Search functionality, there are differences in the Java UI and MFC UI. The differences are as follows:

- In the Java UI and MFC UI, Indexing and Hold columns are provided for certain reports. To retrieve information for indexing and hold columns from the MFC UI and Java UI, you can use CLs for the following reports:

Table 7-6 CLIs for Java and MFC UIs

| Report | Column Absent | CLI for retrieving column information |
|--------------------------------------|-------------------|---|
| Client Backups Report | Indexing and Hold | bpimage.exe/bpimagelist.exe/bpimmeida.exe |
| Images on media Report | Indexing and Hold | bpimmeida.exe |
| Tape Reports - Images on Tape Report | Indexing and Hold | bpimmeida.exe |
| Tape Reports - Tape Written Report | Hold | bpmedialist.exe/nbemmcmd.exe |
| Tape Reports - Tape Lists Report | Hold | bpmedialist.exe/nbemmcmd.exe |
| Disk Reports - Images on disk Report | Indexing and Hold | bpimage.exe/bpimagelist.exe |

- Backup Policy Configuration Wizard
In the Client List page the Indexing column is present in the Java UI and absent in the MFC UI.
- Backup Policy Attributes
The shortcut key to **Enable indexing for search** is **I** on the Java UI and **X** on the MFC UI.

About obsolete search criteria and results for Files & Folder searches

The results of a saved search can become obsolete for the **Files & Folder Search** for the following reasons:

- The master server that is used by the search is deleted or the master server is deleted from Symantec NetBackup OpsCenter itself.
- The master server that is used by the search is deleted from Symantec NetBackup OpsCenter
- A view that is used by the search is deleted.
- The index master server is un-configured thus leaving the associated master server un-indexed. A master server with no index server association is not valid for a search. If such a master server is part of the search criteria, the search is obsolete.

Note: The master server that is associated with Symantec NetBackup OpsCenter with or without indexing server is applicable for the **Image Search**. But for **Files & Folder Search** the master server that is associated with an indexing server is only applicable.

The workaround to remove this error is to re-run the search or edit or save the search criteria again.

Fixing collection-service issues

Sometimes, the `collection-service.exe` on the indexing server might crash resulting in core dumps. It may even cause the indexing jobs to fail. This situation can occur due to disk errors on the indexing server. You must check the system logs or event logs of your computer to find if any disk errors exist. You can also run the `chkdsk` utility to check for disk errors.

You must resolve any disk errors that you find, and then try re-indexing the jobs. If the indexing jobs repeatedly fail even after the disk errors are resolved, the index might have been corrupted. In this case, you must mark that index as invalid, and then re-index the failed indexing jobs.

More information is available about marking an index as invalid.

See [“Marking an index as invalid”](#) on page 35.

More information is available about re-indexing jobs.

See [“Re-indexing backup images”](#) on page 35.

Index

A

- antivirus software 39
- attributes 49

B

- backup images
 - export details 65
 - list by indexing state 33
 - re-index 35
 - remove from indexing queue 33
 - remove indexing references 33
- backup selections 49
- bpexptime 93
- bpimage 92
- bpimagelist 92
- bpimmedia 92
- bpmedialist 93

C

- clients 49
- clustered environments 22
- collection-service
 - issue 129
- configuration 27–28
- configuring
 - indexing server 27

D

- debug logging
 - enable 112
- deployment configurations 20

E

- Enterprise Vault
 - Prerequisites for ingesting the restored data into Enterprise Vault 101
 - restoring data on hold 101
- Enterprise Vault ingest logs 110
- error code
 - 5027 122

H

- hold 16
 - finding media information 95
 - releasing 87
 - reports 90
 - restoring and ingesting data into Enterprise Vault 101
 - viewing hold details 83
- hold operations logs 109
- hold reports 90
 - viewing 91
- holds
 - placing 78

I

- index 15
- index cleanup for search 36
 - purge index 36
 - remove references 36
- index for search 36
- indexing
 - historical backup images 31
 - manual backup images 30
 - on-going backup images 30–31
 - scheduled backup images 30
- indexing engine 11
- indexing engine services
 - start 56
 - stop 56
- indexing jobs 36
 - multiple jobs in parallel 38
 - re-initiating failed jobs 120
 - recovering from disk-error situations 126
 - recovering from disk-full situations 125
 - resolving errors while sending data to the master server 120
 - resume 45
 - suspend 45
- indexing logs 108
- indexing manager 11
- indexing queue 32

- indexing server
 - migrating 41
- indexing servers 11
 - adding 39
 - adding or modifying schedules 45
 - backup 51
 - best practices for protecting 55
 - configuring in a backup policy 48
 - decommissioning 40
 - protecting 49
 - configuring a backup policy 50
 - restoring the indexing database from a backup image 53
- ingesting data into Enterprise Vault 102
 - prerequisites 101
- installation 20
 - clustered environments 22
- invalid index 35

J

- Java and MFC UI differences 127

L

- legal hold 79
- local hold 82
- log files 108
- logs for other NetBackup Search operations 111

M

- mass restore
 - about 96
 - error messages 103
 - preparing 96
 - resolve begin_store operation failures 127
 - resolve nbholdrestorehelper operation failures 127
 - sharing the staging directory 97
 - submit requests 98
 - updating the restoreconfig.ini file 98
- media information for backup images on hold 95

N

- nbauditreport 94
- nbemmcmd 93
- nbholdutil -create 82
- nbholdutil.exe -list 83
- NBIM 11

- nbindexutil -add 32
 - bid 32
 - force 32
 - indexserver 32
 - operation 32
 - priority 33
- nbindexutil -invalidateindices 35
 - index 35
 - indexserver 35
- nbindexutil -list 34
 - failed 34
 - indexed 34
 - indexserver 34
 - inprogress 34
 - out 34
 - waiting 34
- nbindexutil -remove 33
 - bid 33
- nbindexutil -resume -indexserver 45
- nbindexutil -suspend -indexserver 45

P

- port specification 28
- protecting indexing servers 49
 - best practices 55
 - configuring a backup policy 50

R

- re-index 35
- release 87
- requirements 18
 - hardware 19
 - licensing 19
 - software 19
- restoreconfig.ini
 - update 98

S

- schedules 49
- search 15
 - date range 62
 - files and folders 59
 - image search 62
 - using wildcards 66
- Search Broker 11
- search criteria 58
 - obsolete for Files & Folder search 128
 - unable to save 118

- Search executor 11
- search ID
 - find 77
- search operation logs 109
- search queries 57
- search query
 - deleting 72
 - editing 70
 - running 71
 - terms 67
- search results
 - deleting 76
 - obsolete for Files & Folder search 128
 - viewing 73
- searches 57
- snapshots 16
- staging directory 27
 - share 97
- status code
 - 25 123
 - 50 124
- status code 5042 37
- status codes 108
- synthetic backups 37, 49

T

- tar ball copies 16

U

- upgrade
 - master server 23
 - media server 25
 - NetBackup Search 22

V

- virtualization
 - enabling indexing with VMware and Hyper-V backup policy types 48
 - enabling indexing with VMware and Hyper-V policy types 31

W

- wildcard characters 66