

Symantec NetBackup™ Search Administrator's Guide

Release 7.6

DRAFT

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

PN: 21220063

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

DRAFT

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

DRAFT

Contents

Technical Support	4
Chapter 1 About NetBackup Search	11
About NetBackup Search	11
How NetBackup Search works	12
What you can do with NetBackup Search	13
Components of NetBackup Search	16
About snapshots and NetBackup Search	17
What's new in NetBackup Search	18
Chapter 2 Installation and Configuration	19
Installing NetBackup Search	19
Installing NetBackup Search in a clustered environment	24
Changing the staging directory and port specifications for NetBackup Search after installation	24
Chapter 3 Indexing Management	27
About indexing of backups	27
About indexing jobs	30
Suspending and resuming indexing jobs	31
Adding indexing servers	32
Migrating one indexing server to another indexing server	32
Adding or modifying indexing server schedules	36
Configuring an indexing server in a policy	39
Protecting indexing servers	40
Configuring a backup policy that protects the indexing server	41
Running indexing server backups	41
Restoring the indexing database from a backup image	44
Best practices for protecting indexing servers	46
Decommissioning an indexing server	47

Chapter 4	Search Queries	51
	About searches queries	51
	Searching for indexed backups or stored images	53
	Search terms	55
	About using wildcard characters in a search	58
	Editing a saved search query	58
	Running a saved search	59
	Viewing search results	61
	Deleting a saved search	61
	Deleting search results	62
Chapter 5	Holds Management	63
	Placing a hold on a backup image	63
	Viewing hold details	69
	Releasing a hold	71
	How to find the media information of images on hold	73
	About restoring the data on hold and ingesting it into Enterprise Vault	74
	Prerequisites for restoring the data on hold and ingesting it into Enterprise Vault	75
	Restore workflow	75
	About the Restoring Process	77
	Ingesting the restored files into Enterprise Vault	77
	Viewing hold reports	79
Chapter 6	Mass Restore	81
	About Mass Restore	81
	Configuring a mass restore location	81
	Submitting mass restore requests	82
Chapter 7	Troubleshooting	85
	Known Issues	85
	About status codes and log files	89
	Resolving indexing job errors while sending data to the master server	93
	Re-initiating indexing jobs that have failed	94
	Fixing indexing jobs failing with error code 5027 after an upgrade	95
	Recovering from disk-full situations	96
	Recovering from disk-error situations	97
	Resolving begin_restore operation failures	98

Resolving nbholdrestorehelper operation failures	99
About Java and MFC UI differences	99
Index	101

DRAFT

DRAFT

About NetBackup Search

This chapter includes the following topics:

- [About NetBackup Search](#)
- [How NetBackup Search works](#)
- [What you can do with NetBackup Search](#)
- [Components of NetBackup Search](#)
- [About snapshots and NetBackup Search](#)
- [What's new in 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 can be expired 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:

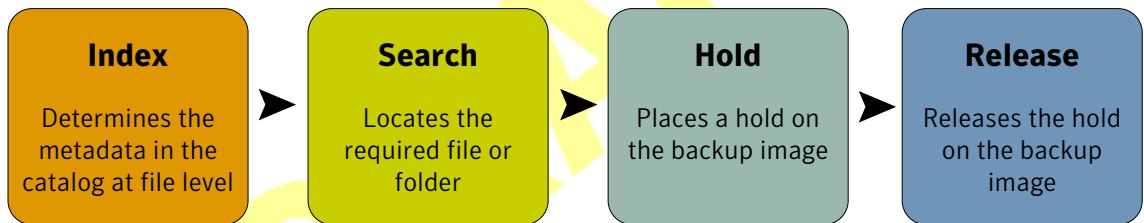
- Advanced search capabilities enable you to find relevant information faster.

- 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 OpsCenter provide insight into size and age of legal hold and length of time of the associated holds.

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 1-1 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 next find and select it from the OpsCenter interface. Then you can place a hold on it.

- **Search**
From the 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 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.

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 like 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 (normal or NDMP agent), 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. NetBackup Search also provides you with an automatic email notification on the completion of every search.

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

When you no longer need the backup image, you can release the hold that you placed on the files through the OpsCenter user interface. (NetBackup Search options are visible in 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.

Components of NetBackup Search

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

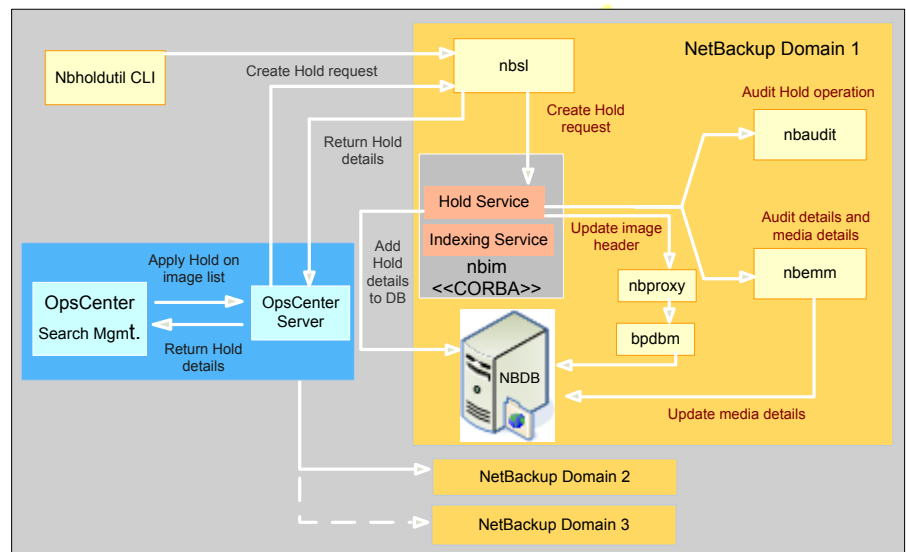
Table 1-1 NetBackup Search components

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.
OpsCenter components	
Search UI	The NetBackup Search user interface is available on the OpsCenter UI. NetBackup Search options are visible to security administrators in OpsCenter only if you have added a valid NetBackup Search license key in OpsCenter.
Search Broker	The Search Broker allows search requests to search across multiple NetBackup domains.
Reports	From the 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 OpsCenter.
Commands that you enter from the command line interface (CLI) of the NetBackup master server	
nbholdutil	The command nbholdutil helps to place a local hold on backup images.
nbindexutil	The command nbindexutil helps to index backup images or delete indexed backup images.
nbsl	The NetBackup Service Layer service facilitates communication between the OpsCenter interface and the core NetBackup components.

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

Component	Description
nbaudit	The NetBackup Audit Manager service records the audit events in the EMM database. It runs on the Master server.
nbproxy	This service allows the multi-threaded NetBackup processes to use existing multi-threaded unsafe libraries.
bpdbm	The NetBackup Database Manager service manages the internal databases and catalogs of NetBackup. It runs on the master server.

Figure 1-3 NetBackup Search components



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 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.

What's new in NetBackup Search

NetBackup Search 7.6 introduces new features that help you to:

- Install a stand-alone indexing server.
With NetBackup Search 7.5, indexing servers were installed on NetBackup media servers. With Version 7.6, you can install the indexing server on its own computer for better indexing performance. All the computer needs is a NetBackup client, which you can install at the same time as you install NetBackup Search 7.6.
See [“Installing NetBackup Search”](#) on page 19.
- Apply holds on images that are searched on the basis of date range.
- Restore backup images to the original or an alternate location.
See [“About Mass Restore”](#) on page 81.
Once you select a job placed on hold you can initiate a mass restore for it. Further, you can search for backup data based on date range and across all NetBackup domains.

Installation and Configuration

This chapter includes the following topics:

- [Installing NetBackup Search](#)
- [Changing the staging directory and port specifications for NetBackup Search after installation](#)

Installing NetBackup Search

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

- **Indexing server**
You can install the NetBackup 7.6 indexing server on a stand-alone server that runs a NetBackup 7.6 client or on a NetBackup media server.
The indexing server is supported only on Windows 2008 R2 (x64) and Windows 2012 (x64) systems. The indexing server can support Pure IPv6. The server must be on a dual stack computer with no public IPv4 address, and the `etc/host` has the following entry:

```
127.0.0.1 localhost loopback
```


For details on support for Pure IPv6 on NetBackup, refer to the *Symantec NetBackup Administrator's Guide*.
- **Search user interface**
The NetBackup Search user interface (UI) is installed as part of Symantec OpsCenter 7.6. No separate installation is needed.
- **Holds management**

The NetBackup holds management software is installed as part of a NetBackup 7.6 master server. No separate installation is needed.

- **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. Refer to the following topic for more information:

See [“Installing NetBackup Search in a clustered environment”](#) on page 24.

The following functions are not supported for NetBackup Search in the NetBackup 7.6 release:

- Upgrade of an existing NetBackup installation to version 7.6 is not included in these instructions. See the main documentation for information about upgrading an existing NetBackup installation to version 7.6.

Deployment configurations:

- **Minimal deployment requires a minimum of two systems (hosts):**

Host 1: NetBackup master server + NetBackup media server or NetBackup client + NetBackup indexing server.

Host 2: Symantec OpsCenter server.

- **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 OpsCenter server.

The following are the recommended hardware prerequisites for the host running the indexing server:

- **Minimum number of CPU cores: 4**

Recommended number of CPU cores: 8

- **Minimum memory: 16 GB**

Recommended memory: 32 GB

- **Disk space: Depends on the size of the index.**

The size of the index is roughly the same as the size of the catalog that was indexed. This size estimation varies based on the nature 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 nature of data, data duplication, backup schedule, and so on.

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

Step	Description
1	Install Symantec OpsCenter.
2	Install a NetBackup 7.6 master server.
3	Install and identify a NetBackup 7.6 media server.
4	Install the NetBackup 7.6 indexing server on a media server or client.
5	Configure NetBackup Search in the NetBackup domain.

To install Symantec OpsCenter

- 1 Install Symantec OpsCenter using the NetBackup 7.6 installation package.
Refer to the main documentation for instructions for installing Symantec OpsCenter.
- 2 Verify that the installation was successful.
Ensure that the **Search & Hold** tab is visible and functional in the OpsCenter UI. You must log in to OpsCenter with an ID that has Security Administrator rights to view the **Search & Hold** tab.
Ensure that the NetBackup Search Broker service is installed and running.

To install a NetBackup 7.6 master server

- 1 Install the master server using the NetBackup 7.6 installation package.
Refer to the main documentation for instructions for installing a master server
- 2 Verify that the installation was successful:
Ensure that the NetBackup indexing manager service is installed and running.
Also, log in to the NetBackup Administration Console and ensure that the policy properties user interface includes indexing properties.

To install and identify a NetBackup 7.6 media server

If you choose to install the indexing server on an existing media server, complete this procedure.

- 1 Install the indexing server using the NetBackup 7.6 installation package.
Refer to the main documentation for instructions for installing a media server
- 2 Verify that the installation was successful.
Ensure that the media server services are running.
Ensure that the media server is registered with the master server. The NetBackup Administration Console should display an entry of the server under the **Media servers** hosts.

DRAFT

To install a stand-alone NetBackup Search 7.6 indexing server

- 1 Install the indexing server using the NetBackup 7.6 installation package. Select **Search Software Installation** from the **Installation** menu of the NetBackup installation wizard.

Note: The installation wizard detects whether a NetBackup 7.6 client is installed on the server. If the installation does not find a NetBackup 7.6 client, it prompts you to install or upgrade the client. The client must run NetBackup 7.6 before you can install the NetBackup Search 7.6 indexing server.

- 2 Follow the prompts that the installer presents to install the indexing server on a stand-alone computer that runs a NetBackup 7.6 client. If NetBackup client software does not already exist on the computer, the installer can install it.

Note: When specifying the install path for the indexing server, specify a location (partition) that has a lot of disk space. 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 media server on that host.

You must exclude the NetBackup Search component directory (`<NBU_Install_Path>\..\Symantec\NetBackupSearch\`) from the antivirus scanning list.

At the end of the installation wizard, there is a checkbox for launching the NetBackup Search Configuration Wizard immediately after the installation completes. This option is enabled by default. However, in case you cleared this option, you can launch the NetBackup Search Configuration Wizard by entering the following command:

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

- 3 Verify that the installation was successful.
Ensure that the NetBackup Search Executor service is installed and running.
For better performance and scalability, you can install multiple indexing servers per domain. See “[Adding indexing servers](#)” on page 32.

To configure NetBackup Search in the NetBackup domain

- 1 Add the indexing server to the NetBackup domain.
See “[Adding indexing servers](#)” on page 32.
- 2 Provide a schedule for indexing server.
See “[Adding or modifying indexing server schedules](#)” on page 36.
- 3 Configure the indexing server in a policy.
See “[Configuring an indexing server in a policy](#)” on page 39.

Installing NetBackup Search in a clustered environment

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

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.

- If OpsCenter is Clustered and NetBackup Master Server is Non-Clustered:
Nodes of OpsCenter: OpsC_Node1, OpsC_Node2
Virtual Name: OpsC_Virtual
You must add the OpsC_Node1, OpsC_Node2, and OpsC_Virtual at following location:
On Windows NetBackup:
`HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\NetBackup\CurrentVersion\Config\Server`
On UNIX NetBackup:
`/usr/openv/netbackup/bp.conf`

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

Changing the staging directory and port specifications for NetBackup Search after installation

Complete this procedure if you want to change the staging directory or the port number for the NetBackup Search indexing server.

To change the staging directory and port specification after installation

- 1 Ensure that no indexing job or search operation is running on the indexing server.
- 2 Stop both the NetBackup Search Executer service and the NetBackup Indexing Engine service with the following command:

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

- 3 Launch the NetBackup Search Configuration Wizard with the following command:

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

- 4 When you are prompted, enter the new staging directory path and port number values.

Note: Ensure that both staging directory and port number values are correct.

- 5 Click **Configure** to complete the configuration changes.
- 6 Exit the NetBackup Search Configuration Wizard.

DRAFT

Indexing Management

This chapter includes the following topics:

- [About indexing of backups](#)
- [About indexing jobs](#)
- [Suspending and resuming indexing jobs](#)
- [Adding indexing servers](#)
- [Migrating one indexing server to another indexing server](#)
- [Adding or modifying indexing server schedules](#)
- [Configuring an indexing server in a policy](#)
- [Protecting indexing servers](#)
- [Decommissioning an indexing server](#)

About indexing of backups

Backups are classified into on-going backups and historical backups.

- **Indexing on-going backups**
The backup policy types that are supported for indexing can be configured for indexing on a particular indexing server. When the backups are completed for policies configured for indexing, their backup image IDs are added to the indexing queue for indexing requests. These images are indexed by the indexing job which is available when the indexing window is open for the indexing schedule of the associated indexing server.
- **Indexing of historical backups**
Older backups or the backup images of the policies which were not configured for indexing are called historical backups. For indexing historical backups,

use the command `nbindexutil` to add the indexing request to the indexing queue.

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

- Backups that are older than NetBackup Search 7.5
- Backups that are already indexed, but you want to reindex them.
- Backups for which the policy is not selected in NetBackup Search indexing server.

To index the backup image files, use the base command `nbindexutil` with the command options `[-add]`, `[-list]`, or `[-remove]` to perform the required operation. You can use the command option `-help` with the other command options to view the help for that option. For example, enter `nbindexutil -help -add` to view the help for `add`.

The command `nbindexutil -add` lets you submit the indexing or purging request for backup images. The following table lists the options and descriptions of the base command `nbindexutil -add`:

Table 3-1 Options of `nbindexutil -add`

Options	Description
<code>-bid <Backup ID> -bid_file <name of the file that contains the backup IDs></code>	Enter the Backup ID with <code>bid</code> or path of the file containing Backup IDs with <code>bid_file</code>
<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 which are in waiting or in progress state.
<code>[-operation <Operation ID>]</code>	Select 1 for adding a new image or 2 for deleting a selected image. By default 1 is selected. Note: The <code>-Indexserver</code> option is not applicable for Delete operation.
<code>[-priority <Priority>]</code>	Set the indexing job Priority to Low or High. The default value is set to Low.

The command `nbindexutil -list` lists the current status of the images being indexed. The following table lists the options and descriptions of the base command `nbindexutil -list`:

Table 3-2 Options of `nbindexutil -list`

Options	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 image(s) 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 options `-indexed` and `-failed` 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 command `[-hoursago hours] |` to list the images that were indexed or failed to index during the last specified hours.

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

The command `nbindexutil -remove` deletes the indexing request for Backup IDs. The following table lists the option and description of the base command `nbindexutil -remove`:

Table 3-3 Options of `nbindexutil -remove`

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>

About indexing jobs

An indexing job collects the metadata of all the files present in a backup image into the indexing engine. Indexing jobs or index cleanup jobs for the images that need to be indexed start when the schedule window opens for that indexing server. Each indexing job or index cleanup job can handle one backup image.

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

Note: 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, modify the `AuditLogTimeoutInHours` at registry location `HKEY_LOCAL_MACHINE\\SOFTWARE\\Symantec\\NetBackupSearch\\CurrentVersion` on the indexing server.

For more information about status code 5042, see the *NetBackup Status Codes Reference Guide*.

Index cleanup jobs remove the references of a backup image from the index. When the copies of an indexed image expire, the image is automatically added to the indexing queue to remove the image from the index.

The index needs to be purged after the reference to one or more images are removed from it. Index cleanup job is started for purging the index. Each job handles one index. These jobs start when the index is untouched for 12 hours after an image is removed from it.

To run multiple indexing jobs in parallel, consider the following factors:

- 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 configured for indexing

If the indexing queue has images from multiple backup clients, multiple indexing jobs are submitted in parallel. For example: For a given backup client, `NBIM` submits the indexing jobs sequentially. A new indexing job for this client is submitted after the earlier job finished. If only one client is configured for indexing, then only one job runs even if the indexing server is a high-end computer.

- Number of indexing jobs that run in parallel

The `MAX_INDEXING_JOBS` parameter in `bp.conf` controls the maximum number of indexing jobs that can run in parallel on an indexing server. For example: `NBIM` may submit eight indexing jobs. If the `MAX_INDEXING_JOBS` parameter is set to 5, only five jobs can run in parallel. The other three jobs are queued.

You need a robust master server because its services `NBIM` and `bpdbm` play an important role in indexing jobs and performing the `search` operation. `NBIM` service initiates the indexing jobs (`nbc`), which index a high volume of data on the indexing server. The indexing jobs search the data from `bpdbm` service which runs on the master server.

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 and resume indexing jobs

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

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

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

Answer the prompt to proceed.

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

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

Note: This command allows new indexing jobs to be submitted.

Answer the prompt to proceed.

Refer to the *NetBackup Commands Reference Guide* for more information about the `nbindexutil` utility and the `-suspend` and `-resume` options.

Adding indexing servers

You can add an indexing server to the NetBackup domain (master server, media server, and client server). The prerequisites for adding an indexing server are as follows:

- Configure a NetBackup domain.
- Install the NetBackup Search application on a Windows 2008 R2 (x64) or Windows 2012 (x64) system. This system is your indexing server. You can choose to install NetBackup Search on a stand-alone computer with a NetBackup client or on a NetBackup media server.

To add an indexing server from the NetBackup Administration Console

- 1 Select **Host Properties > Indexing Servers** from the task panel.
- 2 From the **Actions** menu, choose **Configure Indexing Server**.
- 3 In the **Choose Indexing Server** window, provide the name of the client or the media server on which the NetBackup Search software is installed. Click **OK**.

Note: If adding an indexing server fails with a short name for the server, try its fully qualified domain name. Symantec recommends that you use the same name for the indexing server and the client or media server.

Next, you must create a schedule for the indexing server. See [“Adding or modifying indexing server schedules”](#) on page 36.

Migrating one 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 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 [“Installing NetBackup Search”](#) on page 19.

- 2 **Note:** This step applies only to migration of a NetBackup Search 7.5 or 7.5.x.x indexing server to a 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 9.

- 3 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 with the following command:

```
nbindexutil -suspend -indexingserver <source index 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 31.

- 4 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: Make sure 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 7.

More information about backing up and restoring indexing server data is available:

See [“Protecting indexing servers”](#) on page 40.

- 5 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_index_server_name -new_indexserver target_index_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_index_server_name -new_indexserver target_index_server_name  
-policyonly
```

Refer to the *NetBackup Commands Reference Guide* for more information about the `nbindexutil` utility and the `-migrateindexserver` and `-policyonly` options.

- 6 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**.

- 7 If you restored indexing data from a backup to the target indexing server in step 4, run the following command:

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

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

- 8 Refresh indexing server references in existing OpsCenter search records with the target indexing server name.

- If OpsCenter runs in a Windows environment, run the following command:

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

- If OpsCenter runs in a UNIX environment, 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.

- 9 **Note:** This step applies only to migration of a NetBackup Search 7.5 or 7.5.x.x indexing server to a 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 a NetBackup Search 7.6 indexing server:

- Copy the files and directories from the temporary location you used in step 2 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:

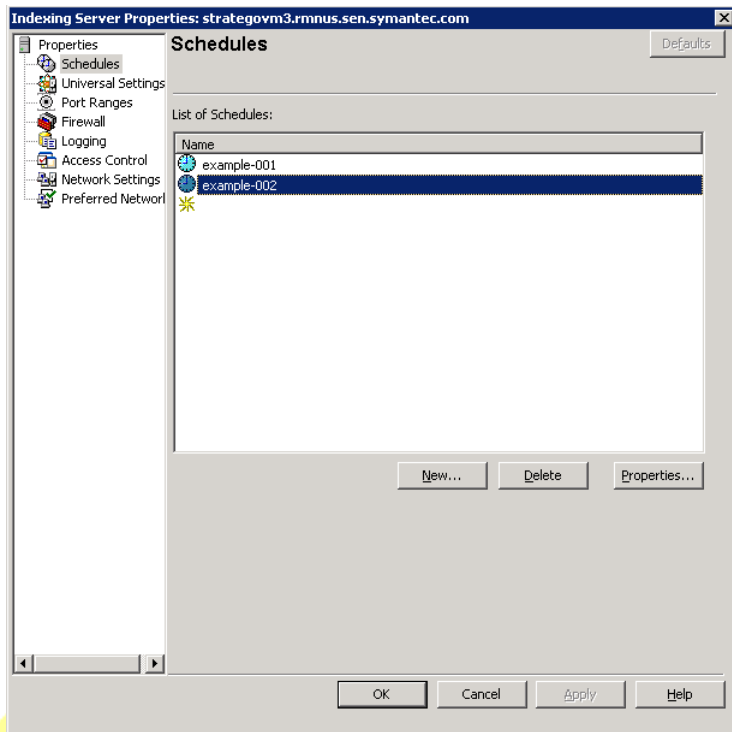
```
<target indexing server install  
path>\NetBackupSearch\bin>admin-cmd.exe unpack-repository
```

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**.

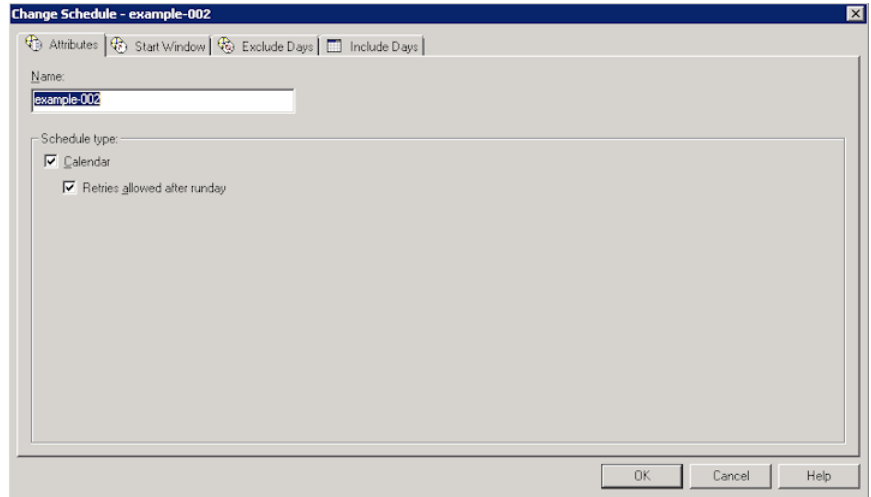


During the configuration of a new indexing server, the **Indexing Server Properties** window opens immediately after you add the indexing server.

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.
Then, click **OK** on the **Indexing Server Properties** window.

Configuring an indexing server in a policy

You must configure the indexing server in a policy to enable indexing of the data backed up by that 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 policy types:

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

Note: 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.

To configure the indexing server in a policy:

- 1 Navigate to the policy's **Attributes** tab.
 - For a new policy, select **Policies** from the task panel.
Select **Actions > New > New Policy**.
Provide a unique name for the policy on the **Add a New Policy** dialog box.
Do **not** select the **Use Policy Configuration Wizard** option.
Click **OK**.
 - For an existing policy, right-click the 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.

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

- | | |
|--------------------------|--|
| Attributes | <ul style="list-style-type: none"> ■ Select Enable indexing for search. ■ From the Indexing Server drop-down list, select the required indexing server. |
| 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 <policy_name> or Change Schedule - Policy <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 <policy_name> or Change Schedule - Policy <policy_name> window. ■ Also select Enable indexing for search for other schedules that are defined for the 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 Enable indexing for search. ■ 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 policy type. |

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. This is a one-time activity and going ahead NetBackup starts protecting 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 policy with these specific policy attributes:

Note: You must also complete the other fields that are required for the 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 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 41.

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 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.

To run indexing server backups with a policy and automated scripts

Note: For more details about the scripts that this procedure references, see the following documents:

[How to use bpstart and bpend notify scripts](#)

NetBackup Administrator's Guide, Volume I

DRAFT

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 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 `bpnd_notify.policy_name.bat`

`policy_name` is the name of the policy that was created in ["Configuring a backup policy that protects the indexing server."](#) The `bpbkar[32]` process runs `bpnd_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 backup 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 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 41.

To run an indexing server backup manually

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

- 1 From a command prompt on the indexing server, stop the indexing engine and related NetBackup Search services:

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

- 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 From a command prompt on the indexing server, restart the indexing engine and related NetBackup Search services:

```
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.

- 4 After the indexing engine starts, restart the Search Executor service. You can start the service from the Services node of the Server Manager or from a command prompt on the indexing server:

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

Restoring the indexing database from a backup image

This section describes how to restore a backup of an indexing server to reinstate the server and resume the indexing operation.

If a disaster involves failure of the server or the indexing server application, then the indexing server must be recovered first. You must install an indexing server on the same or new hardware and configure it.

To restore the indexing database from a backup

- 1 Reinstall the NetBackup and NetBackup Search software.

Information about installing NetBackup Search software is available:

See [“Installing NetBackup Search”](#) on page 19.

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 related NetBackup Search 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 From a command prompt on the indexing server, restart the indexing engine and related NetBackup Search services:

```
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.

- 6 After the indexing engine starts, restart the Search Executor service. You can start the service from the Services node of the Server Manager or from a command prompt on the indexing server:

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

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. In the next step, you can add these new backup images to the restored indexing server.

- 7 Re-index any backup images that were created since the last indexing server backup.

To re-index all backup images that were backed up after given time, run the following command:

```
nbindexutil -reindex -indexserver <indexing_server_name>  
-indexed_after <mm/dd/yyyy [hh:mm:ss]>
```

Use the timestamp of the indexing server's backup image for the `-indexed_after` values. This value ensures that only the indexed backups that were created after the date are reindexed.

- 8 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 topics 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 stand-alone 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.
- Make sure 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.

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 one indexing server to another indexing server”](#) on page 32.

Warning: If you recover a NetBackup master server catalog that includes backup images from the decommissioned indexing server, then 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, issue the following command:

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

This command removes all index server references and data from the master server index tables. All existing backup policies are updated by removing index 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, rerun the command to complete the removal of the indexing server references.

- 2 Ensure that all indexing server references and data have been removed:

- Run the following command from a command prompt to ensure that no policies refer to the indexing server that you want to decommission:

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

You should 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
```

- Run the following command from a command prompt to ensure that no indexed images exist on the indexing server that you want to decommission:

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

You should 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
```

- Optionally, you can confirm that the indexing server no longer appears on the indexing server list.

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

Select **View > Refresh All**. Make sure that you select **Refresh All** rather than **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: To decommission a media server that included an indexing server, follow the instructions to decommission an indexing server. Then, see the following topics in *Symantec NetBackup Administrator's Guide, Volume I, Release 7.6, Chapter 6: Managing Media Servers*:

About decommissioning a media server

Decommissioning a media server

DRAFT

DRAFT

Search Queries

This chapter includes the following topics:

- [About searches queries](#)
- [Searching for indexed backups or stored images](#)
- [Search terms](#)
- [About using wildcard characters in a search](#)
- [Editing a saved search query](#)
- [Running a saved search](#)
- [Viewing search results](#)
- [Deleting a saved search](#)
- [Deleting search results](#)

About searches queries

Use NetBackup Search to search for data in indexed backups and the 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 for indexed backups or stored images”](#) on page 53.

See [“Search terms”](#) on page 55.

See [“About using wildcard characters in a search”](#) on page 58.

See [“Editing a saved search query”](#) on page 58.

See [“Running a saved search”](#) on page 59.

See [“Viewing search results”](#) on page 61.

See [“Deleting a saved search”](#) on page 61.

See [“Deleting search results”](#) on page 62.

DRAFT

Searching for indexed backups or stored images

To create a new search for data in indexed backups or stored images:

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

You can search for backed up data based on **Files and Folders** or **Image Search** and **Backup Date Range**.

Note: For Image Search the data is not indexed, the images are stored in the OpsCenter database. You can retrieve the images (across all the policies) by entering the data range in the **Backups Taken in** field.

From the Search For drop-down list select **Files and Folders** to get the required set of images by creating a search based on Files and Folders. You can select **Images Search** to get the required set of images by creating a search based on the backup date range.

Make sure that index data collection has completed. If you select **Files and Folders**, the left pane of the **New Search Criteria** page displays the numbers of masters, 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. Note that if there are two master servers for which index data is in the process of being collected, the left pane does not include those two master servers in the master count. Also note that the numbers in the left pane change appropriately when you select a master, client, user, or view in the right pane.

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

- 2 Select the appropriate criteria for the search. To refine the search, click **Advanced** and add one or more of the criteria that is displayed. Detailed information about the search terms is available:

See [“Search terms”](#) on page 55.

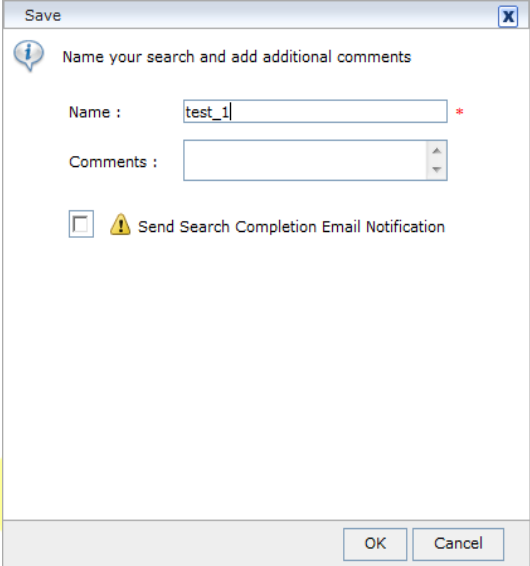
See [“About using wildcard characters in a search”](#) on page 58.

3 Click **Save** to save the selected search criteria.

Provide a unique **Name** for the search. For example, you can name the search so that it corresponds with an ongoing legal proceeding.

Optionally, provide a description of the search criteria in **Comments**.

Optionally, select **Send Search Completion Email Notification** (only for **File & Folder** search) to send a message when the search completes, and then select recipients. The list of recipients is defined in 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 OpsCenter, select **Settings > Recipients > Email**. See *About managing recipients in OpsCenter* for detailed information about email notifications through OpsCenter. Also, ensure that an SMTP server has been configured through OpsCenter. Select **Settings > Configuration > SMTP** to configure an SMTP server. See *Configuring SMTP server settings for OpsCenter* for detailed information about SMTP settings in OpsCenter.

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

Next, a list of saved searches is displayed. The list is sorted initially by name. Click the plus symbol next to the name of a saved search to display information about it.

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 checkbox 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>
Advanced	<p>Click this link to display the advanced search criteria.</p>

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

Field	Description
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)	<p>Click the ellipses to select the names of the views you want to include in this search.</p>
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.

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.

Editing a saved search query

To edit a saved search for data in indexed backups

- 1 From the 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 55.

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 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 OpsCenter, select **Settings > Recipients > Email**. See *About managing recipients in OpsCenter* for detailed information about email notifications through 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 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

The screenshot shows the Symantec OpsCenter Analytics interface. The top navigation bar includes 'Home', 'Monitor', 'Manage', 'Reports', 'Search & Hold' (selected), and 'Settings'. The 'Search & Hold' section has tabs for 'New', 'Saved', and 'Holds'. The 'Saved Searches' section displays a table of saved searches. The table has columns: Name, Hold, Last Saved, Status, Last Run, and Last Sync Time. The first search is '02' with status 'Never Run'. The second search is '12' with status 'Completed: (44 Hits Found)'. The third search is '12' with status 'Never Run'. The bottom of the table indicates 'Total 13 Rows, 1 Page(s)'. The Symantec logo is in the bottom right corner.

Name	Hold	Last Saved	Status	Last Run	Last Sync Time
02	-	Jul 11, 2012 10:02:18 AM	Never Run	-	-
12	1212	Jun 28, 2012 3:18:50 PM	Completed: (44 Hits Found)	Jun 28, 2012 3:19:30 PM	Jun 28, 2012 3:19:30 PM
12	-	Jul 11, 2012 2:39:40 PM	Never Run	-	-

Viewing search results

To view search results

- 1 From the 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 To view search results, find the saved search and select the Status link. For example, **Completed**, **In Progress**, or **Failed**.

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

- 4 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. Then click the plus sign next to the date to view the corresponding backup image details.

This view displays detailed information about a backup images that can be placed on hold.

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: 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.

- 5 To place a hold for **Files & Folder Search** select the backups that you want to hold and then click **Hold** or **Hold All**. For **Image Search** you can only click **Hold All** to place a Hold.

More information about holds is available:

See [“Placing a hold on a backup image”](#) on page 63.

Deleting a saved search

Use this procedure to delete a saved search.

To delete a saved search

- 1 From the 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?**

Click **OK** to delete the search. Click **Cancel** to keep the saved search.

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 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.

Holds Management

This chapter includes the following topics:

- [Placing a hold on a backup image](#)
- [Viewing hold details](#)
- [Releasing a hold](#)
- [How to find the media information of images on hold](#)
- [About restoring the data on hold and ingesting it into Enterprise Vault](#)
- [Viewing hold reports](#)

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 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 OpsCenter server, the Hold Agent must initialize to perform any hold operation. Ensure that the hold status is started on the **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** displays.

To place a legal hold on a backup image through OpsCenter

- 1 From the 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**.

DRAFT

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

For **File & Folder Search**, refer to the below figure:

The screenshot shows the Symantec OpsCenter Analytics interface. The top navigation bar includes 'Home', 'Monitor', 'Manage', 'Reports', 'Search & Hold' (selected), and 'Settings'. The user is logged in as 'admin'. Below the navigation bar, there are tabs for 'New', 'Saved', and 'Holds'. The main content area is titled 'Search Results' and shows '320 files found for "True Image Files_LastMonth"'. It includes a 'SEARCHED FOR' section with filters: 'User: All', 'File Modified Any', and 'File Type All'. There are buttons for 'Hold All' and 'Hold', and a status '1 Backup Image Selected'. On the left, there is a 'Filter by' section with 'Domain' (Masters: (1) Clients: (1)), 'User and Group' (Users: (1) User and Group: (1)), and 'File Type' (Others: 320). The main table displays 'Total Backup Images : (1)' and 'Total Search Hits : (320)'. The table has columns: File/Folder Name, Size, User, User Group, File Created, and File Modified. The first row shows a file named '/D/data-class /1.v2i' with size 0 B, user Admin, and file created on Oct 5, 2012. The second row shows a file named '/D/data-class - Copy.v2i' with size 0 B, user Admin, and file created on Oct 5, 2012. The third row shows a file named '/D/data-class - Copy.v2i' with size 0 B, user Admin, and file created on Oct 5, 2012. The table has pagination controls at the bottom right.

Note: For **Image Search** you have to click **Hold All** to place the image(s) on hold. You can select **Export** to generate a CSV file of the search results.

For **Image Search**, refer to the below figure:

The screenshot shows the Symantec OpsCenter Analytics interface. The top navigation bar includes links for Home, Monitor, Manage, Reports, Search & Hold (highlighted), and Settings. A user is logged in as [admin]. Below the navigation bar, there are tabs for New, Saved, and Holds. The main section is titled "Search Results" and displays a search for "all". The search criteria are "Backups Taken in: From :: Sep 1, 1970 To :: Sep 5, 2012". A "See all" link is available. Below the search criteria, there is a summary for the search results for Backup Images. This summary includes buttons for "Hold All" and "Export". A table displays the search results with columns: Master Server, Client Count, Image Count, Disk Size, and Tape Size. The table shows one row for Master Server XYZ-5 with 2 clients, 108990 images, and 9.043 GB of disk size. The total number of rows is 1, and there is 1 page(s).

Master Server ▲	Client Count	Image Count	Disk Size	Tape Size
XYZ-5	2	108990	9.043 GB	-

Total 1 Rows , 1 Page(s)

- 6 Click **Hold** to place the selected images on hold. You can click **Hold All** to place all the images on hold.
You can also select all backup images that are displayed on a page, by enabling the checkbox in the column heading. The checkbox in the column heading is only for selecting all images on a single page. Move to the next pages to select images from subsequent pages.
- 7 Provide the following information in the **Create Hold** dialog:
 - Provide a unique **Name** for the hold. For example, you can name the hold so that it corresponds with an ongoing legal proceeding.
 - Optionally, provide a description of the hold in **Comments**. Comments 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, choose **Existing Groups**. Select the existing group from the drop-down list.
 - To add this hold to a new group of holds, choose **New Group**. Provide a unique name for the new group.

- Optionally, provide a description of the group in **Comments**.
Hold groups are useful in cases where multiple holds are related to a single legal case.
- Optionally, enable **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 17. for more information.

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 Group: Select a hold group

☐ New Group:

Comments :

☒ Hold any copies that were not selected

OK Cancel

- 8 Click **OK** to complete the creation of the hold.

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

- 1 From the command line interface of 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 that is 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.

See [Table 5-1](#) for more information about related command options.

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

```
nbholdutil.exe -list
```

See [Table 5-2](#) for more information about related command options.

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

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

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

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> -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 hold details

You can view the details of the images placed on hold. The Hold view displays the following tabs:

- **Release**
See [“Releasing a hold”](#) on page 71.
- **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 placed on hold.

To view hold details

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

The list of holds that is displayed can contain two types of holds:

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

- **Legal Holds** are created using 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 contains a list of images that are a part of a hold and details of any errors that occurred when this hold was in progress.

A hold goes in the **Orphan** state when the OpsCenter database crashes and is restored to a stage in the past when the hold was not created. An Orphan hold is a Legal hold present on NetBackup but 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 for any reason, click **Retry** to try the operation again 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.

Releasing a hold

You can release local holds and legal holds through OpsCenter. However, you can release only local holds through the command line interface.

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

Hold

[Release](#) [Export](#) [Refresh](#)

	Name	Media	Backups	Size	Files	Created By	Placed On	Status
Total 46 Rows , 4 Pages								
<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

Symantec.

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

To release a hold through OpsCenter

- From the OpsCenter interface, select **Search & Hold > Holds**.
- 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 they 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 through 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 brief description of the release of this hold. For example, for audit purposes:

See [Table 5-3](#) for more information about related command options.

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 base command `nbholdutil -delete`:

Table 5-3 Options of nbholdutil -delete

Option	Description
-holdid <holdid> -holdname <hold name>	Provide either the hold ID or the name for the hold.
[-force]	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.
[-reason <reason>]	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*.

How to find the media information of 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. 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 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 to the right of the backup 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, you can issue the following command from a command prompt 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:              /diskstu1/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.

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. To facilitate this task, NetBackup also provides a utility for restoring the data that is placed on hold. The light-weight utility generates input files and batch files with the pre-formatted `bprestore` commands that restore the required data on legal hold.

The 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 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, even in Enterprise Vault.

Prerequisites for restoring the data on hold and ingesting it into Enterprise Vault

You must have a good understanding of the NetBackup tasks and the concepts of Enterprise Vault. The prerequisites for restoring data under legal holds and ingesting the data into Enterprise Vault are as follows:

- **NetBackup**

You should deploy the NetBackup Search solution and be aware of the deployed index 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 steps need to be performed separately for each NetBackup domain. Since the backup data can be from Windows, Linux or Unix or NDMP clients, during restore, a separate host of each type needs to be specified as a destination client.

- **Enterprise Vault**

After you restore the data, you have to consolidate it to a single windows host that acts as a client for Enterprise Vault. The host needs to have Enterprise Vault ECM SDK v9.0 or install a higher version. Also, the host should have write permissions on shared archives into which the data is ingested. The ECM SDK is an independent component shipped with Enterprise Vault.

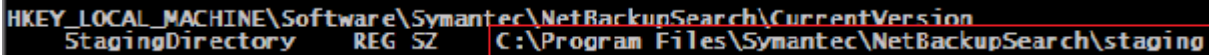
Restore workflow

You have to restore data that has been put on Legal Hold using the NetBackup Search interface available in OpsCenter.

For one time configuration:

- 1 On every Index server, share the configured *staging* folder; a read-only share is sufficient. To identify the location of the staging folder, on the individual Index server run the following command:

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



```
HKEY_LOCAL_MACHINE\Software\Symantec\NetBackupSearch\CurrentVersion  
StagingDirectory REG_SZ C:\Program Files\Symantec\NetBackupSearch\staging
```

- 2 Identify a host to perform the processing of the Search results to determine the storage requirements on a per-client basis. The host should have Server privileges on the NetBackup master, since it needs to perform alternate client restores. It is recommended to use an existing Index server as a Processing host.
- 3 On the Processing host create a file 'RestoreConfig.ini' in the <NetBackup>/bin/goodies folder based on the template provided at:

<http://www.symantec.com/docs/DOC5787>

In the RestoreConfig.ini update the following values:

- **General\ProcessingDir:** You have to create the processed data here.
- **IndexServers\Server:** One entry for each index 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:** If you want to ingest data into Enterprise Vault, provide the location on the EV client host where all the restored data from various alternate restore clients is consolidated.

Note: You have to update the configuration provided in the above steps when either an index server is added or removed or the alternate restore clients or locations need to be updated.

You can restore the Legal Hold placed on Files and Folders, for more details See [“Submitting mass restore requests”](#) on page 82.

About the Restoring Process

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 having detailed status on a per-job id basis is also created.

The total number of restore jobs initiated depends on the number of backup images being restored and the value of `[General\RestoreBatchSize]` specified by you in the `RestoreConfig.ini` file. Also, the total number of concurrent active restore jobs is governed by the value of `[General\MaxConcurrentRestoreJobs]` parameter specified by you in `RestoreConfig.ini` file.

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

```

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

The `nbholdrestorehelper` utility internally uses the `bprestore` CLI for initiating the restore jobs; hence imply the same troubleshooting steps here too.

Ingesting the restored files into Enterprise Vault

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

Additionally, an `EVingest.bat` file is created to help in the ingestion process, refer to the below image:

While 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. The custom attributes are searchable from the Enterprise Vault console using the Discovery Accelerator product; this provides an important advantage during legal workflows.

The EV ingest workflow is as follows:

- 1 **Consolidate restored data** - The restored data can be present across multiple hosts or restore locations based on the inputs provided in the RestoreConfig.ini file. Once the restore is complete, the data from the alternate restore client's needs to be consolidated on the host that would 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** - While ingesting into EV, you have to 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
```
- 4 You can leverage the ingestion into Enterprise Vault to search for files based on content and original metadata, and put individual files under legal hold using the Discovery Accelerator product (as against the backup image-level hold using NetBackup Search in NetBackup).

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 ingested into Enterprise Vault are content-indexed).
- Refine the searches based on the files' original metadata attributes (set as custom attributes in Enterprise Vault)
- Put file-level legal hold from Discovery Accelerator on the final search results.

Parameter	Searchable	Retrievable
NetBackup Master	Yes	Yes
Backup client	Yes	Yes
Policy type	Yes	Yes
Group nam	Yes	Yes

Parameter	Searchable	Retrievable
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, then it is a part of the result set and can be displayed in the UI that shows the search results.

Viewing hold reports

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

You can view Hold reports only if you have added a valid NetBackup Search license key in OpsCenter and you log on to OpsCenter as a Security Administrator.

To view a hold report

- 1 From the 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

DRAFT

Mass Restore

This chapter includes the following topics:

- [About Mass Restore](#)
- [Configuring a mass restore location](#)
- [Submitting mass restore requests](#)

About Mass Restore

NetBackup Search helps you to restore the backup images placed under a hold to a required location. To perform a restore, you must use the OpsCenter UI and the command line interface.

The restore operation supports individual Holds and not 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, and if you back-up the data using MS-Windows policy the data is restored to a windows host.

Configuring a mass restore location

You have to initiate a separate mass restore operation for each master that is a part of the Hold. A restore location is a path to a directory on file server of one of the clients of that master server, where the restores from that master server can be redirected.

Note: The host from where the restore jobs are initiated need to have server privileges on the master server.

You can also override the default restore location of the master server by specifying a different restore location.

Submitting mass restore requests

You can submit a mass restore request by using the `nbholdrestorehelper` command. Mass restore is applicable only for **Files & Folder Searches** and not for **Image Search**. The `nbholdrestorehelper` utility processes the search results from NetBackup Search. When you submit the mass restore request, you need to know the Search ID of the saved backup image.

To get the Search ID:

- 1 From the 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 displays. You can note the Search ID from the Search Criteria details view.

To perform a mass restore from the command line, you must first create the configuration file. To create the configuration file, you can download the sample configuration file, save it as your configuration file, and update the entries as required. The default name of the config file is `RestoreConfig.ini`. You have to share the staging folder from each of the indexing server and mention it in the restore config file. See the following sample configuration file:

[Sample config file](#)

To perform mass restore from the command line:

- 1 Create the BackupID (BID) file; 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: The attribute [-f conf_file] is optional if the configuration 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:

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

If you need to cancel the operation at any stage during the restore process, 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

DRAFT

Troubleshooting

This chapter includes the following topics:

- [Known Issues](#)
- [About status codes and log files](#)
- [Resolving indexing job errors while sending data to the master server](#)
- [Re-initiating indexing jobs that have failed](#)
- [Fixing indexing jobs failing with error code 5027 after an upgrade](#)
- [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](#)

Known Issues

The following are the known issues of NetBackup Search in the NetBackup 7.6 release:

- The NetBackup indexing engine service does not start or stop by using the `bpup` or `bpdown` commands.

Workaround: 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"
```

To stop the NetBackup indexing engine service, enter the following commands from a command prompt:

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

The commands `net start "NetBackupIndexingEngine"` and `net stop "NetBackupIndexingEngine"` start or stop the indexing engine service. The commands `net start "NetBackup Search Executor Service"` and `net stop "NetBackup Search Executor Service"` start or stop any search requests that are currently linked with the indexing engine service.

- Some of the indexing service processes continue to run even after you stop the NetBackup indexing service.

Workaround: To shut down all indexing services, enter the following command:

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

This command stops both the NetBackup Search Executer service and the NetBackup Indexing Engine service.

- The NetBackup Search indexing processes crash if antivirus software scans the index locations, namely - `<NetBackupSearch install location>\data` directory.

Workaround: Exclude the `<NetBackupSearch install location>\data` directory from the antivirus scanning list.

- NetBackup Search does not currently support synthetic backups.
- It takes a long time to view the last page of search results for backup images with a large number of hits.
The request may time out when you attempt to view backup images with approximately one million or more hits.
- 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*.
- In NBAC mode, the catalog node on the NetBackup Administration Console shows incorrect statuses for hold and indexing.
- NetBackup Search does not support pure IPv6 Master at this time.
- Indexing of imported images must be performed manually.
- Holds do not persist after backup images are imported to NetBackup. If you import images that previously were placed on hold, you must re-apply the holds after images are successfully imported.

- 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.
- Some reports on NetBackup Administration Console user interface are not consistent with the reports in Java user interface with regards to Hold and Indexing status.
- The Hold and Index columns in the Catalog node of the NetBackup Administration Console are overlapped with other columns. You may need to expand them manually.
- The `velocity.exe` program may crash occasionally when an indexing job is running.
- Both the NetBackup Administration Console and Java UIs do not validate the existence of the search server package when you configure the indexing server.
- Occasionally, some indexing jobs may remain in progress for hours.
- 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. This situation may occur when the 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.
- Policy validation fails if Indexing is selected and 'enable File recovery from VM' option is not selected
Indexing is not supported for unmapped backups, hence the indexing job fails with the error status 5028 for the following scenarios:
 - Policy type is VMware, indexing is selected, and 'enable File recovery from VM' is not selected.
 - Policy type is VMware, indexing is selected, and 'enable File recovery from VM' is selected. However, the guest operating system should be other than Windows and Linux.

The scenarios are applicable for VMware and Hyper-V policy types.
- NCFNBCI generates 500GB of logs in two days.
If NCFNBCI generates 500GB of logs in two days for each indexing server, the log levels of NCFNBCI should be reduced to 3 or less than 3. If the logging levels increases, then do the following:


```
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.
- NBCI consumes high memory when logging is high during indexing.

If `NBCI` is consuming high memory when logging is high during indexing, reduce the log levels of `NBCI` to 3 or less than 3.

- After the first batch of indexing jobs run, the subsequent indexing jobs are not triggered for the indexing server.

If the indexing server is configured on a computer that has less than recommended hardware configuration, the RAM and core do not get updated in the database after the first indexing job.

To activate the indexing server and update the RAM and core in the database, perform the following tasks:

- Upgrade the hardware.
- Decommission the indexing server.
See [“Decommissioning an indexing server”](#) on page 47.
- Reconfigure the indexing server.
- Re-run the indexing jobs that completed in the first run. Use the command `nbindexutil` for running the jobs.
See [“Re-initiating indexing jobs that have failed”](#) on page 94.

The RAM and core are updated in the database with successive indexing jobs.

- When you add a new client to a policy in NetBackup, the checkbox to enable indexing for search appears as a tristate box.
Workaround: You must select or clear the checkbox. The third state ‘indeterminate’ is not applicable.
- When you edit multiple client in a NetBackup policy, ensure that the checkbox to enable indexing for search is enabled. Otherwise, the status of indexing may appear to be incorrect.
Workaround: You have to manually update the indexing status for the clients that have an incorrect status.

- The ‘Last Sync Time’ column on the OpsCenter UI does not change for a considerable duration when a search operation is run.

When you run the search operation, OpsCenter receives results for the Search and updates the ‘Last Sync Time’ column. The ‘Last Sync Time’ column lists the most recent time when 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: You have to analyze the progress information present on the Search Broker at

`<install_path>\SearchBroker\var\progress\<search-id>.csv` to know

about status of the search on related hosts. You may have to stop and re-run the search operation.

- In cases where one Legal Hold spans across masters including a 7.5 version, the data from the 7.5 version cannot be restored using the method documented here.
- In NetBackup 7.6, the “Image Search” feature is introduced within the OpsCenter UI. Image Search allows searching for images based on backup date range and Master or Clients hosts without the need for indexing. After an image search, a Legal Hold can be applied on these images. However, the restores of such Holds is not supported.
- The error message "Client backup was not attempted because backup window is closed" is displayed when the indexing window is not open.
The error message is displayed only when the index window is too small for example, less than 1 minute, and the policy execution manager or the job manager have not determined the job type.

About 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			
<code>install_path\NetBackup\logs\nbim</code>	NetBackup master server	51216	371
<code>install_path\NetBackup\logs\bpdbm</code>	NetBackup master server	N/A	N/A
<code>install_path\NetBackup\logs\nbsl</code>	NetBackup master server	51216	132
<code>install_path\NetBackup\logs\wingui</code>	NetBackup master server	51216	263
<code>install_path\NetBackup\logs\user_ops\nbjlogs</code>	NetBackup master server	N/A	N/A

Table 7-1 Indexing Logs (*continued*)

Log Folder	Resides on	UL Product ID	Originator ID
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
<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\nbcij	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	OpsCenter server	58330	147
UNIX: <i>install_path</i> /SYMCOpsCenterGUI/logs			

Table 7-2 Search Operations Logs (*continued*)

Log Folder	Resides on	UL Product ID	Originator ID
Windows: <i>install_path</i> \OpsCenter\server\logs UNIX: <i>install_path</i> /SYMCOpsCenterServer/logs	OpsCenter server	58330	148, 149
<i>install_path</i> \Searchbroker\logs	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	OpsCenter server	58330	147
Windows: <i>install_path</i> \OpsCenter\server\logs UNIX: <i>install_path</i> /SYMCOpsCenterServer/logs	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</i> \OpsCenter\gui\logs UNIX: <i>install_path</i> /SYMCOpsCenterGUI/logs	OpsCenter server	58330	147
Windows: <i>install_path</i> \OpsCenter\server\logs UNIX: <i>install_path</i> /SYMCOpsCenterServer/logs	OpsCenter server	58330	148, 149
<i>install_path</i> \NetBackup\logs\admin	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\nbim	NetBackup master server	51216	371, 372

Table 7-3 Hold Operations Logs (*continued*)

Log Folder	Resides on	UL Product ID	Originator ID
<i>install_path</i> \NetBackup\logs\bpdbm	NetBackup master server	N/A	N/A
<i>install_path</i> \NetBackup\logs\nbemmm	NetBackup master server	51216	111
<i>install_path</i> \NetBackup\logs\nbemmm	NetBackup master server	N/A	N/A
Use Case: Local Hold operations (add hold, release hold)			
<i>install_path</i> \NetBackup\logs\admin	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\nbim	NetBackup master server	51216	371, 372
<i>install_path</i> \NetBackup\logs\bpdbm	NetBackup master server	N/A	N/A
<i>install_path</i> \NetBackup\logs\nbemmm	NetBackup master server	51216	111
<i>install_path</i> \NetBackup\logs\nbemmm	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 nbevingest.exe			
<i>install_path</i> \NetBackup\logs\nbevingest	NetBackup client	51216	398
Use Case: Restore data searched using NetBackup Searchnbrestorehelper.exe			
Windows temp directory [%TMP%]	NetBackup client	N/A	N/A
<i>install_path</i> \NetBackup\logs\nbholdrestorehelper	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			
<i>install_path</i> \NetBackupSearch\logs	NetBackup indexing server	N/A	N/A
Use Case: PBX operations			
Program Files\VERITAS\VxPBX\logs	OpsCenter server NetBackup master server NetBackup indexing server	N/A	N/A
Use Case: Search progress (.cvs file)			
<i>install_path</i> \SearchBroker\var\progress	OpsCenter server	N/A	N/A
Use Case: Search error details (.error file)			
<i>install_path</i> \SearchBroker\var\progress	OpsCenter server	N/A	N/A

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 94.

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 failing with error code 5027 after an upgrade

After an upgrade of the indexing server from 7.5, the indexing jobs may fail with the error code **5027**. The `nbci.j` logs on the indexing server provides the following error message for the error code:

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

After upgrading the Search software package from NetBackup 7.5 to NetBackup Beta build, 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.xmlReference files are as follows:
[Sample application api-soap.xml](#)
[Sample iopro.xml](#)

Open a command prompt

- 3 Traverse to the folder "`<install-path>\NetBackupSearch\bin\`"
Make sure that NetBackupIndexingEngine 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 94.

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 94.

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 that the queued jobs are not indexed.

- 6 Correct the system failure.

- 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 94.

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 CLIs 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	<code>bpimage.exe/bpimagelist.exe/bpimdeida.exe</code>
Images on media Report	Indexing and Hold	<code>bpimdeida.exe</code>

Table 7-6 CLIs for Java and MFC UIs (*continued*)

Report	Column Absent	CLI for retrieving column information
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.

Index

B

backups
 historical 27
 on-going 27

C

clustered environments 24
configuration 24

D

deployment configurations 20

E

Enterprise Vault
 restoring data on hold 74

H

holds
 finding media information 73
 placing 63
 releasing 71
 restoring and ingesting into Enterprise Vault 74
 viewing hold details 69
 viewing hold reports 79

I

indexing engine 16
indexing jobs 30
 re-initiating failed jobs 94
 recovering from disk-error situations 97
 recovering from disk-full situations 96
 resolving errors sending data to the master
 server 93
indexing manager 16
indexing server
 protecting 40
indexing servers 16
 adding 32
 adding or modifying schedules 36

indexing servers *(continued)*
 configuring in a policy 39
 decommissioning 47
installation 19
 clustered environments 24

J

Java and MFC UI differences 99

K

known issues 85

L

legal holds 64
local holds 68
log files 89

M

media information for images on hold 73

N

NBIM 16

P

port number 24
protecting indexing servers 40

S

Search Broker 16
Search executor 16
searches
 creating a new search 53
 deleting a saved search query 61
 deleting search results 62
 editing a saved search query 58
 running a saved search query 59
 terms 55
 using wildcards 58
 viewing search results 61

- snapshots 17
- staging directory 24
- status code 5042 30
- status codes 89

T

- tar ball copies 17

W

- wildcard characters 58

DRAFT