Symantec NetBackup™ Search Administrator's Guide

Release 7.5

21220063

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: 7.5

Legal Notice

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.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

About NetBackup Search

This chapter includes the following topics:

About NetBackup Search

NetBackup Search provides a mechanism to index the file system metadata that is associated with backup images. This mechanism makes searching for relevant information simple, powerful, and fast. Once information is found, the user is able to take actions on that information. NetBackup Search provides a robust legal hold mechanism. This mechanism 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.

With NetBackup Search you can determine the data in the catalog at file level and locate any file or folder from the repository. Further, you can select the required files or folders (backup images) and retain them by placing them on hold. After you release the Hold, the files or folders can be expired.

The following capabilities are provided with this feature:

- Advanced search capabilities enable you to find relevant information faster:
  - Search across multiple domains.

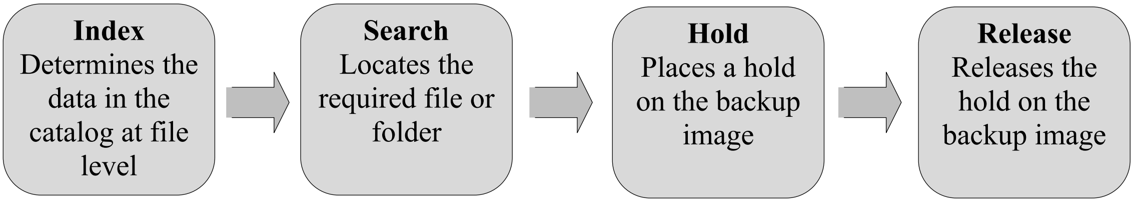
- Save and edit search queries for legal traceability.

- Robust solution for legal hold management.
  - Legal holds provide a mechanism to retain backup images regardless of existing retention levels. Legal holds ensure that backup images and associated media are retained 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
Determines the data in the catalog at file level
Search
Locates the required file or folder
Hold
Places a hold on the backup image
Release
Releases the hold on the backup image

- 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.

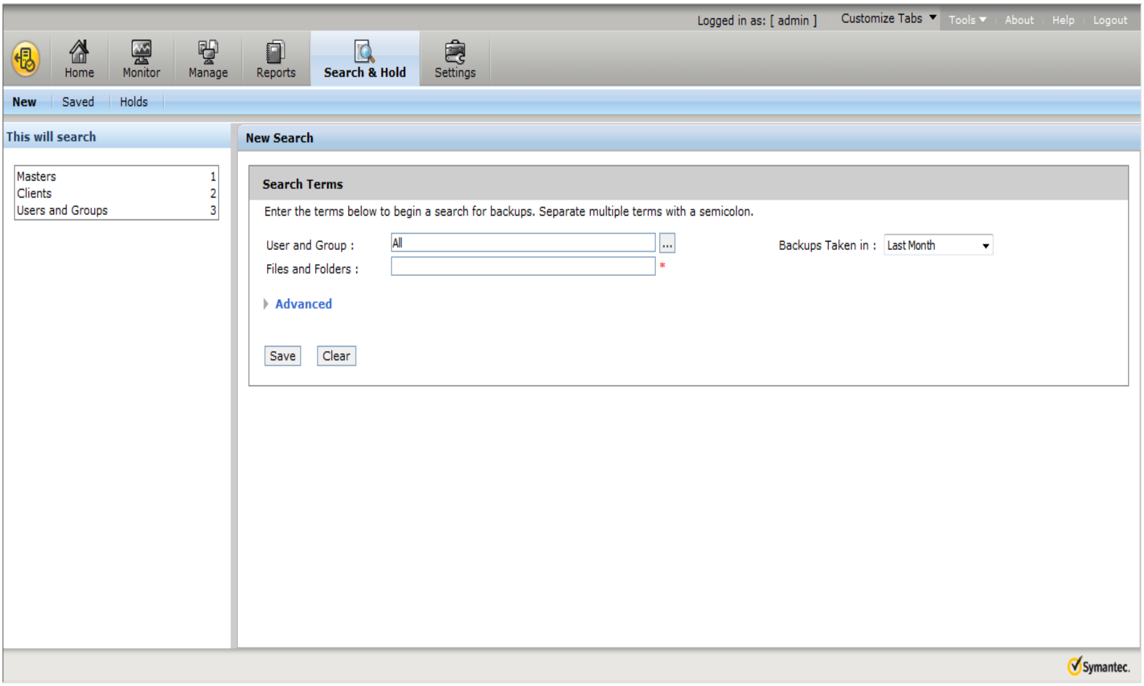
The data includes personal files, legal files, administration files, and much more. To remove the legal files, you may have to look through numerous NetBackup storage servers to find the files on which you applied the hold. This leads to another problem; are you sure that there are no other holds applied 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



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

User and Group : All

Files and Folders :

Backups Taken in : Last Month

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:

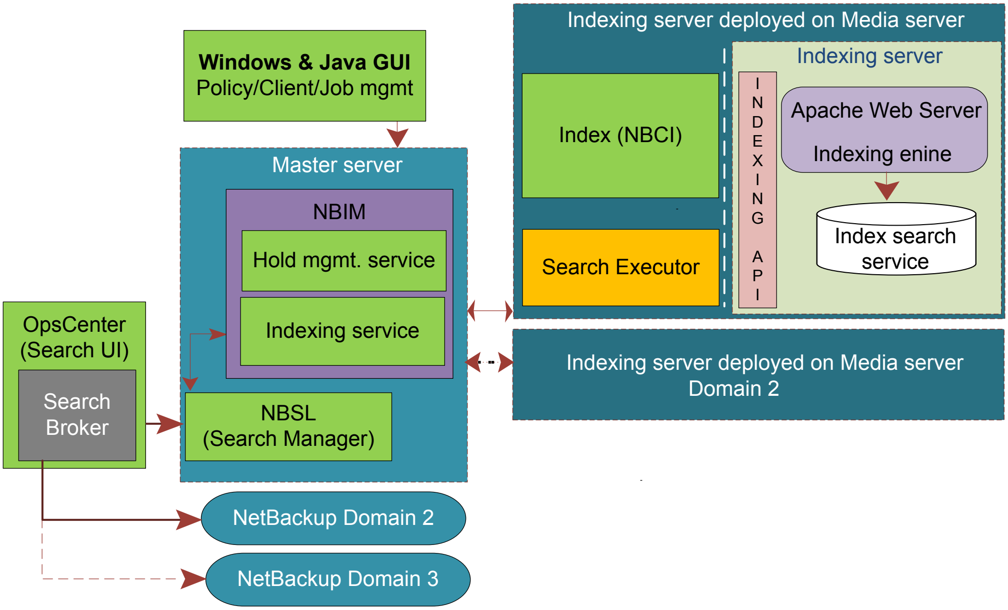
Table 1-1 NetBackup Search components

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 media server. The indexing engine and the Search executor run on indexing 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 in OpsCenter only if you have added a valid NetBackup Search license key in OpsCenter and you log on as a Security Administrator.)
Search Broker	The Search Broker allows search requests to search across multiple NetBackup domains.

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

Component	Description
Reports	From the OpsCenter **Reports** tab, you can view hold reports. The Hold reports are visible only if you have added a valid NetBackup Search license key in OpsCenter and when you log on as a Security Administrator.
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.

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.

Chapter 2

Installation and Configuration

This chapter includes the following topics:

Installing NetBackup Search

The following deployment scenarios are supported for NetBackup Search in the NetBackup 7.5 release:

- Indexing server

  The NetBackup indexing server must be installed on a NetBackup media server. The indexing server is supported only on Windows 2008 R2 (x64) systems. The Indexing server can support Pure IPv6 if it is 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 NetBackup Administrators guide.

- Search user interface

  The NetBackup Search user interface (UI) is installed as part of Symantec OpsCenter 7.5. No separate installation is needed.

- Holds management

  The NetBackup holds management software is installed as part of a NetBackup 7.5 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 21.

The following functions are not supported for NetBackup Search in the NetBackup 7.5 release:

- Upgrade of an existing NetBackup installation to version 7.5 is not included in these instructions. See the main documentation for instructions for installing NetBackup 7.5 for information about upgrading an existing NetBackup installation to version 7.5.

Deployment configurations:

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

  Host 1: NetBackup master server + NetBackup media server + 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 + 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 that is obtained by the SIS (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 7.5 release

Step	Description
1	Install a NetBackup 7.5 master server.

Table 2-1 Overview of the installation and configuration of NetBackup Search in the NetBackup 7.5 release *(continued)*

Step	Description
2	Install and identify a NetBackup 7.5 media server.
3	Install the NetBackup 7.5 indexing server on a media server.
4	Install Symantec OpsCenter.
5	Configure NetBackup Search in the NetBackup domain.

To install a NetBackup 7.5 master server

1. Install the master server using the NetBackup 7.5 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 7.5 media server

1. Install the media server using the NetBackup 7.5 installation package.

   Refer to the main documentation for instructions for installing a master 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.

To install the NetBackup 7.5 indexing server on a media server

1 Install the indexing server using the NetBackup 7.5 installation package. Select **Search Software Installation** from the main menu of the NetBackup installation wizard.

2 Follow the prompts that the installer presents to install the indexing server on the NetBackup media server.

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 29.

To install Symantec OpsCenter

1 Install Symantec OpsCenter using the NetBackup 7.5 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 configure NetBackup Search in the NetBackup domain

1 Add the indexing server to the NetBackup domain.

See “ Adding indexing servers” on page 29.

2 Provide a schedule for indexing server.

See “Modifying indexing server schedules” on page 30.

3 Configure the indexing server in a policy.

See “Configuring an indexing server in a policy” on page 31.

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 names to `bp.conf` on UNIX or on the Windows registry. Refer to the following scenarios while running NetBackup Search in a clustered environment:
  For NetBackup cluster mode, the Search Broker server list must contain the name of each NetBackup node in the cluster and the virtual server of NetBackup cluster. 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 NetBackup Master Server is Clustered and OpsCenter is Non-Clustered:
    Nodes of NetBackup Master Server: NBU_Node1, NBU_Node2
    Virtual Name: NBU_Virtual
    You must add the NBU_Node1, NBU_Node2, and NBU_Virtual at following location:
    On Windows OpsCenter:
    `HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\SearchBroker\CurrentVersion\Config\Server`
    On UNIX OpsCenter:
    `/opt/SYMCSearchBroker/bp.conf`
  - 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`
  - If NetBackup and OpsCenter both are clustered:

Nodes of NetBackup Master Server: NBU_Node1, NBU_Node2

Virtual Name: NBU_Virtual

You must add the NBU_Node1, NBU_Node2, and the NBU_Virtual on each node of OpsCenter at the following location:

On Windows OpsCenter:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\SearchBroker\CurrentVersion\Config\Server
```

On UNIX OpsCenter:

```
/opt/SYMCSearchBroker/bp.conf
```

Nodes of OpsCenter: OpsC_Node1, OpsC_Node2

Virtual Name: OpsC_Virtual

You must add the OpsC_Node1, OpsC_Node2, and the OpsC_Virtual on each node of NetBackup 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 NetbackupIndexingEngine 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.

About protection of the indexing servers

The procedures to protect a NetBackup indexing server uses tools, techniques, and practices available in NetBackup. As such, it assumes a certain level of familiarity with administration of the product.

For information about the protection of indexing servers, refer to the following document:

Indexing Server Protection

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

- Configuring a backup policy for protecting indexing servers
- Running the backup of an indexing server
- Restoring the index database from a backup

The document also includes recommended best practices for most common scenarios as well as some alternative practices in non-standard scenarios.

Chapter 3

Indexing Management

This chapter includes the following topics:

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 7.5 indexing server.

To index the backup image files, use the base command `nbindexutil` with the command `[-add]` or `[-list]` or `[-remove]` to perform the required operation. You can use the command `nbindexutil -help` with the command add or list or remove to view the help for that command. For example: enter the command `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
`-bid <Backup ID> | -bid_file` <name of the file that contains the backup IDs>	Enter the Backup ID with bid or path of the file containing Backup IDs with bid_file
`-indexserver <Indexing Server Name>`	Enter the indexing server Name, it is required for adding the images for indexing.
`[-force]`	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.
`[-operation <Operation ID>]`	Select 1 for adding a new image or 2 for deleting a selected image. By default 1 is selected. **Note:** The -Indexserver option is not applicable for Delete operation.
`[-priority <Priority>]`	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
`-inprogress|`	Lists all the images for which indexing is in progress.
`-waiting|`	Lists all the images which are in a queued state for indexing.
`-indexed`	Lists the indexed images.
`-failed`	Lists the image(s) for which indexing has failed.
`-indexserver <Indexing Server Name>`	Enter the indexing server Name.
`[-out <Filepath>]`	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
`-bid <Backup ID>| -bid_file` <name of the file that contains the backup IDs>	Enter the Backup ID with the bid or path of the file containing Backup IDs with bid_file

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`.

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.
- `MAX_INDEXING_JOBS` parameter in `bp.conf`
  This parameter 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 as its services NBIM and bpdbm play an important role in indexing jobs and performing the search operation. NBIM service initiates the indexing jobs (nbci), 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.

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 Windows 2008 R2 media server system.
  This system is your indexing server.

To add an indexing server from the NetBackup Administration Console:

1 From the task panel click **Host Properties** > **Media Servers**.

The media servers are listed in the details panel.

Note: Select a media server that is configured with Windows 2008 R2 and has the NetBackup Search installed on it. You can set the media server as the indexing server.

If required, you can add multiple indexing servers by selecting the media servers that meet the prerequisites.

2 From the Menu, click **Actions** > **Configure Index Servers** or click **Host Properties** > **Indexing Servers**

The **Choose Index Server** window opens.

3 Enter the name of the media server you selected as the indexing server. Click **OK**.

Note: If while adding indexing server with a short name fails, try with its fully qualified domain name. It is recommended to use the same name for the configuration of the media server and the indexing server.

You have to create a schedule for the index server. See “Modifying indexing server schedules” on page 30.

Modifying indexing server schedules

You can view and modify the properties of the configured indexing server from the **Indexing Server Properties** window. The **Indexing Server Properties** window opens after you add the index server.

Note: You can only view the configuration properties and modify the schedule of the indexing server.

The properties of the indexing server are provided in the details panel.

To modify the schedules, click **Schedules**, a list of schedules is provided. You can view or delete these schedules or add a new schedule. The following points help you to view or delete schedules from the **Indexing Server Properties** window:

- Select a schedule and click **Properties** to view its properties.

- Select a schedule and click **Delete** to delete the schedule of the indexing server.

You can add and modify a new schedule from the **Add New Schedule** wizard as follows:

To add and modify a new schedule:

1 Click **New**. The **Add New Schedule** wizard opens.

2 Under **Attributes** enter the name of the schedule. Click **OK**.

You can select **Calendar** to determine the specific days to run a policy. The **Calendar Schedule** tab displays. Under the **Calendar Schedule** tab you can schedule the days to run a task by indicating specific dates, recurring weekdays, recurring days of the month.

For more information, see the **Calendar Schedule** chapter of the NetBackup Administrator's Guide, Volume I.

3 Click **Start Window** tab.

You have to set the time periods during which NetBackup can start indexing using a schedule. Click **OK**

You can exclude the specific dates from a schedule by clicking the **Exclude Dates** tab. 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. After you exclude the dates, click **OK**.

You have successfully added and modified the schedule.

If a schedule is not available or not added to an index server then the indexing server becomes non-operational. However, you cannot remove an index server that is configured to a media server or master server.

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. From the **Add New Policy** wizard, you must select the **Enable indexing for search** option on the **Attribute**, **Schedule**, and **Clients** tabs.

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 From **Add New Policy > Attributes**, select **Enable indexing for search**.

From the **Indexing Server** drop-down list, select the required indexing server.

2 Click **Schedules** > **New**. The **Add New Schedule - Policy <policy_name>** window opens. Select **Enable indexing for search**, and click **OK**.

3 Click **Clients > New**. The **Client Hardware and Operating System** window opens. Select **Enable indexing for search**, and click **OK**.

4 Click **OK** on the **Add New Policy** window.

Decommissioning an indexing server

This procedure explains how to decommission an indexing server. You may need to decommission an indexing server to install software updates or to migrate an indexing server to another server.

This procedure also contains a reference to the procedures to decommission a media server. If you want to decommission a media server on which you have installed an indexing server, you must decommission the indexing server first.

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 Ensure that no indexing jobs are scheduled on the indexing server that you want to decommission.

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

- Select the indexing server that you want to decommission.
- Select **Properties > Schedules**.

  To decommission the indexing server while indexing schedules are active, suspend indexing for indexing server. From a command prompt, issue the following command:

  ```
  nbindexutil -suspend -indexingserver <index 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. If you choose to proceed with decommissioning the indexing server before jobs complete, those jobs will fail.

2 Delete all indexing schedules for the indexing server.

From **Properties > Schedules** on the NetBackup Administration Console, select all indexing schedules and click **Delete**.

3 To migrate the indexing server to a different indexing server, complete the following steps:

- Back up existing images that are indexed on the indexing server that you want to decommission. From a command prompt, issue the following commands:

  ```
  nbindexutil -list -indexserver <index server name> -waiting
  -out<output file path>
  ```

  ```
  nbindexutil -list -indexserver <index server name> -inprogress
  -out<output file path>
  ```

  ```
  nbindexutil -list -indexserver <index server name> [-date_from
  mm/dd/yyyy [HH:MM:SS]] [-date_to mm/dd/yyyy [HH:MM:SS]] -out
  <output file path>
  ```

  ```
  nbindexutil -list -indexserver <index server name> -failed
  [-date_from mm/dd/yyyy [HH:MM:SS]] [-date_to mm/dd/yyyy
  [HH:MM:SS]] -out <output file path>
  ```

  The date must be later than January 1, 1970. To list the images indexed after January 2,1970, you can give the following command on indexing server `hpindexSever. nbindexutil -list -indexed -indexserver hpindexSever -date_from 01/02/1970.`

  Note: If you do not specify the date for `-indexed` and `-failed` options , `nbindexutil`lists the images that were indexed or failed to index on that day. It is recommended to give `-date_from` option with an older date.

- Back up all backup policy names. From a command prompt, issue the following command:

  ```
  nbindexutil -listpolicies -indexserver <index server name>
  -out <ouput file of policy names>
  ```

After you successfully decommission the indexing server, you can complete the migration to the new indexing server.

Note: As per the migration process, you have to submit the Backup Ids for Indexing or re-Indexing on another Index Server. It does not migrate the indexed data.

See step 8 for more instructions.

4 Remove indexing server references from the master server. From a 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.

If this command fails with an error, rerun the command to ensure cleaner removal of the indexing server references.

5 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>
  ```

- 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
  ```

- Ensure that the indexing server no longer appears on the indexing server list.
  From the NetBackup Administration Console, select **Host Properties > Indexing Servers**.
  Select **Refresh All** from the **View** menu.
  Confirm that the indexing server is not listed.

6. Uninstall the NetBackup Search software using the NetBackup Installation and Configuration Wizard.

7. To decommission the media server, see the following topics in *Symantec NetBackup Administrator's Guide, Volume I, Release 7.5, Chapter 6: Managing Media Servers*:

   - *About decommissioning a media server*
   - *Decommissioning a media server*

8. To complete the migration to another indexing server, complete the following steps:

   - Re-index the images that you backed up in step 3. From a command prompt, issue the following command:

     ```
     nbindexutil -add -bid_file <filename> -indexserver <index server name>
     ```

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

     The `bid_file` should contain backup IDs separated by a newline character. For example, the command may provide the following output:

     ```
     clmachine1_1091560981
     clmachine1_1091560997
     clmachine1_1091561013
     clmachine1_1091561029
     clmachine1_1091561045
     ```

   - From the NetBackup Administration Console, enable indexing in the policies that you backed up in step 3.

Chapter 4

Search Queries

This chapter includes the following topics:

About searches queries

Use NetBackup Search to search for data in indexed backups. Backed up data is searched based on the criteria that you provide in the query page.

More information is available:

See "Searching for indexed backups" on page 38.

See "Editing a saved search query" on page 44.

See "Running a saved search" on page 46.

See "Viewing search results" on page 47.

See "Deleting a saved search" on page 48.

See "Deleting search results" on page 48.

Searching for indexed backups

To create a new search for data in indexed backups

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

Make sure that index data collection has completed. 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. 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 41.

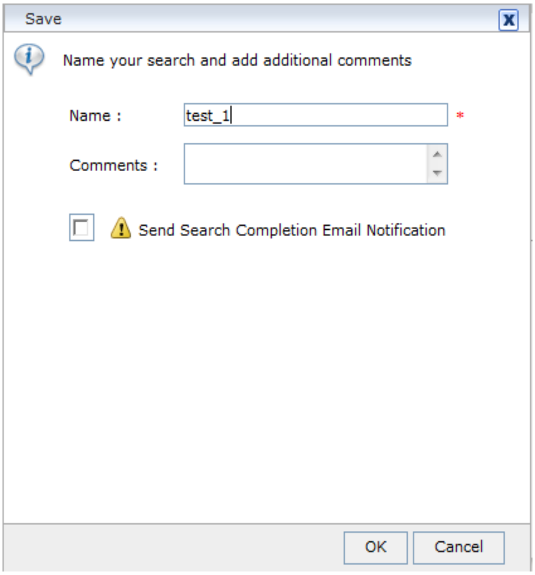
See “About using wildcard characters in a search” on page 43.

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** 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**


Save

Name your search and add additional comments

Name : test_1 *

Comments :

□ Send Search Completion Email Notification

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.

More information is available:

See “Editing a saved search query” on page 44.

See “Running a saved search” on page 46.

See “Viewing search results” on page 47.

See “Deleting a saved search” on page 48.

See “Deleting search results” on page 48.

Search terms

Table 4-1 Field descriptions for New Search - Search Terms

Field	Description
Users and Groups	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. 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". To include all users and groups on the displayed page, select the checkbox at the top of the left-most column.
Backups Taken in	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.
Files and Folders	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: ■ 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"** These criteria are required for a valid search.
Advanced	Click this link to display the advanced search criteria.

Table 4-1 Field descriptions for New Search - Search Terms *(continued)*

Field	Description
Domain **Views**	Choose to search Domains or Views: ■ 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)	Click the ellipses to select the names of the NetBackup master servers you want to include in this search. Separate multiple names with semicolons. 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". From the **Version** drop-down list, select a version number to find the master servers that are running a specific version of NetBackup.
Name **Note: (Views** selection only)	Click the ellipses to select the names of the views you want to include in this search.
Clients **Note: (Domain** selection only)	Click the ellipses to select the names of the clients you want to include in this search. Separate multiple names with semicolons. 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". To view clients on other master servers and select them if required for this search, select the **Master Servers** from the drop-down list.
File Type	Select one or more of the following file types to include in the search: ■ Excel Spreadsheets (`xls` and `xlx`) ■ PDF Documents (`pdf`) ■ PowerPoint Presentation (`ppt` and `pptx`) ■ Text Files (`txt` and `rtf`) ■ Word Documents (`doc` and `docx`) ■ (Other) / Specify . Use a semicolon to specify multiple file types; for example: `exe;png;mp3` and so on. Separate multiple values with semicolons.

Table 4-1 Field descriptions for New Search - Search Terms *(continued)*

Field	Description
File Created	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.
File Modified	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 **Backups Taken in**, **File Created**, and **File Modified** fields, the valid date options 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.

More information is available:

See "About using wildcard characters in a search" on page 43.

See "Searching for indexed backups" on page 38.

See "Editing a saved search query" on page 44.

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 querry ?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.

More information about searches is available:

See "Searching for indexed backups" on page 38.

See "Search terms" on page 41.

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. Click the **Name** of the saved search that you want to edit.
3. Make the changes you want to the criteria for the search. Detailed information about the search terms is available:

   See "Search terms" on page 41.

   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.

4 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.

More information is available:

See "Searching for indexed backups" on page 38.

See "Running a saved search" on page 46.

See "Viewing search results" on page 47.

See "Deleting a saved search" on page 48.

See "Deleting search results" on page 48.

Running a saved search

To run a saved search

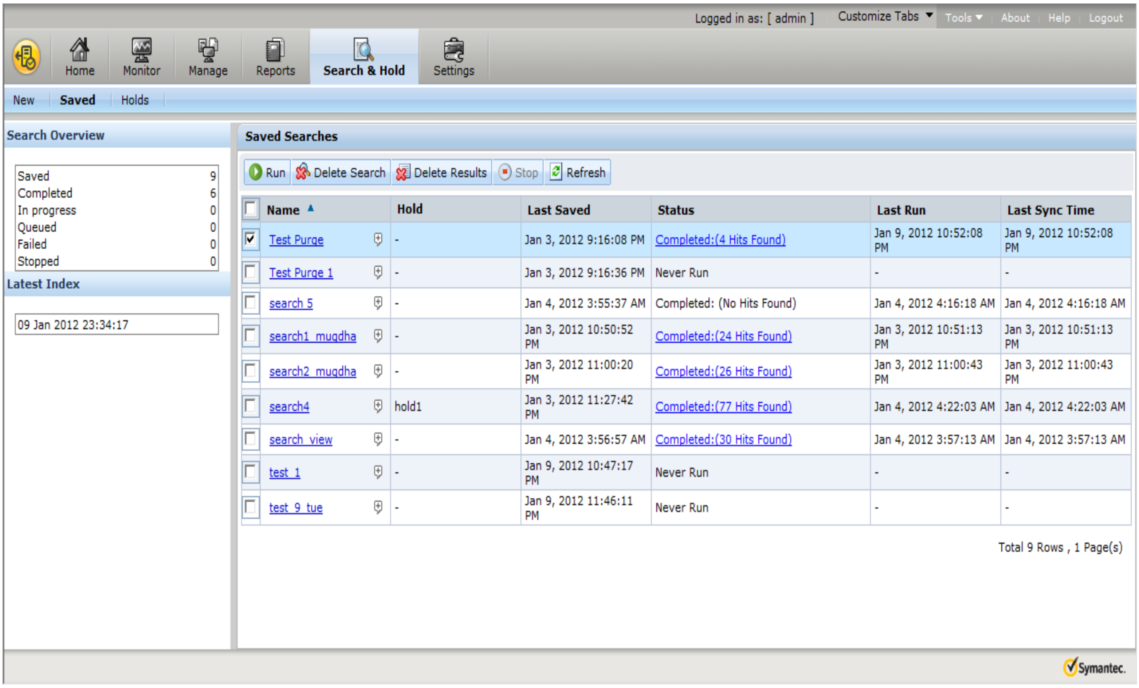
1. From the OpsCenter interface, select **Search & Hold > Saved** to view the list of saved searches.
2. Select the saved search you want to run. You may select multiple searches from the list.

> **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.

3. 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



Saved	9
Completed	6
In progress	0
Queued	0
Failed	0
Stopped	0

09 Jan 2012 23:34:17

☐	Name ▲	Hold	Last Saved	Status	Last Run	Last Sync Time
☑	Test Purge	-	Jan 3, 2012 9:16:08 PM	Completed:(4 Hits Found)	Jan 9, 2012 10:52:08 PM	Jan 9, 2012 10:52:08 PM
☐	Test Purge 1	-	Jan 3, 2012 9:16:36 PM	Never Run	-	-
☐	search 5	-	Jan 4, 2012 3:55:37 AM	Completed: (No Hits Found)	Jan 4, 2012 4:16:18 AM	Jan 4, 2012 4:16:18 AM
☐	search1 mugdha	-	Jan 3, 2012 10:50:52 PM	Completed:(24 Hits Found)	Jan 3, 2012 10:51:13 PM	Jan 3, 2012 10:51:13 PM
☐	search2 mugdha	-	Jan 3, 2012 11:00:20 PM	Completed:(26 Hits Found)	Jan 3, 2012 11:00:43 PM	Jan 3, 2012 11:00:43 PM
☐	search4	hold1	Jan 3, 2012 11:27:42 PM	Completed:(77 Hits Found)	Jan 4, 2012 4:22:03 AM	Jan 4, 2012 4:22:03 AM
☐	search view	-	Jan 4, 2012 3:56:57 AM	Completed:(30 Hits Found)	Jan 4, 2012 3:57:13 AM	Jan 4, 2012 3:57:13 AM
☐	test 1	-	Jan 9, 2012 10:47:17 PM	Never Run	-	-
☐	test 9 tue	-	Jan 9, 2012 11:46:11 PM	Never Run	-	-

Total 9 Rows , 1 Page(s)

More information is available:

See "Searching for indexed backups" on page 38.

See "Editing a saved search query" on page 44.

See "Viewing search results" on page 47.

See "Deleting a saved search" on page 48.

See "Deleting search results" on page 48.

Viewing search results

To view search results

1. From the OpsCenter interface, select **Search & Hold > Saved** to view the list of saved searches.
2. 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.
3. 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.
4. To filter the backups in the search results, enable filter criteria 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, select the backups that you want to hold and then click **Hold**.

   More information about holds is available:

   See "Placing a hold on a backup image" on page 51.

More information is available:

See "Searching for indexed backups" on page 38.

See "Editing a saved search query" on page 44.

See "Running a saved search" on page 46.

See "Deleting a saved search" on page 48.

See "Deleting search results" on page 48.

Deleting 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 saved search you want to delete. You may select multiple searches from the list.
3. Click **Delete Search**.
4. 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.

More information is available:

See "Searching for indexed backups" on page 38.

See "Editing a saved search query" on page 44.

See "Running a saved search" on page 46.

See "Viewing search results" on page 47.

See "Deleting search results" on page 48.

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 saved search you want to delete. You may select multiple searches from the list.

3 Click **Delete Search Results**.

4 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.

More information is available:

See “Searching for indexed backups” on page 38.

See “Editing a saved search query” on page 44.

See “Viewing search results” on page 47.

See “Running a saved search” on page 46.

See “Deleting a saved search” on page 48.

Holds Management

This chapter includes the following topics:

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.

To place a legal hold on a backup image through OpsCenter

1. From the OpsCenter interface, select **Search > Saved**.
2. Find the saved search that contains the backup images that you want to hold.

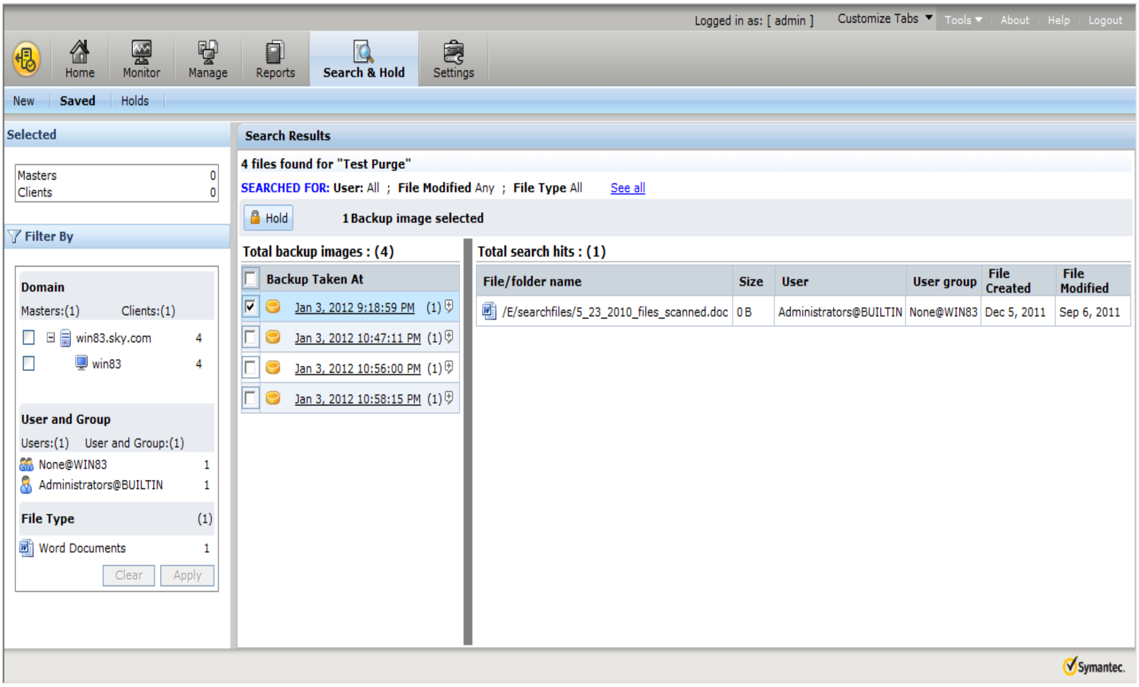
3 Click the **Completed** link in the **Status** column of the saved search.

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

---

4 From the **Backup Taken At** list, enable the checkboxes next to the backup images that you want to hold.

To select all backup images that are displayed on a page, enable 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.



Masters	0
Clients	0

Domain
Masters:(1) Clients:(1)

□	⊟ win83.sky.com	4
□	win83	4

User and Group
Users:(1) User and Group:(1)

None@WIN83	1
Administrators@BUILTIN	1

File Type (1)

Word Documents	1

4 files found for "Test Purge"

SEARCHED FOR: User: All ; File Modified Any ; File Type All See all

1 Backup image selected

Total backup images : (4)

□	Backup Taken At
☑	Jan 3, 2012 9:18:59 PM (1)
□	Jan 3, 2012 10:47:11 PM (1)
□	Jan 3, 2012 10:56:00 PM (1)
□	Jan 3, 2012 10:58:15 PM (1)

Total search hits : (1)

File/folder name	Size	User	User group	File Created	File Modified
/E/searchfiles/5_23_2010_files_scanned.doc	0 B	Administrators@BUILTIN	None@WIN83	Dec 5, 2011	Sep 6, 2011

5 Click **Hold**.

6 Provide the following information in the **Create Hold** dialog:

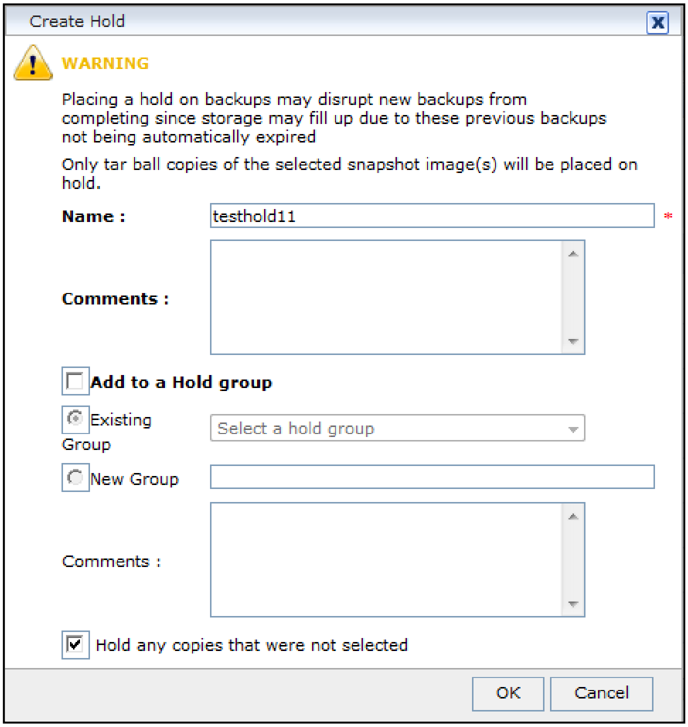
- Provide a unique **Name** for the hold. For example, you can name the hold so that it corresponds with an ongoing legal proceeding.
- Optionally, provide a description of the hold in **Comments**. Comments provide the reason for the hold for audit purposes.

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 14. 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

7 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
`-holdname` *`<hold name>`*	Enter a unique name for the hold.
`[-reason` *`<reason>`*`]`	Enter a description of the hold . The comment provides the reason for the hold for audit purposes. This option is optional.
`-filepath` *`<filepath>`* `| -backupid` *`<backup ID>`* `-primarycopy | -allcopy`	Specify the file path or the backup ID to the backup image. Also, include one of the following copy methods: ■ To include only the primary copy of the specified backup image, specify `-primarycopy` or `-p`. ■ To include all copies of the specified backup image, specify `-allcopy` or `-a`.

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
`[-holdname` *`<hold name>`*`]`	Enter the name for the hold. This option is optional.

`[-backupid` *`<backup ID>`*
`-primarycopy | -allcopy]`
	Specify the backup ID for the backup image.
	Also, include one of the following copy methods:
	■ To include only the primary copy of the specified backup image, specify `-primarycopy` or `-p`.
	■ To include all copies of the specified backup image, specify `-allcopy` or `-a`.
	This option is optional.

`[-U]`	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

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.

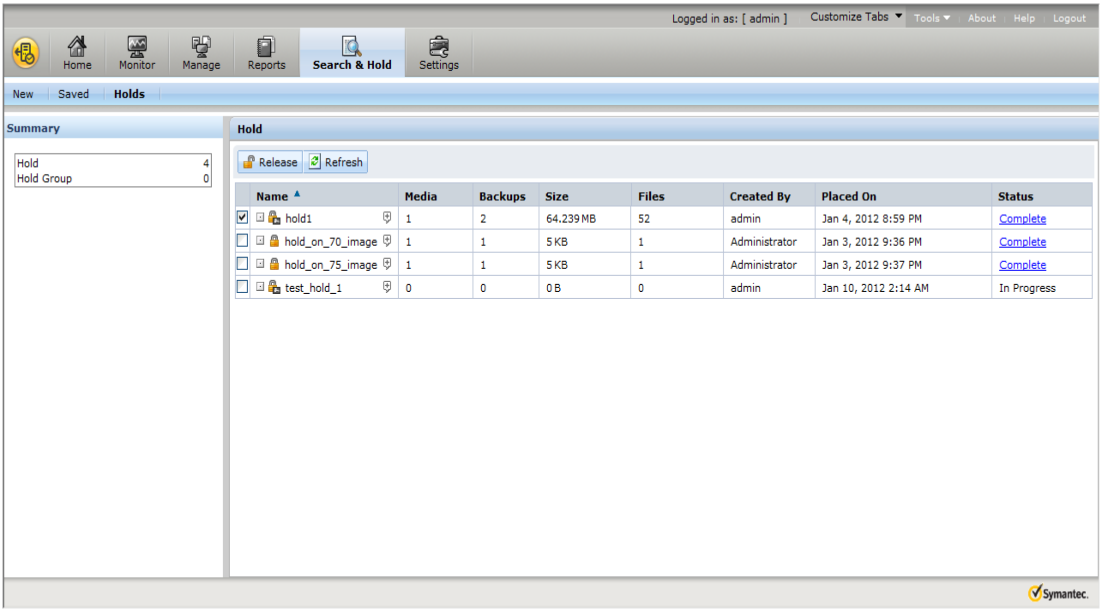
If a hold creation or hold deletion fails for any reason, click **Retry** to try the operation again after you resolve any issue that caused the failure.

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



Hold	4
Hold Group	0

	Name ▲	Media	Backups	Size	Files	Created By	Placed On	Status
☑	hold1	1	2	64.239 MB	52	admin	Jan 4, 2012 8:59 PM	Complete
□	hold_on_70_image	1	1	5 KB	1	Administrator	Jan 3, 2012 9:36 PM	Complete
□	hold_on_75_image	1	1	5 KB	1	Administrator	Jan 3, 2012 9:37 PM	Complete
□	test_hold_1	0	0	0 B	0	admin	Jan 10, 2012 2:14 AM	In Progress

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

To release a hold through OpsCenter

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

2 In the **Name** column, find the hold or the hold group that you want to release.

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

To view the details of the hold, click the plus sign after the hold name or the hold group name.

3 Select the holds or the hold groups that you want to release.

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

4 Click **Release**.

The following message appears:

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

Table 5-3 Options of `nbholdutil -delete` *(continued)*

Option	Description
`[-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 7.5 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.

For details about restoring data on hold and ingesting into Enterprise Vault, refer to the following document:

Restoring Data Under Legal Holds and Ingesting It into Enterprise Vault

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

Troubleshooting

This chapter includes the following topics:

Known Issues

The following are the known issues of NetBackup Search in the NetBackup 7.5 release:

- Indexing engine service does not start with the `bpup.exe` or when search is initiated.

  The NetBackup indexing engine service (webserver service) does not start or stop with `bpup` or `bpdown` CLI.

  Workaround: The NetBackup indexing engine service (webserver service) resides on the indexing server and starts when installation completes. If the indexing engine service does not start or stop by using the CLIs `bpup` or `bpdown`, start it manually.

  Note: If any service fails or restarts, the existing search operation fails. You have to restart the search operation to make it function with the current service.

- The NetBackup Search component crashes if antivirus software scans it while it runs an indexing job.

  Workaround: Exclude the NetBackup Search component directory from the antivirus scanning list.
- NetBackup Search does not currently support synthetic backups.

  Synthetic backups are not taken by the NetBackup Search directory.
- It takes a long time to view the last page of search results for backup images with large number of hits.

  The request may time out when you attempt to view backup images with approximately one million or more hits.
- Some of the indexing service processes continue to run even after you stop the NetBackup indexer service.

  Workaround: If you want to shut down all indexing services, you have to use the velocity-shutdown command present in the NetbackupSearch\bin folder.
- The indexing server is supported only on Windows 2008 R2. The indexing server must be installed and configured on a NetBackup media server.

  NetBackup Search supports master servers and OpsCenters servers on all of the platforms that NetBackup 7.5 supports.
- 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 Administrative Console. General information about access control is available in the *NetBackup Security and Encryption Guide*.
- 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.
- In NBAC mode, the catalog node on the NetBackup Administration Console shows incorrect statuses for hold and indexing.
- Occasionally, some indexing jobs may remain in progress for hours.
- On Linux VCS clusters, indexing schedules are not visible after saving. However, indexing performs properly.
- Indexing jobs may exit with the status 5028 (nothing to index) if there is no data to index in the backup image. This situation occurs when a backup image contains only special files such as device files.
- 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. The guest operating system is other than Windows and Linux.

  The scenarios are applicable for VMware and Hyper-V policy types.
- `NCFNBCI` generates 500GB of logs in 2 days.

  If `NCFNBCI` generates 500GB of logs in 2 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 32.
  - 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 67.

  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 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.

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 document provides the locations of the log files that are associated with NetBackup Search.

  Symantec NetBackup Search 7.5 Logging Information

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.*

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
   ```

   This command restarts the indexing engine.

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 67.

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 occours, 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
   ```

   This command restarts the indexing engine.
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 67.

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*.

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/or Hold columns are provided for certain reports. To retrieve information for indexing and/or hold column from the MFC UI and/or Java UI, you can use CLs for the following reports:

Table 6-1 CLIs for Java and/or MFC UI

Report	Column Absent	CLI for retrieving column information
Client Backups Report	Indexing and Hold	`bpimage.exe/bpimagelist.exe/bpimmeida.exe`
Images on media Report	Indexing and Hold	`bpimmeida.exe`
Tape Reports - Images on Tape Report	Indexing and Hold	`bpimmeida.exe`
Tape Reports - Tape Written Report	Hold	`bpmedialist.exe/nbemmcmd.exe`
Tape Reports - Tape Lists Report	Hold	`bpmedialist.exe/nbemmcmd.exe`
Disk Reports - Images on disk Report	Indexing and Hold	`bpimage.exe/bpimagelist.exe`

- Backup Policy Configuration Wizard

  In the Client List page the Indexing column is present in the Java UI and absent in the MFC UI.

- Backup Policy Attributes

  The short-cut key to **Enable indexing for search** is **I** on the Java UI and **X** on the MFC UI.

Index