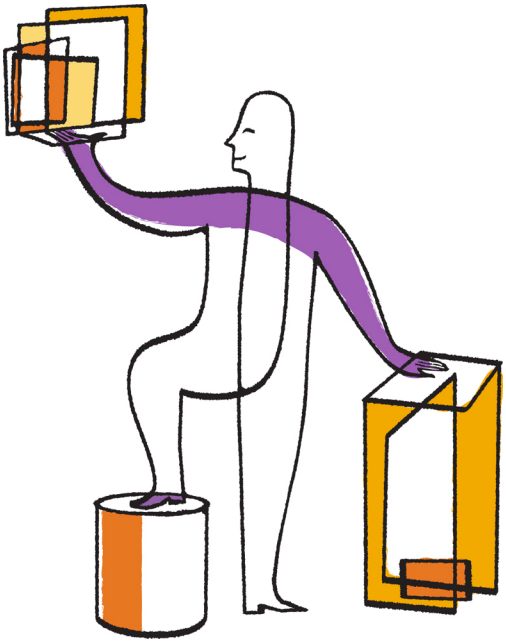
NetApp® Plug-in 1.1 for Symantec® NetBackup™

Installation and Administration Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-07096_B0
December 2013

Contents

Understanding NetApp Plug-in for Symantec NetBackup

In a Symantec NetBackup Replication Director environment, you can use NetApp Plug-in for Symantec NetBackup, an OpenStorage technology, to manage storage systems. The plug-in enables NetBackup to use Snapshot replication technologies to back up and replicate Snapshot copies between storage systems.

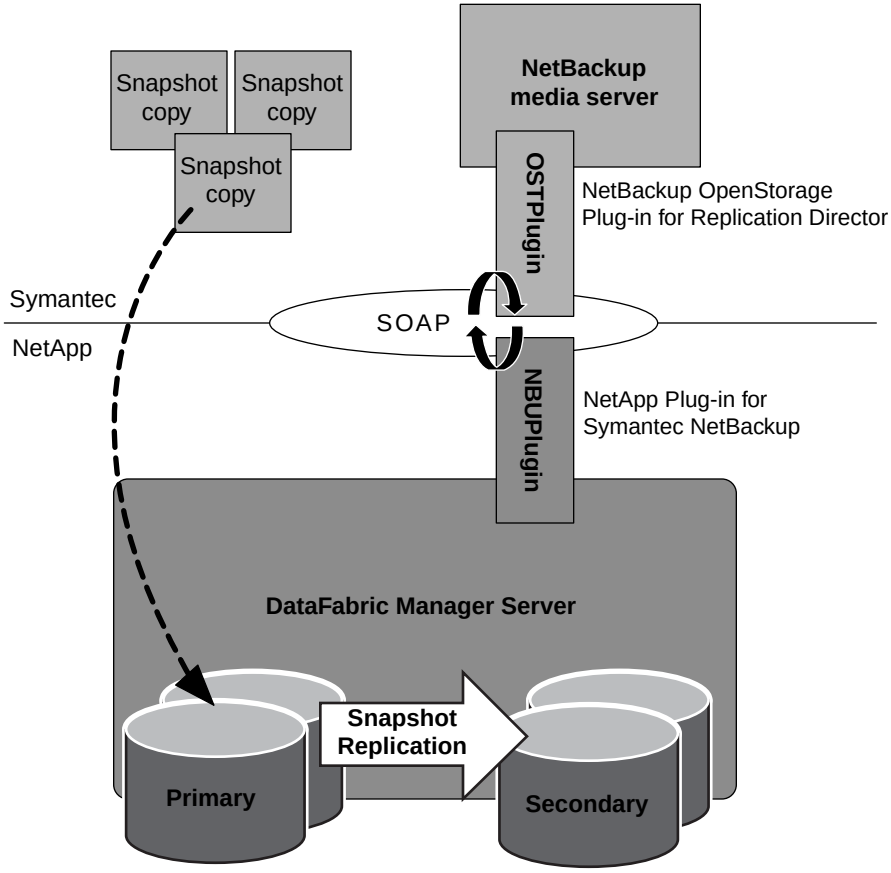
In the Replication Director environment, you must install the plug-in on the system that hosts the storage server. The DataFabric Manager server is configured as the storage server.

Overview of Replication Director

In a Replication Director environment, Symantec NetBackup uses NetApp Snapshot and replication technologies to provide incremental and unified data protection. NetBackup enables you to create storage lifecycle policies for unified protection of data from primary storage systems to secondary and tertiary storage systems.

Replication Director, a NetBackup OpenStorage backup environment, consists of a media server that accesses storage systems through the DataFabric Manager server. The NetBackup administrator configures the DataFabric Manager server as the storage server in NetBackup. The DataFabric Manager server hosts NetApp Plug-in for Symantec NetBackup.

The following illustration shows the components of a Replication Director environment:



The NetBackup media server communicates with the DataFabric Manager server through the NetBackup OpenStorage Plug-in for Replication Director (OSTPlugin) and NetApp Plug-in for Symantec NetBackup.

OSTPlugin uses XML-based messaging SOAP to communicate with the DataFabric Manager server. OSTPlugin is installed by default on the system in which NetBackup resides. For more information, see *Introducing NetBackup Replication Director* chapter in the *Symantec NetBackup Replication Director Solutions Guide*.

The DataFabric Manager server creates Snapshot copies on the storage systems and replicates the Snapshot copies to the secondary storage systems, based on the storage lifecycle policies configured in NetBackup. The Snapshot copies can also be replicated to a tertiary storage system or backed up to a tape device.

Related information

NetBackup documentation on the Symantec Site: www.symantec.com/docs/DOC5332

What Symantec NetBackup does

In a Replication Director environment, NetBackup enables you to implement end-to-end protection management by performing unified policy management, and Snapshot copy monitoring and management. The NetBackup media server also manages client backups by replicating Snapshot copies between storage systems.

NetBackup provides the following features:

- Unified policy management
  You can use the centralized backup infrastructure to manage the lifecycle of all the data.
- Snapshot management
  You can create Snapshot copies and Snapshot schedules, and configure the total number of copies to be created and the retention period for each Snapshot copy.
- Snapshot monitoring
  You can monitor the creation of Snapshot copies and view reports of the replication environment.
- Snapshot indexing
  You can index Snapshot copies and store in the NetBackup catalog for file search and granular restore.
- Managing replication relationships
  You can manage SnapMirror and SnapVault relationships and Snapshot copy retention as part of a NetBackup storage lifecycle policy.

During a data restore operation, NetBackup manages the transfer of data from the storage system to the client. You can restore data from a Snapshot copy that is managed by NetBackup from the primary, secondary, or tertiary storage systems. You can perform the following restore operations:

- File-level restore
  Individual file or directories are restored from the Snapshot copy.
- Volume-level restore
  A volume is restored from the Snapshot copy.

For more information see *NetBackup configuration* chapter in the *Symantec NetBackup Replication Director Solutions Guide*.

Related information

NetBackup documentation on the Symantec Site: www.symantec.com/docs/DOC5332

What the DataFabric Manager server does

In a Replication Director environment, the DataFabric Manager server enables you to provision and manage storage systems. The server presents the storage systems as resource pools to NetBackup. In

NetBackup, these resource pools are represented as volumes in disk pools and are used for creating storage lifecycle policies.

The DataFabric Manager server enables you to perform the following operations from NetBackup:

- Provision and manage secondary and tertiary storage systems.
- Create datasets and use resource pools to group storage systems.
- Create data protection policies to protect data on the primary, secondary, and tertiary storage systems.

Note: At any given time, a maximum of 100 on-demand backup jobs can run in the DataFabric Manager server. The subsequent jobs that are triggered are queued in NetApp Plug-in for Symantec NetBackup.

Introduction to NetApp storage

NetApp storage systems are hardware- and software-based data storage and retrieval systems. They respond to network requests from clients and fulfill them by writing data to or retrieving data from disk arrays. They provide a modular hardware architecture running the Data ONTAP operating system and WAFL (Write Anywhere File Layout) software.

Data ONTAP is the operating system for all NetApp storage systems. It provides a complete set of storage management tools through its command-line interface, through System Manager, and through remote management devices such as the Baseboard Management Controller (BMC), the Service Processor (SP), and the Remote LAN Module (RLM).

For information about all of the models of NetApp storage systems, see the NetApp Products page.

Related information

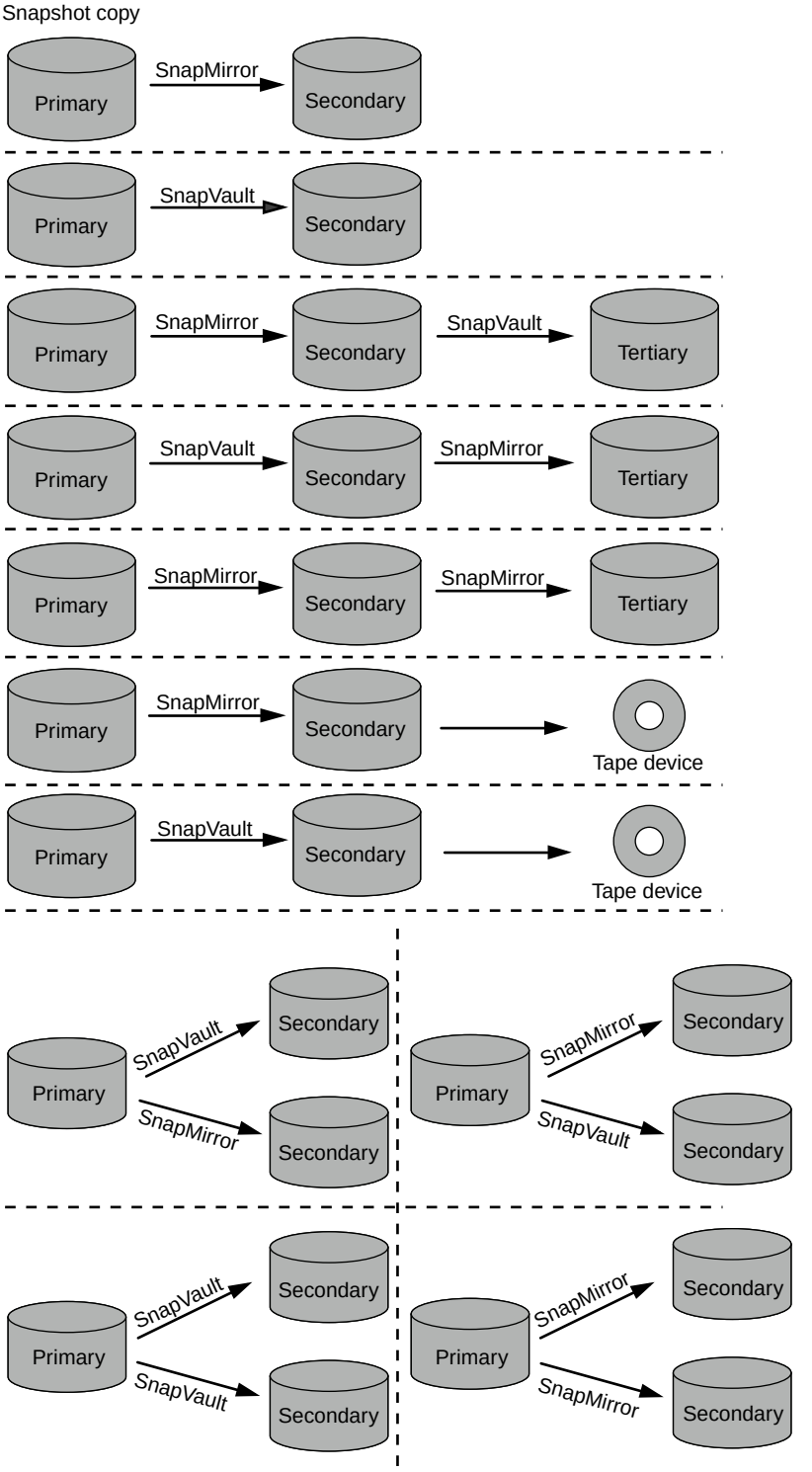
NetApp Support Site: support.netapp.com

Supported storage topologies

The Replication Director environment supports different storage topologies that enable you to establish a SnapMirror or SnapVault relationship between the storage systems.

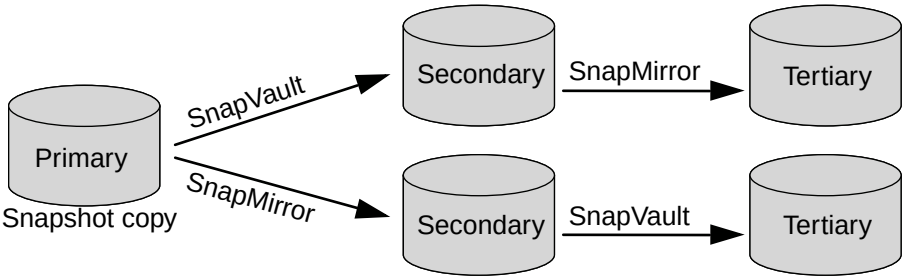
The Snapshot copies of the client data are stored on the primary storage tier. The primary Snapshot copy can be replicated to secondary and tertiary storage systems. You can also back up the Snapshot copies to a tape device from the primary, secondary, or tertiary storage system.

You can provision a backup policy to establish SnapMirror or SnapVault relationships to secondary and tertiary storage tiers by using any of the methods illustrated in the following image:


Snapshot copy
Primary
SnapMirror
Secondary
Primary
SnapVault
Secondary
Primary
SnapMirror
Secondary
SnapVault
Tertiary
Primary
SnapVault
Secondary
SnapMirror
Tertiary
Primary
SnapMirror
Secondary
SnapMirror
Tertiary
Primary
SnapMirror
Secondary
Tape device
Primary
SnapVault
Secondary
Tape device
Primary
SnapVault
Secondary
SnapMirror
Secondary
Primary
SnapMirror
Secondary
SnapVault
Secondary
Primary
SnapVault
Secondary
SnapMirror
Secondary
Primary
SnapMirror
Secondary
SnapVault
Secondary

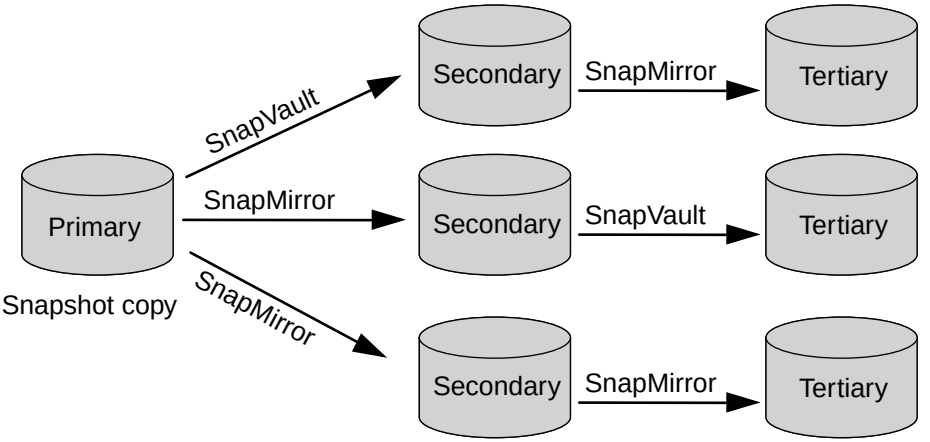
Two-way fanout topology

The following illustration displays a two-way fanout topology with cascade:



Three-way fanout topology

The following illustration displays a three-way fanout topology with cascade:



You can provision a three-way fanout topology with cascade using any combination of SnapVault and SnapMirror relationships in the different fanout paths. However, you cannot have SnapVault relationships from primary to secondary storage tiers and secondary to tertiary storage tiers in any of the fanout paths.

Data ONTAP features supported by Symantec NetBackup

Symantec NetBackup supports some of the Data ONTAP features, such as volume SnapMirror, Snapshot copies, SnapVault, SAN and NAS backup, and point-in-time restore operations for NAS backup. You can modify or disable scheduled updates to a particular volume or qtree.

Note: Symantec NetBackup does not support point-in-time restore operations for SAN backup.

For more information about the supported Data ONTAP features, see the Interoperability Matrix.

Related tasks

Viewing supported configurations in Interoperability Matrix on page 58

Related information

Interoperability Matrix: support.netapp.com/NOW/products/interoperability

How SnapMirror works with NetBackup

You can use SnapMirror to perform mirror type backups.

When using SnapMirror with NetBackup, you can perform the following operations:

- Create multiple paths for a SnapMirror relationship.
- Verify the status of data transfer to determine the status of all the existing SnapMirror relationships that are defined.

How SnapVault works with NetBackup

You can back up data from NetBackup by creating a SnapVault Snapshot copy on the secondary storage system.

When using SnapVault with NetBackup, you can perform the following operations:

- View a list of Snapshot copies to confirm which version of the primary qtree data is backed up.
- Restore data from the secondary storage system in the event of data loss on the primary storage system.
- Verify the status of an ongoing SnapVault transfer and abort it if there is a new Snapshot copy or if an immediate system restart or shutdown is required.
- Schedule Snapshot copy creation on the primary and secondary storage systems.

How SnapDrive works with NetBackup

You can use SnapDrive to automate storage provisioning tasks and to manage data in Microsoft Windows environments.

Following are the features provided when SnapDrive is used with NetBackup:

- Enable online storage configuration and LUN expansion.
- Enable connection of up to 168 LUNs.
- Integrate Data ONTAP Snapshot technology, which creates point-in-time images of data stored on LUNs.
- Enable SnapDrive management on multiple hosts.
- Enable SnapDrive support on Microsoft cluster configurations.
- Enable iSCSI or FC session management.

Support for multiple NICs

You can configure multiple NICs on a destination storage system and host IP address or host name on a source storage system to isolate redundant and different types of network traffic.

In some scenarios, different networks are used for isolating different types of network traffic. For example, a data replication job uses WAN network and tape backup job uses the local network. The NetBackup Replication Director enables you to configure the appropriate network to complete the job.

Note: The multiple NIC configurations are applicable only to NDMP policies.

NICs in the destination storage system

In a multiple NIC environment, you can configure the preferred interface on the destination storage system to specify the network to be used for exporting the backup images.

The preferred interface is applicable only to secondary or destination storage systems.

On the destination storage system, the `ndmpd.preferred_interface` option should be configured. When a request to export the backup image is received from NetBackup, the plug-in queries the destination storage system and returns the IP address or short host name or FQDN of destination host that is present for the `ndmpd.preferred_interface` option to NetBackup to access the image. An interface can have multiple IP addresses, and the first IP address received from the destination storage system is provided to NetBackup.

If the `ndmpd.preferred_interface` option is not configured, the plug-in returns the FDQN of the host provided by the DataFabric Manager server.

If the `ndmpd.preferred_interface` option is configured and the plug-in is unable to get the FDQN for the preferred interface, then the IP address of the preferred interface is returned.

NICs in the source storage system

When a request to access the source data is received from NetBackup, the plug-in returns either the host IP address or host name that is configured in NetBackup. Therefore, the IP address used to configure the storage system in NetBackup should be appropriately chosen in case of multiple NICs.

Setting up the Replication Director environment

Before you start working in the Replication Director environment, you must understand the setup workflow of the environment. The workflow includes installing OnCommand Core Package, NetApp Management Console, NetApp Plug-in for Symantec NetBackup, and Symantec NetBackup; adding destination systems and resource pools; and configuring NetBackup.

About this task

During the NetApp Plug-in for Symantec NetBackup installation, the default values of the DataFabric Manager server parameters are changed to new values for optimal use of DataFabric Manager server in Replication Director environment. You should be aware of the *changed values* on page 18.

You should not change the parameters to their default values.

Steps

1. Install OnCommand Core Package on a Windows or Linux host.

   You should use the DataFabric Manager server only for the Replication Director environment.

   For more information about installing OnCommand Core Package, see the *OnCommand Unified Manager Installation and Setup Guide*.

2. Install *NetApp Management Console* on page 16 on a Windows or Linux host.
3. Install *NetApp Plug-in for Symantec NetBackup on a Windows host* on page 32 or *NetApp Plug-in for Symantec NetBackup on a Linux host* on page 33 on which OnCommand Core Package is installed.

   Note: If the DataFabric Manager server services are not running during the installation of the plug-in, then you must run the `create-group` script manually after starting the DataFabric Manager server services.

   You should not delete objects that are created by the plug-in in the DataFabric Manager server to avoid potential issues.

4. Install Symantec NetBackup, if you have not done so already.

   For more information, see the *Symantec NetBackup Replication Director Installation Guide*.

5. Install SnapDrive for Windows SAN support on NetBackup client.

   For more information, see the *Symantec NetBackup Replication Director Solutions Guide*.

6. Use the NetApp Management Console to perform the following tasks in the DataFabric Manager server:

   a) *Add destination storage systems* on page 17.

b) *Add resource pools* on page 18.

Note: You must ensure that you do not name the resource pool as `NetBackup`.

7. Add all the resource pools to NetBackup groups by using NetApp Management Console.

   When the plug-in is installed on the DataFabric Manager server, a NetBackup group is automatically created on the DataFabric Manager server. You should use the NetApp Management Console to add the resource pools to the NetBackup group so that the resource pools can be detected by NetBackup. If the NetBackup group contains no resource pools, no logical storage units (LSUs) are displayed in the disk pool configuration wizard.

8. Configure NetBackup by adding the storage server, disk pools, storage unit, storage lifecycle policies, and backup policies.

   For more information, see the following information in the *Symantec NetBackup Replication Director Solutions Guide*:

   - Adding the storage server credentials to a NetBackup server
   - Configuring disk pools for snapshot and replication
   - Creating a storage unit example
   - Creating a storage lifecycle policy example
   - Configuring backup policies to create snapshots and snapshot replication

Related information

NetBackup documentation on the Symantec Site: www.symantec.com/docs/DOC5332
NetApp Support Site: support.netapp.com

Important cautions

You need to be aware of the important cautions to identify and resolve issues that might affect the operation of NetApp Plug-in for Symantec NetBackup.

You must ensure that the following conditions are met:

- A resource pool should not be named `NetBackup` or `PrimarySnapshot` to avoid potential issues.
- The resource pool name should not contain non-ASCII characters.
- In a volume or qtree, file names protected by NetBackup should not contain non-alphanumeric (special) characters such as the at sign (@), asterisk (*), and number sign (#).
- Use the same language settings for root volume on source and destination storage systems.
- Enable the volume language setting using UTF-8 so that the correct language format is used for the NAS data.
- When a volume is specified as backup selection in NetBackup, the name of the volume should not end in a forward slash.
  The volume name is listed in the Backup Selections tab of a NetBackup policy. For example, /vol/volA is correct; however, /vol/volA/ or /vol/volA// is incorrect.

Installing NetApp Management Console

You can download and install NetApp Management Console through the OnCommand console. NetApp Management Console is required to perform many of your physical storage tasks. You must install NetApp Management Console 3.3, which contains bug fixes found in the 3.2 version.

Before you begin

You must be authorized to perform all the steps of this task; your RBAC administrator can confirm your authorization in advance.

About this task

During this task, the OnCommand console launches the Operations Manager console. Depending on your browser configuration, you can return to the OnCommand console by using the Alt-Tab key combination or clicking the OnCommand console browser tab. After the completion of this task, you can leave the Operations Manager console open, or you can close it to conserve bandwidth.

Steps

1. Log in to the OnCommand console if necessary.
2. Click the **File** menu, and then click **Download Management Console**.

   A separate browser tab or window opens to the Management Console Software page in the Operations Manager console.
3. Click the download link for the Linux or Windows installation.
4. In the download dialog box, click **Save File**.

   The executable file is downloaded to your local system, from the system on which the OnCommand Core Package was installed.
5. From the download directory, run the `nmconsole-setup-xxx.xxx` executable file.

   The NetApp Management Console installation wizard opens.
6. Follow the prompts to install NetApp Management Console.

Result

After installation, you can access NetApp Management Console from the following locations:

- On Windows systems, the default installation path is `C:\Program Files\NetApp \Management Console`.

  You can launch the console from the NetApp directory on the Start menu.
- On Linux systems, the default installation path is `/usr/lib/NetApp/management_console/`.

  You can launch the console from `/usr/bin`.

Related tasks

Setting up the Replication Director environment on page 14

Adding a storage system

You can add storage systems to the hosts list to make them available for inclusion in data management actions. When you add storage systems to NetApp Management Console, you also add the storage to the DataFabric Manager database.

Before you begin

Have the following information available for the storage system that you want to add:

- Host name or IP address
- Host credentials (user name and password)
- License code
- SnapVault Access Control List, if licensed for SnapVault
- SnapMirror Access Control List, if licensed for SnapMirror
- NDMP credentials (user name and password)

You must be authorized to perform all the steps of this task; your RBAC administrator can confirm your authorization in advance.

Steps

1. From the menu bar, click **Hosts > Storage Systems**.
2. Click **Add** to start the **Add Storage System** wizard.

   Enter or select information as requested in the wizard.

   Note: In this wizard, clicking Next implements the operations on each page. Clicking Back or Cancel does not undo operations performed on previous pages.
3. Verify that the storage system that you added is included in the hosts list in the **Storage Systems Hosts** window.

   You might need to update the window before you can view the new host in the host list.

Result

You can now manage data located on the new storage system or use the storage as a secondary storage system for backups or mirror copies.

Adding a resource pool

You can create resource pools from collections of unused physical storage resources. Resource pools are associated with one or more datasets, providing the physical resources for provisioning primary storage by using a provisioning policy and for backup or mirror protection on nonprimary nodes.

Before you begin

- The hosts you are adding to the resource pool must have the proper configuration and licensing for their intended use.
- You must have gathered the following information to complete this task:
  - Resource pool name (required)
  - Description (optional)
  - Owner (optional)
  - Contact email address for alerts (optional)
  - Time zone (optional)
  - Physical resources (required)
  - Resource pool label (optional)
  - Space thresholds (optional to modify the default)
- You must be authorized to perform all the steps of this task; your RBAC administrator can confirm your authorization in advance.

About this task

This task is performed from the NetApp Management Console.

Steps

1. From the menu bar, click **Data > Resource Pools**.
2. Click **Add** to open the **Add Resource Pool** wizard and then complete the wizard.
3. Verify the creation and content of the resource pool by viewing the results that are displayed in the **Resource Pools** window.

DataFabric Manager server parameters that are changed during the plug-in installation

The default values of the DataFabric Manager server parameters are changed to new values during the NetApp Plug-in for Symantec NetBackup installation for optimal use of DataFabric Manager

server in the Replication Director environment. You should be aware of the parameters that are changed, and their default and new values.

Parameters specific to the Replication Director solution

Parameter	Default value	New value
dpMaxFanInRatio	1	4
pmMaxSvRelsPerSecondaryVol	Not set	250
purgeJobsOlderThan	Jobs	30d
dpSrcVolUsedPct	Not set	100
perfAdvisorEnabled	Yes	No
snmpTrapListenerEnabled	Yes	No

The unit of measure “d” denotes day.

Interval monitoring parameters specific to the Replication Director solution

Parameter	Default value	New value
statusUpdateInterval	Not set	15m
cpuMonInterval	5m	1h
dpReaperInterval	30m	168h
dsConformanceMonInterval	1h	24h
dsProtectionMonInterval	15m	24h
opsMonInterval	10m	24h
shareMonInterval	1h	1d
snapMirrorMonInterval	30m	2h
snapshotMonInterval	30m	1h
snapvaultmoninterval	30m	2h
userQuotaMonInterval	1d	1w
ifMonInterval	15m	1d
diskMonInterval	4h	24h
sysInfoMonInterval	1h	8

The units of measure “w” denotes week, “d” denotes day, “h” denotes hours, and “m” denotes minutes.

Parameters not specific to Replication Director solution

Parameter	Default value	New value
respoolSpaceMonInterval	1h	0
vserverMonInterval	1h	0
agentMonInterval	2m	0
backupDirMonInterval	8h	0
ccMonInterval	4h	0
cfMonInterval	5m	0
clusterMonInterval	15m	0
envMonInterval	5m	0
hostRBACMonInterval	1d	0
perfAdvThreshViolationMonInterval	15m	0
SANHostMonInterval	5m	0
lunMonInterval	30m	0

These parameters, which provide monitoring capability, are not specific to Replication Director and are therefore turned off.

Requirements for setting up Replication Director

You must ensure that you meet all the requirements for setting up Replication Director using NetApp storage systems, DataFabric Manager server, and Symantec NetBackup.

NetBackup setup requirements

You must install and configure NetApp Plug-in for Symantec NetBackup and the storage systems before you configure NetBackup Replication Director to manage NetApp Snapshot copies and replication.

You must enable OpenStorage from the base NetBackup system. The NetBackup OpenStorage Disk Option license activates OpenStorage. For information about entering NetBackup licenses, see the *Symantec NetBackup Administrator's Guide, Volume I*.

Optionally, you can enable NDMP to configure NDMP policies or perform NDMP backup to tape.

For more information about setting up NetBackup Replication Director, see *NetBackup configuration* in the *Symantec NetBackup Replication Director Solutions Guide*.

Related information

NetBackup documentation on the Symantec Site: www.symantec.com/docs/DOC5332

License requirements

Before you use NetApp Plug-in for Symantec NetBackup, you must install licenses for each of the NetApp components. Your sales or support representative can provide you with license keys that you can use to enable certain features on your storage system.

You must install the following storage system licenses:

- SnapMirror license
  You must install the license key on both the source and destination storage systems in a SnapMirror relationship.
- SnapVault license
  You must install the SnapVault primary license key on the SnapVault primary storage systems and install the SnapVault secondary license key on the SnapVault secondary storage system.
- SnapRestore license
  You must install the SnapRestore license key on all the source storage systems where you want to enable fast, pointer-based FlexVol level restores from primary Snapshot copies. The SnapRestore license is also required on all SnapVault destination storage systems. Additionally, for the

Primary-SnapVault-SnapMirror (PVM) topology, you must install the license key on the SnapMirror destination.

- FlexClone license for NAS policies

  You must install the FlexClone license key on the secondary or tertiary storage system that contains the SnapVault destination volumes. Additionally, for the Primary-SnapVault-SnapMirror (PVM) topology, you must install the license key on the SnapMirror destination.
- FlexClone license for SAN policies

  You must install the FlexClone license on the primary or secondary storage system that is used for indexing, restoring, or performing a streaming (tar) backup of block data. For Snapshot copy only topology, the FlexClone license is not required for the primary storage system.
- CIFS license

  You must install the CIFS license key on the storage system that is in a SnapMirror and SnapVault relationship and contains the CIFS files.
- NFS license

  You must install the NFS license key on the storage system that is in a SnapMirror and SnapVault relationship and contains the NFS files.
- SnapDrive license

  You must install the SnapDrive license key either on the local host or on the storage system that is managed by SnapDrive.

  Note: SnapDrive license is required to manage data in a Windows server for storage systems in a SAN environment.
- iSCSI and FC licenses

  You must install either iSCSI or FC license keys in a SAN environment on both the source and destination storage systems.

License keys are provided on a per-system basis and have to be added on each system for features to work correctly.

Note: You can display the features that are currently licensed on the storage system by using the `license` command.

For more information about NetBackup licenses, see the *Symantec NetBackup Replication Director Solutions Guide*.

Related information

NetBackup documentation on the Symantec Site: www.symantec.com/docs/DOC5332

Enabling SnapMirror by entering license codes

Before any SnapMirror replication process can begin, you must add the SnapMirror license on the system and enable SnapMirror.

Step

1. To add the SnapMirror license code, enter the following command:

   `license add xxxxxxx`

   xxxxxxx is the license code you purchased.

Turning SnapMirror on

Before using SnapMirror you need to enable the SnapMirror license on both the source and the destination systems.

Steps

1. To turn SnapMirror on, enter the following command on both the source system and destination system:

   `options snapmirror.enable on`

   Alternatively, you can use the `snapmirror on` command to turn SnapMirror on.

   Note: This setting persists across reboots.

2. Depending on whether you use the `snapmirror.access` option or the `/etc/snapmirror.allow` file to specify allowed destinations, choose one of the actions from the following table:

If you choose...	Then...
`snapmirror.access` option	On the source, enter the following command as a single line: **`options snapmirror.access host=[dest_system1,dest_ system2,...]`** The default value for the `snapmirror.access` option is `legacy`, which lets the `/etc/snapmirror.allow` file define the access permissions. This option persists across reboots.
`/etc/snapmirror.allow` file	Add the names of the destination systems, each on a separate line, in the `/etc/snapmirror.allow` file.

Enabling SnapVault

You can set up SnapVault backup on the primary systems by preparing the primary storage systems and SnapVault secondary storage systems to perform their backup tasks.

You must install the SnapVault primary and SnapVault secondary licenses on the same storage system to use SnapVault to back up data to the same storage system. You must license and prepare your storage systems before you can use SnapVault to back up data.

Enabling licenses for SnapVault

You need to enable the appropriate licenses on the SnapVault primary and secondary systems. If you are using an HA pair, you must enable a SnapVault primary license on one node and a SnapVault secondary license on the other node.

Steps

1. To enter the SnapVault secondary system license code, on the system, enter the following command:

   `license add` ***`xxxxxxx`***

   xxxxxxx is the license code you purchased.

   This setting persists across reboots.

2. To enter the SnapVault primary system license code, on the system, enter the following command:

   `license add` ***`xxxxxxx`***

   xxxxxxx is the license code you purchased.

   This setting persists across reboots.

   For more information about entering license codes, see the information about licensing in the *Data ONTAP 7-Mode System Administration Guide*.

Enabling the snapvault.enable option

You can set the `snapvault.enable` option to `on` to perform SnapVault data transfers and to create Snapshot copies.

Before you begin

You must have entered the SnapVault primary system license code on the primary system.

Step

1. On primary systems, enter the following command:

```
options snapvault.enable on
```

This option persists across reboots.

Installing the SnapRestore license

You must install the license code before you can use SnapRestore.

Step

1. Install the SnapRestore license by entering the following command:

   ```
   license add license_code
   ```

Installing the FlexClone license

You must install the license code before you can use the FlexClone feature.

Step

1. Install the FlexClone license by entering the following command:

   ```
   license add license_code
   ```

Configuring CIFS licenses

To be able to set up and use CIFS functionality, your storage system must have a CIFS license installed. You can use the `license` command to configure licenses on the storage system.

Before you begin

You need to be sure that you have obtained a valid CIFS license from your sales or support representative.

Steps

1. Display the features that are currently licensed on the storage system by entering the following command:

   ```
   license
   ```

2. Perform one of the following actions:

If the CIFS feature...	Then...
Displays a license code	Your storage system is already licensed for CIFS and you do not need to take any further action.
Displays `not licensed`	Install a CIFS license by entering the following command: **`license add license_code`**

Configuring NFS licenses

To be able to set up and use NFS functionality, your storage system must have an NFS license installed. You can use the `license` command to configure licenses on the storage system.

Before you begin

You need to be sure that you have obtained a valid NFS license from your sales or support representative.

Steps

1. Display the features that are currently licensed on the storage system by entering the following command:

   `license`

2. Perform one of the following actions:

If the NFS feature...	Then...
Displays a license code	Your storage system is already licensed for NFS and you do not need to take any further action.
Displays `not licensed`	Install an NFS license by entering the following command: **`license add license_code`**

SnapDrive licensing

Your SnapDrive license can reside either on the local host or on the storage systems that you are using SnapDrive to manage.

If you choose to install SnapDrive with licensing per storage system rather than with a host-side license, you can execute SnapDrive operations only on storage systems that have a SnapDrive or SnapManager license installed.

Enabling the iSCSI license

You must enable the iSCSI license to use the iSCSI target service.

About this task

For Data ONTAP 7.3.x or 8.0.x, the following options are automatically enabled when the iSCSI service is turned on:

- `volume option create_ucode` is set to `on`
- `cf.takeover.on_panic` is set to `on`

You should not change these options.

Step

1. Depending on the Data ONTAP versions, choose the appropriate action:

If the system version is...	Then...
Data ONTAP 7.3.x or 8.0.x or 8.1.x	Add the iSCSI license by entering the following command: **`license add`** ***`license_code`***
Data ONTAP 8.2.x	• Enable the `iscsi` option by entering the following command: **`options licensed_feature.iscsi.enable on`** • Add the iSCSI license by entering the following command: **`license add`** ***`iscsi_license_code`*** **Note:** You must enable the `iscsi` option for the FAS2040, 30xx, 31xx, and 60xx hardware platforms.

Enabling the FC license

You must enable the FC license to use the FCP target service.

Step

1. Depending on the Data ONTAP versions, enter the appropriate command to enable FC license:

If the system version is...	Then...
Data ONTAP 7.3.x or 8.0.x or 8.1.x	Add the FC license by entering the following command: **`license add`** ***`license_code`***

If the system version is...	Then...
Data ONTAP 8.2.x	Perform one of the following actions: • Enable the `fcp` option by entering the following command: **`options licensed_feature.fcp.enable on`** • Add the FC license by entering the following command: **`license add`** ***`license_code`*** **Note:** For the FAS2040 hardware platform, you must enable the `fcp` option.

`license_code` is the license code you received when you purchased the FC license.

Installing or upgrading NetApp Plug-in for Symantec NetBackup

In a Replication Director environment, NetApp Plug-in for Symantec NetBackup enables NetBackup to access NetApp storage systems and use NetApp Snapshot technology through the DataFabric Manager server. You can install or upgrade the plug-in on a Microsoft Windows operating system or Linux operating system, which hosts the DataFabric Manager server.

System requirements for installing or upgrading NetApp Plug-in for Symantec NetBackup

You must ensure that you meet the system requirements to install NetApp Plug-in for Symantec NetBackup on a Windows or Linux server and to set up NetApp storage systems. NetApp Plug-in 1.1 for Symantec NetBackup supports NetBackup 7.6.

NetApp hardware and software requirements

You must ensure that you meet the NetApp hardware and software requirements before installing NetApp Plug-in for Symantec NetBackup.

Software requirements

For a detailed list about the supported software version, see the Interoperability Matrix.

Hardware requirements

For a detailed list about the supported storage systems, see the *Hardware Universe* (formerly the *System Configuration Guide*) at *support.netapp.com/knowledge/docs/hardware/NetApp/syscfg/index.shtml*.

Related tasks

Viewing supported configurations in Interoperability Matrix on page 58

Related information

NetApp Support Site: support.netapp.com

Interoperability Matrix: support.netapp.com/NOW/products/interoperability

Windows server requirements

You must ensure that you meet the requirements for systems running Windows 32-bit and Windows 64-bit operating system.

Operating system requirements

You should be using one of the following operating systems:

- Windows Server 2003 and 2003 R2, Enterprise or Standard edition
- Windows Server 2008 and 2008 R2, Enterprise or Standard edition
- Windows Server 2003 running on VMware ESX
- Windows Server 2008 or 2008 R2 running on VMware ESX
- Windows Server 2003 running on Hyper-V
- Windows Server 2008 or 2008 R2 running on Hyper-V

Note: If you want to use `rsh` and you are installing the DataFabric Manager server on Windows Server 2008, you must install Subsystem for UNIX-based Applications (SUA) or Service for UNIX (SFU) to support the execution of `rsh` commands.

Hardware requirements for Windows Server 2003 and Windows Server 2008 are similar to OnCommand Core Package 5.0.2 and OnCommand Core Package 5.2. For more details, see the Interoperability Matrix.

Related tasks

Viewing supported configurations in Interoperability Matrix on page 58

Related information

Interoperability Matrix: support.netapp.com/NOW/products/interoperability

Linux server requirements

You must ensure that you meet the operating system and hardware requirements for systems running Linux servers in 32-bit and 64-bit environments.

Operating system requirements

You should be using one of the following operating systems:

- Red Hat Enterprise Linux Advanced Platform 5.x
- Red Hat Enterprise Linux Advanced Platform 6.x
- SUSE Linux Enterprise Server 10
- SUSE Linux Enterprise Server 11
- Red Hat Enterprise Linux Advanced Platform 5.x running on VMware ESX

- SUSE Linux Enterprise Server 10 running on VMware ESX
- SUSE Linux Enterprise Server 11 running on VMware ESX
- Red Hat Enterprise Linux 5.x running on Hyper-V
- SUSE Linux Enterprise Server 10 running on Hyper-V
- SUSE Linux Enterprise Server 11 running on Hyper-V

Note: Hardware requirements for the Linux server are similar to OnCommand Core Package 5.0.2 and OnCommand Core Package 5.2. For more details, see the Interoperability Matrix.

Related tasks

Viewing supported configurations in Interoperability Matrix on page 58

Related information

Interoperability Matrix: support.netapp.com/NOW/products/interoperability

Prerequisites for installing or upgrading NetApp Plug-in for Symantec NetBackup

You must ensure that you meet all the requirements before installing or upgrading NetApp Plug-in for Symantec NetBackup.

You must complete the following tasks before you upgrade from NetApp Plug-in 1.0.1 for Symantec NetBackup to NetApp Plug-in 1.1 for Symantec NetBackup:

- Ensure that the NetBackup components are upgraded.
  NetApp Plug-in 1.1 for Symantec NetBackup does not support NetBackup 7.5.x.
- Ensure that you create a backup of the `NBUPlugin.cfg` and `configure.cfg` files.
  New data is appended to the existing data in the files when the upgrade is completed.
- Ensure that all storage lifecycle policy jobs running on NetBackup are completed.

You must complete the following tasks before you install NetApp Plug-in for Symantec NetBackup:

- Uninstall Open Systems SnapVault (if it is installed) from the host system on which you want to install the plug-in.
- Disable automatic storage system schedules for the volumes that are managed by NetBackup.
  You can disable schedules from the Data ONTAP command-line interface or from the DataFabric Manager server.
- Ensure that port 8085 or 8086 is free.
  The plug-in uses port 8085 in HTTP mode or port 8086 in HTTPS mode to communicate with NetBackup.
- Enable iSCSI or FC on storage systems.
- Enable SnapMirror and SnapVault licenses on the storage systems.
- Install OnCommand Core Package.

- Ensure that resource or destination pools are created and added to the NetBackup group in the DataFabric Manager server.
- Ensure that NDMP is enabled.
  You can verify the NDMP status by using the `ndmpd status` command.
- Download the NetApp Plug-in for Symantec NetBackup installation package from the NetApp Support Site.

Related information

NetApp Support Site: support.netapp.com

Installing NetApp Plug-in for Symantec NetBackup on a Windows host

You can install NetApp Plug-in for Symantec NetBackup on a Windows platform to enable NetBackup to manage the storage systems.

Before you begin

- You must have the login credentials for a Windows administrator account.
- The DataFabric Manager server must be online.
- You must have reviewed the *Prerequisites for installing the NetApp Plug-in for Symantec NetBackup* on page 31.

About this task

- You must ensure that you select either 8085 or 8086 as the communication port, because the plug-in uses port 8085 in HTTP mode or port 8086 in HTTPS to communicate with NetBackup.
- By default, the plug-in is installed in the `Program Files (x86)\NetApp\NBUPlugin` directory for a 64-bit Windows system and in `Program Files\NetApp\NBUPlugin` for a 32-bit Windows system.

Steps

1. Navigate to the directory to which you saved the plug-in installation files.
2. Run the executable file.
3. Browse to the path where you want to install the plug-in.
4. Follow the on-screen prompts in the setup wizard.
5. Click **Finish** to complete the installation.
6. Verify that the communication between the plug-in and NetBackup is established from NetBackup GUI.

Installing NetApp Plug-in for Symantec NetBackup on a Linux host

You can install NetApp Plug-in for Symantec NetBackup on a Linux platform to enable NetBackup to manage the storage systems.

Before you begin

- You must have the login credentials for a Linux root account.
- The DataFabric Manager server must be online.
- You must have reviewed the *Prerequisites for installing the NetApp Plug-in for Symantec NetBackup* on page 31.

About this task

- You must ensure that you select either 8085 or 8086 as the communication port because the plug-in uses port 8085 in HTTP mode and port 8086 in HTTPS to communicate with NetBackup.
- By default, the plug-in is installed in the `/usr/NetApp/NBUPlugin` directory.

Steps

1. Log in as root.
2. Navigate to the directory that contains the plug-in installation package by entering the following command:

   `cd: path_name`

3. Enter the following command:

   `sh NBUPlugin_x86_1.1.sh`

4. Follow the on-screen prompts to complete the installation.
5. Verify that the communication between the plug-in and NetBackup is established from the NetBackup GUI.

Configuring NetApp Plug-in for Symantec NetBackup

After installing the plug-in, you must configure it to enable IPv6, convert existing directories to Unicode format, and generate events and self-signed certificates.

Configuring IPv6

You can configure IPv6 on the system on which NetApp Plug-in for Symantec NetBackup is installed by editing the `NBUPlugin.cfg` file. By default, the plug-in is configured for IPv4.

Steps

1. Locate the `NBUPlugin.cfg` file in the *`install_path\config`* directory.

   `install_path\config` is the directory in which NetApp Plug-in for Symantec NetBackup is installed.

2. Open the `NBUPlugin.cfg` file in a text editor.

3. Depending on whether you want to configure only IPv6 or both IPv6 and IPv4, perform the appropriate action:

If you want to configure...	Edit the following...
Only IPv6 for Windows 2003	*`[NBUPlugin:host]`* **`Value=::0`**
Only IPv4 for all versions of Linux and Windows	*`[NBUPlugin:host]`* **`Value=0.0.0.0`**
IPv6 and IPv4 (dual stack) for Linux and Windows 2008 and later	*`[NBUPlugin:host]`* **`Value=::0`**

4. Save the file.

5. Restart NetApp Plug-in for Symantec NetBackup.

Configuring events in NetApp Plug-in for Symantec NetBackup

NetApp Plug-in for Symantec NetBackup periodically generates events to notify users about volumes that are not protected by NetBackup.

About this task

You can configure parameters in the `NBUPlugin.cfg` file to control the number of events that are generated and passed to NetBackup based on the event severity.

You can configure the following event-related parameters in the `NBUPlugin.cfg` file:

- `DisableEventGeneration`
- `DisableEventGenerationTypes`
- `DisableEventTypes`
- `DisableEventSeverity`

Steps

1. Locate the `NBUPlugin.cfg` file in the *`InstallPath`*`\config` directory.

   `InstallPath` is the directory in which NetApp Plug-in for Symantec NetBackup is installed.
2. Open the `NBUPlugin.cfg` file in a text editor.
3. Depending on the parameter you want to modify, perform the appropriate action:

If you want to...	Do this...
Disable event generation	**a.** Edit the following: [NBUPlugin:DisableEventGeneration] Value=TRUE The default value of the parameter is FALSE. **b.** Restart the plug-in. **Note:** NetBackup continues to receive events generated by the DataFabric Manager server.

If you want to...	Do this...
Disable generation of a specific event	Edit the following: [NBUPlugin:DisableEventGenerationTypes] Value=*`eventType`* The possible values for *`eventType`* are as follows: • `ntap:n-adap-Unprotected-Dataset:DMA protected` This value disables generation of *Volume protected by DataFabric Manager server* events. • `ntap:n-adap-Unprotected-Dataset:DMA protection broken` This value disables generation of *Volume not protected by DataFabric Manager server* events.
Filter a specific event	Edit the following: [NBUPlugin:DisableEventTypes] Value=*`eventType`* The possible values for *`eventType`* are as follows: • `ntap:n-adap-Unprotected-Dataset:DMA protected` This value disables generation of *Volume protected by DataFabric Manager server* events. • `ntap:n-adap-Unprotected-Dataset:DMA protection broken` This value disables generation of *Volume not protected by DataFabric Manager server* events. • `Volume Almost Full` This value disables generation of *Volume almost full* events.
Filter events based on severity	Edit the following: [NBUPlugin:DisableEventSeverity] Value=*`severity`* The possible values for *`severity`* are as follows: • `information` • `warning` • `critical`

Note: All event types and severities are case-sensitive.

For disabling generation of a specific event or filtering a specific event, you can specify two or more event types or severity by using the exclamation point and comma (!,) as separators.

Example

[NBUPlugin:DisableEventTypes]
Value=ntap:n-adap-Unprotected-Dataset:DMA protected!,ntap:n-adap-Unprotected-Dataset:DMA protection broken

4. Save the file.

Generating self-signed certificates

You can generate SSL certificates for the storage system and servers to use SSL connections for secure communication.

About this task

Certificates must use the Privacy Enhanced Mail (PEM) format and follow a certain naming convention.

Generating self-signed certificates is optional.

Steps

1. Stop the NetApp Plug-in for Symantec NetBackup services.
   - Windows: Click **Start > Control Panel > Administrative Tools > Services > NBUPlugin** to stop the services.
   - Linux:
     a. Navigate to `/usr/NetApp/NBUPlugin`.
     b. Run the following command to stop the services:

        ```
        sh startup.sh stop
        ```

2. Generate an RSA key by using the `openssl genrsa` command.

   Example

   ```
   openssl genrsa -out privkey.pem 2048
   ```

   2048 is the size of the key (in bits).

3. Generate a self-signed certificate by using the `openssl req` command.

   Example

   ```
   openssl req -new -x509 -key privkey.pem -out server.pem -days 1095
   ```

4. Navigate to the installation directory and replace the old certificate with the new certificate.
5. Restart the NetApp Plug-in for Symantec NetBackup services.

- Windows: Click **Start > Control Panel > Administrative Tools > Services > NBUPlugin** to start the services.
- Linux:
  a. Navigate to `/usr/NetApp/NBUPlugin`.
  b. Run the following command to start the services:

     ```
     sh startup.sh start
     ```

Related information

Keys: www.openssl.org/docs/HOWTO/keys.txt
Certificates: www.openssl.org/docs/HOWTO/certificates.txt

Converting existing directories to Unicode format

When a CIFS client first accesses a directory, it triggers the Unicode conversion. If your storage environment already contains existing NFS directories with large numbers of subdirectories and files, the automatic on-first-access conversion can have a performance impact on the storage system. There are methods to prevent this performance impact.

About this task

You can proactively convert existing NFS directories to Unicode format manually under controlled conditions. You can also configure Data ONTAP to trigger Unicode conversion upon access from both NFS and CIFS clients to distribute the load.

Step

1. Perform one or more of the following actions:

If you want to...	Then...
Trigger Unicode conversion manually	From a CIFS client, use Windows Search or equivalent function to scan all CIFS accessible volumes on the storage system. This triggers Unicode conversion on NFS directories that previously have not been accessed by CIFS clients. **Note:** Perform this step only during non-business hours or a maintenance window. The action triggers Unicode conversion on multiple directories, leading to a significant performance impact on the storage system while conversion is taking place. Depending on the number of subdirectories and files the directories contain, Unicode conversion can take hours or even days, so plan accordingly.

If you want to...	Then...
Reduce the time required for Unicode conversion of a directory	**a.** If you have a directory that contains more than 50,000 files, create a new CIFS directory from a Windows client on the same volume. **b.** In the same qtree as the directory you want to convert, use the NFS `mv` command to move the files into the directory you just created. **c.** Optionally, remove the old directory and assign its name to the new directory.
Trigger Unicode conversion when directories are accessed by either CIFS or NFS clients	Enter the following command: **`vol options volume_name convert_ucode on`** **Note:** Do not enable the `convert_ucode` option when you have directories that contain more than 50,000 files. This operation might fail if a nondisruptive volume movement is being performed on the target volume.
Move non-Unicode volume contents to a Unicode volume	**a.** Verify that on the source volume the `convert_ucode` option is set to `off`. **b.** Create a new volume. **c.** Configure Unicode on the new volume by entering the following commands: **`vol options volume_name create_ucode on`** **`vol options volume_name convert_ucode on`** **d.** Use `ndmpcopy` or qtree SnapMirror to move the data from the source volume to the destination volume. For more information about `ndmpcopy`, see the *Data ONTAP 7-Mode Data Protection Tape Backup and Recovery Guide*. For more information about qtree SnapMirror, see the *Data ONTAP 7-Mode Data Protection Online Backup and Recovery Guide*.

NetBackup configuration

You must configure Symantec NetBackup after the NetApp storage systems and NetApp Plug-in for Symantec NetBackup are installed and configured. After the NetApp storage systems are configured, the DataFabric Manager server presents the storage system as volumes to NetBackup.

Configuration of DataFabric Manager server as NetBackup storage server

You must configure the DataFabric Manager server as a storage server by using the NetBackup Storage Server Configuration Wizard.

The NetBackup Storage Server Configuration Wizard enables you to configure the disk pools and storage units that are required for the Replication Director configuration.

Note: You must ensure that objects such as resource groups or resource pools are created with unique names in the DataFabric Manager server.

For more information about configuring the DataFabric Manager server as a storage server, see *Configuring a NetBackup storage server* in the *Symantec NetBackup Replication Director Solutions Guide*.

For more information about disaster recovery and high-availability support for DataFabric Manager server, see the technical reports *TR 3655: Disaster Recovery Support for DataFabric Manager Data Using SnapDrive* and *TR 3767: High-Availability Support for DataFabric Manager Server*.

Related information

NetBackup documentation on the Symantec Site: www.symantec.com/docs/DOC5332

Managing disk pools and resource pools

Changes that are made in resource pools affect the NetBackup disk pools. The NetBackup administrator must refresh the disk pools in the Change Disk Pool window from the NetBackup Administration Console to view the changes.

Refreshing the disk pool enables NetBackup to locate any new volumes or changes in the storage server. You can add new volumes to the existing disk pools. The storage lifecycle policies succeed only if the disk pools associated with that storage lifecycle policy are refreshed.

If a resource pool is deleted or renamed from the DataFabric Manager server, then all the storage lifecycle policies that refer to a specific resource pool must be updated.

For more information about managing disk pools and resource pools from NetBackup, see *Configuring a NetBackup storage server* chapter in the *Symantec NetBackup Replication Director Solutions Guide*.

Related information

NetBackup documentation on the Symantec Site: www.symantec.com/docs/DOC5332

Importing datasets and Data ONTAP relationships to Symantec NetBackup

In a Symantec NetBackup Replication Director environment, you can manage the backup operations from NetBackup that were earlier managed by the DataFabric Manager server and by Data ONTAP. You must use the import tool to import DataFabric Manager server datasets, and Data ONTAP SnapVault and SnapMirror relationships, to NetBackup.

Understanding the Import tool

In a Replication Director environment, the Import tool enables you to import DataFabric Manager server datasets, and SnapVault and SnapMirror relationships, to NetBackup. The Import tool is packaged along with NetApp Plug-in for Symantec NetBackup.

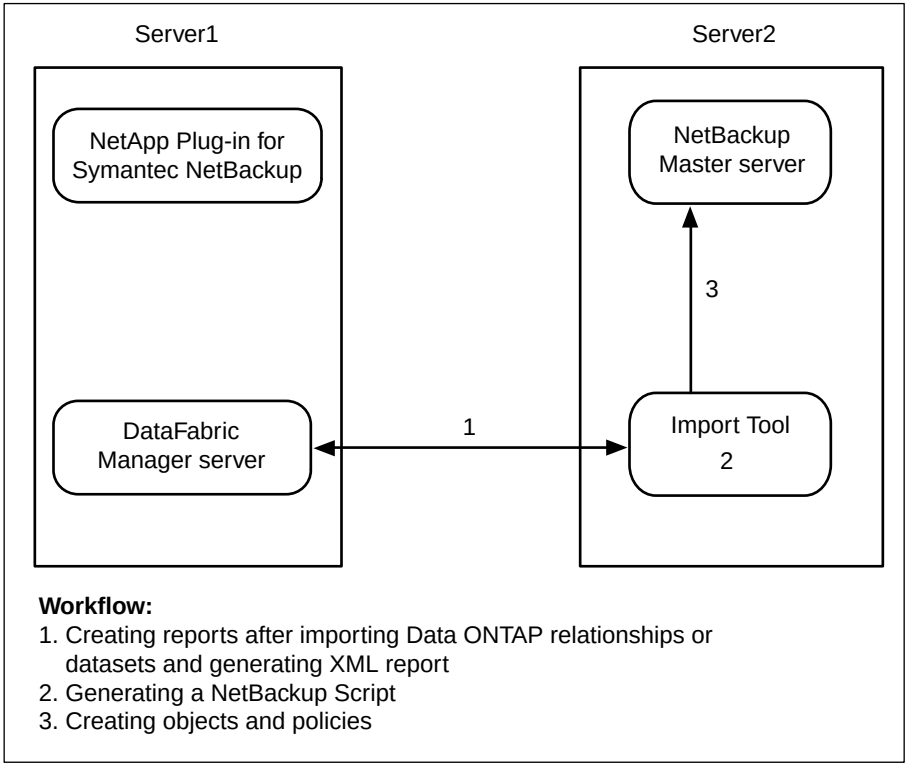
The Import tool allows only incremental updates after a nondisruptive SnapVault and SnapMirror transition.

The Import tool supports NAS file systems and all the storage topologies that are supported by NetApp Plug-in for Symantec NetBackup.

How the Import tool works

The Import tool enables you to import DataFabric Manager server datasets, and SnapVault and SnapMirror relationships, to NetBackup. Importing involves creating a report, generating a NetBackup script, and importing the datasets to NetBackup.

The following illustration shows the workflow of Import tool:



1. Creating reports

The Import tool collects all the details of the datasets and Data ONTAP relations and creates an XML file. The XML file includes details of the disk pools, storage units, storage lifecycle policies, NetBackup policies, and the type of SnapVault and SnapMirror relationships that are created in NetBackup. You can modify the XML file to change any of the resources that are used in the datasets. A log file is created along with the XML file, which includes details of the import operation.

2. Generating a NetBackup script

The Import tool reads the XML file and creates a NetBackup script that contains the NetBackup commands for creating disk pools, storage units, NetBackup policies, and storage lifecycle policies. You can edit this script to modify the NetBackup commands.

3. Importing datasets

The datasets are imported to NetBackup. The Import tool creates the disk pools, storage units, NetBackup policies, and storage lifecycle policies, if they do not exist on NetBackup. The storage lifecycle policies that are created correspond to the DataFabric Manager server datasets, and the SnapVault and SnapMirror relationships.

When importing SnapVault or SnapMirror relationships, the Import tool discovers the external relationships that are defined in the DataFabric Manager server, which are associated to a specific

destination volume and creates a DataFabric Manager server dataset. This dataset is then imported to NetBackup.

Note: The DataFabric Manager server does not support volume SnapVault relationships; therefore, the SnapVault relationships that are created with a volume as source are not identified as external relationships by the DataFabric Manager server. Only relationships with qtrees as source can be imported into the DataFabric Manager server.

The files that are created during the import operation are stored in the directory specified in `-outputdir`. If the directory is not specified in `-outputdir`, then the files are stored in the root of the file system. For example, `c:\import-dfm-vmlnx-66-84` for windows and `/import-dfm-vmlnx-66-84` for Linux.

For more examples and instructions on using Import tool, see the `readme.txt` file that is included with the Import tool.

Support for incremental import

The Import tool supports incremental import operations to import datasets and Data ONTAP relationships periodically to NetBackup in separate batches.

An incremental import operation requires the output directory created during the previous import operation. The output directory contains information about storage objects such as the storage lifecycle policies, storage units, and disk pools that were created during the previous import operation. Because the output directory is retained, duplicate storage objects are not created, thus reducing the rate of import failure.

You must ensure that the host name and IP address of the output directory is used in subsequent import operations.

Managing backups from NetBackup using the Import tool

You can run the Import tool, from a Linux or Windows-based NetBackup host. Using the Import tool you can import DataFabric Manager server datasets, and SnapVault and SnapMirror relationships, to NetBackup.

System requirements for using the Import tool

You must ensure that you meet the system requirements to run the Import tool from a Linux-based or Windows-based NetBackup host.

You must meet the following requirements for Linux-based NetBackup host:

- Red Hat Enterprise Linux Advanced Platform 5.x
- Perl 5.10
- The following Perl RPMs must be installed:

- perl-String-CRC32
- perl-HTML-Parser
- perl-XML-Simple
- perl-XML-NamespaceSupport
- perl-URI
- perl-XML-Parser
- perl-XML-SAX
- perl-Compress-Zlib
- perl-HTML-Tagset
- perl-XML-Dumper
- perl-XML-LibXML
- perl-XML-LibXML-Common
- UserAgent.pm for Solaris

You must meet the following requirement for a Windows-based NetBackup host:

- Active Perl 5.10

Prerequisites for using the Import tool

You must ensure that you meet all the requirements before using the Import tool.

You must have completed the following tasks:

- Installing NetApp Plug-in for Symantec NetBackup
- Configuring the DataFabric Manager server
- Backing up the DataFabric Manager server datasets and the NetBackup server
- Ensuring that there are no updates to the DataFabric Manager server datasets and the NetBackup policies
- Ensuring that the DataFabric Manager server discovers the dataset relationships by running the `dfm host discover` command

General cautions for using the Import tool

You must be aware of certain cautions before you start using import tool.

- The output directories should not be deleted because NetBackup objects, such as disk pools, storage units, storage lifecycle policies, are stored in these directories.

  Incremental upgrade operations fail if the output directories are deleted.
- When an import fails, you should not delete the storage lifecycle policies created in NetBackup.
- You should not run the NetBackup script manually.
- Ensure that the DataFabric Manager server discovers the Data ONTAP relationships by running the DataFabric Manager server host `discover` command to import the Data ONTAP relationships.

- If you want to start a new import operation—for example, to import datasets from a different DataFabric Manager server—then you must delete the output directory created during the previous import operation.
- Ensure that the resources assigned to the dataset are available in the DataFabric Manager server.
- Ensure that the required space for the resources is available in the DataFabric Manager server.
- Ensure that the storage server information is added to NDMP hosts in the NetBackup server.

Running the Import tool

You must run the Import tool from the NetBackup master server to import DataFabric Manager server datasets, and SnapVault and SnapMirror relationships, to NetBackup.

Before you begin

- You must have the login credentials for a Linux account with root level privileges on the NetBackup host or you must have the login credentials for a Windows administrator account.
- The plug-in must be installed and running.
- You must have reviewed the *System requirements for using the Import tool* on page 44.
- You must have reviewed the *Prerequisites for using the Import tool* on page 45.

Steps

1. Log in as root or administrator to both the server where you saved the plug-in installation directory and to the NetBackup host.
2. Navigate to the plug-in installation directory.
3. Copy the `import` directory from the plug-in installation directory to the NetBackup master server.
4. Navigate to the `import` directory in the NetBackup master server.
5. Run the executable file from the NetBackup master server.

Importing DataFabric Manager server datasets

You can import the DataFabric Manager server datasets to NetBackup by specifying either the dataset names or the number of datasets you want to import, or by specifying both the name and number of the datasets to manage the backup operations from NetBackup.

Before you begin

- You must have the login credentials for a Linux account with root level privileges on the NetBackup host or you must have the login credentials for a Windows administrator account.
- The NetBackup host and the DataFabric Manager server must be online.
- You must have reviewed the *Prerequisites for using the Import tool* on page 45.
- You must have reviewed the *System requirements for using the Import tool* on page 44.

- You must have copied the `import` directory from the plug-in installation directory to the NetBackup master server.

About this task

In a single import operation, the Import tool can import either DataFabric Manager server datasets or SnapVault and SnapMirror relationships, but not a combination of both.

You should use the `–skipfanin` option with the appropriate commands if you want to skip importing the following:

- DataFabric Manager server datasets that have the same destination volume from many SnapVault primary volumes.
- SnapVault relationships that have the same destination volume from many SnapVault primary volumes.

During an import operation, if the report action is run consecutively without the subsequent import operation, then the information collected from the first report action is erased.

If you want to start a new import operation, for example, to import datasets from a different DataFabric Manager server, then you must delete the output directory created during the previous import operation.

Steps

1. From the NetBackup command shell prompt, export the path by entering the following command:

   `export PATH=$PATH:/usr/openv/netbackup/bin/admincmd`

2. Navigate to the folder to which you extracted the contents of the Import tool directory.
3. Generate an XML file that includes the DataFabric Manager server datasets by performing the appropriate action:

If you want to...	Enter the command...
Specify the name of a dataset	**`perl import.pl -dfmserver dfm_server_hostname|IP -dfmuser dfm_user_name -dfmpassword dfm_password -nbumedia NBU_server_hostname|IP -outputdir /root -dataset DFM_dataset_name -action report`**
Specify multiple dataset names	**`perl import.pl -dfmserver dfm_server_hostname|IP -dfmuser dfm_user_name -dfmpassword dfm_password -nbumedia NBU_server_hostname|IP -outputdir /root -dataset DFM_dataset_name -dataset DFM_dataset_name_1 -action report`**
Specify the number of datasets	**`perl import.pl -dfmserver dfm_server_hostname|IP -dfmuser dfm_user_name -dfmpassword dfm_password -nbumedia NBU_server_hostname|IP -outputdir /root -numdatasets num -action report`**

If you want to...	Enter the command...
Specify the dataset names and number of datasets	**perl import.pl -dfmserver *dfm_server_hostname|IP* -dfmuser *dfm_user_name* -dfmpassword *dfm_password* -nbumedia *NBU_server_hostname|IP* -outputdir /root -dataset *DFM_dataset_name* -numdatasets *num* -action report**
Include all the datasets	**perl import.pl -dfmserver *dfm_server_hostname|IP* -dfmuser *dfm_user_name* -dfmpassword *dfm_password* -nbumedia *NBU_server_hostname|IP* -outputdir /root -action report**

dfm_server_hostname|IP is the host name or IP address of the DataFabric Manager server.

dfm_user_name is the user name of the DataFabric Manager server that has root level privileges.

dfm_password is the password of the DataFabric Manager server account.

NBU_server_hostname|IP is the host name or IP address of the NetBackup host.

DFM_dataset_name and *DFM_dataset_name_1* are the names of the DataFabric Manager server datasets.

num is the number of DataFabric Manager server datasets for which you want to create a report.

The `-dataset` option is a regular expression and the script retrieves all the dataset names that partially match the entered string. If you specify the `-dataset` option and the `-numdatasets` option when creating the XML file, then the dataset names that match the entered string are located first and then the specified number of datasets are included.

The XML file is created in the output directory `/root/import-dfm-`*dfm_server_hostname|IP*.

Note: The output directories should not be deleted because NetBackup objects like disk pools, storage units, storage lifecycle policies, and so on are stored in these directories. Incremental upgrade operations fail if the output directories are deleted.

4. Generate a NetBackup script that includes the NetBackup commands to create disk pools, storage units, and storage lifecycle policies on NetBackup by entering the following command:

   perl import.pl -dfmserver *dfm_server_hostname|IP* -dfmuser *dfm_user_name* -dfmpassword *dfm_password* -nbumedia *NBU_server_hostname|IP* -outputdir /root -action script

   The NetBackup script is created in the output directory `/root/import-dfm-`*dfm_server_hostname|IP*.

5. Import the DataFabric Manager server datasets to NetBackup by entering the following command:

```
perl import.pl -dfmserver dfm_server_hostname|IP -dfmuser dfm_user_name
-dfmpassword dfm_password -nbumedia NBU_server_hostname|IP -outputdir /
root -action import
```

6. From the **NetBackup Administration Console**, verify that the DataFabric Manager server datasets are imported to NetBackup.

Importing SnapVault and SnapMirror relationships

You can import Data ONTAP replication relationships based on the volume that is set as destination volume in an external relationship and the SnapVault or SnapMirror relationships that are associated with that specific destination volume. You can view the external relationships in the DataFabric Manager server.

Before you begin

- You must have the login credentials for a Linux account with root level privileges on the NetBackup host.
- The NetBackup host and the DataFabric Manager server must be online.
- You must have reviewed the *Prerequisites for using the Import tool* on page 45.
- You must have reviewed the *System requirements for using the Import tool* on page 44.
- You must have copied the `import` directory from the plug-in installation directory to NetBackup master server.

About this task

- During a single import operation, the Import tool can import either DataFabric Manager server datasets or SnapVault and SnapMirror relationships, but not a combination of both.
- The SnapVault or SnapMirror relationships that are similar and associated with the same destination volume are imported as a single dataset.
- At the end of an import operation, an NDMP policy is created in NetBackup.
- Destination volumes that are not provisioned by using DataFabric Manager server (externally managed relationships) and which are imported into the DataFabric Manager server datasets cannot be automatically resized using the dynamic secondary volume sizing feature of the DataFabric Manager server. Therefore, if the source volume size increases, you must manually resize the destination volumes to avoid replication job failures.

Steps

1. From the NetBackup command shell prompt, export the path by entering the following command:

   ```
   export PATH=$PATH:/usr/openv/netbackup/bin/admincmd
   ```

2. Navigate to the folder to which you have extracted the contents of the Import tool package.
3. Generate an XML file that includes the SnapVault and SnapMirror relationships by entering one of the following commands:

If you want to...	Enter the command...
Specify the Data ONTAP replication relationship	**perl import.pl -dfmserver *dfm_server_hostname|IP* -dfmuser *dfm_user_name* -dfmpassword *dfm_password* -nbumedia *NBU_server_hostname|IP* -outputdir /root -volume *storage_system_name*:/*volume_name* -action report**
Specify cascading Data ONTAP replication relationships	**perl import.pl -dfmserver *dfm_server_hostname|IP* -dfmuser *dfm_user_name* -dfmpassword *dfm_password* -nbumedia *NBU_server_hostname|IP* -outputdir /root -volume *storage_system_name*:/*volume_name* -volume *storage_system_name_1*:/*volume_name_1* -action report**

dfm_server_hostname|IP is the host name or IP address of the DataFabric Manager server.

dfm_user_name is the user name of the DataFabric Manager server that has root level privileges.

dfm_password is the password of the DataFabric Manager server account.

NBU_server_hostname|IP is the host name or IP address of the NetBackup host.

storage_system_name and *storage_system_name_1* are the names of the storage systems on which the destination volume resides.

volume_name and *volume_name_1* are the names of the destination volumes.

The XML file is created in the output directory /root/import-dfm-*dfm_server_hostname|IP*.

4. Generate a NetBackup script that includes the NetBackup commands to create disk pools, storage units, and storage lifecycle policies on NetBackup by entering the following command:

   perl import.pl -dfmserver *dfm_server_hostname|IP* -dfmuser *dfm_user_name* -dfmpassword *dfm_password* -nbumedia *NBU_server_hostname|IP* -outputdir /root -action script

   The NetBackup script is created in the output directory /root/import-dfm-*dfm_server_hostname|IP*.

5. Import the datasets to NetBackup by entering the following command:

   perl import.pl -dfmserver *dfm_server_hostname|IP* -dfmuser *dfm_user_name* -dfmpassword *dfm_password* -nbumedia *NBU_server_hostname|IP* -outputdir /root -action import

6. From the **NetBackup Administration Console**, verify that the datasets are imported to NetBackup.

What the cleanup tool does

You can use the cleanup tool to delete DataFabric Manager server datasets and Data ONTAP relationships that are associated with the NetBackup policy. The tool is packaged along with the NetApp Plug-in for Symantec NetBackup install file.

You must run the tool on the server where NetApp Plug-in for Symantec NetBackup and the DataFabric Manager server are installed.

The cleanup tool does not check whether the DataFabric Manager server datasets or Data ONTAP relationships that are being deleted are still referring to old and valid backup IDs or catalog entries in NetBackup. Therefore, before initiating the cleanup operation, you must ensure that the NetBackup policy is not associated with any old and valid backup IDs or catalog entries.

For more information, see the `readme.txt` file that is included with NetApp Plug-in for Symantec NetBackup.

Troubleshooting NetApp Plug-in for Symantec NetBackup

If you encounter unexpected behavior during the installation of or when using NetApp Plug-in for Symantec NetBackup, you can use the logs and trace files to identify and resolve the cause of such issues.

You can contact technical support, if you cannot troubleshoot or resolve the issue.

NetApp Plug-in for Symantec NetBackup logs and trace files location

You can access the log files to check the status of the plug-in and track the communication between the plug-in and NetBackup. Log files are refreshed on a daily basis. You can use the trace files for debugging.

You can access the plug-in logs and trace files for different platforms as listed in the table below:

Host platform	Trace files location	Logs location
32-bit Windows host	`Program Files (x86)\NetApp\NBUPlugin`	`Program Files (x86)\NetApp\NBUPlugin`
Windows host	`Program Files (x86)\NetApp\NBUPlugin \trace`	`Program Files (x86)\NetApp\NBUPlugin \log`
Linux host	`/usr/NetApp/NBUPlugin/ trace`	`/usr/NetApp/ NBUPlugin/log`

To enable additional tracing, you should set the TRACE:TRACE_TO_FILE parameter to TRUE in the `NBUPlugin.cfg` file in the `InstallPath\config` directory.

Example:

```
[TRACE:TRACE_TO_FILE]
Value=TRUE
```

Error messages in NetApp Plug-in for Symantec NetBackup

You might encounter some error messages when using NetApp Plug-in for Symantec NetBackup. You can view the error messages in the user interface of Symantec NetBackup.

Filer read issue when creating a Snapshot copy

Message	`Error 13: Filer read failed`
Possible cause	The error is triggered from NetBackup.
Next action	Contact Symantec support to troubleshoot this issue.

Filer write issue when creating a Snapshot copy

Message	`Error 14: Filer write failed`
Possible cause	The error is triggered from NetBackup.
Next action	Contact Symantec support to troubleshoot this issue.

Snapshot copy creation fails

Message	`Error 20: Snapshot creation failed`
Possible cause	• The error is triggered from NetBackup or NetApp Plug-in for Symantec NetBackup. • Storage system is not accessible. • Another Snapshot copy with a similar name exists in the resource pool.
Next action	• Ensure that the storage system is accessible. • Search the NetApp Plug-in for Symantec NetBackup log files with the volume name to identify the reason for the Snapshot copy failure. • Contact Symantec support to troubleshoot this issue.

Snapshot copy issue when creating a Snapshot copy

Message	`Error 156: Snapshot error encountered`
Possible cause	• The error is triggered from NetApp Plug-in for Symantec NetBackup. • Storage system is not accessible. • Another Snapshot copy with a similar name exists in the resource pool.

Next action

- Ensure that the storage system is accessible.
- Search the NetApp Plug-in for Symantec NetBackup log files with the volume name to identify the reason for the Snapshot copy failure.

Media write issue when creating datasets or exporting Snapshot copies

Message `Error 84: Media write error`

Possible cause

- Invalid resource pools.
- Dataset cannot be created or found.
- Snapshot copy export failed.
- FlexClone and SnapRestore licenses not found.

Next action

- Ensure that the storage units used in NetBackup are mapped to the appropriate resource pools in the DataFabric Manager server.
- Ensure that the target storage unit in NetBackup is online and accessible.
- Ensure that the FlexClone and SnapRestore licenses are installed on the secondary storage system.
- Check the NetApp Plug-in for Symantec NetBackup logs to locate the cause of the failure.
- Contact NetApp technical support if you are unable to resolve the issue.

Media manager system issue when DataFabric Manager server job fails

Message `Error 174: Media manager system error occurred`

Possible cause The DataFabric Manager server job failed.

Next action Search the NetApp Plug-in for Symantec NetBackup log file for the NetBackup job error code `NBUjob`. In the search results, verify if the DataFabric Manager server job was successfully completed.

- If the DataFabric Manager server job failed, then check the DataFabric Manager server logs to understand the issue.
- If the DataFabric Manager server job was successful, but NetBackup reports that the job failed, then contact NetApp technical support.

DataFabric Manager server job request fails

Message `Error 34: Failed waiting for child process`

Possible cause

- Invalid request.

- Cannot find or create a dataset, which prevents the DataFabric Manager server from triggering a DataFabric Manager server job.
- Cannot obtain the status of a triggered DataFabric Manager server job.
- NetApp Plug-in for Symantec NetBackup was restarted.

Next action Search the NetApp Plug-in for Symantec NetBackup log file for the NetBackup job error code `NBUjob`. In the search results, verify if the DataFabric Manager server job was successfully completed. If the DataFabric Manager server job number is not available in the search results, then contact NetApp technical support.

Media open issue when specifying a Snapshot copy

Message `Error 83: Media open error`

Possible cause Invalid Snapshot copy specified.

Next action

- Ensure that the Snapshot copy is valid by checking the NetApp Plug-in for Symantec NetBackup log file.
- Enable tracing and ensure that NetApp Plug-in for Symantec NetBackup has sent the correct error code to the Snapshot copy API request.

  Perform the following steps to enable tracing:

  1. Change the `Trace` option value to `TRUE` in the `configure.cfg` file.
  2. Restart NetApp Plug-in for Symantec NetBackup.
- If tracing is enabled, check if NetApp Plug-in for Symantec NetBackup takes a long time to respond to the API request.

NetBackup job cancelled manually

Message `Error 150: Termination requested by Administrator`

Possible cause NetBackup job was cancelled by the administrator.

Next action Check whether the NetBackup job was cancelled manually. If the job was not cancelled manually, then check for the first occurrence of the error in the job details window, and follow the troubleshooting tips provided for that error number.

Disk is offline

Message `Error 2074: Disk down error`

Possible cause

- Unable to communicate with the DataFabric Manager server.
- Unable to get details of a storage unit.

Next action

- Ensure that the DataFabric Manager server is accessible.
- Ensure that the storage server points to a valid resource pool in the DataFabric Manager server.
- Enable tracing and check if NetApp Plug-in for Symantec NetBackup takes more than 60 seconds to respond to the API request.

  Perform the following steps to enable tracing:

  1. Change the `Trace` option value to `TRUE` in the `configure.cfg` file.
  2. Restart NetApp Plug-in for Symantec NetBackup.

Storage server is offline

Message `Error 2106: Storage server down error`

Possible cause

- Unable to communicate with the DataFabric Manager server.
- Unable to get details of a storage unit.

Next action

- Ensure that the DataFabric Manager server is accessible.
- Ensure that the storage server points to a valid resource pool in the DataFabric Manager server.
- Enable tracing and check if NetApp Plug-in for Symantec NetBackup takes more than 60 seconds to respond to the API request.

  Perform the following steps to enable tracing:

  1. Change the `Trace` option value to `TRUE` in the `configure.cfg` file.
  2. Restart NetApp Plug-in for Symantec NetBackup.

Plug-in installation fails

Message

```
[root@vmrhel5u4x64-187-43 /]# ./NBUPlugin_x86_1.1.sh

Extracting the installer...

NBUPlugin Version 1.1

Have you read and agreed to the terms of the license?
(y = yes, n = no, d = display license) [d]:y
License accepted.
Specify the install location [/usr/NetApp/NBUPlugin]:
Specify the http port on which NBUPlugin will listen [8085]:
Port 8085 is free
Specify the https port on which NBUPlugin will listen [8086]:
Port 8086 is free
Preparing...
########################################### [100%]
  1:NBUPlugin
```

```
########################################## [100%]
NBUPlugin version 1.1 installed on Wed Jan  9 06:15:55 EST 2013
/usr/NetApp/NBUPlugin/processmanager: error while loading shared
libraries: /usr/lib/libsv.so: cannot restore segment prot after
reloc: Permission denied
/usr/NetApp/NBUPlugin/processmanager: error while loading shared
libraries: /usr/lib/libsv.so: cannot restore segment prot after
reloc: Permission denied
/usr/NetApp/NBUPlugin/processmanager: error while loading shared
libraries: /usr/lib/libsv.so: cannot restore segment prot after
reloc: Permission denied
```

Possible cause The error is triggered from NetApp Plug-in for Symantec NetBackup while loading shared libraries.

Next action Run the following command and install the plug-in: `[root@vmrhel5u4x64-187-43 NBUPlugin]# setenforce 0`

Where to find more information

You can access Technical Support and documentation for all NetApp products on the NetApp Support Site at *support.netapp.com*. In addition to product documentation, NetApp provides other product information, such as technical reports and white papers.

Viewing supported configurations in Interoperability Matrix

You can view the supported configurations in the Interoperability Matrix for any storage solution.

Steps

1. Access the Interoperability Matrix at *support.netapp.com/matrix*.
2. Enter your user name and password and click **Login**.
3. Click **Change** to select the storage solution.

   A window listing all the storage solutions is displayed.
4. Select the required storage solution.

   #### Example

   In the Backup and Recovery section, you can click **NetApp Plug-in for Symantec NetBackup** as the storage solution.
5. Click **Show Results** to view the configurations that match the selected storage solution.

   The supported configurations for the selected storage solution are displayed.

Copyright information

Trademark information

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

L

M

N

O

P

R

S

T

U

W