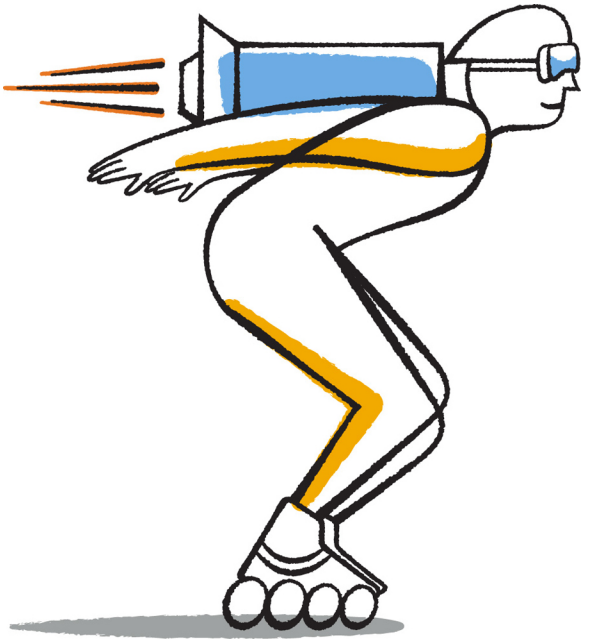
SnapProtect® Management Software 10.0

Express Guide

For VMware vSphere



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: 215-09071_A0
July 2014

Contents

Deciding whether to use this guide

This guide describes how to quickly configure SnapProtect to perform scheduled backups of VMware VMs, including primary Snapshot copies, mirrored Snapshot copies, and Snapshot copies archived to disk. You should use this guide if you want a standard backup configuration following NetApp best practices, and you do not want to see all the available options or a lot of conceptual information.

This guide is based on the following assumptions:

- You are using clustered Data ONTAP 8.2.2.
- The source and destination clusters for SnapMirror and SnapVault replication are peered, with peered storage virtual machines (SVMs).
- Your VMs are running Windows.
- Your VMs are using VMFS, not RDM, for disk access.
- Your production data and swap files reside in different datastores.
- You have not enabled Windows Firewall on the hosts for the SnapProtect CommServe and Virtual Server Agent (VSA), and you have not configured a firewall between the hosts.
- You have verified SnapProtect support for your configuration in the *NetApp Interoperability Matrix Tool* (IMT).

If these assumptions are not correct for your installation, or if you want more conceptual information, you should use the following documentation instead:

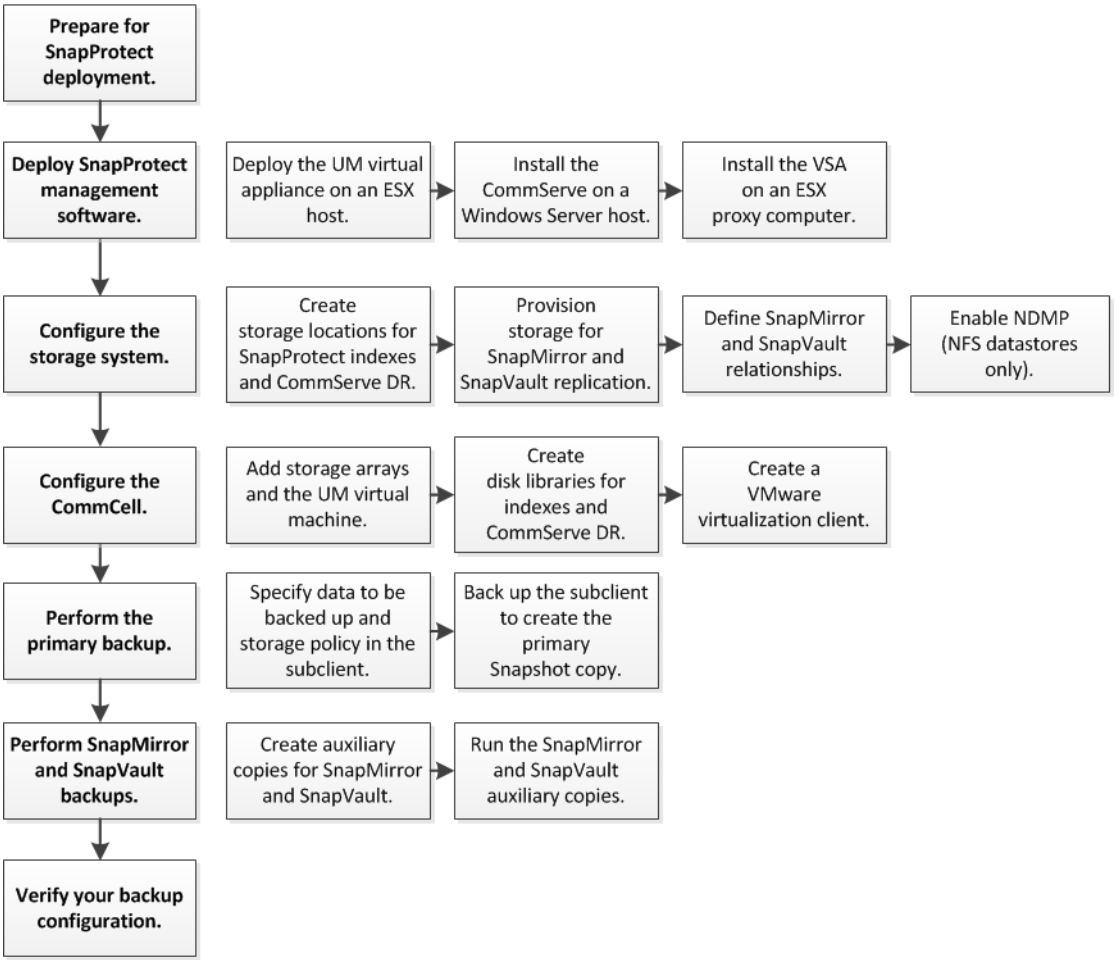
- *SnapProtect Management Software 10.0 Books Online*

  Describes how to back up and restore data with SnapProtect for all supported platforms and applications.
- *Clustered Data ONTAP 8.2 Cluster and Vserver Peering Express Guide*

  Describes how to quickly configure peer relationships between clusters and SVMs.

SnapProtect for VMware workflow

Before you configure backups with SnapProtect, you need to set up the CommCell infrastructure. The CommCell contains the SnapProtect management software, the primary, secondary, and tertiary storage arrays, and the vCenter Server for the VMs you want to back up. When the CommCell is in place, you can identify the VMs to be backed up and the backup policy.



Preparing for SnapProtect deployment

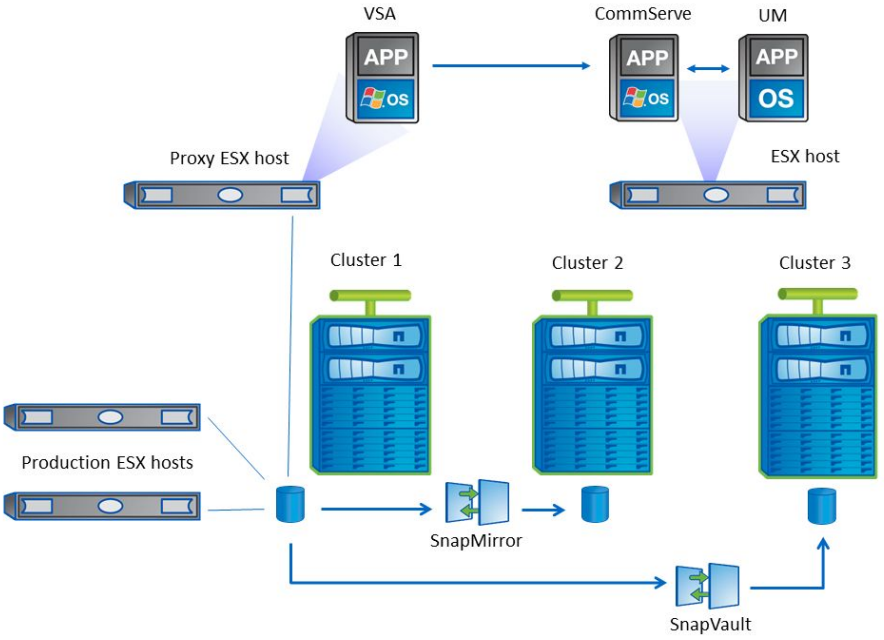
SnapProtect management software consists of NetApp OnCommand Unified Manager, the SnapProtect CommServe, and one or more ESX proxy computers. The proxy computer is any host running a SnapProtect Virtual Server Agent (VSA). The CommServe and VSA must run on different hosts.

- *OnCommand Unified Manager (UM)* interoperates with SnapProtect to perform SnapMirror and SnapVault replication. You deploy the virtual appliance for Unified Manager on an ESX host.
- The *CommServe* is the master server for the SnapProtect CommCell. You install the CommServe on a Windows Server 2008 or Windows Server 2012 host. The host can be physical or virtual.

  Tip: Many sites install the CommServe in a Windows Server virtual machine running on the same ESX host as the UM virtual machine.
- A *proxy computer* is any host running a SnapProtect Virtual Server Agent (VSA). You install the VSA on a Windows virtual machine running on an ESX host. The ESX host should have access to production datastores on the primary storage array.

  Tip: Proxy computers offload backup operations from ESX production servers. You can have as many proxies as you want, but you must have at least one.

The following illustration shows a typical SnapProtect deployment:



Unified Manager worksheet

By default, the Unified Manager installer uses the Dynamic Host Configuration Protocol (DHCP) to assign an IP address to the UM virtual machine. If you prefer to configure a static IP address for the VM, or if your network does not have a DHCP server, you should complete the following network configuration worksheet:

UM network configuration information	**Your values**
Host name	
IP address	
Network mask	
Default gateway	
Primary DNS address	
Secondary DNS address (optional)	
Search domains (optional)	

Storage array worksheet

You should complete the following worksheet before configuring the primary, secondary, and tertiary arrays in Unified Manager:

Cluster configuration information	**Your values**
Primary array	
Host name or cluster management IP address	
Data ONTAP administrator user name and password	
Protocol (HTTP or HTTPS)	
Port number	
Secondary array	
Host name or cluster management IP address	
Data ONTAP administrator user name and password	
Protocol (HTTP or HTTPS)	

Cluster configuration information	**Your values**
Port number	
Destination aggregate for SnapMirror replication	
Tertiary array	
Host name or cluster management IP address	
Data ONTAP administrator user name and password	
Protocol (HTTP or HTTPS)	
Port number	
Destination aggregate for SnapVault replication	

VSA worksheet

You should complete the following worksheet before installing the VSA:

Network configuration information	**Your values**
CommServe host name	

Deploying SnapProtect management software

SnapProtect management software consists of a master server and one or more ESX proxy computers. It also includes OnCommand Unified Manager (UM), which interoperates with SnapProtect to perform SnapMirror and SnapVault replication.

Related tasks

Deploying the UM virtual appliance on page 9
Installing the SnapProtect CommServe on page 10
Installing the SnapProtect Virtual Server Agent (VSA) on ESX proxy computers on page 12

Deploying the UM virtual appliance

You use the VMware vSphere Client to deploy the OnCommand Unified Manager (UM) virtual appliance to an ESX host. The deployed appliance creates a UM virtual machine from the OVF template.

About this task

You can also use the vSphere Web Client to deploy the virtual appliance. That deployment procedure is similar to the following one.

Steps

1. Download the `OnCommandUnifiedManager-6.1.ova` file from the NetApp Support Site to a location accessible to your vSphere Client.

   NetApp Support

2. In the vSphere Client, log in to the vCenter Server.
3. Select the host for UM and choose **File > Deploy OVF Template**.

   The Deploy OVF Template wizard opens.

4. Follow the prompts in the wizard:

On this page...	Do this...
Source	Select the OVA file for the UM virtual appliance.
OVF Template Details	Review the OVF template details for the UM virtual appliance.

On this page...	Do this...
End User License Agreement	Review the post-deployment procedure for the UM virtual appliance, then click **Accept**.
Name and Location	Specify the name and inventory location for the UM virtual machine, or accept the defaults.
Storage	Select the datastore for the UM virtual machine.
Disk Format	Select the disk format for the UM virtual machine. **Note:** Select **Thin Provision** if you are using a VMFS datastore or an NFS datastore with Hardware Acceleration. Thin provisioning allows the UM database to efficiently grow to the maximum available capacity as you add resources to your datacenter.
Properties	Enter the information you recorded in the network configuration worksheet for the UM virtual machine. Leave the fields blank if you are using DHCP.
Ready to complete	Select **Power on after deployment** to power on the virtual machine automatically after deployment, then click **Finish**.

The vSphere Client deploys the UM virtual appliance. When deployment is complete, the VM powers on and Unified Manager boots.

5. In the vSphere Client, select the VM and click the **Console** tab to monitor UM startup and configure the VM:
   a. At the prompts, specify your geographic area and time zone.
   b. If the vCenter Server is unable to connect to the VM with the static network configuration information you entered in the wizard, you are prompted to correct your entries. Enter the information you recorded in the network configuration worksheet for the UM virtual machine.
   c. At the prompts, enter the user name and password for Unified Manager.

Result

When network configuration is complete, the **Console** tab displays the IP address of the Unified Manager VM. Use the IP address to open Unified Manager in a web browser.

Installing the SnapProtect CommServe

The CommServe is the master server for the SnapProtect CommCell. You install the CommServe on a Windows Server 2008 or Windows Server 2012 host. The host can be physical or virtual.

About this task

A SnapProtect media agent is automatically installed with the CommServe software. The media agent manages transmission of data between clients and backup media.

Steps

1. Download the SnapProtect Download Manager application for Windows from the NetApp Support Site.

   NetApp Support

2. Double-click the Download Manager application, then click **Run** when prompted.
3. Specify the destination folder for the SnapProtect installation wizard, or accept the default.
4. Click **Extract**.

   The SnapProtect installation wizard opens.

5. Follow the prompts in the wizard to install the CommServe:

On this page...	Do this...
License Agreement	Click **I accept the terms in the license agreement**.
Install Type	Click **Install Packages**.
Installation Type	Click **Standard**.
Installation Options	Click **Create a New CommCell**.
Packages to install	Accept the preselected **CommServe Module** and **Media Agent** packages.
Destination Folder	Select the destination folder for the CommServe software, or accept the default.
Summary	Review your selections and click **Install**. **Note:** If the Microsoft .NET Framework is not already installed on the host, you are prompted to install it first. Click **Yes**. If the Java Runtime Environment is not already installed on the host, it is automatically installed.

   The installer copies program files to the specified destination. On completing the installation, the SQL Server database engine is installed.

   Note: You might be prompted to reboot the host when the copy files operation is complete. Click **Yes**.

6. Follow the prompts in the wizard to configure the CommServe:

On this page...	Do this...
SQL User Password	Enter the password for the SQL Server system administrator ("sa") account.
Database Path	Select the destination folder for the SQL Server database files, or accept the default.
CommServe Database	Click **Create a New Database**.
Administrator Account	Enter the user name and password for the CommCell Console administrator account.

On this page...	Do this...
Software Cache Setup	Click **Setup Software Cache**. **Note:** CommServe uses the cache to push software to other hosts and to download CommServe updates.
Completion Report	You are notified that CommServe setup is complete. Click **Finish**.

After you finish

You should disable automatic updates when you complete the CommServe installation, as described in *Adding storage arrays and the UM virtual machine* on page 19.

Installing the SnapProtect Virtual Server Agent (VSA) on ESX proxy computers

A proxy computer is any host running a SnapProtect Virtual Server Agent (VSA). You install the VSA on a Windows VM running on an ESX host. The ESX host should have access to production datastores on the primary storage array.

Before you begin

You should have filled out the worksheet for the SnapProtect Virtual Server Agent (VSA). You can find the worksheet in *Preparing for SnapProtect deployment* on page 6.

About this task

A SnapProtect media agent is automatically installed with the CommServe software. The media agent manages transmission of data between clients and backup media.

Proxy computers offload backup operations from ESX production servers. You can have as many proxies as you want, but you must have at least one.

Tip: The following procedure describes how to run the SnapProtect installation wizard locally. You can run the installation remotely from the CommServe host if you prefer. Click **Download Packages** on the Install Type page of the installation wizard, then follow the prompts.

Steps

1. Download the SnapProtect Download Manager application for Windows from the NetApp Support Site.

   NetApp Support
2. Double-click the Download Manager application, then click **Run** when prompted.
3. Specify the destination folder for the SnapProtect installation wizard, or accept the default.
4. Click **Extract**.

The SnapProtect installation wizard opens.

5. Follow the prompts in the wizard to install the VSA:

On this page...	Do this...
License Agreement	Click **I accept the terms in the license agreement**.
Install Type	Click **Install Packages**.
Installation Type	Click **Standard**.
Installation Options	Click **Join an Existing CommCell**.
Packages to install	Click **Virtualization**.
Destination Folder	Select the destination folder for the VSA software, or accept the default.
Summary	Review your selections and click **Install**. **Note:** If the Microsoft .NET Framework is not already installed on the host, you are prompted to install it first. Click **Yes**.

The installer copies program files to the specified destination.

6. Follow the prompts in the wizard to configure the VSA:

On this page...	Do this...
Firewall Configuration	Accept the default.
CommServe Name	Enter the fully qualified domain name of the CommServe host.
Communication Interface Name	Accept the local NetBIOS name of the host, or enter a user-friendly name. If the proxy host has multiple network interfaces, select the preferred interface name for communications with the CommServe.
Client Certificate	Leave the **Certificate Export File Name** field blank.
Policy Selection	Accept the defaults.
Completion Report	You are notified that VSA setup is complete. Click **Finish**.

After you finish

If the ESX host does not have access to production datastores on the primary storage array, you need to enable access before you configure backups with SnapProtect.

Configuring the storage system

Before you perform backups in SnapProtect, you need to create storage locations for SnapProtect indexes and CommServe disaster recovery. You also need to provision storage for SnapMirror and SnapVault replication. The source and destination clusters for SnapMirror and SnapVault replication must be peered, with peered storage virtual machines (SVMs).

Related tasks

Creating storage locations for SnapProtect indexes and CommServe DR on page 14
Provisioning storage for SnapMirror and SnapVault replication on page 15
Defining SnapMirror and SnapVault relationships on page 17
Enabling NDMP on page 18

Creating storage locations for SnapProtect indexes and CommServe DR

SnapProtect indexes provide fast, highly granular access to data during restore operations. Indexes are stored in disk libraries with paths that point to NetApp primary storage. You need to create a storage location for indexes and another location for the default backup created for CommServe data in the event of a disaster.

Before you begin

You must be a cluster administrator or a storage virtual machine (SVM) administrator to perform these tasks.

About this task

Follow the guidelines in the table below to allocate space for indexes:

Data backed up per week	Space to allocate for indexes
40-60 TB	1 TB
20-40 TB	500 GB
Up to 20 TB	200 GB

Steps

1. Create a storage location for indexes:

a. Create a volume for indexes with the `volume create` command.

Example

The following command creates a 500-GB volume named SPIndex in SVM1 on the aggregate aggr1:

```
cluster1::> volume create -vserver SVM1 -volume SPIndex -aggregate aggr1 -size 500GB
```

b. Create a LUN for indexes with the `lun create` command.

Example

The following command creates a 200-GB LUN named SPIndex in SVM1 at `/vol/SPIndex`:

```
cluster1::> lun create -vserver SVM1 -path /vol/SPIndex/SPIndex -size 200G
```

2. Create a storage location for CommServe DR information:

a. Create a volume for CommServe DR information with the `volume create` command.

Example

The following command creates a 500-GB volume named DRBackup in SVM1 on the aggregate aggr1:

```
cluster1::> volume create -vserver SVM1 -volume DRBackup -aggregate aggr1 -size 500GB
```

b. Create a LUN for CommServe DR information with the `lun create` command.

Example

The following command creates a 200-GB LUN named DRBackup in SVM1 at `/vol/DRBackup`:

```
cluster1::> lun create -vserver SVM1 -path /vol/SPIndex/DRBackup -size 200G
```

After you finish

Map the LUNs to igroups for the protocol in use at your site.

Provisioning storage for SnapMirror and SnapVault replication

You use a group of aggregates called a *resource pool* to provision storage for SnapMirror and SnapVault replication. You need to create a resource pool for SnapMirror secondary storage and

another resource pool for SnapVault tertiary storage. There is no need to create a resource pool for primary storage.

Before you begin

The source and destination clusters for SnapMirror and SnapVault replication must be peered, with peered storage virtual machines (SVMs). For more information, see the *Clustered Data ONTAP 8.2 Cluster and Vserver Peering Express Guide*.

You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

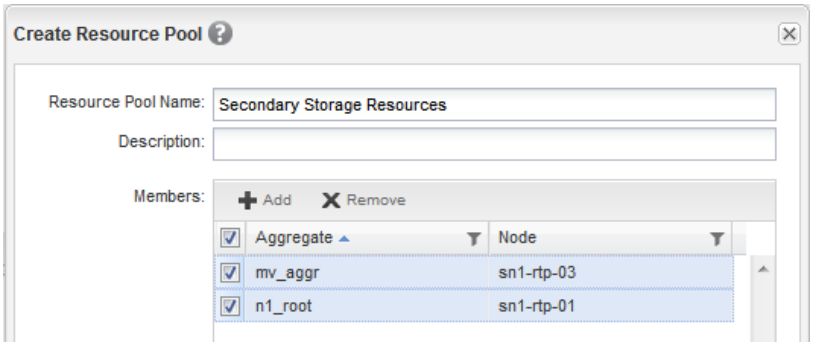
About this task

Resource pools can contain aggregates from different clusters. The same aggregate cannot belong to different resource pools.

Steps

1. Log in to OnCommand Unified Manager.
2. Click **Storage > Resource Pools**.
3. On the Resource Pools page, click **Create**.

   The Create Resource Pool dialog is displayed.
4. In the **Resource Pool Name** field, enter the name of the resource pool for SnapMirror replication.
5. Click **Add**, then add the aggregates you want to assign to the resource pool.



6. When you are satisfied with your choices, click **Create**.

   Unified Manager creates the resource pool.
7. Repeat these steps to create a resource pool for SnapVault replication.

Defining SnapMirror and SnapVault relationships

You define a SnapMirror relationship by creating an association between the SVM for the primary storage array and the SVM for the secondary storage array. You define a SnapVault relationship by creating an association between the SVM for the primary storage array and the SVM for the tertiary storage array. SnapProtect uses these associations to determine which aggregates to write replication data to during backup.

Before you begin

The source and destination clusters for SnapMirror and SnapVault replication must be peered, with peered storage virtual machines (SVMs). For more information, see the *Clustered Data ONTAP 8.2 Cluster and Vserver Peering Express Guide*.

You must be assigned either the OnCommand Administrator role or the Storage Administrator role to perform this task.

Steps

1. Log in to OnCommand Unified Manager.
2. Click **Storage > Storage Virtual Machine Associations**.
3. Click **Create**.

   The Create Storage Virtual Machine Associations wizard opens.
4. Follow the prompts in the wizard to create an association between the SVM for the primary storage array and the SVM for the secondary storage array:

On this page...	Do this...
Select Source Vserver	Click **Select Particular Storage Virtual Machine**, then select the SVM for the primary storage array. In **Allow these kinds of relationships**, click **SnapMirror**.
Select Protection Destination(s)	Select the SVM for the secondary storage array and click **Finish**.

   Unified Manager defines a SnapMirror relationship between primary and secondary storage.
5. Follow the prompts in the wizard to create an association between the SVM for the primary storage array and the SVM for the tertiary storage array:

On this page...	Do this...
Select Source Vserver	Click **Select Particular Storage Virtual Machine**, then select the SVM for the primary storage array. In **Allow these kinds of relationships**, click **SnapVault**.

On this page...	Do this...
Select Protection Destination(s)	Select the SVM for the tertiary storage array and click **Finish**.

Unified Manager defines a SnapVault relationship between primary and tertiary storage.

Enabling NDMP

If you are using NFS datastores, you need to enable NDMP on all arrays.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Use the `system services ndmp on` command to enable NDMP on the primary array.

   #### Example

   The following command enables the NDMP service on every node in cluster1:

   ```
   cluster1::> system services ndmp on
   ```

2. Repeat this step for the secondary and tertiary arrays.

Configuring the SnapProtect CommCell

The CommCell contains the hosts for SnapProtect management software; the primary, secondary, and tertiary storage arrays; and the vCenter Servers for the virtual machines you want to back up. You use the CommCell Console on the CommServe host to configure a CommCell.

Related tasks

Adding storage arrays and the UM virtual machine on page 19
Creating disk libraries for indexes and CommServe disaster recovery on page 20
Creating a VMware virtualization client on page 21

Adding storage arrays and the UM virtual machine

You need to provide the IP address and credentials of the cluster management server for each storage array you add to the CommCell. You also need to specify the IP address and credentials of the UM virtual machine.

Steps

1. Log in to the **CommCell Console** with the user name and password you provided in the CommServe installation and configuration wizard.

   Note: The first time you log in to the CommCell Console you should disable automatic updates. In the CommCell Browser, expand the Client Computers tree and select the CommServe node. Click **All Tasks > Add/Remove Software > Download Software** in the right-click menu. On the **General** tab of the Download and Sync Cache Options dialog, deselect **Download Updates**.

2. In the **CommCell Console**, click **Storage > Array Management**.

   The Array Management dialog opens.

3. Click **Add**.

   The Filer Properties dialog opens.

4. Enter the properties of the primary storage array:

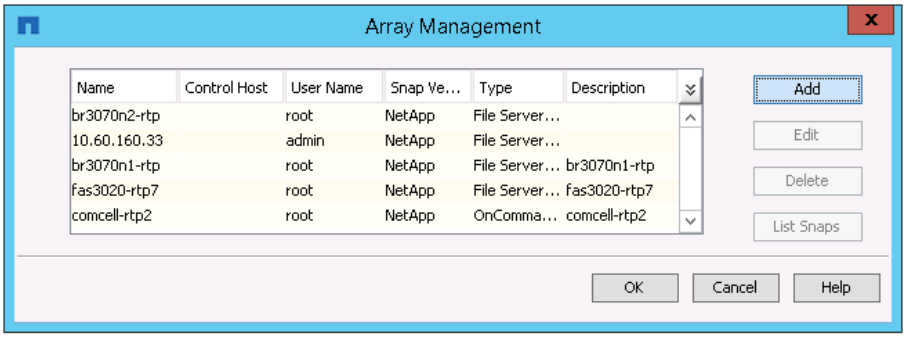
   a. In the **Name** field, enter the IP address of the cluster management server (also called the admin SVM).
   b. In the Credentials area, click **Change**, then enter the user name and password for the cluster management server.
   c. In the Type area, click **File Server**, then click **Primary**.
   d. When you are satisfied with your entries, click **OK**.

SnapProtect connects to the primary storage array using the information you provided.

5. Repeat these steps with the appropriate data for the secondary and tertiary storage arrays. In the Type area, leave **Primary** unselected.
6. Repeat these steps with the appropriate data for OnCommand Unified Manager. In the **Name** field, enter the IP address of the UM virtual machine. In the Type area, click **OnCommand Unified Manager**.

Result

SnapProtect lists each host in the Array Management dialog. It displays the nodes for the hosts in the CommCell Browser.



Creating disk libraries for indexes and CommServe disaster recovery

Indexes and backup information for CommServe disaster recovery are stored in disk libraries with paths that point to NetApp primary storage. You need to identify the locations you created for these resources when you add disk libraries to the CommCell.

Before you begin

You should have created storage locations for indexes and CommServe disaster recovery. For more information, see *Creating storage locations for SnapProtect indexes and CommServe disaster recovery* on page 14.

About this task

You should create the disk library for CommServe disaster recovery before you create the disk library for indexes. SnapProtect automatically uses the first library you create for DR backups.

Steps

1. In the CommCell Browser, expand the **Storage Resources** tree and choose **Libraries** > **Add** > **Disk Library** in the right-click menu.

   The Add Disk Library dialog opens.

2. Enter the information for the CommServe DR disk library:

   a. In the **Name** field, enter the name of the disk library.
   b. In the **MediaAgent** drop-down, select the media agent installed on the CommServe host.
   c. Click **Local Path**, then browse for the drive representing the LUN you are using to store CommServe DR information.

3. When you are satisfied with your entries, click **OK**.

   SnapProtect accesses the storage location using the information you provided.

4. Enter the information for the SnapProtect indexes disk library:

   a. In the **Name** field, enter the name of the disk library.
   b. In the **MediaAgent** drop-down, select the media agent installed on the VSA host.

      Note: If you have configured more than one proxy computer, you must create an indexes disk library for each media agent installed on the proxy.

   c. Click **Local Path**, then browse for the drive representing the LUN you are using to store index information.

5. When you are satisfied with your entries, click **OK**.

   SnapProtect accesses the storage location using the information you provided.

Result

SnapProtect displays the disk libraries in the **Storage Resources** > **Libraries** tree of the CommCell Browser.

Creating a VMware virtualization client

A virtualization client identifies the vCenter Server for the VMs that you want to back up. You can create as many virtualization clients as there are vCenter Servers in your environment.

Steps

1. In the **CommCell Browser**, select **Client Computers** and choose **New Client** > **Virtualization** > **VMware vCenter** in the right-click menu.

   The Create VMware vCenter Client dialog opens.

2. Enter the information for the vCenter client:

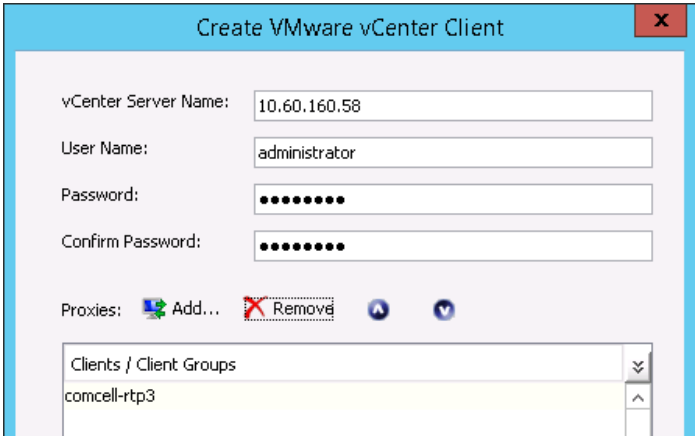
   a. In the **vCenter Server Name** field, enter the host name or IP address of the vCenter Server.

b. In the **User Name** and **Password** fields, enter the credentials for the vCenter Server.
c. In the Proxies area, click **Add**.

   The Select Clients/Client Groups dialog opens.
d. Select the VSA proxy computer, then click **Include**.

   Tip: You can select as many proxy computers as you like. Only the first proxy computer is used to perform backups. If the first proxy is not available, SnapProtect uses the next available proxy in the list.
e. When you are finished making your selections in the **Select Clients/Client Groups** dialog, click **OK**.

   The selected proxy computers are listed in the Create VMware vCenter Client dialog.



f. When you are satisfied with your entries in the **Create VMware vCenter Client** dialog, click **OK**.

Result

SnapProtect displays the node for the virtualization client in the CommCell Browser.

Performing the primary backup

You create the primary Snapshot copy by backing up a virtualization subclient. The virtualization subclient defines the data to be backed up, the storage policy, and the proxy computer for Snapshot copy mount operations.

Related tasks

Specifying the data to be backed up and the storage policy in the subclient on page 23
Backing up the subclient to create the primary Snapshot copy on page 25

Specifying the data to be backed up and the storage policy in the subclient

A virtualization subclient defines the data to be backed up, the storage policy, and the proxy computer for Snapshot copy mount operations.

About this task

If you anticipate that you will be migrating VMs between datastores frequently, you should use a datastore-based discovery rule to define the VMs to be backed up. The rule should discover all VMs with VMDKs in vCenter production datastores (or in some practical subset of vCenter production datastores). Using a datastore-based rule ensures that any VMs you add to the vCenter inventory are backed up automatically.

It also ensures against unnecessary baseline transfers. Ordinarily, SnapProtect performs a full baseline transfer of data from primary storage to secondary storage, or from primary storage to tertiary storage, the first time it replicates data to a mirror or vault. On subsequent backups, it performs an incremental mirror or vault copy only.

When you migrate a VM to a different production datastore, however, SnapProtect will perform a full baseline transfer whether or not one is necessary. It treats the VM as if you had just added it to the inventory. You can prevent that from occurring by specifying a criterion for your discovery rule that is broad enough to include any production datastore that might be a target for VM migration.

Important: Make sure to include only production datastores in the rule criterion. Do not include datastores for swap files.

Steps

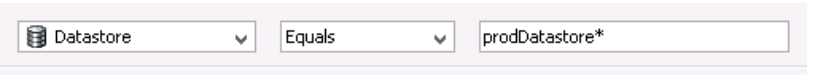
1. In the **CommCell Browser**, expand the node for the virtualization client.
2. Select the defaultBackupSet and choose **All Tasks > New Subclient** in the right-click menu. The Subclient Properties dialog opens.

3. On the **General** tab, enter the name of the subclient in the **Subclient name** field.
4. On the **Content** tab, click **Add**.

   The Add Rule dialog opens.
5. Specify the discovery rule you want to use to define the VMs to be backed up:

   a. In the left-hand drop-down, select **Datastore**.
   b. In the center drop-down, select the operator for the rule.
   c. In the right-hand drop-down, enter a matching pattern for the rule.
   d. When you are satisfied with the rule, click **OK**.

   In the following example, the rule discovers all VMs with VMDKs in production datastores matching the specified pattern: prodDatastore1, prodDatastore2, prodDatastore3, and so forth.



   SnapProtect lists the discovery rule on the **Content** tab.

   Tip: You can test the rule by selecting it and clicking **Preview**.
6. On the **Storage Device** tab, click **Create Storage Policy**.

   The Create Storage Policy Wizard opens.
7. Follow the prompts in the wizard to create a storage policy:

On this page...	Do this...
Enter the storage policy name	Enter the name of the storage policy.
Select a location to store the Index Information	In the **Library** drop-down, select the disk library you created for indexes.
Select a MediaAgent for this copy	In the **MediaAgent** drop-down, accept the default.
Enter the retention criteria for this policy	Click **Retain by Jobs**, then specify the number of jobs in the adjacent combo box.
Select/Add the OnCommand Unified Manager information	In the **Select** drop-down, select the host for OnCommand Unified Manager.
Review your selections	Review your selections and click **Finish**.

   SnapProtect lists the storage policy in the **Storage Device** tab and displays the policy in the Policies area of the CommCell Browser.
8. On the **SnapProtect Operations** tab, click **Select ESX server for snap mount**.

   The Browse for ESX server dialog opens.
9. Select the VSA proxy computer, then click **OK**.

SnapProtect displays the IP address of the proxy computer in the **Host** field on the **SnapProtect Operations** tab.

10. Click **OK**.

    The Backup Schedule dialog opens.

11. Click **Do Not Schedule**.

    You can create the backup schedule when you back up the subclient.

Result

SnapProtect displays the subclient you created in the **defaultBackupSet** tab in the main window of the CommCell Console. It displays the storage policy you defined in the **Policies > Storage Policies** tree in the CommCell Browser.

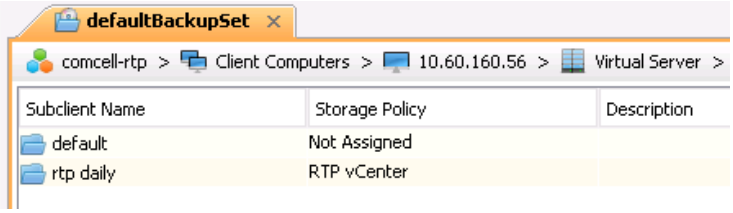
Backing up the subclient to create the primary Snapshot copy

You create the primary Snapshot copy by backing up a virtualization subclient. You can define a schedule for Snapshot copies when you configure the backup of the subclient.

Steps

1. In the **CommCell Browser**, expand the node for the virtualization client, then select the defaultBackupSet.

   The **defaultBackupSet** tab opens in the main window of the CommCell Console.



2. In the **defaultBackupSet** tab, select the virtualization subclient you want to back up and choose **Backup** in the right-click menu.

   The Backup Options for Subclient: *subclient name* dialog opens.

3. In the Select Backup Type area, click **Full**.

   Note: This setting has no effect on subsequent scheduled Snapshot copies. SnapProtect performs the correct type of backup whether or not you have performed a full backup earlier.

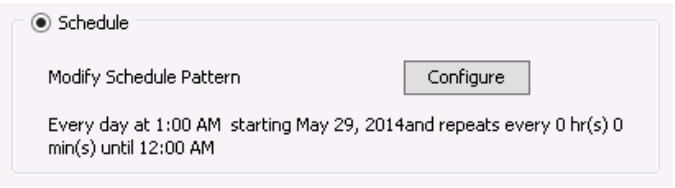
4. In the Job Initiation area, click **Schedule**, then click **Configure**.

The Schedule Details dialog opens.

5. Specify the schedule details:
   a. In the **Schedule Name** field, enter the name of the schedule.
   b. In the left-hand area, select the interval for backups.

      The dialog changes dynamically to reflect your selection.
   c. Complete the schedule details for the interval you selected.
   d. When you are satisfied with your entries, click **OK**.

   The schedule details are displayed in the Job Initiation area.



6. Click **Advanced** at the bottom of the **Backup Options for Subclient:** *subclient name* dialog.

   The Advanced Backup Options dialog opens.

7. Click **Enable Granular Recovery for SnapProtect**, then click **OK**.

   Tip: By enabling granular recovery, you can restore anything from an entire vCenter to a single VM file.

8. When you are satisfied with your entries in the **Backup Options for Subclient:** *subclient name* dialog, click **OK**.

   SnapProtect backs up the subclient at the scheduled interval.

Performing SnapMirror and SnapVault backups

You create SnapMirror and SnapVault copies from the primary Snapshot copy. SnapProtect determines which aggregates to write to based on the relationships you defined for SnapMirror and SnapVault replication.

Related tasks

Creating auxiliary copies for SnapMirror and SnapVault on page 27
Defining SnapMirror and SnapVault relationships on page 17

Creating auxiliary copies for SnapMirror and SnapVault

Backups for SnapMirror and SnapVault replication are called *auxiliary copies*. The *protection type* of the auxiliary copy determines whether SnapProtect performs a mirror or vault copy.

Before you begin

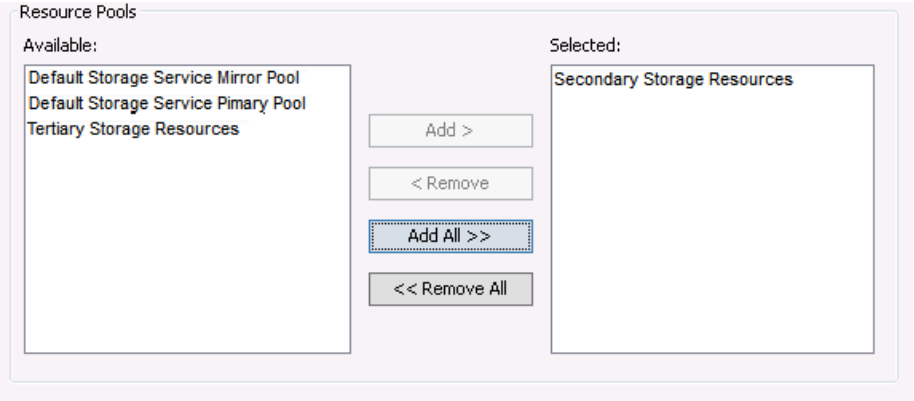
In OnCommand Unified Manager, you should have created the following:

- Resource pools for SnapMirror and SnapVault replication
- Associations between the SVMs for the primary and secondary storage arrays
- Associations between the SVMs for the primary and tertiary storage arrays

Steps

1. In the **CommCell Browser**, expand the **Policies > Storage Policies** tree.
2. Select the storage policy you assigned to the virtualization subclient and choose **All Tasks > Create New Snapshot Copy** in the right-click menu.

   The Snap Copy Properties (Storage Policy:`storage policy name`) dialog opens.
3. On the **General** tab, enter the name of the SnapMirror auxiliary copy in the **Copy Name** field.
4. In the Protection Type area, click **Mirror**.
5. On the **Copy Policy** tab, select Primary(Snap) in the **Specify Source for Auxiliary Copy** drop-down.
6. On the **Provisioning** tab, select the resource pool you created for SnapMirror replication in the list of available resource pools, then click **Add** to move the resource pool to the list of selected resource pools.



7. When you are satisfied with your entries in the **Snap Copy Properties** (Storage Policy:*storage policy name*) dialog, click **OK**.
8. Repeat these steps with the appropriate data for the SnapVault auxiliary copy. On the **General** tab, deselect **Selective Copy**.

Result

SnapProtect displays the auxiliary copies in the tree for the selected storage policy.

Related tasks

Defining SnapMirror and SnapVault relationships on page 17
Running the SnapMirror and SnapVault auxiliary copies on page 28
Provisioning storage for SnapMirror and SnapVault replication on page 15

Running the SnapMirror and SnapVault auxiliary copies

You create replication backups for SnapMirror and SnapVault by running auxiliary copy jobs. You can define a schedule for the backups when you configure the jobs.

About this task

SnapProtect automatically creates volumes for SnapMirror and SnapVault replication when you run an auxiliary copy job.

Steps

1. In the **CommCell Browser**, expand the **Policies > Storage Policies** tree.
2. Select the storage policy you assigned to the virtualization subclient and choose **All Tasks > Run Auxiliary Copy** in the right-click menu.

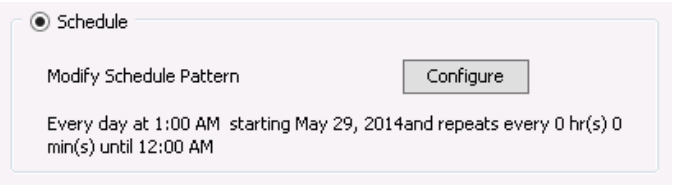
   The Auxiliary Copy Job Options dialog opens.

3. On the **General** tab, click **Select a Copy**, then select the auxiliary copy for SnapMirror replication from the drop-down.
4. In the **Job Initiation** tab, click **Schedule**, then click **Configure**.

   The Schedule Details dialog opens.
5. Specify the schedule details:
   a. In the **Schedule Name** field, enter the name of the schedule.
   b. In the left-hand area, select the interval for backups.

      The dialog changes dynamically to reflect your selection.
   c. Complete the schedule details for the interval you selected.
   d. When you are satisfied with your entries, click **OK**.

   The schedule details are displayed in the Job Initiation area.



6. When you are satisfied with your entries in the Auxiliary Copy Job Options dialog, click **OK**.
7. Repeat these steps with the appropriate data for SnapVault replication.

Result

SnapProtect creates replication backups for SnapMirror and SnapVault at the scheduled intervals.

Verifying your backup configuration

You can verify your backup configuration by restoring a single file. For verification purposes, it is usually easiest to restore the file to a network share.

About this task

SnapProtect uses the *copy precedence* to determine which copy of the data to restore from. You specify the copy precedence on the **Copy Precedence** tab of the storage policy properties.

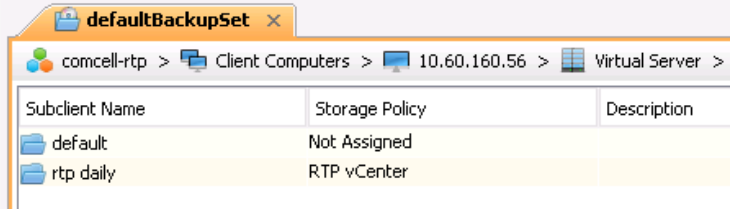
By default, the copy precedence of the SnapMirror and SnapVault types is based on the order in which you created the types. The following table shows the default copy precedence for the order in which you created auxiliary copies in this guide:

Precedence	Copy type
1	Primary (Snap)
2	Primary (Classic) (tape backup)
3	SnapMirror
4	SnapVault

Steps

1. In the **CommCell Browser**, expand the node for the virtualization client, then select the **defaultBackupSet**.

   The **defaultBackupSet** tab opens in the main window of the CommCell Console.



2. In the **defaultBackupSet** tab, select the virtualization subclient that contains the file you want to restore and choose **Browse and Restore** in the right-click menu.

   The Browse and Restore Options dialog opens.

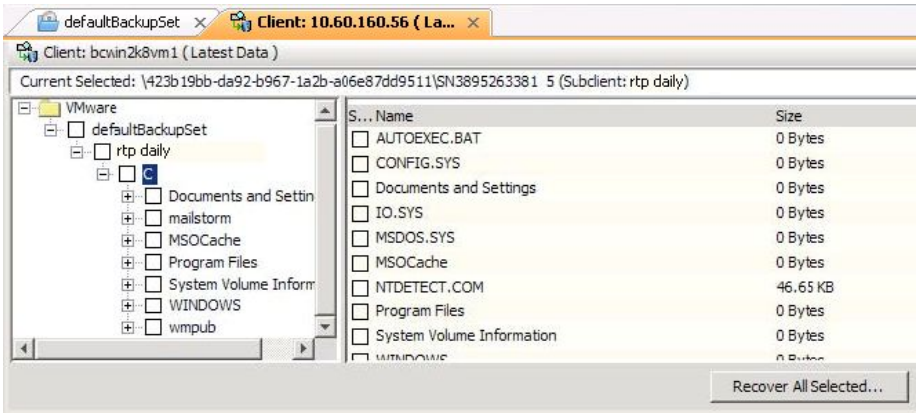
3. On the **Virtual Server** tab, click **Guest Files and Folders**.

4. On the **Advanced Options** tab, click **Browse from copy precedence** and select the precedence for the copy type you want to restore from.

   Note: Make sure the **Use MediaAgent** field is set to the VSA proxy computer.

5. Click **View Content**.

   The ***virtualization client name*** tab opens in the main window of the CommCell Console.



6. Expand the file tree for the virtualization client, then select the file you want to restore in the right-hand pane and click **Recover All Selected...**.

   The Restore Options for All Selected Items dialog opens.

7. Specify the network share for the restored file:

   a. Select the host for the network share in the **Destination** client drop-down.
   b. Select the path of the network share in the **Specify Destination Path** field.
   c. Click **Impersonate User** and enter the user name and password of the network share owner.

8. When you are satisfied with your entries in the **Restore Options for All Selected Items** dialog, click **OK**.

   SnapProtect restores the selected file to the specified location.

Where to find additional information

After you have verified your backup configuration, you can perform full or partial restores as necessary. You can also explore other important SnapProtect features, such as tape backup and deduplication.

You can find more information about these features in the following documentation, available on the NetApp Support Site:

- *SnapProtect Management Software 10.0 Books Online*
  Describes how to back up and restore data with SnapProtect for all supported platforms and applications
- *SnapProtect Management Software 10.0 Upgrade Guide*
  Describes how to upgrade SnapProtect 9.0 to SnapProtect 10.0
- *NetApp Technical Report 3920: NetApp SnapProtect Management Software: Overview and Design Considerations*
  Provides an overview of SnapProtect technology and describes basic configuration steps
- *NetApp Technical Report 4213: FlexPod Datacenter with SnapProtect Implementation Guide*
  Describes how to deploy SnapProtect in a FlexPod architecture

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

T

U

V

W