

# **Provisioning Manager and Protection Manager Administration Guide**

For Use with DataFabric<sup>®</sup> Manager Server 3.8

NetApp, Inc.  
495 East Java Drive  
Sunnyvale, CA 94089 USA  
Telephone: +1 (408) 822-6000  
Fax: +1 (408) 822-4501  
Support telephone: +1 (888) 4-NETAPP  
Documentation comments: [doccomments@netapp.com](mailto:doccomments@netapp.com)  
Information Web: <http://www.netapp.com>  
Part number: 210-04386\_A0  
May 2009



# Contents

<b>Copyright information.....</b>	<b>9</b>
<b>Trademark information.....</b>	<b>11</b>
<b>Contact information.....</b>	<b>13</b>
<b>About this guide.....</b>	<b>15</b>
Audience.....	15
Terminology.....	15
Command, keyboard, and typographic conventions.....	17
Special messages.....	18
<b>What's new in this release.....</b>	<b>21</b>
Overview of new and changed features.....	21
Automated offline dataset and vFiler unit migration .....	22
Custom name prefix for dataset volumes, qtrees, and Snapshot copies.....	22
Deduplication.....	22
Dynamic secondary volume sizing.....	23
SnapVault and SnapMirror relationship cleanup.....	23
Member-level export protocol settings.....	25
Backup of multiple primary volumes to a single secondary volume.....	25
Manual resource selection during primary provisioning.....	25
Data transfer enhancements.....	26
vFiler unit enhancements.....	27
New AutoSupport message information.....	28
Licensing enhancements.....	28
Installation enhancements.....	29
User interface changes.....	29
New and modified CLI commands.....	31
New events.....	35
Limitations.....	36
Application support.....	37
<b>Introduction to provisioning and protection.....</b>	<b>39</b>
What Provisioning Manager is.....	39
What Protection Manager is.....	40

Data management concepts.....	40
What datasets are.....	41
What policies are.....	41
What resource pools are.....	42
What aggregate overcommitment is.....	42
What vFiler units are.....	43
Credentials.....	43
Policies, consistency, and conformance.....	44
Simplifying data and resource management.....	44
Organizing and managing data using datasets.....	45
Protection of discovered data.....	45
Protection Manager automated provisioning for secondary storage.....	45
Provisioning Manager provisioning.....	46
Dataset and vFiler unit migration.....	46
Efficient change implementation.....	47
Provisioning and protection monitoring.....	47
End-to-end status monitoring.....	48
Dashboards for high-level monitoring.....	48
Disaster recovery concepts.....	49
What disaster recovery protection is.....	49
Disaster recovery terminology.....	49
Standard protection or disaster recovery protection of datasets.....	51
Deduplication support.....	52
What deduplication is.....	52
What happens during deduplication.....	53
Role-based access control (RBAC).....	54
<b>SAN resource provisioning example workflow .....</b>	<b>55</b>
SAN provisioning workflow setup.....	55
Develop a SAN provisioning strategy .....	56
SAN provisioning example configuration assumptions.....	58
Configure the storage system to host the vFiler unit.....	61
Create a resource pool.....	63
Create a vFiler template.....	64
Create a vFiler unit.....	65
Create a SAN provisioning policy.....	66
Create a dataset and provision a LUN.....	68

<b>Dataset migration example workflow.....</b>	<b>71</b>
Dataset migration example setup.....	71
Develop a dataset migration strategy .....	72
Dataset migration workflow assumptions.....	73
Add a physical resource to the resource pool.....	74
Start the dataset migration.....	75
Update the migration SnapMirror relationships.....	76
Cut over to the new dataset storage destination.....	77
Clean up the dataset migration.....	78
Manually delete old IPspace and VLAN .....	78
<b>Protection example workflow.....</b>	<b>81</b>
Protection example setup.....	81
Develop a protection strategy.....	82
Protection example configuration assumptions.....	83
Configure the host storage systems.....	86
Create the resource pools.....	88
Evaluate and modify the protection schedules.....	90
Determine the schedule for the primary data node.....	91
Determine the schedule for the connection between the primary and backup nodes.....	91
Determine the schedule for the connection between the backup and mirror nodes.....	93
Create the protection policy and modify the settings.....	93
Evaluate the primary data node.....	94
Evaluate the connection between the primary and backup nodes.....	96
Evaluate the backup node.....	98
Evaluate the connection between the backup and mirror nodes.....	99
Create groups.....	101
Create datasets.....	103
Assign the protection policy to the datasets.....	105
Import discovered relationships.....	106
Verify the protection of the dataset.....	107
Configure alarms.....	107
<b>NAS resource provisioning and data protection example workflow.....</b>	<b>109</b>
NAS provisioning and protection example setup.....	109
Develop a NAS provisioning strategy .....	110

Develop a protection strategy.....	111
NAS provisioning and protection example configuration assumptions.....	112
Configure the hosts.....	114
Create the resource pools.....	117
Create provisioning policies.....	118
Completing the provisioning and protection example workflow.....	119
<b>Disaster recovery example workflow .....</b>	<b>121</b>
Disaster recovery protection example setup.....	121
Develop a disaster recovery strategy.....	122
Disaster recovery protection example assumptions.....	123
Configure the hosts for disaster recovery protection.....	125
Create the resource pools.....	126
Create a failover script.....	127
Create the disaster recovery protection policy.....	129
Create the disaster recovery-capable dataset.....	131
Assign the disaster recovery protection policy to the datasets.....	133
Verify the disaster recovery protection of the dataset.....	134
Test the failover script.....	134
Perform an unscheduled update.....	135
Fail over to the disaster recovery node.....	136
Prepare for recovery after a disaster.....	137
Manual failback using the command line interface.....	138
<b>Combined Protection Manager and SnapManager</b>	
<b>database protection example workflow.....</b>	<b>141</b>
Protected database backup.....	141
Details of the target database .....	142
Primary and secondary storage configuration and topology.....	142
Backup schedule and retention strategy.....	146
Workflow summary for database protected backup.....	147
Protected backup configuration and execution.....	148
Use Protection Manager to configure a secondary resource pool.....	148
Use Protection Manager to configure secondary backup schedules.....	149
Use Protection Manager to configure a secondary backup	
protection policy.....	151
Use SnapManager for Oracle to create the database profile	
and assign a protection policy.....	152

Use Protection Manager to provision the new dataset.....	154
Use SnapManager for Oracle to create a protected backup.....	155
Use SnapManager for Oracle to confirm backup protection.....	156
Use SnapManager for Oracle to restore backups from secondary storage.....	156
<b>Troubleshooting.....</b>	<b>159</b>
Data ONTAP 7.2 issues impacting protection on vFiler units.....	159
Display issue in the Diagnose OSSV Host wizard.....	160
Viewing Windows directories with Unicode characters in their names.....	160
Backup of directory named with non-ASCII characters fails.....	162
Adding directory to dataset fails with error.....	162
Temporary conformance impact of deleting volumes or qtrees.....	162
Deleting unnecessary secondary volumes.....	163
Message: “qtree is not the source for the snapmirror destination”.....	164
Number of bytes of data transferred during backup is not accurate.....	164
Using the NetApp Management Console with DataFabric	
Manager prior to 3.5.....	165
Provisioning failure despite sufficient space.....	165
SnapMirror job fails with "process was aborted" message.....	165
Ways to investigate problems with hosts.....	166
Locating information about the client configuration.....	167
<b>NetApp Management Console.....</b>	<b>169</b>
What NetApp Management Console is.....	169
Applications that run in NetApp Management Console .....	170
NetApp Management Console window layout and navigation.....	171
NetApp Management Console window customization.....	172
NetApp Management Console data filtering.....	173
Printing Help topics.....	174
<b>Administrator roles and capabilities.....</b>	<b>175</b>
<b>List of events.....</b>	<b>177</b>
<b>Index.....</b>	<b>197</b>





# Copyright information

---

Copyright © 1994-2009 NetApp, Inc. All rights reserved. Printed in the U.S.A.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S.A. patents, foreign patents, or pending applications.

**RESTRICTED RIGHTS LEGEND:** Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).



# Trademark information

---

All applicable trademark attribution is listed here.

NetApp, the Network Appliance logo, the bolt design, NetApp-the Network Appliance Company, Cryptainer, Cryptoshred, DataFabric, DataFort, Data ONTAP, Decru, FAServer, FilerView, FlexClone, FlexVol, Manage ONTAP, MultiStore, NearStore, NetCache, NOW NetApp on the Web, SANscreen, SecureShare, SnapDrive, SnapLock, SnapManager, SnapMirror, SnapMover, SnapRestore, SnapValidator, SnapVault, Spinnaker Networks, SpinCluster, SpinFS, SpinHA, SpinMove, SpinServer, StoreVault, SyncMirror, Topio, VFM, VFM (Virtual File Manager), and WAFL are registered trademarks of NetApp, Inc. in the U.S.A. and/or other countries. gFiler, Network Appliance, SnapCopy, Snapshot, and The evolution of storage are trademarks of NetApp, Inc. in the U.S.A. and/or other countries and registered trademarks in some other countries. The NetApp arch logo; the StoreVault logo; ApplianceWatch; BareMetal; Camera-to-Viewer; ComplianceClock; ComplianceJournal; ContentDirector; ContentFabric; EdgeFiler; FlexShare; FPolicy; Go Further, Faster; HyperSAN; InfoFabric; Lifetime Key Management, LockVault; NOW; ONTAPI; OpenKey, RAID-DP; ReplicatorX; RoboCache; RoboFiler; SecureAdmin; Serving Data by Design; Shadow Tape; SharedStorage; Simplicore; Simulate ONTAP; Smart SAN; SnapCache; SnapDirector; SnapFilter; SnapMigrator; SnapSuite; SohoFiler; SpinMirror; SpinRestore; SpinShot; SpinStor; vFiler; Virtual File Manager; VPolicy; and Web Filer are trademarks of NetApp, Inc. in the U.S.A. and other countries. NetApp Availability Assurance and NetApp ProTech Expert are service marks of NetApp, Inc. in the U.S.A.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the U.S.A. and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the U.S.A. and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the U.S.A. and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks. NetApp, Inc. NetCache is certified RealSystem compatible.



# Contact information

---

Information about how to contact NetApp is listed here.

NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Documentation comments: doccomments@netapp.com
Information Web: <a href="http://www.netapp.com/">http://www.netapp.com/</a>



# About this guide

---

Here you can learn what this document describes and who it is intended for, what special terminology is used in the document, what command, keyboard, and typographic conventions this document uses to convey information, and other details about finding and using information.

This document provides examples of typical workflows that administrators can perform by using Protection Manager and Provisioning Manager applications. These applications simplify data protection, disaster recovery, and provisioning tasks, as shown in the end-to-end workflows included in this document.

This guide does not cover administration tasks except as part of a specific workflow. The Protection Manager and Provisioning Manager Help systems provide all of the individual tasks you can perform with these applications, as well as related conceptual and reference material.

## Next topics

[Audience](#) on page 15

[Terminology](#) on page 15

[Command, keyboard, and typographic conventions](#) on page 17

[Special messages](#) on page 18

## Audience

Here you can learn who this document is written for and the assumptions that were made about the preexisting knowledge and experience you have.

This document is for system administrators and others interested in protecting and provisioning data on primary and secondary storage systems by using Protection Manager and Provisioning Manager.

This document is written with the assumption that you are familiar with the following technology:

- Data ONTAP operating system software
- The protocols you use for file sharing or transfers, such as NFS, CIFS, iSCSI, FCP, or HTTP
- The client-side operating systems (UNIX, Linux, or Windows)

## Terminology

To understand the concepts in this document, you might need to know the terms defined here.

## General storage system terminology

- Storage systems that run Data ONTAP are sometimes referred to as *filers*, *appliances*, *storage appliances*, or *systems*. The name of the FilerView graphical user interface for Data ONTAP reflects one of these common usages.
- *Controller* or *storage controller* refers to the component of a storage system that runs the Data ONTAP operating system and controls its disk subsystem. Controllers or storage controllers are also sometimes called *storage appliances*, *appliances*, *storage engines*, *heads*, *CPU modules*, or *controller modules*.

## Active/active configuration terminology

- An *active/active configuration* is a pair of storage systems configured to serve data for each other if one of the two systems becomes impaired. In Data ONTAP documentation and other information resources, active/active configurations are sometimes also referred to as *clusters* or *active/active pairs*.
- When in an active/active configuration, systems are often called *nodes*. One node is sometimes called the *local node*, and the other node is called the *partner node* or *remote node*.
- *Controller failover*, also referred to as *cluster failover* or *CFO*, refers to the technology that enables two storage systems to take over each other's data, thus improving data availability.
- *Fabric-attached MetroCluster* refers to an active/active configuration running the *syncmirror\_local* and *cluster\_remote* licenses, where the nodes are attached to two pairs of Fibre Channel switches, and they are separated by more than 500 meters.
- *FC direct-attached topologies* are topologies in which the hosts are directly attached to the storage system. Direct-attached systems do not use a fabric or FC switches.
- *FC dual fabric topologies* are topologies in which each host is attached to two physically independent fabrics that are connected to storage systems. Each independent fabric can consist of multiple FC switches. A fabric that is zoned into two logically independent fabrics is not a dual fabric connection.
- *FC single fabric topologies* are topologies in which the hosts are attached to the storage systems through a single FC fabric. The fabric can consist of multiple FC switches.
- *iSCSI direct-attached topologies* are topologies in which the hosts are directly attached to the storage controller. Direct-attached systems do not use networks or Ethernet switches.
- *iSCSI network-attached topologies* are topologies in which the hosts are attached to storage controllers through Ethernet switches. Networks can contain multiple Ethernet switches in any configuration.
- *Mirrored active/active configuration* is similar to the standard active/active configuration, except that there are two copies, or *plexes*, of the data. This is also called *data mirroring*.
- *Remote storage* refers to the storage that is accessible to the local node, but is at the location of the remote node.
- *Single storage controller configurations* are topologies in which there is only one storage controller used. Single storage controller configurations have a single point of failure and do not support cfmodes in FC SAN configurations.



- *Standard active/active configuration* refers to a configuration set up so that one node automatically takes over for its partner when the partner node becomes impaired.
- *Stretch MetroCluster* refers to an active/active configuration running the `syncmirror_local` and `cluster_remote` licenses, where the nodes are separated by up to 500 meters, and no switches are used between the nodes. This configuration is also sometimes called a *nonswitched MetroCluster*.

## Storage hardware terminology

- *AT-FCX* refers to an enhanced FC-AL to Serial ATA (SATA) bridge used in some disk shelves.
- *Disk shelf* refers to a unit of the disk subsystem component of the storage system.
- *ESH (Embedded Switching Hub)* disk shelf module refers to a component that provides a means of managing an FC-AL loop in an intelligent manner, such that a single drive failure does not take down the loop. It also contains the enclosure services processor, which communicates the environmental data of the disk shelf.
- *ESH2* disk shelf module refers to a second-generation ESH module.
- *ESH4* disk shelf module refers to a third-generation ESH module.
- *FC HBA for Disk* or *FC HBA* refers to the Fibre Channel host bus adapter that connects the node to the switch or to the disks.
- *Host bus adapters (HBAs)* are FC or iSCSI I/O adapters that connect a host I/O bus to a computer's memory system in SCSI environments.
- *LRC (Loop Resiliency Circuit)* disk shelf module refers to a component that keeps the Fibre Channel-Arbitrated Loop (FC-AL) intact during the addition and removal of disks within a disk shelf. It also contains the enclosure services processor, which communicates the environmental data of the disk shelf.
- *Target adapters* are I/O adapters that reside on the storage system and receive data from the host. A target adapter that is already attached to the storage system controller is an onboard adapter; a target adapter that is separately installed in one of the system's available slots is a target expansion adapter. Onboard adapters can also be configured to operate in initiator mode in which they connect to disk shelves. Most storage systems also support the use of expansion adapters that operate in initiator mode.

## General terms

- The term *enter* means pressing one or more keys on the keyboard and then pressing the Enter key, or clicking in a field in a graphical interface and typing information into it.
- The term *type* means pressing one or more keys on the keyboard.

# Command, keyboard, and typographic conventions

This document uses command, keyboard, and typographic conventions that help you enter commands.

## Command conventions

In examples that illustrate commands executed on a UNIX workstation, the command syntax and output might differ, depending on your version of UNIX.

## Keyboard conventions

- When describing key combinations, this document uses the hyphen (-) to separate individual keys. For example, "Ctrl-D" means pressing the "Control" and "D" keys simultaneously.
- This document uses the term "Enter" to refer to the key that generates the digital equivalent of a carriage return, although the key is named "Return" on some keyboards.

## Typographic conventions

The following table describes typographic conventions used in this document.

Convention	Type of information
<i>Italic font</i>	Words or characters that require special attention.  Placeholders for information you must supply. For example, if the guide says to enter the <code>arp -d hostname</code> command, you enter the characters "arp -d" followed by the actual name of the host.  Book titles in cross-references.
Monospaced font	Command names, option names, keywords, and daemon names.  Information displayed on the system console or other computer monitors.  The contents of files.
<b>Bold monospaced font</b>	Words or characters you type. What you type is always shown in lowercase letters, unless you must type it in uppercase letters.

## Special messages

This document might contain the following types of messages to alert you to conditions you need to be aware of. Danger notices and caution notices only appear in hardware documentation, where applicable.

**Note:** A note contains important information that helps you install or operate the system efficiently.

**Attention:** An attention notice contains instructions that you must follow to avoid a system crash, loss of data, or damage to the equipment.

**Danger:** A danger notice warns you of conditions or procedures that can result in death or severe personal injury.

**Caution:** A caution notice warns you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous.



# What's new in this release

---

This chapter describes new features and changes in the Protection Manager and Provisioning Manager applications. These applications operate with DataFabric Manager server 3.8 or later. Detailed information about the features is provided in the NetApp Management Console online Help.

## Next topics

[\*Overview of new and changed features\*](#) on page 21

[\*User interface changes\*](#) on page 29

[\*New and modified CLI commands\*](#) on page 31

[\*New events\*](#) on page 35

[\*Limitations\*](#) on page 36

[\*Application support\*](#) on page 37

## Overview of new and changed features

Provisioning Manager and Protection Manager in DataFabric Manager server 3.8 contains new and changed features as described in this section.

## Next topics

[\*Automated offline dataset and vFiler unit migration\*](#) on page 22

[\*Custom name prefix for dataset volumes, qtrees, and Snapshot copies\*](#) on page 22

[\*Deduplication\*](#) on page 22

[\*Dynamic secondary volume sizing\*](#) on page 23

[\*SnapVault and SnapMirror relationship cleanup\*](#) on page 23

[\*Member-level export protocol settings\*](#) on page 25

[\*Backup of multiple primary volumes to a single secondary volume\*](#) on page 25

[\*Manual resource selection during primary provisioning\*](#) on page 25

[\*Data transfer enhancements\*](#) on page 26

[\*vFiler unit enhancements\*](#) on page 27

[\*New AutoSupport message information\*](#) on page 28

[\*Licensing enhancements\*](#) on page 28

[\*Installation enhancements\*](#) on page 29

## Automated offline dataset and vFiler unit migration

Provisioning Manager supports automated offline dataset and vFiler unit migration to another storage system. Offline migration means that at some point in the migration process, you need to shut down all applications that use the data in the vFiler unit or dataset.

You can migrate a dataset only if all of the storage for the dataset is in one vFiler unit. In addition, that vFiler unit must contain all of the volumes for the dataset and no other volumes, with the exception of the root volume or root qtree. Therefore, you migrate a dataset when your storage strategy is focused on datasets; you migrate a vFiler unit when your storage strategy is focused on vFiler units. When you create a dataset, you can specify an existing vFiler unit or you can have the provisioning application create a new vFiler unit for the dataset.

If Protection Manager is also licensed, the protection application automatically performs the migration and relationships do not need to be rebaselined.

## Custom name prefix for dataset volumes, qtrees, and Snapshot copies

When creating or editing a dataset, you can choose a custom name prefix for the volumes and qtrees in that dataset to easily locate volumes, qtrees, and Snapshot copies.

For NAS provisioned primary dataset nodes, you can specify a custom name prefix for all volumes included within the dataset. You can name the qtrees within those volumes at the time you create the qtree. If you do not use a custom name prefix, the dataset name is used.

For nonprimary nodes, you can specify a custom name prefix to apply to all volumes and qtrees in backups and mirrored copies. If your primary node is unavailable, you can locate the appropriate volumes and qtrees on a nonprimary node, using the custom name prefix you specified when you created or edited your dataset.

Snapshot copies include a date stamp prefix. The full name of the Snapshot copy includes the retention type, host name, volume name, and qtrees included within the Snapshot copy.

This feature is implemented only on new relationships. Volumes, qtrees, and Snapshot copies that existed in your environment prior to this release are not affected.

## Deduplication

Deduplication is a provisioning application option that you can enable on your storage nodes to eliminate duplicate data blocks and thereby reduce the amount of storage space used to store active data.

On the affected volumes, deduplication allows you to reduce the amount of space used to store active data, or even allows you to purposely over-deduplicate and store more bytes of data than the capacity of the available physical storage.

You can enable your provisioning policies to support three modes of deduplication:

### **On-demand deduplication**

Deduplication is executed on a selected volume when you click the Dedupe Now button on the Provisioning tab.

- Automated** If this option is enabled on a dataset node, deduplication is run automatically on any volume in that node when the amount of new data written to that volume reaches 20% of total volume space.
- Scheduled deduplication** If this option is enabled on a dataset node, deduplication is run automatically on the volumes in that node on the days of the week, time period, and at a frequency that you have specified.

If a secondary volume has deduplication enabled, snapshots are updated without disrupting the deduplication of blocks.

When assigning a provisioning policy to a dataset implementing secondary deduplication, you must use SnapVault relationships, rather than Qtree SnapMirror relationships.

## Dynamic secondary volume sizing

Dynamic secondary volume sizing enables the protection application to set the size of new volumes in proportion to the primary data and its replication copies. It also enables modification of the size of existing destination volumes.

This volume sizing feature is enabled or disabled by using the `dpDynamicSecondarySizing` option in Operations Manager. The option is disabled by default when upgrading from DataFabric Manager 3.7.1 or prior releases, to maintain backward compatibility. In new installations, the option is enabled by default.

When the option is enabled, the protection application sizes new secondary volumes to a size capable of containing the primary data plus replication copies. It also resizes existing secondary volumes when necessary to provide enough space for a data transfer or when a new backup or mirror relationship is added. When the option is disabled, the secondary volume is thin-provisioned to the size of the aggregate that contains the volume.

If the dynamic secondary volume sizing option is enabled and the `dpMaxFanInRatio` option (which is a ratio of multiple primary volumes to a single secondary volume) is set to a number larger than 1, then the secondary volume is sized to the sum of all source volumes.

The volume sizing feature applies only to the following configurations:

- Volumes must be managed by the protection application and associated with a dataset.
- The dataset must have a backup policy assigned to it and be using either SnapVault or Qtree SnapMirror protection.

Dynamic secondary volume resizing does not take place for Volume SnapMirror-based transfers (protection application Mirror operations) or for Open Systems SnapVault transfers.

## SnapVault and SnapMirror relationship cleanup

You can control the rules used by Protection Manager for the cleanup of relationships that had been part of a dataset. This feature includes two new configurable global options.

## dpReaperCleanupMode

The new global option `dpReaperCleanupMode` is configurable using the `dfm option set` command. This option supports the following values:

- Orphans

Command: `dfm option set dpReaperCleanupMode=Orphan`

This is the default setting.

During the relationship cleanup process, the Orphan setting allows deletion of orphan relationships only from nonimported relationships that are no longer in a dataset. This setting also prevents the cleanup of any redundant relationships. Any relationship that was originally imported into Protection Manager (in other words, was not created by Protection Manager) is not deleted and becomes an orphan. An imported relationship can be identified by using the `dfpm relationship list -x` command.

- Automatic

Command: `dfm option set dpReaperCleanupMode=Automatic`

In this mode, all relationships that are currently not in any dataset, but were previously part of a dataset that has been deleted, are removed within 1 to 2 hours after the dataset is deleted. This means that all relationships, including imported relationships, are removed from storage systems. The secondary volumes for these removed relationships remain on the destination storage system, but they are removed from the Protection Manager database. The volumes are rediscovered by Protection Manager 15 minutes later, but are no longer managed by Protection Manager, nor are they marked as imported or orphan. To maintain legacy behavior for systems upgrading to the current release, use the Automatic setting.

- Never

Command: `dfm option set dpReaperCleanupMode=Never`

During the cleanup process, orphan relationships are deleted only from nonimported relationships that are no longer in a dataset. A relationship that is imported has the "imported" property visible in the output of the `dfpm relationship list -x` command.

For new installations and upgrades of Protection Manager, the `dpReaperCleanupMode` global option is set to the Orphans value. If a user reverts a database to a previous version, the `dpReaperCleanupMode` option is removed.

## dpReBaselineMode

The new global option `dpReBaselineMode` is configurable using the `dfm option set` command. This option supports the following values:

- Confirm

Command: `dfm option set dpReBaselineMode=Confirm`

This is the default setting.

When the option is set to Confirm and the system identifies that a relationship is broken, the dataset is marked as nonconformant and a user confirmation is required before the protection application tries to reestablish the relationship and reestablish the data baseline.



- Automatic

Command: `dfm option set dpReBaselineMode=Automatic`

To maintain the legacy behavior of no user confirmation for systems upgrading to the current release, use the Automatic setting.

## Member-level export protocol settings

The Provisioning wizard gives you the option of enabling a different set of export protocols for each member that you add to a dataset through the Provisioning wizard.

If you have not already specified an enabled set of export protocols in the provisioning policies that you assign to your dataset nodes, you can use the Provisioning wizard to assign individual sets of export protocols to each new dataset member that you add through the Provisioning wizard.

## Backup of multiple primary volumes to a single secondary volume

Protection Manager now supports the backup of multiple volumes in primary storage to a single volume in secondary storage for SnapVault and Qtree SnapMirror.

When the 500-volume limit for storage systems might not allow a one-to-one ratio of primary volumes to secondary volumes, you can configure the protection application through the Operations Manager global option `dpMaxFanInRatio`

The following limitations apply:

- The protection application does not support volume SnapMirror-based mirroring from multiple primary volumes to a single secondary volume.
- All the primary volumes and the secondary volume must be members of the same dataset.
- The protection application implementation of Open Systems SnapVault backup is not affected by the `dpMaxFanInRatio` option.

## Manual resource selection during primary provisioning

You can now manually select storage resources for primary node provisioning.

In previous releases of Provisioning Manager, the selection of aggregates for provisioning on a primary node could only be done automatically. The provisioning application selected an aggregate for provisioning from the resource pool attached to the primary node of the dataset. Now you can manually select a single storage system or aggregate from the resource pool during primary provisioning. Selecting multiple aggregates or storage systems is not supported.

Allowing Provisioning Manager to select the appropriate resource for provisioning is still the recommended approach, as it saves time and improves capacity utilization. However, the option to manually select volumes or aggregates can be useful in some circumstances.

If you manually select a storage system, the resource selector chooses the aggregate on that storage that it determines best meets the needs of the provisioning request and displays the aggregate name in the

dry run results. If the selected aggregate does not meet the criteria of the provisioning policy, the request fails and other aggregates are tried for provisioning.

If you select an aggregate, dry run results display for that aggregate. If the selected aggregate does not meet the criteria of the provisioning policy, the request fails, and the application does *not* try to select an alternative aggregate. If resources are not manually selected, Provisioning Manager performs automatic selection of resources for provisioning.

## Data transfer enhancements

Several new features improve the scalability, performance, and planning capability of data transfers in Protection Manager environments.

### Next topics

[Data transfer reporting](#) on page 26

[Parallel data restore operations](#) on page 26

[Increased number of concurrent streams](#) on page 27

## Data transfer reporting

New data transfer reports provide detailed information about Open Systems SnapVault, SnapVault, and SnapMirror jobs.

There are two types of reports: individual transfer reports and "rollup" reports. The individual transfer reports display information about all data transfer jobs that occurred in the preceding 24-hour period and that relate to a particular mirror or backup relationship. The information reported includes how much data was transferred from primary to secondary, the rate of the transfer, the time a transfer started, and the time a transfer stopped.

The "rollup" reports display summarized transfer activities for each relationship on a weekly, monthly, quarterly, and yearly basis.

Reports are grouped into three categories:

- Dataset reports display the transfer details for each mirror and backup relationship within the dataset.
- Mirror reports display information about mirror data transfers.
- Backup reports display information about backup data transfers.

## Parallel data restore operations

Restore operations can now be performed in parallel for transfers going to the same destination.

You can perform parallel restore operations only for data that is in different qtrees. You can adjust the number of transfers that can occur in parallel by using the global option `dpRestoreTransfersPerHost`. The maximum number of transfers per destination is 64; the default value is 8.

## Increased number of concurrent streams

Data ONTAP has increased the number of concurrent NDMP data transfer operations that can be run, improving Protection Manager scalability.

This can increase the overall backup rate for your storage environment. Some platforms running Data ONTAP 7.2.4 and 7.3 allow a maximum of 128 NDMP transfer operations. This number increases to 512 for some platforms running Data ONTAP 7.3.1 and higher. The protection application optimizes use of these transfer rates as the backup loads require.

The maximum allowable number of concurrent replication operations is determined by a combination of the platform and the version of Data ONTAP running on the platform, and the replication technology that is licensed. A matrix of the maximum number of concurrent replication operations per platform and application license is available in the *Data ONTAP 7.3 Data Protection Online Backup and Recovery Guide*. Setting the `maxActiveDataTransfers` option higher than the recommended value can cause performance issues due to data transfer retries on the system.

### Related information

*Data ONTAP Data Protection Online Backup and Recovery Guide -*  
[http://now.netapp.com/NOW/knowledge/docs/ontap/ontap\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml)

## vFiler unit enhancements

There are several enhancements to the vFiler unit creation workflow, providing the ability to create VLANs and to configure active/active partner interfaces and IPspaces. New reports and events, and the ability to view vFiler unit setup details, have also been added.

### Next topics

*VLAN creation* on page 27

*Active/active partner interface and IPspace creation* on page 28

*vFiler unit setup details* on page 28

*New reports and events for storage system and vFiler unit services* on page 28

## VLAN creation

Provisioning Manager now supports the creation of VLAN interfaces as part of vFiler unit creation.

The provisioning application binds the IP addresses of the vFiler unit to the newly created VLAN. You can specify a physical interface or a virtual interface, and you can provide a VLAN tag or an identifier to create a new VLAN interface during the vFiler unit creation and setup workflow. The VLANs are persistent across reboots.

This feature is available on systems running Data ONTAP 7.0 or higher.

## Active/active partner interface and IPspace creation

Active/active partner interfaces and IPspaces can be created during the process of creating and setting up a vFiler unit.

During the creation of a vFiler unit, you can configure new IPspaces and new VLAN interfaces. If the vFiler unit is part of an active/active configuration, a corresponding VLAN interface is created on the active/active partner node to provide appropriate failover capabilities.

An IPspace is also created on the partner node when a vFiler unit is created on a nondefault IPspace, if an IPspace is not present on the node already. Interface configurations and VLANs remain persistent across reboots. Provisioning Manager does not support creation and configuration of partner interfaces for preexisting interfaces.

This feature is available on systems running Data ONTAP 7.0 or higher.

## vFiler unit setup details

Configuration information for a vFiler unit is now displayed in Protection Manager, for vFiler units created on Data ONTAP 7.3.1 or higher.

## New reports and events for storage system and vFiler unit services

Reports, custom report catalog fields, and database views have been added for reporting service availability of CIFS, NFS, iSCSI, and Fibre Channel services for storage systems and vFiler units. Events are now triggered when the service availability changes for a storage system or vFiler unit.

## New AutoSupport message information

The Provisioning Manager section of DataFabric Manager-generated AutoSupport messages now contains data migration information related to deduplication policy options and deduplication job execution.

## Licensing enhancements

Provisioning Manager and Protection Manager in DataFabric Manager server 3.8 implements several changes related to licensing.

- Node counts

There is now a mechanism to count and report the number of nodes managed by Provisioning Manager and Protection Manager. This information is reported in the Configuration Details dialog box, which is accessed by clicking **Help > About > Configuration**.

The `dfm about` and `dfm diag` commands also list the node limits and current node counts for Provisioning Manager and Protection Manager licenses.

- Node limits

Alerts are now generated if the node limit is approached or is reached.

## Installation enhancements

Provisioning Manager and Protection Manager in DataFabric Manager server 3.8 implements a new, more robust NetApp Management Console installation wizard for Windows and Linux.

The new wizard supports the installation of multiple versions and multiple users concurrently accessing the same installation. During upgrades, the wizard uninstalls the previous software version, deleting all files except the existing log files and preferences.

For new installations and upgrades on Windows, the default install location is C:\Program Files\NetApp\Management Console\. The default log location is C:\Documents and Settings\<username>\.netapp\management\_console\<version>.

For Linux, an RPM installation package is now used. Installations or upgrades can also be completed using the RPM commands `rpm -i <rpm filename>` and `rpm -U <rpm filename>`. The Linux installation files are located at `/usr/lib/netapp/management_console/<version>`. You can launch the application from `/usr/bin/nmconsole-<version>`. Log files are stored in a `.netapp/management_console` directory within the user's home directory.

## User interface changes

Provisioning Manager and Protection Manager include significant changes to the graphical user interface to support the new and changed features in DataFabric Manager server 3.8.

For detailed information about the new features, see [Overview of new and changed features](#) on page 21 and the NetApp Management Console Help.

**Usability changes** Significant redesign of the user interface is implemented to improve the user experience:

- Changed the Unprotected Data dashboard and window
- Added filters to several user interface windows
- Modified the Edit Datasets wizard
- Modified the Groups user interface
- Changed the user interface main navigation
- Modified the Add Datasets wizard
- Modified the Datasets Overview tab
- Renamed and changed the locations of some items:
  - "System" changed to "Notifications" and now contains only Events and Alarms
  - Groups and Jobs were moved under Data

**Support for the migration feature**

Changes made to the user interface to support the new provisioning migration capability include the following:

- Added a Migration tab to the Datasets window
- Added a Data Migration wizard
- Added a vFiler Migration wizard
- Modified the Add Dataset wizard
- Modified the Edit Dataset wizard
- Added the "Migration capable" column to the Dependencies tab on the Data Resource Pools window
- Added the "Migration status" column to the Hosts vFiler Units window

**Support for the deduplication feature**

Changes made to the user interface to support the new provisioning deduplication capability include the following:

- The Add Provisioning Policy and the Provisioning Policy edit dialog box now display options that enable deduplication and specify deduplication modes.
- The Datasets window Provisioning tab displays a Dedupe Now button that enables you to start deduplication on-demand on those dataset nodes that are enabled for deduplication.
- The Datasets window Provisioning tab contains a Deduplication tab that enables you to review the deduplication status and space savings on selected volumes.
- The Provisioning Policies displays the deduplication status and the deduplication schedule, if applicable, of the selected provisioning policy
- The Jobs window might display events related to deduplication or over-deduplication conditions.

**Dataset wizard changes**

Changes made to the Dataset wizard include the following:

- Added a Dataset Migration page that contains an option to enable or disable dataset migration
- Added a Resource Selection page that contains an option to allow the system to automatically select a resource or to allow the user to manually select a resource from the attached resource pools
- Added a Member Level Export Settings page that contains an option to enable or disable member level export settings

**vFiler wizard changes**

Changes made to the user interface to support VLAN creation and active/active configurations include the following:

- Partner interface displayed in active/active configurations

- VLAN column added
- IP addresses and network masks support both IPv4 and IPv6 formats

### **Support for the custom name prefix for volumes and qtrees**

Changes are made to the user interface to support the addition of custom name prefixes for dataset volumes and qtrees and for Snapshot copies.

## **New and modified CLI commands**

Provisioning Manager and Protection Manager include several new and changed CLI commands to support the new and modified features in DataFabric Manager server 3.8.

For detailed information about these commands, see the DataFabric Manager (dfm and dfpm) man pages. For information related to the new features, see the NetApp Management Console.

### **Dataset and vFiler unit migration**

New commands include the following:

- `dfpm migrate cancel`
- `dfpm migrate cleanup`
- `dfpm migrate cutover`
- `dfpm migrate fix`
- `dfpm migrate start`
- `dfpm migrate status`
- `dfpm migrate update`

Modified commands include the following:

- `dfpm dataset create`

New option: `-e ip-address:netmask`

- `dfpm dataset modify`

New option: `-e ip-address:netmask`

New option: `-f`

- `dfm host set` (Operations Manager command)

New option: `defaultvFilerInterface`

## Deduplication

New commands include the following:

- `dfpm dataset dedupe abort`
- `dfpm dataset dedupe start`
- `dfpm dataset dedupe status`
- `dfpm dataset undedupe start`

Modified commands include the following:

- `dfpm policy get`

New options: `volOverDeduplicatedThreshold`,  
`volNearlyOverDeduplicatedThreshold`

New output: `dedupe`, `dedupeSchedule`

- `dfpm policy set`

New options: `dedupe`, `dedupeSchedule`

New output: `dedupe`, `dedupeSchedule`

- `dfm options set` (Operations Manager command)

New options: `volOverDeduplicatedThreshold`,  
`volNearlyOverDeduplicatedThreshold`,  
`aggrOverDeduplicatedThreshold`,  
`aggrNearlyOverDeduplicatedThreshold`

- `dfm options list` (Operations Manager command)

New output: `aggrNearlyOverDeduplicatedThreshold`,  
`aggrOverDeduplicatedThreshold`,  
`volNearlyOverDeduplicatedThreshold`,  
`volOverDeduplicatedThreshold`

- `dfm aggr get` (Operations Manager command)

New output: `Aggregate Nearly Over Deduplicated Threshold`,  
`Aggregate Over Deduplicated Threshold`

- `dfm aggr set` (Operations Manager command)

New options: `aggrOverDeduplicatedThreshold`,  
`aggrNearlyOverDeduplicatedThreshold`

- `dfm volume get` (Operations Manager command)



New output: Volume Nearly Over Deduplicated Threshold, Volume Over Deduplicated Threshold

- `dfm volume set` (Operations Manager command)

New options: `volOverDeduplicatedThreshold`,  
`volNearlyOverDeduplicatedThreshold`

**vFiler unit management** New commands include the following:

- `dfpm vfiler info`

Modified commands include the following:

- `dfpm vfiler setup`

New option: `-i ip-interface-bindings`

**Provisioning export settings**

Modified commands include the following:

- `dfpm dataset list`
- `dfpm dataset provision`

**Provisioning and protection licensing**

Modified commands include the following:

- `dfm about`
- `dfm diag`

**Provisioning policy**

Modified commands include the following:

- `dfpm policy set`

**Provisioning AutoSupport**

Modified commands include the following:

- `dfm autosupport view`

**Custom prefix names for volumes, qtrees, and Snapshot copies**

Modified commands include the following:

- `dfpm dataset create help`

New option: `-q volume-qtree-name-prefix`

- `dfpm dataset create`

New option: `-q volume-qtree-name-prefix`

- `dfpm dataset list`
- `dfpm dataset modify`

New option: `-q volume-qtrees-name-prefix`

- `dfpm dataset modify help`

New option: `-q volume-qtrees-name-prefix`

- `dfm option list` (Operations Manager command)
- `dfm option set` (Operations Manager command)

New option: `pmCustomNameUsePrefix`

### **SnapVault and SnapMirror relationship management**

`dfpm relationship list`

New options: `-a, -i, -m, -o, -r, -x`

### **Snapshot copy name management**

`dfm option set` (Operations Manager command)

New option: `pmUseSDUCompatibleSnapshotNames`

### **Dataset relationship listing**

Command option combinations with modified outputs include the following:

`dfpm dataset list -R`

### **Operations Manager global options for provisioning**

New global options include the following:

- `dpMaxFanInRatio`  
Values: 1 through 50 (although 50 is not an absolute upper limit, it is a practical limit)
- `dpDynamicSecondarySizing`  
Values: enable, disable
- `dpReaperCleanupMode`  
Values: Orphans, Automatic, Never
- `dpReBaselineMode`  
Values: Confirm, Automatic

## New events

DataFabric Manager server 3.8 includes a number of new events to support new and changed features.

### Migration events

Event name	Severity level
Dataset Not Migrating	Normal
Dataset Migrating	Normal
Dataset Migrated With Errors	Warning
Dataset Migrated	Normal
Dataset Migrate Failed	Error
vFiler Unit Not Migrating	Normal
vFiler Unit Migrating	Normal
vFiler Unit Migrated With Errors	Warning
vFiler Unit Migrated	Normal
vFiler Unit Migrate Failed	Error

### Deduplication events

Event name	Severity level
Aggregate Nearly Over Deduplicated	Warning
Aggregate Not Over Deduplicated	Normal
Aggregate Over Deduplicated	Error
Volume Nearly Over Deduplicated	Warning
Volume Not Over Deduplicated	Normal
Volume Over Deduplicated	Error
Dataset Member Dedupe Operation Failed	Info
Dataset Member Dedupe Operation Succeeded	Info

### Network services events

Event name	Severity level
CIFS Service - Up	Normal
CIFS Service - Down	Warning
NFS Service - Up	Normal
NFS Service - Down	Warning
iSCSI Service - Up	Normal
iSCSI Service - Down	Warning
FCP Service - Up	Normal
FCP Service - Down	Warning

### Management station events

Event name	Severity level
Protection Manager Node Limit Nearly Reached	Warning
Protection Manager Node Limit OK	Normal
Protection Manager Node Limit Reached	Error
Provisioning Manager Node Limit Nearly Reached	Warning
Provisioning Manager Node Limit OK	Normal
Provisioning Manager Node Limit Reached	Error

## Limitations

NetApp Management Console in DataFabric Manager server 3.8 does *not* include the following functionality for Provisioning Manager and Protection Manager.

Provisioning Manager for use with DataFabric Manager server 3.8 does not support the following:

- Migration
  - Migration of a dataset that is not attached to a vFiler unit
  - Migrations of volumes or qtrees that use SnapMirror

- Support for IPv6 during migration
- Migration of SAN FC LUNs
- Migration of performance data associated with the migrated vFiler unit
- Deduplication
  - Deduplication on datasets configured for disaster recovery protection
  - The maximum size of volumes for which deduplication is enabled is constrained by the model of the storage system and the version of Data ONTAP that it is running.

## Application support

You can run the protection and provisioning storage management applications on any of several Windows or Linux server platforms.

The Protection Manager and Provisioning Manager applications are viewable through the NetApp Management Console client. The console supports the following server platforms:

- Windows XP
- Windows Vista
- Windows 2008
- Windows 2003
- Red Hat Enterprise Linux versions 4 and 5
- Oracle Enterprise Linux
- SUSE Linux Enterprise Server versions 9 and 10

Beginning with Operations Manager 3.8, NetApp Management Console no longer supports Solaris operating systems.



# Introduction to provisioning and protection

---

This chapter describes the functionality of the Provisioning Manager and Protection Manager applications that run in NetApp Management Console.

It describes the data-management objects the provisioning and protection applications use and how these objects can be used to help you protect your data and provision your resources easily and efficiently.

The Provisioning Manager and Protection Manager applications can be installed on Linux-based or Windows-based systems running Open Systems SnapVault.

You can view more information about provisioning and protection concepts and tasks in the NetApp Management Console Help.

## Next topics

[\*What Provisioning Manager is\*](#) on page 39

[\*What Protection Manager is\*](#) on page 40

[\*Data management concepts\*](#) on page 40

[\*Policies, consistency, and conformance\*](#) on page 44

[\*Simplifying data and resource management\*](#) on page 44

[\*Provisioning and protection monitoring\*](#) on page 47

[\*Disaster recovery concepts\*](#) on page 49

[\*Deduplication support\*](#) on page 52

[\*Role-based access control \(RBAC\)\*](#) on page 54

## What Provisioning Manager is

Provisioning Manager simplifies and automates the tasks of provisioning and managing storage for NAS and SAN access, and it improves efficiency in storage utilization.

Provisioning Manager is a licensed application for use with DataFabric Manager. The provisioning application can be accessed through NetApp Management Console, which is the client platform for NetApp Manageability Software applications.

The provisioning application provides the following capabilities:

- User-defined policies to automate storage provisioning and configure default settings for exporting storage
- Periodic conformance checking to ensure the provisioned storage conforms to the provisioning policy
- Manual controls for resizing space and capacity of existing storage

- Manual controls for provisioning new and existing storage
- Offline automated migration of data to new storage systems

Anyone using Provisioning Manager should be familiar with general storage provisioning concepts.

## What Protection Manager is

Protection Manager helps you manage your backup and mirror relationships and perform failover operations easily and efficiently by eliminating repetitive tasks and automating some tasks.

Typically, data and resource management is time consuming because it involves manual analysis and management of storage capacity, network bandwidth, schedules, retention policies, and other infrastructure variables. Protection Manager simplifies this work by employing configuration policies, convenient wizards, and automated verification of certain aspects of the data protection configuration. It lets you launch a backup, restore, or failover operation with a single click.

The protection application can perform the following actions:

- Use policies to manage primary data, storage, and backup and mirror relationships
- Manage local and remote backups and mirror copies
- Provision the secondary storage for backups and mirrored copies based on policies you assign
- Enable disaster recovery capability if you install the licensed disaster recovery option
- Automatically validate your backup and disaster recovery configuration with a conformance checker

Anyone using Protection Manager should be familiar with general data-protection and disaster recovery concepts. Protection Manager uses Data ONTAP data-protection technologies, such as Snapshot copies, SnapVault, Open Systems SnapVault, and SnapMirror.

## Data management concepts

It is helpful to have a basic understanding of some concepts that apply to provisioning and protection activities in NetApp Management Console.

### Next topics

[What datasets are](#) on page 41

[What policies are](#) on page 41

[What resource pools are](#) on page 42

[What aggregate overcommitment is](#) on page 42

[What vFiler units are](#) on page 43

[Credentials](#) on page 43



## What datasets are

In the simplest terms, a *dataset* is a collection of user data you manage as a single unit, plus all the replicas of that data. The data is identified by the volume, qtree, or directory in which it is located.

Because you manage a dataset as a single unit, its members should have common management requirements. In Protection Manager, members of a dataset should share the same data-protection requirements. In Provisioning Manager, each node in a dataset might not share the same provisioning requirements, but all members of each node should share the same provisioning requirements.

For example, different types of data supporting the same application would probably share the protection requirements of the application. You would want to collect that data in the same dataset, even if the data were stored in different volumes or qtrees. By configuring protection appropriate for the application the data supports and applying that protection to the dataset, you apply it to all the dataset members.

For provisioning, if a dataset had a protection policy that created primary, backup, and mirror nodes, your provisioning requirements for each node might be different. You might want to provision the primary node on high-availability storage but provision the mirror node on less expensive, low-availability storage.

## What policies are

A *policy* is a set of rules that specifies the intended management of dataset members. You can apply the same policy to multiple datasets, leveraging your configuration of the policy across the datasets. If you update a policy, the update is propagated across all the datasets to which the policy is applied.

From the NetApp Management Console, you can use the following policies to quickly implement changes across an entire organization:

- **Protection policies**

A protection policy defines when data copies used for backups and mirror copies are created on the primary storage, when to transfer the copies, and what is the maximum amount of data to transfer at scheduled times. The protection policy settings define how long to retain copies at each backup location and the warning and error thresholds for lag time. You cannot override a policy for specific members of a dataset; if some members of a dataset require different policy parameters, you need to move those members to a different dataset.

- **Disaster recovery policies**

A protection policy that supports failover from a primary to a secondary node is considered to be capable of disaster recovery. The disaster recovery node is always directly connected to the primary node, and its storage is made available after a disaster.

- **Provisioning policies**

A provisioning policy defines how you want to have storage provisioned, exported, and managed, and what your space requirements are. For example, a provisioning policy might specify that when a storage container reaches the Nearly Full or Full threshold, an event message is sent or the size of the volume is increased (which provides more space for all the qtrees in the volume).

A provisioning policy applies to all volumes, qtrees, or LUNs in a dataset node. You cannot assign different provisioning policies to individual members within a dataset.

If you also have the protection license and the dataset has a mirror or backup node, you can create and assign a different policy that defines provisioning and storage management on a secondary and tertiary node.

## What resource pools are

A *resource pool* is a collection of unused physical storage (such as storage systems or aggregates) from which new volumes or LUNs can be provisioned to contain data. If you assign a storage system to a resource pool, all aggregates on that storage system become available for provisioning.

Any unused physical resource in a resource pool is potentially eligible for provisioning. You can organize physical resources into resource pools by location, performance, or other important factors.

The protection and provisioning applications automatically provision volumes or LUNs to meet the necessary requirements for compatible software version, licensing, and available space.

In the licensed protection application, you assign a resource pool to the backup and mirror destinations of a dataset. The protection application can then automatically provision volumes out of the physical resources in the resource pool to contain backups and mirror copies. To prevent conflicts, physical storage assigned to one resource pool cannot be assigned to a second resource pool.

With the licensed provisioning application, you can use resource pools to fulfill requests for storage space for the primary or secondary data of a dataset. By applying a provisioning policy to a dataset node, the provisioning application applies the resiliency characteristics and space settings in the policy to automatically select the resources needed to fulfill a provisioning request.

## What aggregate overcommitment is

You can increase the size of a volume to be larger than its containing aggregate, which is referred to as *aggregate overcommitment* or thin provisioning.

Aggregate overcommitment provides flexibility to the storage provider. By using aggregate overcommitment, you can appear to provide more storage than is actually available from a given aggregate.

Using aggregate overcommitment could be useful if you are asked to provide greater amounts of storage than you know will be used immediately. Additionally, if you have several volumes that sometimes need to grow temporarily, the volumes can dynamically share the available space with each other.

The volume size is not limited by the aggregate size. In fact, each volume could, if required, be larger than the containing aggregate. The storage provided by the aggregate is consumed only as LUNs are created or data is appended to files in the volumes.

To use aggregate overcommitment, you must initially create your aggregates with the proper space guarantee settings. This can be done by using Data ONTAP commands. See the *Data ONTAP Storage Management Guide* for details.

You can set the aggregate overcommitment thresholds by using the **Add Resource Pool** wizard or the **Properties** sheet on the **Resource Pools** window.

There are two aggregate overcommitment thresholds:

<b>Overcommitted</b>	Indicates the total number of aggregates in a resource pool for which the committed space exceeds the overcommitted threshold. Status is applied to the individual aggregates of a resource pool. If one of the aggregates exceeds the overcommit limits, an event is generated.
<b>Nearly Overcommitted</b>	Indicates the total number of aggregates in a resource pool for which the committed space exceeds the nearly overcommitted threshold. Status is applied to the individual aggregates of a resource pool. If one of the aggregates exceeds the overcommit limits, an event is generated.

#### Related information

*Data ONTAP Storage Management Guide -  
[http://now.netapp.com/NOW/knowledge/docs/ontap/ontap\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml)*

## What vFiler units are

A *vFiler unit* is a partition of a storage system and the associated network resources. Each vFiler partition appears to the user as a separate storage system on the network and functions as a storage system.

Access to vFiler units can be restricted so that an administrator can manage and view files only on an assigned vFiler unit, not on other vFiler units that reside on the same storage system. In addition, there is no data flow between vFiler units. When using vFiler units, you can be sure that no sensitive information is exposed to other administrators or users who store data on the same storage system.

You can assign volumes or LUNs to vFiler units in NetApp Management Console. You can create up to 65 vFiler units on a storage system.

To use vFiler units you must have the MultiStore software licensed on the storage system that is hosting the vFiler units.

You can use vFiler templates to simplify creation of vFiler units. You create a template by selecting a set of vFiler configuration settings, including CIFS, DNS, NIS, and administrative host information. You can configure as many vFiler templates as you need.

## Credentials

The host login and Network Data Management Protocol (NDMP) credentials must be properly set on each host you are using.

The host login credentials are the user name and password that DataFabric Manager uses to log in to the host.

The NDMP login credentials are the user name and password that DataFabric Manager uses to communicate with the host over NDMP. DataFabric Manager automatically manages the password based on the user name provided.

For vFiler units, DataFabric Manager uses the login and NDMP credentials of the system that is hosting the vFiler unit.

## Policies, consistency, and conformance

All organizations have requirements that specify how frequently you must back up data and how long you must keep backup copies of data. Protection Manager policy-based protection provides consistency and, therefore, conformance predictability.

When using traditional data-protection methods in an enterprise environment, there is always the danger that inconsistent deployment or operator error might make data nonconformant with requirements. The consistency provided by Protection Manager enables you to focus on addressing other threats to data conformance, such as network outages.

After you assign a policy and resource pools to a dataset, the protection defined by that policy applies until you redefine the policy. System outages and other problems might temporarily interfere with protection, but if a policy is defined to meet certain requirements and the dataset conformance status is Conformant and its protection status is Protected (green), the protection defined in the policy is being achieved.

The policies you apply to datasets are also a statement of intent of how you plan to protect data in that dataset. In reviewing your data protection implementation, you can infer the protection requirements of data in a given dataset, because the policy applied to that dataset defines the protection intended to meet business requirements.

## Simplifying data and resource management

Provisioning Manager and Protection Manager help you leverage your provisioning and protection strategies through the consolidated control of relationships, the use of policies, the automated provisioning of secondary storage, and the discovery of hosts and existing relationships.

### Next topics

[\*Organizing and managing data using datasets\*](#) on page 45

[\*Protection of discovered data\*](#) on page 45

[\*Protection Manager automated provisioning for secondary storage\*](#) on page 45

[\*Provisioning Manager provisioning\*](#) on page 46

[\*Dataset and vFiler unit migration\*](#) on page 46

[\*Efficient change implementation\*](#) on page 47

## Organizing and managing data using datasets

Organizing data with the same provisioning or protection requirements into a dataset enables you to manage the data's provisioning and protection relationships as a single unit, leveraging each task across the membership.

In Protection Manager, managing protection relationships as a single unit means that each choice you make for the dataset is applied to the protection of each dataset member. These choices can include which protection policy best serves the data's restore or disaster recovery requirements, which schedule to use, which resource pool is appropriate for each node of the policy, and so on.

In Provisioning Manager, each choice you make for the dataset node is applied to the provisioning of each volume, qtrees, and LUN in the dataset node. These choices can include which provisioning policy best serves that node's provisioning and storage export requirements, which resource pool is appropriate for provisioning each dataset node, storage sizes for data and for Snapshot copies, and so on.

Datasets also decrease the number of factors you need to consider in developing a provisioning or protection strategy. Instead of having to track the specific requirements of each individual dataset member, you only need to evaluate which data and which resources share the same provisioning or protection requirements, add them to a dataset, and track them as a unit. After the dataset is created, deploying satisfactory provisioning or protection for the dataset results in deploying satisfactory provisioning or protection for each individual dataset member.

## Protection of discovered data

When Protection Manager automatically detects new storage or hosts, what happens next depends on whether the data is protected by a policy.

If the data is unprotected, the application reports the data in the dashboard. From the **Unprotected Data** panel, you can drill-down to find detailed information that helps you decide whether to back up and mirror the data.

If new data is created in volumes, qtrees, or directories on a storage system, Open Systems SnapVault client, vFiler unit, or aggregate that is already protected, that protection is extended automatically to the new data. For example, if you create a FlexVol volume on a storage system that is a member of a protected dataset, the protection configured for that dataset is applied automatically to the data in the new FlexVol volume. Protection Manager creates backup and mirror relationships for the new data, as defined in the policy applied to the dataset, and provisions storage on the destination systems for copies of the new data.

Automatically protecting new data created on protected hosts and aggregates decreases the risk of new data going unprotected until its presence is detected.

## Protection Manager automated provisioning for secondary storage

Protection Manager automatically provisions secondary storage, saving you considerable time and effort.

One of the most time-consuming and complicated aspects of a traditional data protection implementation is provisioning storage for backups and mirror copies. There are many factors that you must consider when looking for a suitable destination for copies of protected data, and you must repeat the process for each relationship in your overall protection strategy.

Protection Manager automatically provisions volumes for backups and mirror copies, as needed, out of the resource pool assigned to each node in a protection policy to ensure that the volumes provisioned for your backups and mirror copies meet your data protection needs.

For example, you could leverage the automated provisioning feature to simplify your resource pools. For each geographic site in your protection plan, you could create two resource pools for backups:

- A Gold-level resource pool for backups of business-critical data, containing physical resources that can support the more rigorous restore requirements of that data
- A resource pool for backups of all the other data you need to protect, containing every other physical resource at the site

You would assign the Gold-level resource pool to the backup node of datasets containing business-critical data. You would assign the other resource pool to the backup node of the other datasets. Protection Manager automated provisioning would then create secondary volumes for the backups from the resource pools. The provisioned secondary volumes support the restore requirements of the data, because the most appropriate volumes were selected or created and the resource pools were populated with physical resources suited to the task.

## Provisioning Manager provisioning

When you create a dataset for provisioning, you can assign a provisioning policy that provides settings for automatically configuring storage for the dataset. You can also manually manage volumes or LUNs in a dataset, and their individual export protocols, by using the **Provisioning** wizard.

If you have enabled the provisioning license only, the primary dataset node is provisioned.

If you also have the protection license enabled, the licensed provisioning application can provision volumes, qtrees, or LUNs on the backup and mirror dataset nodes.

When a storage container runs out of space, the actions taken are determined by the provisioning policy. The licensed application might send space warning messages and delete old Snapshot copies, or for SAN storage, might try to increase the container size.

The provisioning application provisions volumes and qtrees (in NAS environments) or volumes and LUNs (in SAN environments) from the resource pool assigned to the dataset.

## Dataset and vFiler unit migration

If a dataset needs more storage, you can automatically migrate it offline to another, larger storage system.

If all of the data in a dataset is exported through a single vFiler unit, the Provisioning Manager application provides controls for migrating the dataset and the vFiler unit in a series of three steps.

The migration is automated, which means that Provisioning Manager automatically migrates the dataset and vFiler unit configurations. The migration is also offline, which means that applications that use the data in the dataset must be shut down during one of the migration steps. However, you can perform each of the three steps at different times when it is most convenient: for example, during a period of low activity.

## Efficient change implementation

By consolidating your provisioning and protection components into datasets, policies, and resource pools, you have fewer items to keep up to date. If business requirements change, there are fewer items you need to modify to support that change, so you can implement changes much more efficiently than by using traditional provisioning and data protection methods.

For example, if you had a dataset of 500 qtrees that frequently missed its backup window, you might choose to start the backups earlier. Using traditional data protection methods, you would have to update each of the 500 backup relationships manually or create a script to update the relationships.

Using Protection Manager, you would update the 500 relationships by modifying one schedule—the schedule assigned to the connection between the primary data and the backup node in the policy applied to the dataset. After you modified the schedule, Protection Manager would update the schedule on each policy to which the schedule was assigned. The change would then be propagated to all the datasets to which the policy was applied, and therefore to all the data in each dataset.

Protection Manager also makes protection topology changes more efficient. For example, if you had a dataset that was backed up to a secondary node, you might want to add a mirror copy of that secondary node. Using Protection Manager, you would change the policy assigned to that dataset from a **Back up** policy to a **Back up, then mirror** policy, then add a resource pool to the mirror node. Protection Manager would determine how to set up the mirror relationships and provision the necessary storage on the mirror node.

## Provisioning and protection monitoring

Protection Manager and Provisioning Manager continually monitor all the components in your data protection implementation to help ensure that your data is protected as defined in the policy applied to its dataset.

### Next topics

*End-to-end status monitoring* on page 48

*Dashboards for high-level monitoring* on page 48

## End-to-end status monitoring

Instead of separately monitoring each component involved in provisioning and protection, you can monitor the status values displayed in the dashboard. The status values indicate whether there are problems in the provisioning or protection of your datasets.

For example, consider the dataset protection status, which you can use to verify that your overall protection implementation is functioning as intended.

If a dataset is protected by the **Back up, then mirror** policy and someone misconfigures the credentials on the host containing the mirror copy, the Protection Manager server cannot log in to the host. The dataset protection status turns from Protected (green) to Partial Failure (yellow). You can configure the system to alert you to the change in status, so you would immediately know which dataset was experiencing protection problems. You could then pursue remedial action according to the priority of the dataset.

Using traditional methods of managing data protection, you would need to monitor the systems storing backups and mirror copies. You would be alerted to a problem on the host containing the mirror copy, but you would have to track the relationship from the problem back to the mirrored data to identify the specific data affected. This approach is especially problematic for data under compliance requirements; you need to be sure that data is protected to meet those requirements.

By monitoring the dataset status in Protection Manager, you can be confident that the data protection you implemented is being carried out as intended.

## Dashboards for high-level monitoring

Provisioning Manager and Protection Manager include a set of “dashboard” panels that provide at-a-glance information on status, protected and unprotected data, resource pool usage, lag times, and recent events. From each dashboard panel, you can click a button to go directly to a window displaying detailed information.

Protection Manager includes the following dashboard panels:

- Failover Readiness
- Failover Status
- Top Five Events
- Dataset Protection Status
- Protected Data
- Unprotected Data
- Dataset Lags
- Resource Pools

Provisioning Manager includes the following dashboard panels:

- Dataset Conformance Status



- Top Five Events
- Dataset Resource Status
- Dataset Space Status
- Resource Pool Space Status
- Resource Pools

## Disaster recovery concepts

The following information describes disaster recovery, its concepts and terminology, and its basic configuration requirements.

### Next topics

*[What disaster recovery protection is](#)* on page 49

*[Disaster recovery terminology](#)* on page 49

*[Standard protection or disaster recovery protection of datasets](#)* on page 51

## What disaster recovery protection is

The disaster recovery feature enhances your data protection services by enabling you to continue to provide data access to your users, even in the event of a mishap or disaster that disables or destroys the storage system in your primary node.

If disaster recovery protection is installed, you can quickly enable your secondary storage systems to provide primary data storage access to your users with little or no interruption, until your primary storage systems are reenabled or replaced.

To use the disaster recovery feature, you must enable the disaster recovery license on your system. You must also have the protection license enabled.

## Disaster recovery terminology

It is helpful to have an understanding of the basic concepts associated with disaster recovery terminology.

The implementation of disaster recovery protection in the licensed protection application relies on the following concepts:

<b>Failover</b>	An automated process which, when invoked, transfers primary storage capability and accessibility from threatened, disabled, or destroyed storage systems in a primary node to secondary storage systems in the disaster recovery node.
<b>Failback</b>	Command-line based procedures that restore primary storage function to the original primary storage site after its storage systems are reenabled or replaced.

<b>Disaster recovery capable</b>	Describes a dataset that is configured with the protection policies and provisioned with the primary storage and secondary storage resources to support disaster recovery protection.
<b>Disaster recovery node</b>	The dataset secondary storage node that is configured to also provide failover primary storage access to users in the event of mishap or disaster making the original primary storage systems unavailable.
<b>Disaster recovery relationship</b>	The type of data protection and failover procedures configured between the primary storage and secondary storage systems (in the disaster recovery node), and between the secondary storage systems and any tertiary storage systems.
<b>Qtree SnapMirror</b>	The technology that supports qtree-to-qtree disaster recovery capable backup relationships in the licensed protection application and possible failover operations between primary storage systems and secondary storage systems. In disaster recovery protection policies, secondary storage is located in the disaster recovery node.
<b>Volume SnapMirror</b>	The technology that supports volume-to-volume disaster recovery capable mirror relationships in the licensed application and possible failover operations between primary storage and secondary storage systems. In disaster recovery protection policies, secondary storage is located in the disaster recovery node.
<b>SnapMirror relationship break</b>	The automated event during failover that breaks the SnapMirror relationship between primary storage and secondary storage in the disaster recovery node.
<b>Failover state</b>	Dashboard status in the licensed application that indicates the progress and success of a failover operation if the failover process is invoked. Possible states include: Ready, Failing over, Failed over, and Failover Error.
<b>Failover readiness</b>	Dashboard status in the licensed application that indicates the readiness of the managed datasets to successfully carry out failover operations.
<b>Failover script</b>	An optional user-authored script that specifies data application-related operations that might need to be performed before and after the failover invoked SnapMirror relationship break between primary storage and secondary storage in the disaster recovery node.
<b>Rebaselining</b>	The protection backup or mirroring of data by the transfer or copy of the entire body of data from primary to secondary or secondary to tertiary storage. All initial backup or mirror operations from primary to secondary or secondary to tertiary storage are baseline operations and can be quite lengthy. Succeeding backup or mirror operations can be incremental, involving only the transfer from source to destination that has changed since the last backup or mirror operation. When assigning a new protection policy (disaster recovery capable or not) after a disaster and successful failover, the most preferable choice might be to assign and set up a protection policy that minimizes rebaselining of data in the primary, secondary, and tertiary storage.

## Standard protection or disaster recovery protection of datasets

Configuration of datasets for disaster recovery protection is similar to configuration of datasets for standard data protection. However, the features provided by disaster recovery protection require some additional dataset configurations.

### Provisioning policies assigned to secondary storage

If you have Provisioning Manager installed and you want to assign an optional provisioning policy to your secondary node. You have the following options:

- In datasets with disaster recovery protection, you can assign either a NAS, SAN, or Secondary storage type provisioning policy to the secondary storage disaster recovery node.
- In datasets with standard protection, you can only assign a Secondary storage type provisioning policy to the secondary node.

**Note:** In all cases, you can chose not to assign a storage policy and assign physical resources directly to each node as was necessary in previous versions of the licensed protection application.

### Exporting data to secondary storage

If you are configuring disaster recovery protection, you have the option to assign an export protocol to the disaster recovery node so that in case of failover, users can access data in the disaster recovery node using the same protocols they used to access data in the original primary node.

- If you have Provisioning Manager installed and you assign a provisioning policy for NAS or SAN type storage to the disaster recovery node, you can also enable export protocols to access that data: CIFS and NFS for NAS type storage; iSCSI and Fibre Channel protocol for SAN type storage. Provisioning Manager also exports secondary storage through a vFiler unit if a disaster recovery node is associated with a vFiler unit.
- If you are only configuring standard protection, not disaster recovery protection, you cannot enable export protocols on the secondary storage node through this management application.

### SnapVault and SnapMirror backup protection requirements


- In datasets configured for disaster recovery backup protection, SnapMirror licenses on the primary and disaster recovery node systems are required to support the backup operation. The protection application will configure underlying Qtree SnapMirror relationships that support backup and failover processes between the primary and disaster recovery nodes.
- In datasets configured for standard backup protection, either SnapVault or SnapMirror licenses on the primary and secondary storage systems will support the backup operation.

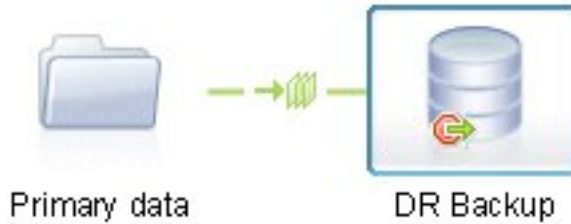
### Changes in the user interface

Several modifications have been made to the Protection Manager user interface to differentiate datasets configured for standard protection and disaster recovery protection.

**Updated  
policy graph**

The policy graph for a protection policy that is capable of disaster recovery looks similar to a policy graph for a regular protection policy, except that the disaster

recovery node is designated with a disaster recovery flag (  ) to indicate the ability of that node to take over primary data node functions if failover is invoked.



**New  
dashboard  
windows**

The Protection Manager dashboard reports on disaster recovery state and status to provide information at-a-glance that all is well or that something needs attention. In this illustration, the **Failover Readiness** panel and **Failover Status** panel use color, icons, and text to display the state and status for datasets that are capable of disaster recovery. The colors and text vary according to the status of the activity.

Policy wizards, Disaster Recovery tab, and the Policy Overview tab have tables that include a disaster recovery column to indicate whether a policy supports disaster recovery.

The disaster recovery policy and uses a policy icon (  ) to indicate that, if applied, it will protect the dataset for disaster recovery.

## Deduplication support

The following information describes what deduplication is and what occurs when it is enabled.

**Next topics**

[What deduplication is](#) on page 52

[What happens during deduplication](#) on page 53

## What deduplication is

Deduplication is a provisioning application option that you can enable on your storage nodes to eliminate duplicate data blocks to reduce the amount of storage space used to store active data.

On the affected volumes, deduplication allows you to reduce the amount of space used to store active data, or even allows you to purposely over deduplicate and store more bytes of data than the capacity of the available physical storage.

You can enable your provisioning policies to support three modes of deduplication.

<b>On-demand deduplication</b>	On-demand deduplication is executed on a selected volume that is enabled for deduplication when you click the <b>Dedupe Now</b> button on your Provisioning tab.
<b>Automated</b>	Automated deduplication, if enabled on a dataset node, is run automatically on any volume in that node when the amount of new data written to that volume reaches 20% of total volume space.
<b>Scheduled deduplication</b>	Scheduled deduplication, if enabled on a dataset node, is run automatically on the volumes in that node on the days of the week, during a particular time period, and at a frequency that you have specified.

## What happens during deduplication

After deduplication is enabled and started, the provisioning application performs a full or incremental consolidation of duplicate data blocks on the volumes on which deduplication has been applied.

- The deduplication process is triggered by one of three possible events:
  - If the "On-demand deduplication" mode is enabled on a dataset node, deduplication is run on-demand by the user on a selected volume.
  - If the "Automated deduplication" mode is enabled on a dataset node, deduplication begins automatically on a volume residing on that dataset node when the amount of new or changed data on that volume reaches 20%.
  - If the "Scheduled deduplication" mode is enabled on a dataset node, deduplication begins automatically according to a user-customized schedule on all volumes in a dataset node.
 

**Note:** In "Scheduled deduplication" mode, deduplication starts on Disaster Recovery capable Mirror destinations only after the SnapMirror relationship between primary storage and the secondary storage nodes on which they reside is broken.
- The initial deduplication operation on a volume is a full volume run. All blocks of data on the volume are scanned for duplication and the duplicate blocks are consolidated (or deduplicated).
 

**Note:** Because the initial deduplication operation is a full volume run, in which all data is scanned, it requires more time to complete than subsequent operations.
- Subsequent deduplication operations are usually incremental operations. Only the new or changed blocks of data on the target volume or volumes are scanned for duplication and possible consolidation.
 

**Note:** In "On-demand deduplication" mode, you have the option of starting a full volume or partial volume run every time you click **Dedupe Now**.

## Role-based access control (RBAC)

Role-based access control (RBAC) provides the ability to control who has access to various client application features.

Applications use RBAC for user authorization. Administrators use RBAC to manage groups of users by defining roles. For example, if you need to control user access to resources, such as groups, datasets, and resource pools, you must set up administrator accounts for them. Additionally, if you want to restrict the information these administrators can view and the operations they can perform, you must apply roles to the administrator accounts you create.

**Note:** RBAC permission checks occur in the DataFabric Manager server. RBAC must be configured using the Operations Manager Web interface or command line interface.

## SAN resource provisioning example workflow

---

This is a step-by-step example of how you might configure your system to provision storage resources. This example workflow assumes that the Provisioning Manager license is enabled on your system (the Protection Manager license is not required for this example).

For descriptions of some of the concepts and terminology associated with Provisioning Manager, see [Introduction to provisioning and protection](#) on page 39 .

For administrative tasks and additional reference and conceptual information associated with Provisioning Manager, see the Provisioning Manager Help.

The following list describes the tasks you need to complete for this example workflow.

### Next topics

[SAN provisioning workflow setup](#) on page 55

[Develop a SAN provisioning strategy](#) on page 56

[SAN provisioning example configuration assumptions](#) on page 58

[Configure the storage system to host the vFiler unit](#) on page 61

[Create a resource pool](#) on page 63

[Create a vFiler template](#) on page 64

[Create a vFiler unit](#) on page 65

[Create a SAN provisioning policy](#) on page 66

[Create a dataset and provision a LUN](#) on page 68

## SAN provisioning workflow setup

In this workflow, assume you are a storage administrator managing, over a high-speed IP network, a shared SAN storage infrastructure consisting of your company's storage systems and your customers' data.

You need to provision LUNs for deploying a new application for your customer. The storage will be accessed by using the iSCSI protocol. To isolate the storage for security purposes, you will use the licensed MultiStore option to create a dedicated vFiler unit for the customer and export all the storage required by the customer over the vFiler unit. The customer data, mostly project files and applications, will be accessed over a virtual private LAN.

## Develop a SAN provisioning strategy

Before configuring the space and provisioning requirements for your systems, you must develop a strategy for how you will group the resources and how the application should respond in out-of-space conditions.

For descriptions of the basic concepts and terminology associated with Provisioning Manager, see [Introduction to provisioning and protection](#) on page 39 .

Your provisioning strategy addresses a variety of considerations, such as the following:

- [General considerations](#) on page 56
- [Security considerations](#) on page 56
- [Availability considerations](#) on page 57
- [Space management considerations](#) on page 57
- [Notification considerations](#) on page 58
- [RBAC considerations](#) on page 58

### General considerations

- What type of storage, NAS or SAN, do you want to provision with this policy?
- Will you use a provisioning policy or manually provision resources in datasets?
- Will you assign resource pools or individual physical resources to your datasets?  
If you intend to allow the provisioning application to provision storage for the dataset, you would want to use resource pools. If you want to import existing data into a dataset, you would want to select individual physical resources.
- What type of dataset container will you use: LUNs, for direct access to storage from hosts, or volumes, for delegating LUN creation to SnapDrive?
- Do you want to enable the dataset for automated offline migration?  
This allows for the automatic migration of data stored on vFiler units and information relevant to the vFiler unit, such as NFS exports, CIFS shares, LUN mappings, and so forth.
- Will you use a custom provisioning script after storage is provisioned?  
You might use a script to perform tasks such as additional configuration operations on the newly provisioned storage.

### Security considerations

- How will the customer's application access data?  
Since the storage type for this example is SAN, determine the access or export protocols that you need to configure for SAN: iSCSI or FCP.
- How can the dataset be accessed?



- How can access to the storage be protected from unauthorized access?  
For example, you might use the MultiStore option to create vFiler units to isolate storage. You could also choose to specify CIFS User ACLS to restrict access.
- Which hosts are allowed access to the data?  
You can restrict access to the LUNs by specifying the host initiator IDs that can access the LUNs.

## Availability considerations

What level of availability protection does the dataset require?

Availability level is determined by how critical the data is that you are protecting and can be one of the following:

- RAID-DP (double disk failure)  
Protects against the simultaneous failure of two disks.
- RAID4 (single-disk failure)  
Protects against the failure of a single disk.
- Externally managed RAID  
The application provisions from V-Series storage. Therefore, RAID protection is determined by the V-Series storage capabilities.
- Storage subsystem failure (aggregate SyncMirror)  
Protects against the failure of disk shelves, adapters, and cables.
- Storage controller failure (active/active configuration)  
Protects against the failure of a storage system within a cluster.

## Space management considerations

- Will you use aggregate overcommitment to thinly provision your storage?
- Do you want to guarantee space for primary data and for Snapshot copies or do you want to grow space for Snapshot copies when needed?  
You can reserve space for LUNs and either reserve or grow space for Snapshot copies so that application writes do not fail due to lack of disk space.
- What actions should occur when a dataset needs more storage space?  
The options are:
  - You can allocate all storage space for data and Snapshot copies or you can use aggregate overcommitment to thinly provision your storage.
  - You can choose to grow space by deleting old Snapshot copies automatically to guarantee space for application data (requires Data ONTAP 7.2.4 or later).
  - You can choose to grow space by deleting Snapshot copies manually when needed. This requires more available space because existing Snapshot copies are preserved during write activity.
  - You can choose not to guarantee space for data or Snapshot copies.

- What is the maximum amount of disk space you want available for Snapshot copies?
- Do you want to enable deduplication to reduce your storage space requirements?

### Notification considerations

- Do you want a space utilization alert to be sent when a space threshold is reached?  
You can enable the Space utilization thresholds and set the values at which alerts will be sent when the Nearly full and Full thresholds are reached.

### RBAC considerations

Your administrator account already has the roles and capabilities assigned to it that you need to perform all the tasks necessary to implement the provisioning strategy. See [Administrator roles and capabilities](#) on page 175 for a list of RBAC roles required for provisioning tasks.

## SAN provisioning example configuration assumptions

The descriptions and procedures in the provisioning workflow are based on the assumptions about your system configuration that are provided in the sections of this chapter.

- [General assumptions](#) on page 58
- [Licenses enabled](#) on page 59
- [Resource pool properties](#) on page 59
- [vFiler template properties](#) on page 59
- [vFiler unit properties](#) on page 60
- [Provisioning policy properties](#) on page 60
- [Dataset properties](#) on page 60

### General assumptions

For this workflow, assume the following:

- You are configuring a storage environment of SAN over iSCSI.
- Your protection strategy has been implemented outside of NetApp Management Console.
- All hardware you intend to use has been configured with appropriate licenses, protocols, settings, and so forth.
- The customer's new application will be installed on a vFiler unit that you will create.
- Aggregates of unused storage space have been preconfigured on the storage system that will host the vFiler unit.
- For any property not specified in this example, use the default value.

## Licenses enabled

For this workflow, you would need the following licenses enabled:

- DataFabric Manager with Provisioning Manager license
- Data ONTAP MultiStore license, on the storage that will host the vFiler unit

**Note:** Other licenses such as SnapMirror or SnapVault might be needed to set up your protection environment, but that is not addressed in this workflow.

- iSCSI license on the storage system that will host the vFiler unit
- A\_SIS deduplication license on the storage that will host the vFiler unit

## Resource pool properties

For this workflow, assume use of the following properties when creating the resource pool.

- Details (general properties)
  - Name: ExampleCo-RP
  - Description: Res pool for ExampleCo vFiler units
- Allocate physical resource: storage-EC-8

## vFiler template properties

For this workflow, assume use of the following properties when creating the vFiler template.

- Name: EC-template
- Description: vFiler template for ExampleCo
- Administrative host: 10.0.0.18
- DNS name: EAST.exampleco.com
- DNS server: 10.0.0.20
- NIS name: ENG
- NIS server: 172.16.3.145

## Dataset migration properties

For this workflow, assume use of the following properties when enabling dataset migration.

- IP address: 172.26.18.10
- Network mask: 255.255.255.10

**Note:** These are the same addresses that are used for creating the vFiler unit that hosts the storage for the dataset.

### **vFiler unit properties**

For this workflow, assume use of the following properties when creating the vFiler unit.

- Name: EC-vFiler-3
- IP space: default-ipospace
- Allowed protocols: iSCSI
- Hosting storage system: Select ExampleCo-RP
- IP address of the vFiler unit: 255.255.255.10172.26.18.10
- Network mask: 255.255.255.10
- Interface: Select e4-20, the VLAN interface you created.
- vFiler template: Select EC-template, the template you used to create the vFiler unit.

### **Provisioning policy properties**

For this workflow, assume use of the following properties when creating the provisioning policy.

- General properties
  - Policy name: provpol-san
  - Policy description: Any meaningful description, such as SAN over iSCSI with LUNs.
  - Storage type: SAN
- Disk failure protection: RAID-DP (Double disk failure)
- Deduplication: Select **Enable deduplication on volumes** and **Automated deduplication**

### **Dataset properties**

For this workflow, assume use of the following properties when creating the dataset and provisioning LUN storage.

- Dataset name: ExampleCo-DS-1
- Provisioning policy: provpol-san
- Export setting: Turn on iSCSI
  - Initiator ID: iqn.1989-03.com.isinit:app1
  - Host operating system: Windows
- Automated offline migration: Enable automated offline migration
  - IP address for data access: 172.26.18.10
  - Network mask: 255.255.255.0
- Resource pool: ExampleCo-RP
- vFiler unit: EC-vFiler-3

- Provision LUNs
  - LUN name: EC-lun
  - LUN description: Any useful description
  - LUN space: 1 GB (default)
  - Maximum space of Snapshot copies: 2 GB (default)
  - Initial space of Snapshot copies: 1 GB (default)
- Resource selection: Allow the system to automatically select a resource from the attached resource pool

## Configure the storage system to host the vFiler unit

After determining your provisioning strategy, your first task is to configure the storage system that will host the vFiler unit. This includes setting the login credentials for the host and ensuring that the appropriate licenses are enabled on the host, according to your provisioning strategy.

### Before You Begin

Have the following information available for the storage system you want to configure.

- The name of the system hosting the vFiler unit: storage-EC-8
- Login credentials for the storage system
- License codes for applications running on the storage systems you plan to use

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

### Considerations

You will now verify the following information for each host that you are using:

- You have the appropriate license codes for applications running on the storage systems you plan to use.
- The Data ONTAP MultiStore license is installed.
- The hosts or aggregates that you intend to use are not already part of another resource pool (resources can only belong to one resource pool).

**Note:** You must configure aggregates of unused space on the storage system before the vFiler unit can be created.

## Steps

1. From the navigation pane, click **Hosts ► Storage Systems**.

2. If not already selected, click **Details** at the bottom of the window.

3. In the list of hosts, you select the host **storage-EC-8**.

For the instructive purposes of this example, you find that login credentials are bad for this host.

4. Click **Edit**.

The properties sheet for the selected host appears. The current credential information for the host is displayed, with password strings masked by asterisks.

5. Update the Login Credentials fields with valid user names and passwords, then click **OK**.

The database is updated with the credentials for the selected host.

6. With the host **storage-EC-8** still selected in the list, verify the following license information:

- The MultiStore license is enabled.
- The iSCSI protocol license is configured.

For the instructive purposes of this example, you notice that the iSCSI protocol is configured, but that the MultiStore license is not enabled.

7. With storage-EC-8 still selected, click **Edit**, then click **Licenses**.

A list of licenses that can be configured on the selected host appears.

8. Type the MultiStore license code in the New License field, then click **OK**.

The MultiStore license is configured on storage-EC-8. Note that it is not necessary to indicate which service the code enables. The code is matched automatically to the appropriate service license.

9. With storage-EC-8 still selected, click the **Usage tab** at the bottom of the window.

The lower area of the window changes.

10. Select **Aggregates** from the Resource Type list.

The aggregates on the host storage-EC-8 are displayed in the tree view.

11. Click on each item in the tree view to verify that neither the host nor any of its aggregates are already associated with a resource pool.

When you click on a name in the tree view, any resource pool or dataset associations are displayed in the dependencies area of the window.

### After You Finish

Now that you have configured the host with login credentials and verified the licenses, the next step is to add the host to a resource pool that the provisioning application uses to provision storage.

## Create a resource pool

Create a new resource pool and add the storage system that you configured.

### Before You Begin

Where needed, you should have already created aggregates of unused space on host storage-EC-8, which you intend to add to a resource pool for the vFiler unit.

Before creating each resource pool, you should have available the information necessary to complete the **Add Resource Pool** wizard:

- The name of the resource pool to be created
- The time zone the policy schedules should assume when timing protection events  
If you do not select one, the default is used.
- The group that contains the hosts or aggregates you plan to assign to the resource pool
- The physical resources to associate with the resource pool
- The Space thresholds for setting alerts for out-of-space conditions
- The Aggregate overcommitted thresholds

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

### Steps

1. From the navigation pane, click **Data ► Resource Pools ► Resources**.
2. Click **Add** to open the **Add Resource Pool** wizard.
3. Complete the wizard, using the following values:

- General properties:

Name: **ExampleCo-RP**

Description: **Res pool for ExampleCo vFiler units**

- Physical resources:

Group: **Global**

Resource type: **Hosts**

Physical resource: **storage-EC-8**

4. Confirm the details of the resource pool, then click **Finish** to complete the wizard.

You can view the new resource pool in the **Resource Pools** window.

### After You Finish

You next create a vFiler template.

## Create a vFiler template

You will now create a vFiler template that you will use to create a new vFiler unit.

### Before You Begin

Before creating a vFiler template, you need to gather the information necessary to complete the **Add vFiler Template** wizard:

- The name of the new template
- The DNS domain settings: name and server
- The NIS domain settings: name and server
- The CIFS settings: not used for this example, so you should accept the defaults

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

### Steps

1. From the navigation pane, click **Policies ► vFiler Templates**.
2. Click **Add** to start the **Add vFiler Template** wizard.
3. Complete the wizard, using the following values:
  - Name: **EC-template**
  - Description: **vFiler template for ExampleCo**
  - Administrative host: **10.0.0.18**
  - DNS domain name: **EAST.exampleco.com**
  - DNS domain server: **10.0.0.20**
  - NIS domain name: **ENG**
  - NIS domain server: **172.16.3.145**
  - CIFS settings: accept the defaults
4. Preview and verify the actions to create the vFiler template.



5. Confirm the details of the template, then click **Finish** to complete the wizard.

Your new policy is listed in the **vFiler Templates** window.

### After You Finish

You next create a vFiler unit.

## Create a vFiler unit

You will now create a dedicated vFiler unit that you will use to isolate and export your customer's storage.

### Before You Begin

Be sure the host on which you want to create a vFiler unit is running Data ONTAP 7.0 or later.

The IP address used by the vFiler unit must not be configured when you create the vFiler unit.

Before creating a vFiler unit, you need to gather the information necessary to complete the **Add vFiler Unit** wizard:

- Name
- IP address
- IP space name
- Protocols to be enabled on the vFiler unit
- Name of the storage system or resource pool to be associated with the vFiler unit
- IP address, network mask, network interface, and VLAN ID of the vFiler unit
- vFiler template being used

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

### Steps

1. From the navigation pane, click **Hosts ► vFiler Units**.
2. Click **Add** to start the **Add vFiler Unit** wizard.
3. Complete the wizard, using the following values:
  - General properties:

Name: **EC-vFiler-3**

IP space: **default-ipspace**

Allowed protocols: **iSCSI**

- Resource pool: **ExampleCo-RP**
- Select: **Create and Setup vFiler unit**
- Network interface settings for the vFiler unit:

IP address: **172.26.18.10**

Network mask: **255.255.255.0**

Network interface: **e4-3**

VLAN ID: **3**

- vFiler template: **EC-template**
- Root password: none

4. Preview and verify the actions to create the vFiler unit.
5. Confirm the details of the vFiler unit, then click **Finish** to complete the wizard.

You can view the new vFiler unit in the host list.

#### **After You Finish**

You next create a provisioning policy.

## **Create a SAN provisioning policy**

You will now create a provisioning policy to apply to a dataset. When assigned to a dataset, the provisioning policy establishes the rules for how the storage space needs to be provisioned for that dataset.

#### **Before You Begin**

Before creating a provisioning policy, you need to gather the information necessary to complete the **Add Provisioning Policy** wizard:

- The name of the new policy
- The type of storage you want to provision with this policy
- The level of protection the dataset requires
- The deduplication settings, if enabled
- The type of container (LUN or volume)
- The space settings
- The space thresholds

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

## Steps

1. From the navigation pane, click **Policies ► Provisioning**.
2. Click **Add** to start the **Add Provisioning Policy** wizard.
3. Complete the wizard, using the following values:
  - General properties:
    - Name: **provpol-san**
    - Description: **SAN policy for ExampleCo**
    - Type of storage: **SAN**
  - Availability properties: **Disk failure protection, RAID-DP (Double disk failure)**
  - Deduplication:
    - Select **Enable deduplication on volumes**
    - Select **Automated deduplication**
  - SAN container properties:
    - Types of containers to provision: **LUN**
    - Space settings: **Guarantee space for LUN and grow space for Snapshot copies on demand: Allow automatic deletion of Snapshot copies when necessary**
  - Space thresholds
    - Enable **Space utilization thresholds**
    - Nearly Full threshold: **80%**
    - Full threshold: **90%**
4. Preview and verify the actions to create the policy.
5. Confirm the details of the policy, then click **Finish** to complete the wizard.

The new policy is listed in the **Provisioning Policies** window.

## After You Finish

You next create a dataset and provision a LUN.

## Create a dataset and provision a LUN

You must now create a dataset to which you will assign the provisioning policy, resource pool, and vFiler unit that you created.

### Before You Begin

Before creating a new dataset, you need to gather the necessary information to complete the **Add Dataset** wizard:

- The name of the new dataset
- The name of and contact information for the owner of the dataset
- The time zone in which the dataset resides
- The name of the group to which the dataset will belong
- The name of the provisioning policy you want to assign to the dataset
- iSCSI export settings
- The name of the resource pool that you want to assign to the dataset
- The IP address and network mask for migration

Use the same addresses that you used for the vFiler unit network interface settings.

- The name of the vFiler unit that you want to assign to the dataset
- The name, description, and size of the LUN you are provisioning

### Steps

1. From the navigation pane, click **Data ► Datasets ► Overview**.

The Overview tab of the **Datasets** window is displayed.

2. Click **Add** to start the **Add Dataset** wizard.

3. Complete the wizard, using the following values:

- General properties:

Dataset name: **ExampleCo-DS-1**

- Group: **Global**
- Select **Provision and attach resources using a policy**
- Provisioning settings:

Provisioning policy: **provpol-san**

iSCSI Export Settings: Click **Turn on now**

iSCSI initiator ID: **iqn.1989-03.com.isinit:app1**

Host operating system: **Windows**

Resource pool: **ExampleCo-RP**

- vFiler unit: **EC-vFiler-3**
- Would you like to provision storage now: **Yes**
- Container name and size:

LUN name: **EC-lun**

LUN description: Any useful description

LUN space: **1 GB**

Maximum space of Snapshot copies: **2 GB**

Initial space of Snapshot copies: **1 GB**

- Resource selection: **Allow the system to automatically select a resource from the attached resource pool(s)**

4. Preview and verify the actions to create the dataset.
5. Confirm the details of the dataset, then click **Finish** to complete the wizard.

The new dataset appears in the list of datasets. You have completed the example workflow for creating a dataset and provisioning storage in a SAN environment.



# Dataset migration example workflow

---

This is a step-by-step example of how you might migrate a dataset to a different storage system.

To understand this example, you must have completed the [SAN resource provisioning example workflow](#) on page 55 and enabled the Provisioning Manager license on your system.

For descriptions of some of the concepts and terminology associated with Provisioning Manager, see [Introduction to provisioning and protection](#) on page 39.

For administrative tasks and additional reference and conceptual information associated with Provisioning Manager, see the Provisioning Manager Help.

The following list describes the tasks you need to complete for this example workflow.

## Next topics

- [Dataset migration example setup](#) on page 71
- [Develop a dataset migration strategy](#) on page 72
- [Dataset migration workflow assumptions](#) on page 73
- [Add a physical resource to the resource pool](#) on page 74
- [Start the dataset migration](#) on page 75
- [Update the migration SnapMirror relationships](#) on page 76
- [Cut over to the new dataset storage destination](#) on page 77
- [Clean up the dataset migration](#) on page 78
- [Manually delete old IPspace and VLAN](#) on page 78

## Dataset migration example setup

This example is a continuation of the SAN provisioning workflow and is based on the same assumptions that you are a storage administrator who is managing a shared SAN storage infrastructure over a high-speed IP network. In this example, you migrate a dataset's primary storage to a new storage location.

Your dataset is running out of space and needs to move to a different storage system. Because a dedicated vFiler unit is assigned to the dataset, the dataset is automatically enabled for migration. (The licensed provisioning application migrates vFiler units. Therefore, if your dataset has a vFiler unit assigned as a host, and if all of the storage for the dataset is provisioned through that vFiler unit, you can migrate the dataset to another storage system.)

In this example, the one storage system in the resource pool is not large enough for the dataset. Therefore, you also have to add an additional system to the resource pool to use as the dataset migration destination.

## Develop a dataset migration strategy

Before starting a dataset migration, you must develop a strategy for selecting the new destination storage, the provisioning policy for the new storage, and the vFiler unit interface you want to use.

Your migration strategy addresses the following considerations:

- [Destination storage selection considerations](#) on page 72
- [Provisioning policy considerations](#) on page 72
- [vFiler unit interface considerations](#) on page 72

For descriptions of the basic concepts and terminology associated with Provisioning Manager, see [Introduction to provisioning and protection](#) on page 39 .

### Destination storage selection considerations

What is the new destination storage system for the dataset's primary storage?

The Dataset Migration wizard displays a list of resource pools and a list of storage systems that you can select from. You must select a resource pool or storage system that has enough space and provides the necessary performance required for the dataset.

### Provisioning policy considerations

Which provisioning policy do you want applied to the migrated dataset?

By default, the currently assigned provisioning policy for the source dataset is selected; however, you can select a different one if a different provisioning policy configuration is needed for the migrated dataset.

### vFiler unit interface considerations

What vFiler unit interfaces do you want to use?

If the vFiler unit associated with the source dataset is not created using the default interface settings, then to which interfaces do you want to bind the IP addresses of the vFiler unit on the destination storage system? You can select from an already-populated list of IP addresses that displays the associated netmask and interface values, and an already-populated VLAN ID. You can also specify a different VLAN ID.

### RBAC considerations

Your administrator account already has the roles and capabilities assigned to it that you need to perform all the tasks necessary to implement the dataset migration strategy. See [Administrator roles and capabilities](#) on page 175 for a list of RBAC roles required for provisioning tasks.



## Dataset migration workflow assumptions

The descriptions and procedures in the dataset migration example are based on a set of assumptions about licenses, resource pools, and other elements of your system configuration.

- [General assumptions](#) on page 73
- [Licenses enabled](#) on page 73
- [Resource pool](#) on page 74
- [vFiler unit](#) on page 74
- [VLAN](#) on page 74
- [Provisioning policy](#) on page 74
- [Dataset](#) on page 74

### General assumptions

For this example, assume the following:

- You are adding a new storage system to your existing resource pool in a SAN-over-iSCSI environment.
- All hardware you intend to use is configured with appropriate licenses, protocols, settings, and so forth.
- Aggregates of available storage space are preconfigured on the new storage system.
- You are assigned the following RBAC roles:
  - DFM.Resource.Control on the source vFiler unit and on the destination storage system
  - DFM.Dataset.Write on the dataset
- No premigration or postmigration scripts will be used.
- For any property not specified in this example, use the default value.

### Licenses enabled

For this example, enable the following licenses:

- DataFabric Manager with Provisioning Manager license

**Note:** Protection Manager and disaster recovery licenses do not need to be enabled.

- Data ONTAP MultiStore license, on the destination storage system.
- SnapMirror license on the destination storage system.
- iSCSI license on the destination storage system.

## Resource pool

For this example, use the following information when adding a physical resource to the resource pool that you created in the provisioning workflow example:

- Details (general properties, no change from the example provisioning workflow)
  - Name: **ExampleCo-RP**
  - Description: **Res pool for ExampleCo vFiler units**
- Allocate physical resource: **storage-EC-9**
- Resource label: None used

## vFiler unit

For this example, use the vFiler unit that you set up in the example provisioning workflow:

- Name: **EC-vFiler-4**
- IP space: **default-ipspace**
- Allowed protocols: **iSCSI**
- Hosting storage system: Select **ExampleCo-RP**
- IP address of the hosting storage system: **172.26.18.10**

## VLAN

For this example, use the VLAN interface named **e4-20** that you created up in the example provisioning workflow.

## Provisioning policy

For this example, use the provisioning policy named **provpol-san** that you created in the example provisioning workflow.

## Dataset

For this example, use the dataset named **ExampleCo-DS-1** that you created in the example provisioning workflow.

# Add a physical resource to the resource pool

Before you start the dataset migration, you must add a storage system to the dataset's resource pool so that it can host the dataset when the dataset is migrated. The new storage system you add is used as the destination storage system for the dataset migration.

### Before You Begin

Before adding physical resources to the resource pool, you should have available the information necessary to edit the resource pool properties:

- The name of the resource pool (required)
- The name of the storage system you want to add (required)

### Steps

1. From the navigation pane, click **Data ► Resource Pools**.
2. In the list of available resource pools, select the resource pool named ExampleCo-RP.
3. Click **Edit** to open the **Properties** sheet, then click **Physical Resources**.
4. Select the storage system named storage-EC-9 in the list "Available physical resources," then click > to add it to the list named "Resources in this resource pool."
5. Click **OK**.

The resource pool's configuration is modified and saved and the destination storage system is added to the resource pool.

You will next start the dataset migration.

## Start the dataset migration

You will now start the migration of the dataset, which begins a baseline transfer to the destination storage system.

### Before You Begin

Have available the information that you need to complete this task:

- The name of the destination storage system (required)

### Considerations

You can cancel a dataset migration any time during the migration start operation.

### Steps

1. From the navigation pane, click **Data ► Datasets ► Migration**.
2. Select the dataset named ExampleCo-DS-1 and make sure it has the status "Not started."

This status indicates that the dataset meets the dataset migration requirements and that a migration is not already in progress.

3. Click **Start migration** to start the **Dataset Migration** wizard.
4. Complete the wizard, using the following values:
  - Destination storage system: **storage-EC-9** (the newly added storage system)
  - Provisioning policy: **provpol-san** (same as currently assigned to the dataset)
  - Interface IP address of the vFiler unit: **172.26.18.10** (same as currently configured for the vFiler unit)
  - Netmask: **255.255.255.10** (same as currently configured for the vFiler unit)
  - VLAN ID: **e4-20** (same as currently configured for the vFiler unit)
5. Confirm the details of the migration, then click **Finish** to complete the wizard.

You can check the job progress displayed in the Tracking Dataset Migration Job display popup window or in the Jobs tab on the **Datasets** window Migration tab.

You will next start the update the SnapMirror relationships that were created in the start migration operation.

## Update the migration SnapMirror relationships

You will now initiate an on-demand update of the SnapMirror relationships that were created as part of the dataset migration start operation. You can perform this task only on a dataset that has finished the migration start operation.

### Considerations

This is an optional step in the dataset migration process, because the migration cutover operation also updates the SnapMirror relationships.

### Steps

1. From the navigation pane, click **Data ► Datasets ► Migration**.
2. Select the dataset named ExampleCo-DS-1 and make sure it has the status "Started, cutover required."

This status indicates that the migration start operation baseline transfer to the new destination storage system is finished.
3. Click **Update**.
4. Click **Yes** in the confirmation dialog box to begin the operation.

You can track the progress of the operation in the **Datasets** window Migration tab Jobs tab, or in the **Jobs** window.

You will next cut over to the new storage system.

## Cut over to the new dataset storage destination

You will now initiate the migration cutover operation. This operation stops access to the vFiler unit on the source storage system from which the data is served, enables access to the vFiler unit on the new destination storage system, and updates the SnapMirror relationships that were created as part of the migration start operation.

### Before You Begin

You can perform this task only on a dataset that has finished the migration start operation.

Because this is an automated offline migration, you must shut down all applications that use the dataset.

### Steps

1. From the navigation pane, click **Data ► Datasets ► Migration**.
2. Select the dataset named ExampleCo-DS-1 and make sure it has the status "Started, cutover required."

This status indicates that the migration start operation baseline transfer to the new destination storage system is finished.

3. Click **Cutover**.
4. Click **Cutover** in the confirmation dialog box to begin the operation.

You can track the progress of the operation in the **Datasets** window Migration tab Jobs tab, or in the **Jobs** window.

After the dataset is switched over to the destination storage system, the backup versions, backup relationships, and DataFabric Manager history for the volumes are transferred to the destination storage system.

### After You Finish

You must restart all applications that use the migrated dataset.

You will next initiate the migration clean up operation.

## Clean up the dataset migration

You will now initiate the migration cleanup operation to delete the volumes that were used by the vFiler unit on the old data storage system.

### Before You Begin

You can perform this task only on a dataset that has finished the migration cutover operation.

### Steps

1. From the navigation pane, click **Data ► Datasets ► Migration**.
2. Select the dataset named ExampleCo-DS-1 and make sure it has the status "Migrated, cleanup required."

This status indicates that the migration cutover operation is finished and the dataset is switched over to the destination storage system, including the data, backup versions, backup relationships, and DataFabric Manager history for the volumes. However, old storage needs to be deleted.

3. Click **Cleanup**.
4. In the confirmation dialog box, look at the list of volumes on the old, source storage system that are to be deleted and make sure that list is correct.
5. Click **Apply** in the confirmation dialog box to begin the operation.

You can track the progress of the operation in the **Jobs** window.

### After You Finish

Next you must manually delete the following (for example, using FilerView) if they are not shared:

- Dynamic references in the old source dataset
- VLANs and IPspaces used by the old source vFiler unit

## Manually delete old IPspace and VLAN

You will now manually delete the VLANs and IPspaces used by the old source vFiler unit.

### Before You Begin

You can perform this task only for a dataset that has finished the migration cleanup operation and only if neither the IPspace nor the VLAN are shared.

**Steps**

1. From the navigation pane, click **Data ► Datasets ► Migration**.
2. Select the dataset named ExampleCo-DS-1 and make sure it has the status "Not started."  
This status indicates that the migration cleanup operation is finished.
3. Using an application like FilerView, delete the IPspace and VLAN in the old storage system named storage-EC-8.





# Protection example workflow

---

This is a step-by-step example of how you might configure your system to protect your user data. The example workflow assumes that the Protection Manager license is enabled on your system (the Provisioning Manager license is not required for this example).

For descriptions of some of the concepts and terminology associated with Protection Manager, see [Introduction to provisioning and protection](#) on page 39 if possible.

For administrative tasks and additional reference and conceptual information associated with Protection Manager, see the Protection Manager Help.

The following list describes the tasks you need to complete for this example workflow.

## Next topics

[Protection example setup](#) on page 81

[Develop a protection strategy](#) on page 111

[Protection example configuration assumptions](#) on page 83

[Configure the host storage systems](#) on page 86

[Create the resource pools](#) on page 88

[Evaluate and modify the protection schedules](#) on page 90

[Create the protection policy and modify the settings](#) on page 93

[Create groups](#) on page 101

[Create datasets](#) on page 103

[Assign the protection policy to the datasets](#) on page 105

[Import discovered relationships](#) on page 106

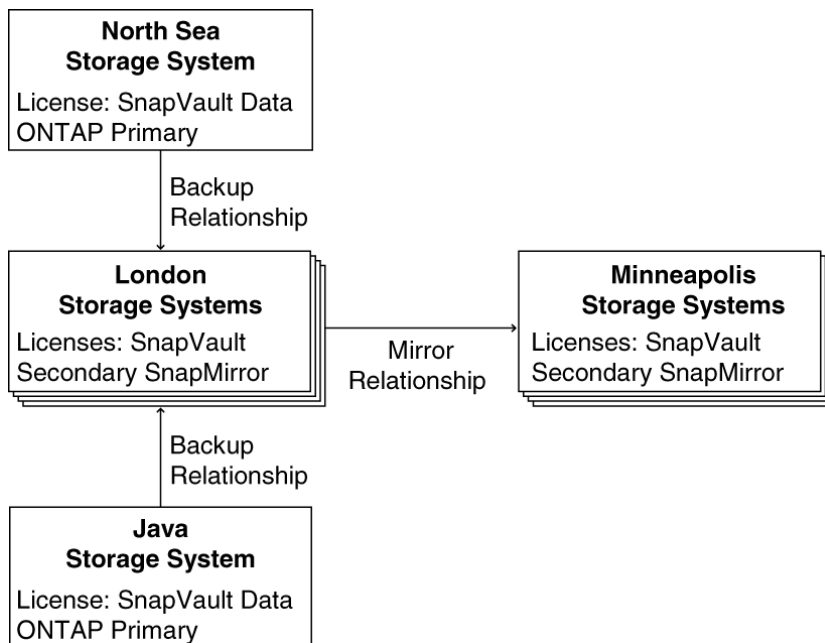
[Verify the protection of the dataset](#) on page 107

[Configure alarms](#) on page 107

## Protection example setup

For this example workflow, assume you are a storage architect for an energy company that needs to protect its seismic test data. The files of seismic test data are on storage systems on oil platforms in the North Sea and off the coast of Java.

The seismic test data files at the North Sea data center are currently protected by SnapVault and SnapMirror but are not yet managed with a dataset. The seismic test data files at the Java data center are not yet protected, but you intend to establish a backup relationship to storage in London and a mirror relationship to storage in Minneapolis.



## Develop a protection strategy

Before implementing a data protection plan, you must work out a strategy for protecting the seismic test data.

For descriptions of the basic concepts and terminology associated with Protection Manager, see [Introduction to provisioning and protection](#) on page 39 if possible.

Your strategy for protecting the data addresses a variety of considerations.

### Schedule considerations

To meet the restore requirements of the data, you determine that the data should be backed up to the data center at company headquarters in London and mirrored to the company's Minneapolis data center.

- How long do you need to retain backups of the data to meet its restore requirements?
- What are the preferred times of day to perform remote backups and mirror copies, based on network and resource loads?
- How often does data on a primary node need to be copied to a destination node to ensure that data on the destination node is never older than the maximum age mandated by your protection requirements?

**Bandwidth considerations**

What is the volume of data to back up and the available bandwidth to transfer copies of the data to a destination system?

**Host considerations**

Which hosts in London and Minneapolis have similar performance and Quality of Service levels?

**Notification considerations**

Which events require alarms and who needs to be contacted for them?

**RBAC considerations**

Your administrator account already has the roles and capabilities assigned to it that you need to perform all the tasks necessary to implement the data protection strategy. See [Administrator roles and capabilities](#) on page 175 for a list of RBAC roles required for protection tasks.

## Protection example configuration assumptions

This chapter identifies the configurations, settings, and properties that are used in this protection example workflow.

- [Licenses enabled](#) on page 83
- [Host properties](#) on page 84
- [Protection schedule and policy properties](#) on page 84
- [Resource pool properties](#) on page 85
- [Dataset properties](#) on page 86

**General assumptions**

For this workflow, assume the following:

- You are configuring a storage environment of NAS over CIFS and NFS protocols.
- All hardware you intend to use has been configured with appropriate licenses, protocols, settings, and so forth.
- For any property not specified in this example, use the default value.

**Licenses enabled**

For this example workflow, you need the following licenses enabled.

- DataFabric Manager with Protection Manager license
- Data ONTAP licenses:

- SnapVault on the primary storage
- SnapVault on the secondary storage
- SnapMirror on the tertiary storage
- Open Systems SnapVault, if you are running SnapVault software on an operating system other than Data ONTAP

### Host properties

For this example workflow, assume use of the following properties for your hosts.

- Primary data needing protection
  - Stored on North Sea and Java storage systems
  - North Sea and Java Data ONTAP licenses enabled: SnapVault primary
- Backup relationship
  - Backups of North Sea and Java systems are stored on London storage systems.
  - London Data ONTAP licenses enabled: SnapVault secondary and SnapMirror
  - Host name used in workflow: london14-geo
- Mirror relationship
  - Mirrored copies from London are stored on Minneapolis storage systems.
  - Minneapolis Data ONTAP licenses enabled: SnapVault secondary and SnapMirror

### Protection schedule and policy properties

For this example workflow, assume use of the following properties when creating the schedules and the protection policy.

- Policy name: Use "Back up, then mirror" for this workflow
- Primary data node

For this example, use the following default settings for the Primary node.

  - Local Backup schedule: Sunday at midnight with daily and hourly  
When applied to the Primary data node, this schedule creates the following:  
Hourly local backups each hour  
A Daily local backup each day at midnight  
A Weekly local backup at midnight on Sundays
  - Retention  
Hourly: 1.0 day  
Daily: 1.0 week  
Weekly: 2.0 weeks  
Monthly: 0.0 weeks

- Lag  
Warning Threshold: 1.5 days  
Error Threshold: 2.0 days
- Connection between the Primary data node and the Backup node  
For this workflow, use the following settings for the Primary data to Backup connection.
  - Backup schedule: Sunday at 8:00 PM plus daily at 8 AM/PM.  
You will need to copy and modify an existing schedule
  - Lag  
Warning Threshold: 1.0 days  
Error Threshold: 1.5 days
- Backup node  
For this workflow, use the following settings for the Backup Retention Durations:  
Hourly: 0.0 day  
Daily: 2.0 weeks  
Weekly: 12.0 weeks  
Monthly: 14.0 weeks
- Connection between the Backup node and the Mirror node  
For this workflow, use the following settings for the Backup to Mirror connection.
  - Mirror schedule: Hourly on the half hour  
You will need to select this existing schedule to replace the default.
  - Lag  
Warning Threshold: 2.0 hours  
Error Threshold: 3.0 hours

## Resource pool properties

For this workflow, assume use of the following properties when creating the resource pools.

- Group: Both pools will be initially created under the default Global group and later added to the Datasets:Test Data group after that group is created.
- Details (general properties)
  - Name: Use London Backup and Minneapolis Mirror
  - Description: Any meaningful description
- Allocate physical resources:  
Select the resources to be included in the resource pool. These resources must meet the licensing and configuration requirements of your provisioning and protection plan.

### Dataset properties

For this workflow, assume use of the following properties when creating and protecting the datasets.

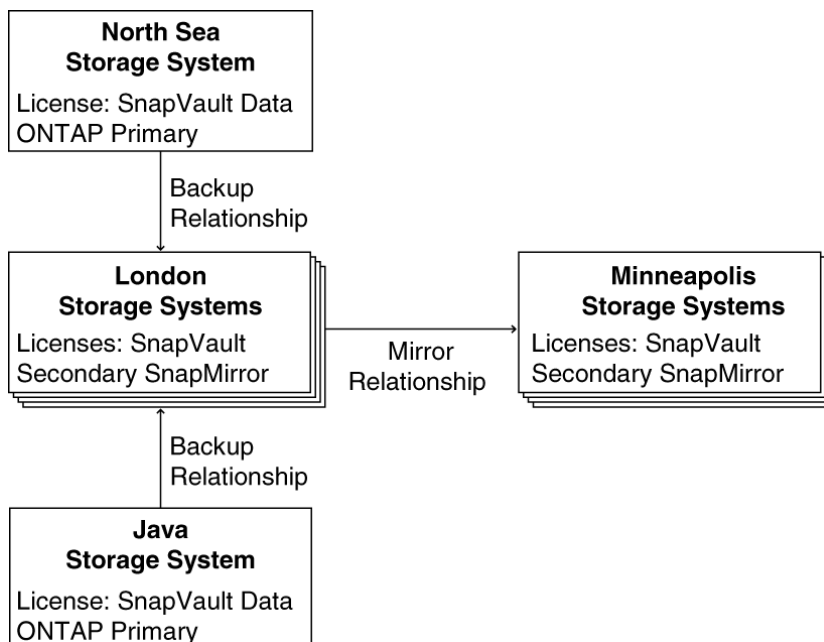
- Name: One dataset will be named North Sea Seismic Test Data and the other will be named Java Seismic Test Data.
- Group: Both datasets will be contained in a new "Datasets:Test Data" group, which will be created under an existing "Data Protection" parent group.
- Protection policy: Use "Back up, then mirror."
- Resources: Select the default, "Use a provisioning policy."
- Provisioning policy: Use the default provisioning policy.
- Resource pools: Select London Backup and Minneapolis Mirror.

## Configure the host storage systems

Your next step is to configure the hosts for use in your protection plan. This includes setting the login and NDMP credentials for the hosts and ensuring that the appropriate licenses are enabled on each host according to the purpose you assign to the host in your protection strategy.

### Considerations

Because you plan to back up the North Sea and Java seismic test data to the London data center and mirror the backup to the Minneapolis data center, enable Data ONTAP licenses as follows:



<b>North Sea storage system</b>	This storage system stores the North Sea seismic test data in need of protection, so enable the SnapVault Data ONTAP Primary license on this system.
<b>Java storage system</b>	This storage system stores the Java seismic test data in need of protection, so enable the SnapVault Data ONTAP Primary license on this system.
<b>London storage systems</b>	These storage systems are to store backups for the seismic data, so enable the SnapVault Data ONTAP Secondary license on these storage systems. Also enable the Data ONTAP SnapMirror license on these systems, because the backups they store are mirrored to Minneapolis.
<b>Minneapolis storage systems</b>	These storage systems are to store mirror copies of the London storage systems, so enable the SnapMirror license on these storage systems. The Minneapolis storage systems also require the SnapVault Data ONTAP Secondary license so that you can restore data from these storage systems if the London storage systems are unavailable.

Before beginning this procedure, you need to gather the necessary Data ONTAP license codes.

## Steps

1. From the navigation pane, click **Hosts ► Storage Systems**.
2. For each host that you plan to use, select the host name from the list and verify the following:
  - System Status is Up and Login Credentials are Good
  - NDMP Status is Up and NDMP Credentials are Good

For the instructional purposes of this example, you find that credentials are set and valid for most of the hosts, but one host you plan to use, minn8-geo, has bad credentials that you need to update.

3. Select **minn8-geo** from the list of hosts.
4. Click **Edit**.

The properties sheet for the minn8-geo host appears, displaying the current credential information for the host.

5. Update the Login Credentials and NDMP Credentials fields with valid user names and passwords, then click **OK**.

The database is updated with the credentials for the selected host. Verify in the host list that the credentials for minn8-geo are now good.

6. For each host that you plan to use, select the host name from the list and verify the following:
  - The necessary SnapMirror and SnapVault licenses are enabled.
  - The CIFS or NFS networking protocols are configured, as appropriate.

You notice that one of the London hosts that you plan to use, london14-geo, is configured with the SnapMirror license but not the SnapVault secondary license.

7. Select **london14-geo** from the list of hosts.

The licensing status for london14-geo is displayed in the Licenses area.

8. Click **Edit**, then click **Licenses**.

The Licenses tab of the properties sheet for the selected host appears.

9. Type the SnapVault secondary license in the New License field, then click **Add**.

The SnapVault secondary license is configured on london14-geo. Note that it is not necessary to indicate which service the code enables; the code is matched automatically to the appropriate service license.

You have configured the hosts with login and NDMP credentials and Data ONTAP licenses.

### After You Finish

The next step is to organize into resource pools the hosts that Protection Manager is to use to provision storage for backup and mirror copies.

## Create the resource pools

Organize the London storage system hosts into a resource pool for backups and the Minneapolis storage system hosts into a resource pool for mirror copies. Protection Manager can provision storage out of these resource pools, as needed.

### Before You Begin

Ideally, hosts in a resource pool are interchangeable in terms of their acceptability as destinations for backups or mirror copies. When developing the protection strategy for the seismic test data, you identified London and Minneapolis hosts with similar performance and quality of service levels that would be suitable members of the same resource pool.

You have already created aggregates of unused space on hosts you intend to assign to resource pools. This ensures that there is adequate space to contain the mirror copies and backups.

Before creating the resource pool, you need to gather the information necessary to complete the **Add Resource Pool** wizard:

- The name of each resource pool to be created



The names should indicate the location and purpose (storing backups or mirror copies) of each resource pool. For example, you use the name **London Backup** for the resource pool of hosts used to store backups in London.

- The time zone that the policy schedules should assume when timing protection events  
For example, setting the time zone of the **London Backup** resource pool to **Europe/London** specifies that scheduled mirror operations originating from London are to be interpreted in the London time zone.
- The physical resources to be included in the resource pool
- The space thresholds for event generation
- The aggregate overcommitted thresholds for event generation

## Steps

1. From the navigation pane, click **Data ► Resource Pools**.

The **Resource Pools** window appears.

2. Click **Add**.

The **Add Resource Pool** wizard starts.

3. Complete the steps in the wizard to create the **London Backup** resource pool.

Use the following settings:

- General properties:

Name: **London Backup**

- Physical resources:

Group: **Global**

Resource type: **Hosts**

Select the storage system hosts that you previously verified have good credentials and have SnapVault Secondary and SnapMirror licenses enabled.

- Resource pool label: none

4. Confirm the details of the resource pool, then click **Finish** to complete the wizard.
5. Click **Add** to start the **Add Resource Pool** wizard again.
6. Create another resource pool using the name **Minneapolis Mirror** and the same settings you used for the **London Backup** resource pool.
7. Confirm the details of the resource pool, then click **Finish** to complete the wizard.

The London Backup and Minneapolis Mirror resource pools can be viewed in the list on the **Resource Pools** window.

### After You Finish

You next evaluate and modify the protection schedules you want to later associate with a protection policy.

## Evaluate and modify the protection schedules

You now determine whether you can use existing schedules to meet your protection strategy needs or if you need to modify or create new schedules. The schedules are later assigned to the protection policy you choose.

### Considerations

As part of developing your protection strategy, you determined that you want to back up and then mirror-copy your data and that you need the following schedules for your backup and mirror jobs:

- On the primary data node: hourly, daily, and weekly backups
- For the primary-to-backup connection: back up twice daily and once weekly
- For the backup-to-mirror connection: hourly every day

The North Sea seismic test data and the Java seismic test data can use the same backup schedules, because their backup schedule requirements and constraints (recovery point objective, bandwidth, backup window, and so on) are the same.

**Note:** As you evaluate the schedules for the nodes and connections, make a notation of the schedules you decide to use because you need that information later.

### Step

1. From the navigation pane, click **Policies ► Protection ► Schedules**.

The Schedules tab on the **Protection Policies** window is displayed.

The next task is to decide which schedules you need and whether you can use or modify existing schedules to meet your needs.

### Next topics

*[Determine the schedule for the primary data node](#) on page 91*

*[Determine the schedule for the connection between the primary and backup nodes](#) on page 91*

*[Determine the schedule for the connection between the backup and mirror nodes](#) on page 93*

## Determine the schedule for the primary data node

Evaluate the schedules already available in Protection Manager to determine if you can use any of them for local backups of the primary data, or if you need to modify an existing schedule.

### Steps

1. Assess what schedule you need for local backups of your primary data.

You determine that you need the following backups:

- Local backups every hour
- Daily local backups each day at 12:00 a.m.
- Weekly local backups each Sunday at 12:00 a.m.

2. From the Schedules tab, review the list of existing schedules and their descriptions to determine if you can use any of them for primary data backups.

You determine that the schedule **Sunday at midnight with daily and hourly** meets your needs and you make note of this information.

### After You Finish

Keep the Schedules tab open so that you can next review schedules for remote backups.

## Determine the schedule for the connection between the primary and backup nodes

Evaluate the schedules already available in Protection Manager to determine if any of the schedules meet the needs for the primary-to-backup connection, or if you need to modify an existing schedule.

### Steps

1. Assess what schedule you need for remote backups of your primary data.

You determine that you need the following backups:

- Daily remote backups at 8:00 a.m.
- Daily remote backups at 8:00 p.m.
- Weekly remote backups each Sunday at 8:00 p.m.

2. From the Schedules tab, review the list of existing schedules and their descriptions to determine if you can use any of them for remote data backups.

You determine that the Weekly schedule "Sunday at 8:00 PM plus daily" is the closest to meeting your needs. It performs a weekly backup every Sunday and daily backups, all at 8:00 p.m. However, you need to add the 8:00 a.m. backup.

You realize that since the Weekly schedule has a daily backup at 8:00 p.m., it accesses the "Daily at 8:00 PM" schedule to define when daily operations occur. So you decide to modify this Daily schedule to add the 8:00 a.m. backup.

3. Select the schedule "**Daily at 8:00 PM**" and click **Copy**.

Directly modifying the "Daily at 8:00 PM" schedule would impact any policy already using that schedule. It would also impact any policy using the schedule "Sunday at 8:00 PM plus daily," because that weekly schedule uses "Daily at 8:00 PM" .

To avoid impacting other policies, you decide to copy "Daily at 8:00 PM" to create a new daily schedule, "Daily at 8:00 AM and PM."

4. Select **Copy of Daily at 8:00 PM** and click **Edit**.
5. On the **General** tab, change the schedule name to the following value: **Daily at 8:00 AM and PM**
6. Click the **Daily Events** tab, then click **Add**.
7. Double-click the row that was added to the list and type the following value: **8:00 AM**  
8:00 p.m. and 8:00 a.m. both show up in the Daily Events list and in the graph.
8. Click **OK**.
9. Select the **Sunday at 8:00 PM plus daily** schedule and click **Copy**.

You now copy and rename the Weekly schedule that you intend to use, so that it does not impact other policies that use the "Sunday at 8:00 PM plus daily" schedule.

10. Click **Copy of Sunday at 8:00 PM plus daily** and click **Edit**.

The **Properties** sheet opens.

11. On the **General** tab, change the schedule name to the following value: **Sunday at 8:00 PM plus daily at 8 AM and PM**.
12. Make note of the names of these Daily and Weekly schedules.

### After You Finish

Keep the Schedules tab open so that you can next review schedules for remote backups.

## Determine the schedule for the connection between the backup and mirror nodes

Evaluate the schedules available with Protection Manager to determine if any of the schedules meet the needs for the backup node-to-mirror node connection.

### Steps

1. Assess what schedule you need for the mirror copies of your backed-up data.

You determine that you need to perform a mirror operation more than once a day.

Although the seismic test data is backed up once a day, the primary data is maintained in two different time zones and, therefore, is backed up at different times. A single mirror operation each day does not provide adequate protection, because some data would be too old by the time it was mirrored to meet its recovery point objective.

You decide to mirror the seismic test data backup each hour, but on the half hour, because data is backed up to the Backup node on the hour. The 30-minute difference in the schedules gives the backup operation ample time to complete before the mirror operation begins.

2. From the Schedules tab, review the list of schedules and their descriptions to determine if you can use an existing schedule for the mirror copies.

You determine that the existing daily schedule, "Hourly on the half hour," meets your needs by providing hourly mirror operations and you make note of this information.

You are not concerned that there are 24 mirror operations each day even though the data to be mirrored is updated only twice a day. Mirror operations send only updated data to the Mirror node. When there is no updated data since the last mirror operation, no load is put on the network.

You have selected and modified all the schedules you need.

### After You Finish

You next create a new policy by copying an existing policy and modifying the policy's settings.

## Create the protection policy and modify the settings

As part of your protection strategy, you want to back up, then mirror, your data. You now copy and rename the existing "Back up, then mirror" protection policy.

### Considerations

Because you previously created new schedules, you know that you need to associate the new schedules with the "Back up, then mirror" policy. The existing "Back up, then mirror" policy might already be

associated with a dataset. Therefore, you do not want to modify the existing policy because this could negatively impact any dataset using that policy. You instead copy the existing "Back up, then mirror" policy so that you can modify the policy's schedules and other settings.

Each protection policy can have a different schedule associated with each node and connection of the policy. Each schedule has its own retention or lag settings. You can modify the schedule and its settings for each component of the policy, which you do in the following tasks.

### Steps

1. From the navigation pane, click **Policies ► Protection ► Overview**.

The Overview tab on the **Protection Policies** window is displayed.

2. Select the **Back up, then mirror** policy from the list and click **Copy**.

"Copy of Back up, then mirror" appears in the policy list, highlighted.

3. With "Copy of Back up, then mirror" still highlighted, click **Edit**.

The **Edit Properties** sheet opens to the general properties.

4. Change the name of the policy to **Test Data: Back up, then mirror**.

5. Retain the description of the policy.

You determine that the description is adequate.

6. Click **Apply**.

The name change is applied to the policy, but the **Properties** sheet remains open.

### After You Finish

With the policy **Properties** sheet still open, you will next associate the schedules, and evaluate and modify the policy settings, for each node and connection of this policy.

### Next topics

*Evaluate the primary data node* on page 94

*Evaluate the connection between the primary and backup nodes* on page 96

*Evaluate the backup node* on page 98

*Evaluate the connection between the backup and mirror nodes* on page 99

## Evaluate the primary data node

With the **Edit Properties** sheet still open for the "Back up, then mirror" policy, review the information for the primary data node.

## Considerations

You previously determined that the local backup schedule **Sunday at midnight with daily and hourly** meets your needs for the primary data. You will now evaluate how long you want the local backups retained and what the lag thresholds should be.

Lag thresholds represent the maximum acceptable lag between the current time on the primary node and the timestamp of the last successfully completed local backup copy on that node. Lags that exceed the specified period trigger either warning or error messages.

## Steps

1. Click **Nodes and Connections** in the **Properties** sheet.

The Nodes and Connections information appears. A graphical representation of the "Back up, then mirror" policy is displayed above the policy settings.

2. From the list, select **Primary data**.

Details about the primary node appear in the information area. The graphic displayed in the information area has the primary node highlighted.

3. Retain the default local backup schedule **Sunday at midnight with daily and hourly**.

You previously determined that this schedule meets your data protection needs for local backups.

4. Assess how long you need local backups of your primary data retained, based on the local backup schedule.

You determine the following:

- The backup schedule includes Daily local backups each hour and you want to retain 24 hourly local backups.
- The backup schedule includes a Daily local backup that you want to retain for seven days.
- The backup schedule includes a Weekly local backup that you want to retain for 14 days.
- The backup schedule includes no Monthly local backups, so you have no Monthly backups to be retained.

- a) Determine the default behavior of the retention settings.

The default settings retain the following:

**Hourly: 1.0 day**

Hourly local backups for one day

**Daily: 1.0 week**

Daily local backups for one week

**Weekly: 2.0 weeks**

Weekly local backups for two weeks

**Monthly: 0.0 weeks**

No monthly backups

- b) Decide what action to take.

The current retention duration settings for local backups meet the protection needs of the seismic test data, so you leave them unchanged.

5. Assess when you want Lag events generated for local backups of your primary data.

You determine the following:

- You do not need an event generated for the hourly backups.
- You want to receive a warning message after one daily backup failure.
- You want to receive an error message after two successive local backup failures.

a) Determine the event generation behavior of the default Lag settings.

The local backup operations on the primary node include hourly local backups, a daily local backup each day at midnight, and a weekly local backup at midnight on Sundays.

The default settings do the following:

**Lag Warning Threshold: 1.5 days** With daily backups at midnight, a lag warning threshold of 1.5 days means that a warning is issued after one local backup failure.

**Lag Error Threshold: 2.0 days** A lag error threshold of 2.0 days means that an error is issued after two successive Daily local backup failures.

b) Decide what action to take.

The default Lag Warning Threshold and Error Threshold meet your needs. You decide to use the default settings.

6. Consider whether you want to use a backup script.

Your protection strategy does not require use of a backup script, so you leave the associated fields blank.

**Note:** Leave the Nodes and Connections tab open for the next task.

### After You Finish

With the Nodes and Connections tab open, you next evaluate the primary-to-backup node connection.

## Evaluate the connection between the primary and backup nodes

With the **Edit Properties** sheet still open for the "Back up, then mirror" policy, review the information for the connection between the primary and backup nodes.



## Considerations

You previously determined that the default backup schedule **First Sunday at 8:00 PM with weekly and daily** did not meet your needs, so you created a new schedule, which you now select. You also evaluate what the lag thresholds should be.

The lag thresholds generate events based on the amount of lag time between remote backup data being sent and successfully backed up to the backup node.

## Steps

1. From the Nodes and Connections list, click the **Primary data to Backup** connection.

Details about the connection appear in the information area. The graphic displayed above the information area has the selected connection highlighted.

2. From the Backup schedule list, select **Sunday at 8 PM plus daily at 8 AM/PM..**

This is the schedule you previously created.

3. Consider whether you want to use a throttle schedule.

Your protection strategy does not require use of a throttle schedule, so you retain the default setting of "none."

4. Assess when you want Lag events generated.

You determine the following:

- You want to receive a warning message after two successive remote backup transfer failures, so you need a lag warning threshold for the backup connection of 1.0 day.
- You want to receive an error message after three successive remote backup transfer failures, so you need a lag error threshold for the backup connection of 1.5 days.

- a) Determine the event generation behavior of the default Lag settings.

The most frequent operation over this connection is the Daily remote backup sent to the Backup node at 8:00 a.m. and 8:00 p.m.

The default settings do the following:

**Lag Warning Threshold: 1.5 days** With remote backups 12 hours apart, a lag warning threshold of 1.5 days means that a warning is issued after three successive remote backup transfer failures.

**Lag Error Threshold: 2.0 days** A lag error threshold of 2.0 days means that an error is issued after four successive remote backup transfer failures.

- b) Decide what action to take.

The default settings do not meet your needs, so you must change them.

5. Change the lag warning threshold to **1.0 day**.
6. Change the lag error threshold to **1.5 days**.
7. Click the **Preview** tab.

The changes you made are checked for conformance issues.

8. Click **Apply**.

Do *not* click OK.

The changes you made are applied to the policy, but the **Properties** sheet remains open.

### After You Finish

With the **Properties** sheet open, you next evaluate the backup node.

## Evaluate the backup node

With the **Edit Properties** sheet still open for the "Back up, then mirror" policy, review the information for the backup node.

### Considerations

You now evaluate how long you want the remote backups retained.

The backup node does not have a schedule associated with it.

### Steps

1. From the Nodes and Connections list, click **Backup**.

Details about the node appear in the information area. The graphic displayed above the information area has the selected node highlighted.

2. Assess how long you need remote backups retained, based on the remote backup schedule you are using.

You determine the following:

- The backup schedule does not include Hourly backups, so you do not have hourly backups to be retained.
- Your backup schedule includes two Daily remote backups that you want to retain for two weeks, providing up to 28 daily remote backups.
- Your backup schedule includes a Weekly remote backup. Because you are not using any Monthly backups, you want to retain Weekly backups for 12 weeks.
- Your backup schedule does not include Monthly remote backups, so you do not have Monthly backups to be retained.

3. Consider whether the "Backup retention durations" settings meet your protection requirements.

a) Determine the default behavior of the retention settings.

The default settings retain the following:

<b>Hourly: 0.0 day</b>	No hourly remote backups are retained.
<b>Daily: 2.0 weeks</b>	Daily remote backups are retained for two weeks.
<b>Weekly: 8.0 weeks</b>	Weekly remote backups are retained for eight weeks.
<b>Monthly: 14.0 weeks</b>	Monthly remote backups are retained for 14 weeks, but because no monthly backups are created, this setting has no impact.

b) Decide what action to take.

- The Hourly, Daily, and Monthly retention duration settings for meet the protection needs of the seismic test data, so you leave them unchanged.
- However, the weekly retention setting does not meet your needs and has to be increased.

4. Change the Weekly retention setting to **12 weeks**.

5. Click the **Preview** tab.

The changes you made are checked for conformance issues.

6. Click **Apply**.

Do *not* click OK.

The changes you made are applied to the policy, but the **Properties** sheet remains open.

### After You Finish

With the policy **Properties** sheet still open, you next evaluate that backup-to-mirror connection.

## Evaluate the connection between the backup and mirror nodes

With the **Edit Properties** sheet still open for the "Back up, then mirror" policy, review the information for the connection between the backup and mirror nodes.

### Considerations

Lag thresholds generate events based on the amount of lag time between remote backup data being sent and successfully backed up to the backup node.

## Steps

1. From the Nodes and Connections list, click the **Backup to Mirror** connection.

Details about the connection appear in the information area. The graphic displayed above the information area has the selected connection highlighted.

2. From the Mirror schedule list, select **Hourly on half hour**.

This is the schedule you previously determined would meet your data protection needs.

3. Consider whether you want to use a throttle schedule.

Your protection strategy does not require use of a throttle schedule, so you retain the default setting of "none."

4. Assess when you want Lag events generated.

You determine the following:

- You want to receive a warning message after two successive mirror transfer failures, so you need a lag warning threshold of 2.0 hours.
- You want to receive an error message after three successive mirror transfer failures, so you need a lag error threshold of 3.0 hours.

- a) Determine the event generation behavior of the default Lag settings.

The most frequent operation over this connection is the Hourly mirror operation on the half hour.

The default settings do the following:

**Lag Warning Threshold: 1.5 days** With mirror operations one hour apart, a lag warning threshold of 1.5 days means that a warning is issued after 36 successive mirror transfer failures.

**Lag Error Threshold: 3.0 days** A lag error threshold of 3.0 days means that an error is issued after 72 successive mirror transfer failures.

- b) Decide what action to take.

The default settings do not meet your needs, so you must change them.

5. Change the lag warning threshold to **2.0 hours**.

6. Change the lag error threshold to **3.0 hours**.

7. Click the **Preview** tab.

The changes you made are checked for conformance issues. The system determines that there are no conformance errors or warnings.

**8. Click **Apply**.**

The changes you made are applied to the policy, but the **Properties** sheet remains open.

**9. Click **Nodes and Connections** and click the **Mirror** node in the list.**

You see that there are no settings to evaluate for the mirror node.

**10. Click **OK** to save the changes you have made and exit the policy **Properties** sheet.**

You return to the **Protection Policies** window.

The modified policy "Test Data: Back up, then mirror" is available for use.

**After You Finish**

You next create groups for your resource pools.

## Create groups

Create a group to contain the **Java Seismic Test Data** and **North Sea Seismic Test Data** datasets and future datasets of test data, and add the **London Backup** and **Minneapolis Mirror** resource pools to an existing group of resource pools.

**Before You Begin**

Before creating the new group for the datasets, you gather the information necessary to complete the **Add Group** wizard:

- The name of the group  
You plan to create a group called **Datasets: Test Data**.
- The parent of the group, if there is one  
You plan to create the new group under an existing parent group called Data Protection.
- The name and e-mail address of the group owner  
You created the datasets that are to be members of the new group, so you decide that you are to be the owner of the new group.
- The names of the objects you want to assign to the group  
You assign the **Java Seismic Test Data** and **North Sea Seismic Test Data** datasets to the new group.

**Considerations**

By default, datasets and resource pools belong to the Global group, which contains all objects managed by applications running with the DataFabric Manager server. You can configure alarms for objects in

a group, including the Global group. However, if you want to configure alarms for a specific set of objects, you need to create a group that contains only those objects.

Putting objects in groups also makes it easier to locate information in Protection Manager. The Group selection list in the toolbar enables you to display only the data that pertains to objects in a selected group, so creating a group can save time later by making it easier to find data in the interface.

Protection Manager provides dataset and resource pool events that you want to use to trigger alarms that notify you about data protection problems. You can configure alarms for datasets and resource pools in the Global group, but you want to configure alarms specific to datasets used for test data and resource pools used for data protection. (You do not need to configure alarms for the hosts; the individual hosts are already configured with alarms that alert storage managers of host-specific problems. )

Creating a group for each dataset would generate too many groups to be manageable, and putting all the datasets in a single group would not give you the granularity you want for filtering. Therefore, you decide to create a group specifically for datasets protecting the various kinds of test data that you expect to create in the future.

Because you can use resource pools to protect more than one dataset, you decide it is best to take the simplest approach and add the London Backup and Minneapolis Mirror resource pools to an existing group of resource pools used for data protection.

## Steps

1. From the navigation pane, click **Data ► Groups**.

The **Groups** window is displayed.

2. From the Group Name list, select the **Data Protection** parent group.

Assume that someone had previously created the Data Protection parent group.

3. Create the "Datasets:Test Data" child group.

- a) Click **Add**.

The **Add Group** wizard starts.

- b) When prompted, name the group:

**Datasets:Test Data**

Do not add members for now. Complete the steps in the wizard and click **Finish**.

The empty Test Data group is created.

4. Include the London Backup and Minnesota Mirror resource pools as members in the parent Data Protection group.

- a) Back in the **Groups** window, reselect the **Data Protection** parent group.
- b) Click **Edit > Members**.

The Edit Group property sheet opens to the Members tab.

- c) When the Member Selection dialog is displayed, select the **Resource Pools** category.
- d) From the list of available members, select **London Backup** and **Minneapolis Mirror**, then click the right-arrow button.

The London Backup and Minneapolis Mirror resource pools are added to the list of selected members.

- e) Click **OK**.

The London Backup and Minneapolis Mirror resource pools are added to the Resource Pools group.

### After You Finish

You next create the datasets and add them to the Datasets:Test Data group.

## Create datasets

You need to put the North Sea and Java seismic test data in datasets. The Java data is not yet protected. The North Sea data is currently protected by SnapVault and SnapMirror but not yet managed with Protection Manager.

### Before You Begin

Before creating a new dataset, you need to gather the necessary information to complete the **Add Dataset** wizard:

- The name of the new dataset  
You plan to identify each dataset by its contents, **North Sea Seismic Test Data** and **Java Seismic Test Data**.
- The name and contact information for the owner of the dataset.  
You are the owner of both datasets.
- The time zone the policy schedules should assume when timing protection events.  
The **North Sea Seismic Test Data** dataset uses the CET time zone. The **Java Seismic Test Data** uses the Asia/Jakarta time zone.
- The group, **Datasets: Test Data**, to which you want to add the dataset.
- The name of the policy you want to assign to the dataset.  
For both datasets, you assign the **Test Data: Back up, then Mirror** policy.
- The names of the resource pools or other physical resources (such as individual storage systems or aggregates) that you want to assign to each node in the dataset.

For both datasets, you assign the London Backup resource pool to the backup node and the Minneapolis Mirror resource pool to the mirror node.

- In a NAS environment, if the licensed provisioning application is active, whether you want to CIFS or NFS.

## Considerations

You want to put the North Sea and Java seismic test data in separate datasets because the data is in different time zones and needs to have scheduled backup operations run in the local time zone. The time zone setting applied to each dataset determines how the schedules attached to each dataset are interpreted. However, because their protection requirements are otherwise identical, you can apply the same policy to both datasets.

Because the North Sea data has existing SnapVault and SnapMirror relationships, you need to create the dataset first, then import the North Sea data into its dataset. You can assign the unprotected Java data to the dataset as part of the process of creating its dataset.

## Steps

1. From the navigation pane, click **Data ► Datasets**.

The datasets overview information is displayed on the **Datasets** window.

2. Click **Add**.

The **Add Dataset** wizard starts.

3. Complete the steps in the wizard to create the **Java Seismic Test Data** dataset.

The new **Java Seismic Test Data** dataset appears in the list of datasets.

4. Click **Add**.

The **Add Dataset** wizard starts.

5. Complete the steps in the wizard to create the **North Sea Seismic Test Data** dataset, but this time do not select any data when the wizard asks you to specify which data to include in the dataset.

The new **North Sea Seismic Test Data** dataset appears in the list of datasets.

## After You Finish

You next attach the protection policy to the dataset.



## Assign the protection policy to the datasets

After you create the datasets, you need to assign a protection policy to each dataset. The protection policy establishes the settings for how data backup and mirror operations should be performed.

### Before You Begin

Before assigning the protection policy, you gather the information necessary to complete the **Dataset Policy Change** wizard:

- The protection plan (backup, mirror, and so on) for this dataset  
You select the **Test Data: Back up, then Mirror** protection policy that you created.
- Whether you want to manually select individual physical resources to provision the nonprimary nodes, or whether you want to select resource pools to provision the nonprimary nodes.  
**Note:** In this example, you provision by resource pool.
- Which resource pools you want to use  
Select the resource pools you created for the backup node and the mirror node, London Backup and Minneapolis Mirror.
- Which vFiler units you use for the backup node and the mirror node

### Steps

1. From the navigation pane, click the Overview tab on the **Datasets** window.
2. Select **Java Seismic Test Data** from the list of datasets.
3. Click **Protection Policy** to start the **Dataset Policy Change** wizard.

**Note:** To assign a resource pool to your nonprimary nodes, click the **Use provisioning policy** option when it is displayed.

4. Complete the wizard and click **Finish**.

The Java Seismic Test Data dataset now has a protection policy associated with it. You must now repeat the task for the North Sea Seismic Test Data dataset.

5. Select **North Sea Seismic Test Data** from the list of datasets.
6. Click **Protection Policy** to restart the **Dataset Policy Change** wizard.
7. Complete the wizard and click **Finish**.

The North Sea Seismic Test Data dataset now has a protection policy associated with it.

### After You Finish

Verify that the protection policies are displayed in the Protection Policy column for the Java Seismic Test Data and North Sea Seismic Test Data datasets.

## Import discovered relationships

You need to import the North Sea data and its SnapMirror and SnapVault relationships into the dataset you created for it.

### Considerations

When you import relationships into a dataset, you associate the relationships with specific connections in the dataset. For the North Sea data, you want to import its existing SnapVault relationship into the connection between the primary data and the backup node in the **North Sea Seismic Test Data** dataset. You also want to import the North Sea data's existing SnapMirror relationship into the connection between the backup node and the mirror node.

### Steps

1. From the navigation pane, click **Data ► Unprotected Data ► External Relationships**.

The External Relationships tab in the **Unprotected Data** window is displayed. This window lists relationships for data protected by SnapMirror or SnapVault but not yet managed with a dataset.

2. Select the SnapMirror and SnapVault relationships for the North Sea seismic test data, then click **Import**.

The **Import Relationships** wizard starts.

3. Complete the steps in the wizard to associate the protection relationships of the North Sea seismic test data with the existing **North Sea Seismic Test Data** dataset.

Protection Manager imports the relationships into the **North Sea Seismic Test Data** dataset.

Protection Manager begins to manage the existing protection relationships as defined in the **Test Data: Back up, then Mirror** policy applied to the **North Sea Seismic Test Data** dataset.

### After You Finish

After successfully importing your existing SnapVault relationships, you should disable the SnapVault schedules on the storage systems from which the relationships were imported.

## Verify the protection of the dataset

To verify that the protection defined in the policy is functioning, you need to monitor the jobs that create the protection relationships and the jobs that back up and mirror-copy the seismic test data. You also need to check the status of the dataset.

### Steps

1. From the navigation pane, click **Data ► Jobs**.

The **Jobs** window is displayed.

2. Click the filter button in the Dataset column and enter **.\*Seismic** in the entry field.

The list displays information only for datasets that include the string "Seismic" in their names, such as **Java Seismic Test Data** and **North Sea Seismic Test Data**.

3. Review jobs for the two datasets as they run, noting whether any show a result other than **In Progress** or **Succeeded**.

4. From the navigation pane, click **Data ► Datasets ► Overview**.

The Overview tab of the **Datasets** window is displayed.

5. Select **Java Seismic Test Data** in the list of datasets.

The protection topology for **Java Seismic Test Data** is displayed in the Policy Diagram area and the properties of the dataset components are displayed in the properties area.

6. Review the protection, conformance, and resource status information for **Java Seismic Test Data**.

The dataset status is Protected and Conformant and the status of its resources is Normal.

7. Repeat Step 5 and Step 6 for the **North Sea Seismic Test Data** dataset.

You have successfully implemented protection for the seismic test data.

## Configure alarms

You want to configure alarms for the "Datasets:Test Data" group. One of the assumptions of this example is that you had already created a Resource Pools group and configured alarms for that group. Because the resource pools London Backup and Minneapolis Mirror are now members of that existing group, you do not need to set up alarms for them.

## Considerations

Before creating the alarms, you need to gather the following information necessary to complete the **Add Alarm** wizard for each alarm:

- The group to which you want to apply the alarm  
You are configuring alarms for the Datasets:Test Data group.
- The event name, event class, or severity type that you want to trigger the alarm  
For example, one of the alarms you plan to configure for the Datasets:Test Data group is triggered by the event **Dataset Protection Lag Error**.
- Who or what you want the event notification sent to
- The time period during which the alarm is active
- Whether you want the event notification repeated until the event is acknowledged and how often the notification should be repeated

## Steps

1. From the navigation pane, click **Notifications ► Alarms**.

The **Alarms** window is displayed.

2. Click **Add**.

The **Add Alarm** wizard starts.

3. Complete the steps in the wizard to create the alarm triggered by the event **Dataset Protection Lag Error**.

Repeat this procedure as needed for each alarm you want to configure for the Datasets:Test Data group.

# NAS resource provisioning and data protection example workflow

---

This is a step-by-step example of how you might configure your system to provision storage resources and protect user data. The example workflow assumes that both the Provisioning Manager license and the Protection Manager license are enabled on your system.

For descriptions of some of the concepts and terminology associated with Provisioning Manager and Protection Manager, see [Introduction to provisioning and protection](#) on page 39 .

For administrative tasks and additional reference and conceptual information associated with provisioning and protection, see the Provisioning Manager and Protection Manager Help.

This example is based on the same setup and configuration information that is used in the [Protection example workflow](#) on page 81 . To complete this combined workflow example, there are additional provisioning tasks you need to perform before implementing the protection tasks.

The following list describes the provisioning tasks for this example workflow. After completing the provisioning tasks, you must perform the tasks identified in the section [Completing the provisioning and protection example workflow](#) on page 119 .

## Next topics

[NAS provisioning and protection example setup](#) on page 109

[Develop a NAS provisioning strategy](#) on page 110

[Develop a protection strategy](#) on page 111

[NAS provisioning and protection example configuration assumptions](#) on page 112

[Configure the hosts](#) on page 114

[Create the resource pools](#) on page 117

[Create provisioning policies](#) on page 118

[Completing the provisioning and protection example workflow](#) on page 119

## NAS provisioning and protection example setup

For this example workflow, assume you are a storage architect for an energy company that needs to protect its seismic test data. The files of seismic test data are on storage systems on oil platforms in the North Sea and off the coast of Java.

The seismic test data files at the North Sea data center are currently protected by SnapVault and SnapMirror but are not yet managed with a dataset. The seismic test data files at the Java data center are not yet protected.

## Develop a NAS provisioning strategy

Before configuring the space and provisioning requirements for your systems, you must work out a strategy for how you will group the resources and how the application should respond in out-of-space conditions.

For descriptions of the basic concepts and terminology associated with Provisioning Manager, see [Introduction to provisioning and protection](#) on page 39 .

Your provisioning strategy addresses a variety of considerations:

### Storage type and protocol considerations

- What type of storage, NAS or SAN, do you want to provision with this policy?
- How will the customer's application access data?

Since the storage type for this example is NAS, determine the access or export protocols that you need to configure: NFS, CIFS, or multiprotocol.

### Availability considerations

What level of availability protection does the dataset require?

This is determined based on how critical the data is that you are protecting. The choices are:

- RAID-DP (Double disk failure)  
Protects against the simultaneous failure of two disks.
- RAID4 (Single-disk failure)  
Protects against the failure of a single disk.
- Storage subsystem failure (Aggregate SyncMirror)  
Protects against the failure of disk shelves, adapters, and cables.
- Storage controller failure (Active/active configuration)  
Protects against the failure of a storage system within a cluster.

### Space management considerations

- If you also have a Protection license, do you want to use the policy to provision storage for a secondary node (backup or mirror copy destination)?
- Do users or groups need to have quota limits set for storage usage?
- How do you want space allocated for user data and Snapshot copies on the primary node?
- What actions should occur when a dataset needs more space?
- Will you guarantee all storage space for data and Snapshot copies or will you use aggregate overcommitment to thinly provision your storage?

**Other Considerations**

- Will you use a custom provisioning script to perform tasks after storage is provisioned?

**Develop a protection strategy**

Before implementing a data protection plan, you must work out a strategy for protecting the seismic test data.

For descriptions of the basic concepts and terminology associated with Protection Manager, see [Introduction to provisioning and protection](#) on page 39 if possible.

Your strategy for protecting the data addresses a variety of considerations.

**Schedule considerations**

To meet the restore requirements of the data, you determine that the data should be backed up to the data center at company headquarters in London and mirrored to the company's Minneapolis data center.

- How long do you need to retain backups of the data to meet its restore requirements?
- What are the preferred times of day to perform remote backups and mirror copies, based on network and resource loads?
- How often does data on a primary node need to be copied to a destination node to ensure that data on the destination node is never older than the maximum age mandated by your protection requirements?

**Bandwidth considerations**

What is the volume of data to back up and the available bandwidth to transfer copies of the data to a destination system?

**Host considerations**

Which hosts in London and Minneapolis have similar performance and Quality of Service levels?

**Notification considerations**

Which events require alarms and who needs to be contacted for them?

**RBAC considerations**

Your administrator account already has the roles and capabilities assigned to it that you need to perform all the tasks necessary to implement the data protection strategy. See [Administrator roles and capabilities](#) on page 175 for a list of RBAC roles required for protection tasks.

## NAS provisioning and protection example configuration assumptions

The descriptions and procedures in the provisioning and protection workflow are based on the following assumptions.

- *General assumptions* on page 112
- *Licenses enabled* on page 112
- *Host properties* on page 112
- *Provisioning policy properties* on page 113
- *Resource pool properties* on page 113
- *Dataset properties* on page 113

### General assumptions

For this workflow, assume the following:

- You are configuring a storage environment of NAS over CIFS and NFS protocols.
- All hardware you intend to use has been configured with appropriate licenses, protocols, settings, and so forth.
- For any property not specified in this example, use the default value.

### Licenses enabled

For this workflow, you would need the following licenses enabled:

- DataFabric Manager with Provisioning Manager and Protection Manager licensed applications
- Data ONTAP licenses:
  - SnapVault on the primary storage system
  - SnapVault on the secondary storage system
  - SnapMirror on the tertiary storage system
  - Open Systems SnapVault
  - MultiStore license, enabled on each host containing vFiler units

### Host properties

For this workflow, assume use of the following properties for your hosts.

- Host configuration
  - Primary data is stored on existing vFilers.



- Backups and mirror copies will be stored on vFilers that you create for this use.
- Open Systems SnapVault agent is configured on the hosts.

## Provisioning policy properties

For this workflow, assume use of the following properties for the provisioning policies.

- General properties
  - Name: Use **provpol-nas** for the policy for primary data and **provpol-secondary** for the policy for the backups and mirror copy.
  - Description: Any meaningful description, such as **NAS policy using CIFS & NFS protocols**
  - Storage type: Use **NAS**
- Availability properties, Disk failure protection: Double disks (RAID-DP)
- NAS container properties, Quota settings: Use defaults of "0" (zero)

## Resource pool properties

For this workflow, assume use of the following properties for the resource pools.

- Details (general properties)
  - Name: Use **London Backup** and **Minneapolis Mirror**
  - Description: Any meaningful description
- Allocate physical resources
 

Select the resources to be included in the resource pool. These resources must meet the licensing and configuration requirements of your provisioning and protection plan. vFiler units are already created on the hosts to be used for the backups and mirror copy.

## Dataset properties

For this workflow, assume use of the following properties for the datasets.

- Name and description (general properties)
 

One dataset will be named **North Sea Seismic Test Data** and the other will be named **Java Seismic Test Data**.
- Group: Select the default, **Global**
- Resources: Select the default, **Use a provisioning policy**
- Provisioning
  - Provisioning policy: Select **provpol-nas**
  - Turn on NFS and CIFS and use the default settings
  - Select the resource pool to associate with the dataset

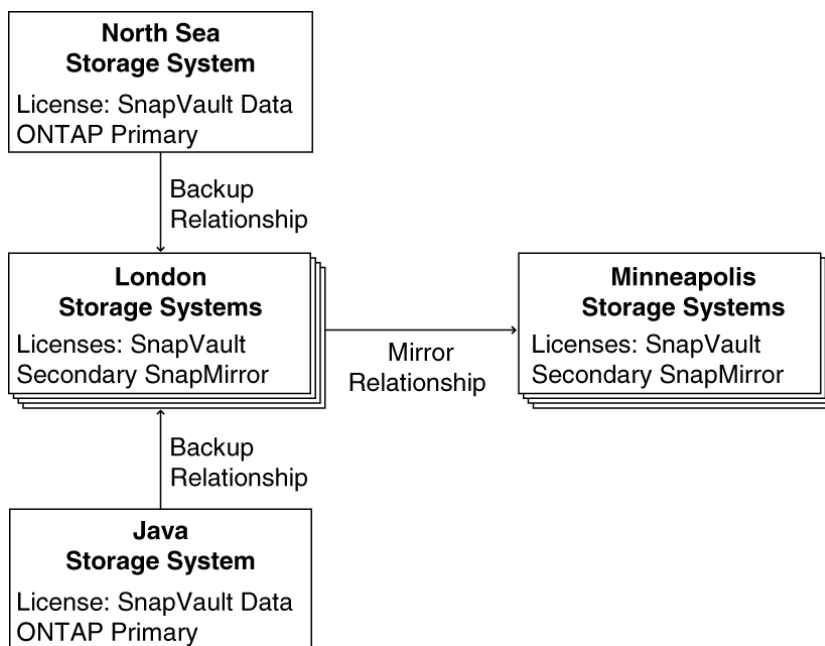
- vFiler unit: Select the vFiler unit that you created to assign to the dataset.
- Resource selection: Allow the system to automatically select a resource from the assigned resource pools.

## Configure the hosts

Your next step is to configure the hosts for use in your protection and provisioning plan. This includes setting the login and NDMP credentials for the hosts and ensuring that the appropriate licenses are enabled on each host according to the purpose you assign to the host in your protection and provisioning strategies.

### Considerations

Because you plan to back up the North Sea and Java seismic test data to the London data center and mirror the backup to the Minneapolis data center, enable Data ONTAP licenses as follows:



#### North Sea storage system

This storage system stores the North Sea seismic test data in need of protection, so enable the SnapVault Data ONTAP Primary license on this system.

#### Java storage system

This storage system stores the Java seismic test data in need of protection, so enable the SnapVault Data ONTAP Primary license on this system.

<b>London storage systems</b>	These storage systems will store backups for the seismic data, so enable the SnapVault Data ONTAP Secondary license on these storage systems. Also enable the Data ONTAP SnapMirror license on these systems, because the backups they store will be mirrored to Minneapolis.
<b>Minneapolis storage systems</b>	These storage systems will store mirror copies of the London storage systems, so enable the SnapMirror license on these storage systems. The Minneapolis storage systems also require the SnapVault Data ONTAP Secondary license so that you can restore data from these storage systems if the London storage systems are unavailable.
<b>All storage systems</b>	<p>Ensure that the appropriate CIFS or NFS licenses are installed and configured on each host that you plan to use.</p> <p>Ensure that the MultiStore license is enabled on each host that you plan to use.</p>

Before beginning this procedure, you need to gather the necessary Data ONTAP license codes.

The naming convention for storage systems at the energy company indicates the geographical location.

You need to verify the following information for each host that you are using:

- The System Status and NDMP Status are UP and the Login Credentials and NDMP Credentials are Good
- The appropriate Data ONTAP licenses are installed
- The appropriate CIFS or NFS networking licenses are installed
- The hosts or aggregates that you intend to use are not already part of another resource pool (resources can only belong to one resource pool)

## Steps

1. From the navigation pane, click **Hosts ► Storage Systems**.

2. Scan the credentials in the list of hosts.

For the instructional purposes of this example, you find that credentials are set and valid for most of the hosts, but one host you plan to use has bad credentials you need to update.

3. In the list of hosts, select the name of the host with bad credentials.

4. Click **Edit**.

The properties sheet for the selected host appears. The current credential information for the host is displayed.

5. Update the Login Credentials and NDMP Credentials fields with valid user names and passwords, then click **Apply**.

The database is updated with the credentials for the selected host. Verify that the credentials are now good.

6. Click the Details tab at the bottom of the window.
7. For each host that you plan to use, select the host from the list and verify the following:
  - The necessary SnapMirror and SnapVault licenses are enabled.
  - The CIFS or NFS networking protocols are configured, as appropriate.

Notice that one of the London hosts you plan to use, london14-geo, is configured with the SnapMirror license but not the SnapVault secondary license.

8. Select **london14-geo** from the list of hosts.

The licensing status for london14-geo is displayed in the Licenses area.

9. Click **Edit**, then click **Licenses**.

The Licenses tab of the properties sheet for the selected host appears.

10. Type the SnapVault secondary license code in the New License field, then click **Add**.

The SnapVault secondary license is configured on london14-geo. Note that it is not necessary to indicate which service the code enables; the code is matched automatically to the appropriate service license.

11. Click the Usage tab at the bottom of the **Storage Systems Hosts** window.

The bottom area of the window changes to display a tree view of the contents of the selected host and any resource pool or datasets that are associated with the host.

12. For each host that you plan to use, select the host in the tree view and verify that neither the host nor any of its aggregates are already associated with a resource pool.

If a storage system or an aggregate is part of a resource pool, the name of the resource pool is displayed. You must individually select each aggregate to in the host to see its dataset or resource pool associations.

Now that you have configured the hosts with login and NDMP credentials and verified the licenses, the next step is to organize the hosts into resource pools that the applications use to provision storage for the primary node and for backups and mirror copies.

## Create the resource pools

Organize the North Sea hosts and the Java hosts into separate resource pools for primary node provisioning. Organize the London hosts enabled with the SnapVault Secondary license into a resource pool for the backups and the Minneapolis hosts enabled with the SnapMirror license into a resource pool for the mirror copies. The applications provision storage out of these resource pools, as needed.

### Before You Begin

Ideally, hosts in a resource pool are interchangeable in terms of their acceptability as destinations for backups or mirror copies. When developing the protection strategy for the seismic test data, you identified London and Minneapolis hosts with similar performance and quality of service levels that would be suitable members of the same resource pool.

Where needed, you created aggregates of unused space on hosts you intend to assign to resource pools to ensure that there is adequate space to contain the mirror copies and backups.

Before creating each resource pool, you should have available the information necessary to complete the New Resource Pool wizard:

- The name of each resource pool to be created  
The names you plan to use can indicate the location and purpose (storing backups or mirror copies) of each resource pool. For example, you use the name London Backup for the resource pool of hosts used to store backups in London.
- The time zone the policy schedules should assume when timing protection events  
For example, setting the time zone of the London Backup resource pool to Europe/London specifies that scheduled mirror operations originating from London are to be interpreted in the London time zone.
- Which physical resources to associate with the resource pool
- The Resource Label, used for filtering resources during provisioning
- The Space Thresholds for setting alerts for out-of-space conditions

### Steps

1. From the navigation pane, click **Data ► Resource Pools ► Resources**.
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.

After you complete the wizard to create the London Backup resource pool, start the wizard again to create three more resource pools: the Minneapolis resource pool for mirror copies, named Minneapolis Mirror; the Java resource pool for primary data, named Java Primary; and the North Sea resource pool for primary data, named North Sea Primary.

### After You Finish

You will next create provisioning policies.

## Create provisioning policies

A provisioning policy describes the properties of storage, such as availability level, space allocation values, and so forth. You assign a provisioning policy to a dataset based on the set of storage properties that the dataset requires. For this example, you need to create two provisioning policies to apply to datasets. One to be assigned to the primary nodes and one to be assigned to the secondary backup and mirror nodes.

### Before You Begin

Before creating a provisioning policy, you need to gather the information necessary to complete the **Add Provisioning Policy** wizard.

- The name of the new policy  
You plan to use the name **provpol-nas** for the primary node NAS policy and **provpol-secondary** for the policy for the backup and mirror nodes.
- The type of storage you want to provision with this policy  
You will select the NAS option for the primary node policy and the Secondary option for the backup and mirror node policy.

Ensure that you are authorized to perform all parts of this task. Your RBAC administrator can confirm your authorization in advance.

### Steps

1. From the navigation pane, click **Policies ► Provisioning**.
2. Click **Add** to start the **Add Provisioning Policy** wizard.
3. On the General Properties page, enter the name and description, and select **NAS** as the storage type.
4. Complete each remaining property page in the wizard.
5. Confirm the details of the policy and click **Finish**.
6. Click **Add** to start the **Add Provisioning Policy** wizard again.
7. On the General Properties page, enter the name and description, and select **Secondary** as the storage type.
8. Complete the wizard and click **Finish**.

### After You Finish

Your new policies are listed in the **Provisioning Policies** window.

## Completing the provisioning and protection example workflow

You have completed the tasks that are specific to the provisioning part of the example. The remaining tasks are exactly the same as the those used in the protection workflow.

After completing the task *Create provisioning policies*, go to the [Protection example workflow](#) on page 81 and complete the following tasks:

- [Evaluate and modify the protection schedules](#) on page 90
- [Create the protection policy and modify the settings](#) on page 93
- [Create groups](#) on page 101
- [Create datasets](#) on page 103
- [Assign the protection policy to the datasets](#) on page 105
- [Import discovered relationships](#) on page 106
- [Verify the protection of the dataset](#) on page 107
- [Configure alarms](#) on page 107





# Disaster recovery example workflow

---

This is a step-by-step example of how you might configure your system to protect your user data and recover from a system failure. The example assumes that the Protection Manager license with the disaster recovery licensed option is enabled on your system (the Provisioning Manager license is *not* enabled).

For descriptions of some of the concepts and terminology associated with Protection Manager, see [Introduction to provisioning and protection](#) on page 39 if possible.

For administrative tasks and additional reference and conceptual information associated with Protection Manager, see the Protection Manager Help.

## Next topics

- [Disaster recovery protection example setup](#) on page 121
- [Develop a disaster recovery strategy](#) on page 122
- [Disaster recovery protection example assumptions](#) on page 123
- [Configure the hosts for disaster recovery protection](#) on page 125
- [Create the resource pools](#) on page 126
- [Create a failover script](#) on page 127
- [Create the disaster recovery protection policy](#) on page 129
- [Create the disaster recovery-capable dataset](#) on page 131
- [Assign the disaster recovery protection policy to the datasets](#) on page 133
- [Verify the disaster recovery protection of the dataset](#) on page 134
- [Test the failover script](#) on page 134
- [Perform an unscheduled update](#) on page 135
- [Fail over to the disaster recovery node](#) on page 136
- [Prepare for recovery after a disaster](#) on page 137
- [Manual failback using the command line interface](#) on page 138

## Disaster recovery protection example setup

For this example, assume you are a storage architect for a company with chain stores throughout the US. An active database that tracks chain store sales transactions is located in primary storage at Company A's San Francisco transaction and data center. The database is updated hourly by store managers sending in sales information from their remote branch locations.

For supporting normal business tracking, Company A's San Francisco site needs to provide the active read/write-capable primary data storage for remote online users sending in transaction data.

For business continuance purposes, Company A's San Jose site needs to be capable of taking over as the active primary storage site and provide continued reporting ability to remote store managers if the original primary storage site in San Francisco is destroyed or made unavailable.

For intermediate-term archival storage and data protection, the mirrored data from these transactions also needs to be backed up to a tertiary storage site in Sacramento.

## Develop a disaster recovery strategy

As Company A's storage architect, you must plan the deployment and configuration of your storage resources to ensure continued availability of primary storage data to remote users even when the primary data storage containers are destroyed or become unavailable .

### Issues to consider

Do you have applicable licenses installed? Which policy is best to use? How do you plan to provision storage on the nodes? These are questions you should consider before creating a dataset that is capable of disaster recovery. Your plans should include the following considerations:

- If you created datasets with a previous version of Protection Manager, do you want to convert them into dataset that supports failover?  
If so, install the disaster recovery and provisioning licenses on the DataFabric Manager server.
- What type of policy do you need? .  
An easy way to review the policies that are capable of disaster recovery is to set the filter in the DR Capable column to Yes in the **Protection Policies** window
- Do you want to manually assign resources to the node?  
You need to check that the resources assigned to the primary and disaster recovery nodes are matched in size and installed applications.
- Do you want to provision storage for disaster recovery nodes using policy-based provisioning?  
Even if you do not have the provisioning application installed, the protection application allows you to assign a default provisioning policy to your dataset and provision the dataset nodes by specifying resource pools.

### Disaster recovery deployment strategy

To support Company A's disaster recovery protection and archival requirements, you decide to deploy your storage system and storage management components in the following locations:

<b>Primary data storage site in San Francisco</b>	Storage systems in the San Francisco site must be set up to hold the primary transaction data accessed and updated by online users.
<b>Secondary storage and disaster recovery node site in San Jose</b>	Storage systems in the San Jose site must be set up to hold hourly copies of the transaction data mirrored from the San Francisco

	site and must be enabled to function as primary storage if the San Francisco site becomes unavailable.
<b>Tertiary or backup storage site in Sacramento</b>	Storage systems in the Sacramento must be set up to hold hourly copies of the transaction data backed up from the mirrored data at the San Jose site.
<b>DataFabric Manager server</b>	The DataFabric Manager server, <code>sacto_dfm</code> , is located at the Sacramento site.
<b>NetApp Management Console</b>	The NetApp Management Console for managing disaster recovery protection is located at the San Jose site.

## Disaster recovery protection example assumptions

This section identifies the configurations, settings, and properties that are used in the disaster recovery protection example workflow.

### General assumptions

- Enabled DataFabric Manager licensed applications: Protection Manager and Disaster Recovery
- Storage environment: NAS over CIFS and NFS protocols

### Licenses enabled

For this workflow, assume the following licenses are enabled:

- Data ONTAP SnapMirror license enabled on all primary, secondary, and tertiary storage systems.
- Protection Manager and disaster recovery license enabled on the NetApp Management Console

### Disaster recovery protection policy assumptions

For this example, assume the following properties when creating and assigning the disaster recovery capable protection policy.

- Policy name: **Company A Transaction Data:Mirror, then Backup**
- Primary data node

For this example, use the following default settings for the Primary node.

- Local Backup schedule: **Hourly on the half hour**  
When applied to the Primary data node, this schedule creates Hourly local backups each hour.
- Lag  
Warning Threshold: **2.0 hours**  
Error Threshold: **3.0 hours**

- Backup Script: none
- Failover Script: [https://sacto\\_dfm.company\\_a.com/transactions/failoverscripts/fo\\_script.sh](https://sacto_dfm.company_a.com/transactions/failoverscripts/fo_script.sh)
- Connection between the Primary data node and the DR Mirror node  
For this example, use the following settings for the "Primary to DR Mirror" connection.
  - Mirror copy schedule: **Hourly on half hour**  
You will need to select this existing schedule to replace the default.
  - Throttle schedule: **none**
  - Lag  
Warning Threshold: **2.0 hours**  
Error Threshold: **3.0 hours**
- Disaster Recovery node (DR Mirror node in this case)  
For this example, you will use the default node name, DR Mirror.
- Connection between the Mirror node and the Backup node
  - Backup schedule: **Hourly on half hour**  
You will need to select this existing schedule to replace the default.
  - Throttle schedule: **none**
  - Lag  
Warning Threshold: **2.0 hours**  
Error Threshold: **3.0 hours**
- Backup node  
For this example, use the following Backup node Retention settings:  
Hourly: **9 days**

### Dataset assumptions

For this example, assume the following properties when creating and protecting the datasets.

- Name: the dataset will be named **company\_a\_transactions**.
- Group: **Global**.
- Protection policy: **Company A Transaction Data: Mirror, then backup** customized from the base policy, **DR Mirror, then back up**.
- Resources: **Use a provisioning policy**.
- Provisioning policy: Use the default provisioning policy.
- Resource pools: Assign **San Jose Mirror** to the disaster recovery node site and **Sacramento Backup** to the Sacramento tertiary data site.

## Configure the hosts for disaster recovery protection

Your next step is to configure the hosts for use in your disaster recovery protection plan. This includes setting the login and NDMP credentials for the hosts and ensuring that the appropriate licenses are enabled on each host according to the purpose you assign to the host in your disaster recovery protection strategy.

### Considerations

Because you plan to mirror the hourly remote user transaction data from the San Francisco site to San Jose and back up the San Jose site to the Sacramento site, enable Data ONTAP licenses as follows:

<b>San Francisco storage systems (in the primary storage site)</b>	These storage systems store and allow user read/write access to the San Francisco transaction data, which you want to mirror to storage systems in San Jose, so enable the SnapMirror Data ONTAP license on this system.
<b>San Jose storage systems (in the disaster recovery site)</b>	These storage systems mirror on an hourly basis the data that is being read and written to at the San Francisco site, so enable the SnapMirror license on these systems. The SnapMirror license also enables backup of the mirrored data at the San Jose site to tertiary storage in Sacramento.
<b>Sacramento storage systems (in the backup tertiary storage site)</b>	These storage systems back up and provide long-term storage on transaction data that was input in San Francisco and mirrored to San Jose. San Jose storage systems are licensed for SnapMirror, so enable the SnapMirror license on the Sacramento storage systems also.

Before beginning this procedure, you need to gather the necessary Data ONTAP license codes.

The naming convention for the storage systems indicates their geographical location and their storage function.

### Steps

1. From the navigation pane, click **Hosts ► Storage Systems**.
2. Scan the list of hosts and verify the following for each host you intend to use:
  - System Status is Online
  - Login Credentials are Good
  - NDMP Status is Up
  - NDMP Credentials are Good
  - SnapMirror is licensed

Now that you have verified the proper configuration of each host you intend to use, the next step is to organize the hosts into resource pools that Protection Manager you use to provision storage for backups and mirror copies.

## Create the resource pools

Organize the San Jose hosts enabled with the SnapMirror license into a resource pool for the disaster recovery node mirror copies and the Sacramento hosts enabled with the SnapMirror license into a resource pool for the tertiary backup. Protection Manager can provision storage out of these resource pools, as needed.

### Before You Begin

Ideally, hosts in a resource pool are interchangeable in terms of their acceptability as destinations for mirror copies or backups. When developing the disaster recovery protection strategy for the remote user transaction data, you identified San Francisco and San Jose hosts with similar performance and capacities that would be suitable members of the same resource pool.

Where needed, you created aggregates of unused space on hosts you intend to assign to resource pools to ensure that there is adequate space to contain the mirror copies and backups.

Before creating the resource pool, you need to gather the information necessary to complete the **Add Resource Pool** wizard:

- The name of each resource pool to be created  
The names you plan to use indicate the location and purpose (storing backups or mirror copies) of each resource pool. For example, you use the name San Jose Mirror for the resource pool of hosts used to store mirror copies in San Jose.
- (Optional) A description of the resource pool
- (Optional) The name and e-mail address of the resource pool owner
- The time zone the policy schedules should assume when timing protection events (in this case, the same for all three sites)

### Steps

1. From the navigation pane, click **Data ► Resource Pools**.

The Resource Pools window appears.

2. Click **Add**.

The **Add Resource Pool** wizard starts.

3. Complete the steps in the wizard to create the **San Jose Mirror** resource pool.

Use the following settings:

- Name: Use **San Jose Mirror**.
- Space threshold defaults:
  - Space thresholds: enabled
  - Nearly Full threshold (for resource pool): 80%
  - Full threshold (for resource pool): 90%

After you complete the wizard to create the San Jose Mirror resource pool, start the wizard again to create the Sacramento Backup resource pool for backups.

## Create a failover script

In most cases an administrator supplies a failover script that specifies tasks that need to be completed at two points during failover: just before the mirror relationship between the San Francisco and San Jose storage is broken, and after the mirror relationship has been broken and the export protocols have been applied to the now active data in San Jose.

### Before You Begin

Ensure that you are assigned an administrator role that enables you to write to the DataFabric Manager server.

### Considerations

In this example, the failover script stops the program enabling new data writes to the San Francisco primary storage just before the mirror relationship break and starts that program at the San Jose disaster recovery node site just after the mirror relationship break.

### Steps

1. Author a failover script by using the passed variables and structure needed to achieve your disaster recovery goals.

For this example, the failover script you use stops and restarts applications that are writing data to the active primary storage data before and after the mirror relationship break.

2. Copy the failover script to the DataFabric Manager server or some other network location.

**Note:** You should avoid locating the failover script at the primary storage site.

For this example, the location of the DataFabric Manager server and the failover script is the Sacramento tertiary storage backup site. The failover script URL is `https://sacto_dfm.company_a.com/transactions/failoverscripts/fo_script.sh`.

## Example of a failover script

### Passed variables

A failover script can include the following variables, which are passed to it from the licensed protection application.

Variable	Description
DP_CONNECTION_ID	A tracking ID generated by the licensed protection application.
DP_DATASET_ID	A tracking ID generated by the licensed protection application.
DP_DATASET_NAME	The name of the dataset to which this script is to be applied.
DP_FAILOVER_SCRIPT_TEST	Whether or not this failover script is being invoked as a test. Starting a test failover by clicking <b>test failover</b> on the Disaster Recovery tab sets this value to 1.
DP_FAILOVER_STATUS	Whether the failover process is currently in the stage before or stage after the failover mirror relationship is broken. Values are either of the following: <ul style="list-style-type: none"> <li>DP_BEFORE_FAILOVER_MIRROR_BREAK</li> <li>DP_AFTER_FAILOVER_MIRROR_BREAK</li> </ul>
DP_JOB_ID	A tracking ID generated by the licensed protection application.
DP_POLICY_ID	A tracking ID generated by the licensed protection application.
DP_POLICY_NAME	The name of the disaster protection policy that is calling this failover script.
DP_SERIAL_NUMBER	The serial number of the DataFabric Manager server software.

### Example failover script

The following simple example script carries out the following functions:

- Checks to see if the failover is a test failover or an actual failover.
- Sends feedback to be displayed in the Job Summary field of the **Jobs** window.
- Stops a data-producing application prior to the failover-induced mirror relationship break.
- Restarts a data-producing application after the failover-induced mirror relationship break and data on the secondary has been exported.

```
#!/bin/sh
if [ "$DP_FAILOVER_SCRIPT_TEST" = "1" ]
then
    echo This is a TEST failover.
else
    echo This is an ACTUAL failover.
```



```

fi
    echo Script called with DP_FAILOVER_STATUS=$DP_FAILOVER_STATUS
    # Perform different operations based on failover status
    case "$DP_FAILOVER_STATUS" in
        DP_BEFORE_FAILOVER_MIRROR_BREAK)
            echo "Perform script operations before mirror break."
            # stop MySQL server
            rsh -l user_a r_host1 /etc/rc.d/init.d/mysqld stop
            ;;
        DP_AFTER_FAILOVER_MIRROR_BREAK)
            echo "Perform script operations after mirror break."
            # start MySQL server
            rsh -l user_a r_host1 /etc/rc.d/init.d/mysqld start
            ;;
        *)
            echo "Unknown DP_FAILOVER_STATUS: $DP_FAILOVER_STATUS"
            exit 1
    esac
    # Return 0 for success.
    # Return 1-255 for failure.
    exit 0

```

**Note:** The **Jobs** window can display up to 2 KB of failover script output for the Mirror Break Script End event. Output exceeding 2 KB is truncated and not recoverable.

## Create the disaster recovery protection policy

You now create a disaster recovery capable protection policy.

### Steps

1. From the navigation pane, click **Policies ► Protection ► Overview**.

The Overview tab on the **Protection Policies** window is displayed.

2. Click **Add Policy** to start the **Add Protection Policy** wizard.
3. Type a policy name, **Company A Transaction Data: Mirror, then Backup** and description, then click **Next**.
4. Select a base policy and click **Next**.

In this example you select **DR Mirror, then backup** as the base policy.

5. Complete the policy property sheets for the primary node and any mirror connection, backup connection, secondary storage, or tertiary storage node that the **Add Protection Policy** wizard displays for you. Use the following values:
  - Primary data node

<b>Node name: Primary data</b>	For this example, use this policy's default name for the primary data node. The primary data node contains the storage systems at Company A's San Francisco site.
<b>Local Backup Schedule: Hourly on the hour</b>	For this example, hourly local backup of the primary data is sufficient frequency.
<b>Backup Retention Duration: Hourly: 1 Day</b>	In this example, the only important retention time is the one-day retention duration you assign to Hourly backups.
<b>Lag Warning Threshold: 1.5 hours</b>	With Hourly backups, a lag warning threshold of 1.5 hours means that a warning would be issued after one local backup failure.
<b>Lag Error Threshold: 2.0 hours</b>	A lag error threshold of 2.0 hours means that an error would be issued after two successive local backup failures.
<b>Failover script:</b> <b><code>https:\\sacto_dfm.company_a.com</code></b> <b><code>\\transactions\\failoverscripts\\fo_script.sh</code></b>	<p>A failover script is commonly stored on the DataFabric Manager server or any place that the server can easily access it.</p> <p><b>Note:</b> You should avoid locating the failover script in a primary node container.</p>
<b>Run as: blank</b>	In this example, the policy's Run as parameter, which can be used to specify another UNIX user under whom to run this script, is left blank.

- Primary data to DR Mirror connection

<b>Mirror schedule: Hourly on half hour</b>	For the current purposes, the Hourly on half hour schedule provides mirror jobs at the required frequency.
<b>Throttle schedule: None</b>	Your protection strategy does not require use of a throttle schedule.
<b>Lag warning threshold: 2.0 hours</b>	You want to receive a warning message after two successive mirror transfer failures, so you need a lag warning threshold of 2.0 hours.
<b>Lag error threshold: 3.0 hours</b>	You want to receive an error message after three successive mirror transfer failures, so you need a lag error threshold of 3.0 hours.

- DR Mirror data node

**Node name: DR Mirror** For this example, use this policy's default name for the secondary storage disaster recovery node. The DR Mirror node contains the storage systems at company A's San Jose site.

- DR Mirror to Backup connection

**Mirror schedule: Hourly on the hour** The 30-minute difference with the Hourly on half-hour schedule assigned to the Primary to Mirror connection will give the mirror operation ample time to be completed before the backup operation begins.

**Throttle schedule: None** Your protection strategy does not require use of a throttle schedule.

**Lag warning threshold: 2.0 hours** You want to receive a warning message after two successive mirror transfer failures, so you need a lag warning threshold of 2.0 hours.

**Lag error threshold: 3.0 hours** You want to receive an error message after three successive mirror transfer failures, so you need a lag error threshold of 3.0 hours.

- Backup node

**Node Name: Backup** For this example, use this policy's default name for the tertiary storage backup node. The Backup node contains the storage systems at Company A's Sacramento site.

**Backup Retention Durations Hourly backups: 9 Days** In this example, you will retain Hourly backups in tertiary storage for 9 days.

After all property sheets are completed, the **Add Protection Policy** wizard displays a summary sheet for the policy that you will create.

6. Click **Finish** to save your changes.

### After You Finish

You next create the dataset to which you can assign the disaster recovery protection policy that you just created.

## Create the disaster recovery-capable dataset

You need to put the Company A transaction data in a dataset.

## Before You Begin

Before creating a new dataset, you need to gather the necessary information to complete the **Add Dataset** wizard:

- The name of the new dataset  
You plan to identify the dataset by its contents, **company\_a\_transactions**
- (Optional) A description of the dataset
- The name and contact information for the owner of the dataset  
You are the owner of the dataset.
- The time zone the policy schedule should assume when timing protection events  
The **company\_a\_transactions** dataset will use the America/Los Angeles time zone.
- The group to which you want to add the dataset
- Whether you want to manually select individual physical resources to provision the primary node, or whether you want to select resource pools to provision the primary node  
**Note:** In this example you will provision the primary node by assigning of physical storage elements at the San Francisco site.
- The names of the individual physical resources that you want to assign to the primary node in the **company\_a\_transactions** dataset

## Considerations

You will assign the Company A transaction data to the dataset as part of the dataset creation process.

## Steps

1. From the navigation pane, click **Data ► Datasets ► Overview**.  
The Overview tab of the **Datasets** window is displayed.
2. Click **Add**.  
The **Add Dataset** wizard starts.
3. Complete the steps in the wizard to create the **company\_a\_transactions** dataset.  
The new **company\_a\_transactions** dataset appears in the list of datasets.

## After You Finish

You next attach the disaster recovery protection policy to the dataset.

## Assign the disaster recovery protection policy to the datasets

After you create the dataset, you need to attach the disaster recovery protection policy to it. The disaster recovery protection policy establishes the settings for how mirror, backup, and, if necessary, failover operations should be performed.

### Before You Begin

Before attaching the disaster recovery protection policy, you gather the information necessary to complete the **Dataset Policy Change** wizard:

- The protection plan (backup, mirror, and so on) for this dataset  
In this example, you will select the **Company A Transaction Data: Mirror, then Back up** protection policy that you created.
- Whether you want to manually select individual physical resources to provision the nonprimary nodes, or whether you want to select resource pools to provision the nonprimary nodes

**Note:** In this example you will provision by resource pool.

- Assign the San Jose Mirror resource pool to the dataset's Mirror node.
- Assign the Sacramento Backup resource pool to the dataset's Backup node.

### Steps

1. From the navigation pane, click the Overview tab on the **Datasets** window.
2. Select the **company\_a\_transactions** dataset from the list of datasets.
3. Click **Protection Policy** to start the **Dataset Policy Change** wizard.

**Note:** To assign a resource pool to your non-primary nodes, click **Use provisioning policy** when it is displayed, then select the **default** option.

4. Complete the wizard and click **Finish**.

The **company\_a\_transactions** dataset now has a protection policy associated with it.

### After You Finish

Verify that the protection policies are now displayed in the Protection Policy column for the **company\_a\_transactions** dataset.

## Verify the disaster recovery protection of the dataset

To verify that the protection defined in the policy is functioning, you need to monitor the jobs that create the protection relationships and the jobs that back up and mirror the transaction data. You also need to check the status of the dataset.

### Steps

1. From the navigation pane, click **Data ► Jobs**.

The **Jobs** window is displayed.

2. Click the filter button in the Dataset column and enter **company\_a\*** in the entry field.

The list displays information only for datasets that include the string "company\_a" in their names, which in this example, will be **company\_a\_transactions**.

3. Review protection jobs for the dataset as they run, noting whether any show a result other than **In Progress** or **Succeeded**.

4. From the navigation pane, click **Data ► Datasets ► Overview**.

The Overview tab of the **Datasets** window is displayed.

5. Select **company\_a\_transactions** in the list of datasets.

The protection topology for **company\_a\_transactions** is displayed in the Policy Diagram area and the properties of the dataset components are displayed in the properties area.

6. Review the protection, conformance, and resource status information for **company\_a\_transactions**.

The dataset status is Protected and Conformant and the status of its resources is Normal.

You have successfully implemented disaster recovery protection for the Company A data.

## Test the failover script

After you have verified the success of the disaster recovery protection configuration, you can test the operation of your optional user-generated failover script to ensure that it operates as designed. You can test the failover script without conducting an actual failover.

### Before You Begin

- Ensure that you are assigned an administrator role that enables you to start and stop applications on the storage systems of the dataset being tested.
- Ensure that the failover script flags are set to prevent actual failover operations from proceeding.

### Steps

1. From the navigation pane, click **Data ► Datasets ► Disaster Recovery**.

The licensed protection application lists all the datasets that have been assigned disaster recovery capable protection policies.

2. Select the dataset on which you want to test the failover script.

In this case, you select the **company\_a\_transactions** dataset.

3. Click **Test**.

The licensed application begins testing the failover script that is stored on the associated DataFabric Manager server and specified in the disaster recovery capable protection policy assigned to the selected dataset.

The failover test adds a job, whose progress you can monitor in the **Jobs** window. However, because the script is executed in test mode, an actual failover with mirror relationship breaks, is not executed.

### After You Finish

If your primary data center in San Francisco is never threatened with destruction, disablement, or unavailability then testing of the failover script might be the last task to complete for implementing disaster recovery protection. However, if emergency forces you to invoke failover from the San Francisco to San Jose site then further tasks must be completed.

## Perform an unscheduled update

If you have advance warning of an impending events that might necessitate a failover and want to update the disaster recovery site with primary site data that has changed since the last scheduled mirror job, you can perform an unscheduled manual update before failover.

### Steps

1. In the Disaster Recovery tab, select the dataset to confirm that it was using the storage system when it crashed, assess what was damaged, and look for indication that the dataset can fail over.
2. Click **Update**.

Protection Manager updates the disaster recovery connection in the forward direction.

### After You Finish

After the update is complete, you can begin the failover process.

## Fail over to the disaster recovery node

If an emergency situation destroys, disables, or makes otherwise unavailable the data in the primary node storage systems, you can start failover to make the mirrored data on the disaster recovery node accessible and writeable by primary storage users.

### Before You Begin

You might want to update the disaster recovery node before you begin this procedure.

### Considerations

In this example, assume that a severed communications cable close to Company A's San Francisco transaction and data center prevents remote users from accessing and updating the transaction data at Company A's primary storage site.

### Steps

1. From the Disaster Recovery tab, select the dataset or datasets on which you want to carry out failover.

In this example, select the **company\_a\_transactions** dataset.

2. Click **Failover**.

The Begin Failover dialog box displays and gives you an opportunity to update the disaster recovery node connection.

3. If you need to update the disaster recovery node connection, click **Cancel** to return to the Disaster Recovery tab and click **Update**.

4. Click **Failover**.

The Begin Failover dialog box displays.

5. Click **Failover**.

The application returns to the Disaster Recovery tab.

6. View the failover job progress for the dataset in the Failover field.

Protection Manager does the following:



- If a failover script is associated with the dataset's protection policy, Protection Manager executes tasks specified in the pre-mirror-relationship-break part of the script.
- Breaks all the disaster recovery mirror copies for the company\_a\_transactions dataset, which makes the secondary storage writable.
- Makes the secondary data in the disaster recovery node system in San Jose accessible to clients and applications by bringing LUNs online and exporting NAS storage.
- If a failover script is associated with the dataset's protection policy, Protection Manager executes tasks specified in the post-mirror-relationship-break part of the script.
- Graphically displays the primary node as offline and the primary-to-mirror relationship as broken for the company\_a\_transactions dataset.

## Prepare for recovery after a disaster

If an emergency situation has forced you to carry out failover to the disaster recovery node systems, you need to take note of the recovery system before deciding which recovery strategy to follow.

### Steps

1. From the dashboard, click the Arrow button on the **Failover Readiness** panel to access the **Datasets** window.

From this window, you can find detailed information about the resource that requires you to take action. If a volume is offline, the icon indicates whether it is unavailable.

In this example, assume all the volumes and qtrees in the Company A Transaction Data dataset were taken offline by a disrupted cable connection to the site.

2. In the Disaster Recovery tab, select the affected dataset to confirm that it was using the storage system when it crashed, assess what was damaged, and look for indication that the dataset can fail over.

Look for matching criteria:

- Physical resources--are they the same storage systems or have the same RAID protections?
- Backup copies--are they the same size?
- Normal status--are the volumes online?

In best cases, you can fix the primary storage or recover lost data from backups, although you may want to failover manually to avoid downtime while fixing the problem. If backups are not available, or hardware and disks are destroyed, you would then fail over to the disaster recovery node.

In this example, assume that the original primary storage systems at the San Francisco site have remained intact. Within a day the severed cable connections have been restored, and the remaining task is to

restore the San Francisco site as the primary site, using a failback process to resynchronize its data and then giving it back its primary storage function.

## Manual failback using the command line interface

Use the `dfpm` and `dfdrm` commands on the DataFabric Manager server to resynchronize data on restored volumes and qtrees.

### Before You Begin

Ensure that you are assigned an administrator role that enables you to restart storage systems on the primary and disaster recovery nodes.

### Considerations

In this example, the volume and qtree resources at the original San Francisco primary site remain intact after the communications cable disruption and failover occurs. The San Jose disaster recovery site continues to provide primary storage function and has received and recorded updated sales data from the various branch stores. Now cable communications to the San Francisco site have been restored, and your task is to complete the following actions.

- Update the San Francisco storage systems with the changes in the transaction data that have occurred and been recorded at the San Jose site after failover was completed.
- Give primary storage function back to the San Francisco data and transaction center.

### Steps

1. Log in to the DataFabric Manager server, `sacto_dfm`.
2. To list all the San Jose secondary storage elements (mirrored volumes and qtrees) in the `company_a_transactions` dataset, enter the command:

```
dfpm dataset list -R company_a_transactions
```

This command lists all the mirror relationships in the `company_a_transactions` dataset. The ones in the "broken\_off" state (this should be all mirror relationships) are the ones you want to restore.

**Note:** In this example assume that in the listed broken off mirror relationships, the San Francisco storage elements are: `sf_obj1`, `sf_obj2`, `sf_obj3`, and `sf_obj4` and their associated San Jose storage elements are: `dr_obj1`, `dr_obj2`, `dr_obj3`, and `dr_obj4`.

3. To resynchronize data in the original primary volumes and qtrees in the San Francisco site with their updated secondary volumes and qtrees in the San Jose site, enter the command:

```
dfdrm mirror resync -r dr_obj1 dr_obj2 dr_obj3 dr_obj4
```

In this command the `-r` parameter temporarily reverses the original mirror relationships so that the original primaries in San Francisco are updated as mirror targets with the most recent data from San Jose.

Wait for the `dfdrm mirror resync -r` job to complete.

4. To confirm the successful completion of the resynchronization, note its job ID and enter the command:

```
dfdrm job list job_ID
```

5. To break the temporary reverse mirror relationship, enter the command:

```
dfdrm mirror break sf_obj1 sf_obj2 sf_obj3 sf_obj4
```

**Note:** Confirm that the `dfdrm mirror break` job is complete before starting the next step.

6. To confirm successful completion of the relationship break, note its job ID and enter the command:

```
dfdrm job list job_ID
```

7. To reestablish the mirror relationship in the forward direction, enter the command:

```
dfdrm mirror resync -r sf_obj1 sf_obj2 sf_obj3 sf_obj4
```

Wait for the `dfdrm mirror resync -r` job to complete.

8. To confirm successful completion of the resynchronization, note its job ID and enter the command:

```
dfdrm job list job_ID
```

9. To restore the dataset DR state to ready, enter the command:

```
dfpm dataset failover state company_a_transactions "ready"
```

After the restoration of disaster recovery state ready to the `company_a_transactions` dataset, Protection Manager displays that dataset as it was displayed before failover was started.



# Combined Protection Manager and SnapManager database protection example workflow

---

This is a step-by-step example of how a database administrator (DBA) operating SnapManager for Oracle, and a storage administrator operating Protection Manager, might integrate a managed Oracle database with a Protection Manager dataset, and configure scheduled, policy-based protected backup of that database to secondary storage.

For descriptions of some of the concepts and terminology associated with Protection Manager, see [Introduction to provisioning and protection](#) on page 39 if possible.

For administrative tasks and additional reference and conceptual information associated with Protection Manager, see the Protection Manager Help. For administrative tasks, command reference, and conceptual information associated with SnapManager for Oracle, see the *SnapManager for Oracle Installation and Administration Guide*. For tasks and conceptual information related to using the SnapManager for Oracle graphical user interface, see the online Help.

The following list describes the concepts and the workflows you and your DBA or storage administrator partner need to complete.

## Next topics

[Protected database backup](#) on page 141

[Details of the target database](#) on page 142

[Primary and secondary storage configuration and topology](#) on page 142

[Backup schedule and retention strategy](#) on page 146

[Workflow summary for database protected backup](#) on page 147

[Protected backup configuration and execution](#) on page 148

[Use SnapManager for Oracle to restore backups from secondary storage](#) on page 156

## Protected database backup

SnapManager and Protection Manager, when installed on a UNIX host and on the DataFabric Manager server respectively, give the SnapManager database administrator (DBA) the ability to configure and perform policy-based Oracle database backups to secondary storage, and to restore, if necessary, the backed up data from secondary to primary storage.

- In SnapManager terminology, non-local database backup from primary storage to secondary storage is called "protected backup."
- Although a typical database backup configuration enables the DBA to perform both local backup on the primary storage system and protected backup to a secondary storage system, this chapter

describes only the configuration tasks necessary to support database protected backup, which requires the coordination of both SnapManager and Protection Manager products.

- To perform protected backup, the DBA of the target database, requires read access to the secondary storage system in addition to the normal read and write access to primary storage systems.
- The storage administrator requires read and write access to both primary storage systems and secondary storage systems.

## Details of the target database

This example of integrated database protection describes the protection of a payroll database. The following data is used in the example.

The database administrator (DBA) at TechCo, a 3000-person company headquartered in Atlanta, must create a consistent backup of the production payroll database, PAYDB. The protection strategy for backing up to primary and secondary storage requires that the DBA and the storage administrator work together to back up the Oracle database both locally on primary storage and also remotely, to secondary storage at a remote location.

### Profile information

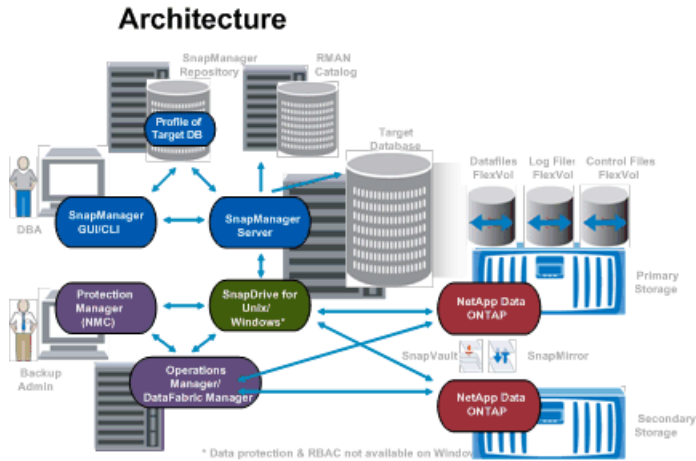
When creating a profile in SnapManager, you need the following data:

- Database name: PAYDB
- Host name: payroll.techco.com
- Database ID: payrolldb
- Profile name: payroll\_prod
- Connection mode: Database authentication
- Snapshot naming scheme:  
*smo\_hostname\_dbsid\_smopprofile\_scope\_mode\_smid* , which translates to "smo\_payroll.xyz.com\_payrolldb\_payroll\_prod\_f\_h\_x"

## Primary and secondary storage configuration and topology

In this example, the TechCo corporation runs its payroll database on a database server that is also a SnapManager for Oracle host and stores its payroll database data and configuration files on primary storage systems at company headquarters. The corporate requirement is to protect that database with daily and weekly backups to local storage as well as backups to storage systems at a secondary storage site fifty miles away.

The following illustration shows the SnapManager for Oracle and Protection Manager components required to support local and secondary backup protection.



**Figure 1: Components for local and secondary backup protection**

To manage the payroll database and support its local and secondary backup protection, the following deployment is used.

**SnapManager host** The SnapManager host, payroll.techco.com, is located at company headquarters and runs on a UNIX server, which also runs the database program that generates and maintains the payroll database.

**Connections** To support local backup and secondary backup protection, the SnapManager host has network connections to the following components:

- SnapManager for Oracle client
- SnapManager repository, which runs the database program, SnapDrive for UNIX, and SnapManager
- Primary storage systems
- Secondary storage systems
- DataFabric Manager server

**Installed products** The SnapManager host is installed with the following products for this example:

- SnapManager server
- SnapDrive for UNIX
- Host Utilities

**TechCo primary storage systems** The payroll database, including associated data files, log files, and control files, reside on the primary storage systems. These are located at TechCo company headquarters along with the SnapManager host and the network connecting primary storage and the SnapManager host. The latest payroll database transactions and updates are written to the primary storage systems. Snapshot copies, which provide local backup protection of the payroll database, also reside on the primary storage systems.

**Connections** To support secondary backup protection, the primary storage systems have network connections to the following components:

- SnapManager host running the database program, SnapDrive for UNIX, and SnapManager
- Secondary storage systems
- DataFabric Manager server

**Installed products** The following licenses must be enabled on these systems for this example:

- Data ONTAP 7.3.1 or later
- SnapVault Data ONTAP Primary
- FlexVol (required for NFS)
- SnapRestore
- NFS protocol

**TechCo secondary storage systems** The secondary storage systems, located at a network-connected secondary storage site fifty miles away, are used to store secondary backups of the payroll database.

**Connections** To support secondary backup protection, the secondary storage systems have network connections to the following components:

- Primary storage systems
- DataFabric Manager server

**Installed products** The following licenses must be enabled on the secondary storage systems for this example:

- Data ONTAP
- SnapVault Data ONTAP Secondary
- SnapRestore
- FlexVol (required for NFS)
- NFS protocol



**DataFabric Manager server** The DataFabric Manager server, techco\_dfm, is located at company headquarters in a location accessible by the storage administrator. The DataFabric Manager server, among other functions, coordinates the backup tasks between primary and secondary storage.

**Connections** To support secondary backup protection, the DataFabric Manager server maintains network connections to the following components:

- NetApp Management Console
- Primary storage systems
- Secondary storage systems

**Installed products** The DataFabric Manager server is licensed for the following server products for this example:

- DataFabric Manager
- Protection Manager

**SnapManager repository** The SnapManager repository, located on a dedicated server, stores the profiles of the target database. The repository records when SnapManager initiated a backup, which files were backed up, and whether or not a clone was created from the backup. When a DBA attempts a full or partial restore, SnapManager queries the repository to identify previous backups.

**Connections** To support secondary backup protection, the secondary storage systems have network connections to the following components:

- SnapManager host
- SnapManager for Oracle client

**NetApp Management Console** The NetApp Management Console is the graphical user interface console used by the storage administrator to configure schedules, policies, datasets, and resource pool assignments to enable backup to secondary storage systems, which are accessible to the storage administrator.

**Connections** To support secondary backup protection, NetApp Management Console has network connections to the following components:

- Primary storage systems
- Secondary storage systems
- DataFabric Manager server

**Installed products** In this example, the following feature must be licensed:

- Protection Manager client

**SnapManager for Oracle client** The SnapManager for Oracle client is the graphical user interface and command line console used by the DBA for the payroll database in this example to configure and carry out local backup and backup to secondary storage.

**Connections** To support local backup and secondary backup protection, SnapManager for Oracle client has network connections to the following components:

- SnapManager host
- SnapManager repository, running the database program, SnapDrive for UNIX, and SnapManager
- Database host (if separate from the host running SnapManager)
- DataFabric Manager server

**Installed products** To support local backup and secondary backup protection, the SnapManager for Oracle client software must be installed on this component.

## Backup schedule and retention strategy

The DBA wants to ensure that backups are available in case of a loss of data, in case of a disaster, and for regulatory reasons. This requires a carefully thought out retention policy for the various databases.

For the production payroll database, the DBA adheres to the following TechCo retention strategy:

Backup frequency	Retention duration	Backup time	Type of storage
Once daily	10 days	7 p.m.	Primary (local)
Once daily	10 days	7 p.m.	Secondary (archive)
Once weekly	52 weeks	Saturdays 1 a.m.	Secondary (archive)

<b>Local backup advantages</b>	<p>Daily local backup provides database protection, which is instantaneous, uses zero network bandwidth, uses a minimum of additional storage space, provides instantaneous restore, and provides finely-grained backup and restore capability.</p> <p>Because the final weekly backups of the payroll database are retained for a minimum 52 weeks at a secondary storage site, there is no need to retain the daily backups any longer than 10 days.</p>
<b>Protected backup advantages</b>	<p>Daily and weekly backups to secondary storage at a remote location guarantee that if the storage systems at the primary storage site are destroyed, the target database is still protected and can be restored from secondary storage.</p> <p>The daily backups to secondary storage are made to protect against primary storage system destruction. Because the final weekly backups of the payroll database are retained for a minimum 52 weeks, there is no need to retain the daily backups any longer than 10 days.</p>

## Workflow summary for database protected backup

In this example, the DBA (using SnapManager) and the storage administrator (using Protection Manager) coordinate actions to configure protected backup of the target database.

The sequence of actions carried out are summarized as follows:

<b>Secondary resource pool configuration</b>	The storage administrator uses Protection Manager to configure a resource pool of storage systems at the secondary site that can be used to store the payroll database backup.
<b>Protected backup scheduling</b>	The storage administrator uses Protection Manager to configure protected backup schedules.
<b>Protection policy configuration</b>	The storage administrator uses Protection Manager to configure a protected backup protection policy for the target database. The protection policy includes the schedules and specifies the base type of protection to implement backup protection (backup, mirror, or a combination of both), and names and retention policies for primary data, secondary, and sometimes tertiary storage nodes.
<b>Database profile configuration and protection policy assignment</b>	<p>The DBA uses SnapManager to create or edit a profile of the target database that supports protected backup. While configuring the profile, the DBA performs the following tasks:</p> <ul style="list-style-type: none"> <li>• Enables backup protection to secondary storage</li> <li>• Assigns the new protection policy, which was created in and retrieved from Protection Manager, to this profile</li> </ul>

Assigning the protection policy automatically includes the target database in a partially provisioned, but nonconformant Protection Manager dataset. When fully provisioned, the dataset configuration enables backup of the target database to secondary storage

**Secondary and tertiary storage provisioning**

The storage administrator uses Protection Manager to assign resource pools to provision the secondary and sometimes tertiary storage nodes (if the assigned protection policy specifies tertiary storage nodes).

**Backup on local storage**

The DBA opens the profile with protection enabled in SnapManager and creates a full backup to local storage. The new backup shows in SnapManager as scheduled for protection, but not yet protected. After the next Protection Manager executed backup occurs the backup is protected.

**Protected backup confirmation**

The DBA uses SnapManager to confirm the completion of the protected backup. After either an on-demand backup or a scheduled backup has been copied to secondary storage, SnapManager changes the backup Protection State from "Not protected" to "Protected."

## Protected backup configuration and execution

Configuring SnapManager and Protection Manager to support database backup to secondary storage requires that the database administrator and the storage administrator coordinate their actions.

**Next topics**

*[Use Protection Manager to configure a secondary resource pool](#) on page 148*

*[Use Protection Manager to configure secondary backup schedules](#) on page 149*

*[Use Protection Manager to configure a secondary backup protection policy](#) on page 151*

*[Use SnapManager for Oracle to create the database profile and assign a protection policy](#) on page 152*

*[Use Protection Manager to provision the new dataset](#) on page 154*

*[Use SnapManager for Oracle to create a protected backup](#) on page 155*

*[Use SnapManager for Oracle to confirm backup protection](#) on page 156*

## Use Protection Manager to configure a secondary resource pool

To support backup of the database to secondary storage, the storage administrator uses Protection Manager to organize the secondary storage systems enabled with the SnapVault Secondary license into a resource pool for the backups.

## Before You Begin

Ideally, storage systems in a resource pool are interchangeable in terms of their acceptability as destinations for backups. When developing the protection strategy for the payroll database, you, as the storage administrator, identified secondary storage systems with similar performance and quality of service levels that would be suitable members of the same resource pool.

You have already created aggregates of unused space on storage systems that you intend to assign to resource pools. This ensures that there is adequate space to contain the backups.

## Steps

1. Go to NetApp Management Console.
2. From the navigation pane, click **Data ► Resource Pools**.

The **Resource Pools** window appears.

3. Click **Add**.

The **Add Resource Pool** wizard starts.

4. Complete the steps in the wizard to create the **paydb\_backup\_resource** resource pool.

Use the following settings:

- Name: Use **paydb-backup\_resource**
- Space thresholds, use the defaults:
  - Space utilization thresholds: enabled
  - Nearly Full threshold (for resource pool): 80%
  - Full threshold (for resource pool): 90%

## Use Protection Manager to configure secondary backup schedules

To support backup of the database to secondary storage, the storage administrator uses Protection Manager to configure a backup schedule.

## Before You Begin

Before configuring the schedule for secondary backups, the storage administrator confers with the DBA partner for the following information:

- The schedule that the DBA wants the secondary backups to follow.  
In this case, once-daily backups at 7 p.m. and once-weekly backups on Saturday at 1 a.m.

## Steps

1. Go to NetApp Management Console.

2. From the navigation pane, click **Policies ► Protection ► Schedules**.

The Schedules tab of the **Protection Policies** window is displayed.

3. Select the Daily schedule **Daily at 8:00 PM** in the list of schedules.

4. Click **Copy**.

A new Daily schedule, **Copy of Daily at 8:00 PM**, is displayed in the list. It is already selected.

5. Click **Edit**.

The Edit Daily Schedule property sheet opens to the Schedule tab.

6. Change the schedule name to **Payroll Daily at 7 PM**, update the description, then click **Apply**.

Your changes are saved.

7. Click the **Daily Events** tab.

The schedule's current Daily backup time of 08:00 PM is displayed.

8. Click **Add** and enter **7:00 PM** in the new time field, then click **Apply**.

The schedule's current Daily backup time is now 07:00 PM.

9. Click **OK** to save your changes and exit the property sheet.

Your new Daily schedule, **Payroll Daily at 7 PM**, is displayed in the list of schedules.

10. Select the Weekly schedule **Sunday at 8:00 PM plus daily** in the list of schedules.

11. Click **Copy**.

A new Weekly schedule, **Copy of Sunday at 8:00 PM plus daily**, is displayed in the list. It is already selected.

12. Click **Edit**.

The Edit Weekly Schedule property sheet opens to the Schedule tab.

13. Change the schedule name to **Payroll Saturday at 1 AM plus daily at 7 PM** and update the description.

14. From the **Daily Schedule** drop-down list, select the Daily schedule you just created, **Payroll Daily at 7 PM**.

Selecting **Payroll Daily at 7 PM** means that this schedule defines when Daily operations occur when the **Payroll Saturday at 1 AM plus daily at 7 PM** schedule is applied to a policy.

15. Click **OK** to save your changes and exit the property sheet.

Your new Weekly schedule, **Payroll Saturday at 1 AM plus daily at 7 PM**, is displayed in the list of schedules.

## Use Protection Manager to configure a secondary backup protection policy

After configuring the backup schedule, the storage administrator configures a protected backup storage policy in which that schedule is to be included.

### Before You Begin

Before configuring the protection policy, the storage administrator confers with the DBA partner for the following information:

- Retention duration to specify for secondary storage
- Type of secondary storage protection required

### Steps

1. Go to NetApp Management Console.
2. From the navigation pane, click **Policies ► Protection ► Overview**.

The Overview tab on the **Protection Policies** window is displayed.

3. Click **Add Policy** to start the **Add Protection Policy** wizard.

4. Complete the wizard with the following steps:

- a) Specify a descriptive policy name.

For this example, enter **TechCo Payroll Data: Backup** and description, then click **Next**.

- b) Select a base policy.

For this example, select **Back up** and click **Next**.

- c) On the Primary Data node policy property sheet, accept the default settings and click **Next**.

**Note:** In this example, the local backup schedule that was configured in SnapManager is applied. Any local backup schedule that is specified through here is ignored.

- d) On the Primary Data to Backup connection property sheet, select a backup schedule.

For this example, select **Payroll Saturday at 1 AM plus daily at 7 PM** as your backup schedule, then click **Next**.

In this example, the schedule that you selected includes both the weekly and daily schedules that you configured earlier.

- e) On the Backup policy property sheet, specify the name for the backup node and the retention times for Daily, Weekly, or Monthly backups.

For this example, specify a Daily backup retention of 10 days and a Weekly backup retention of 52 weeks. After you complete each property sheet, click **Next**.

After all property sheets are completed, the **Add Protection Policy** wizard displays a summary sheet for the protection policy that you want to create.

5. Click **Finish** to save your changes.

The **TechCo Payroll Data: Backup** protection policy is listed among the other policies configured for Protection Manager.

## Use SnapManager for Oracle to create the database profile and assign a protection policy

To create a protected backup, the DBA must create a profile in SnapManager for Oracle, enable protection in the profile, and assign a protection policy.

### Considerations

A profile holds the information about the database being managed, including its credentials, backup settings, and protection settings for backups. Once a profile is created, the DBA does not need to specify database details each time the DBA performs an operation, such as a backup—simply supply the profile name. A profile can reference only one database, but that same database can be referenced by more than one profile.

### Steps

1. Go to the SnapManager for Oracle client.
2. From the SnapManager Repositories tree, right-click the host you want associated with this profile and select **Create Profile**.
3. In the Profile Configuration Information page, enter the following information and click **Next**.
  - Profile name: payroll\_prod2
  - Profile password: payroll123
  - Comment: Production Payroll database
4. In the Database Configuration Information page, enter the following information and click **Next**.
  - Database name: PAYDB
  - Database SID: payrolldb
  - Database host: Accept the default. Because you are creating a profile from a host in the repository tree, SnapManager displays the host name.



5. In the second Database Configuration Information page, accept the following database information and click **Next**:

- Host Account, representing the Oracle user account: oracle
- Host Group, representing the Oracle group: dba

6. In the Database Connection Information page, click **Use database Authentication** to allow users to authenticate using database information.

For this example, enter the following information and click **Next**.

- SYSDBA Privileged User Name, representing the system database administrator who has administrative privileges: sys
- Password (SYSDBA password): oracle
- Port to connect to database host: 1521

7. In the RMAN Configuration Information page, click **Do not use RMAN** and click **Next**.

Oracle Recovery Manager (RMAN) is an Oracle tool that helps you back up and recover Oracle databases using block-level detection.

8. In the Snapshot Naming Information page, specify a naming convention for the Snapshots associated with this profile by selecting variables. The only variable that is required is the **smid** variable, which creates a unique snapshot identifier.

For this example, do the following:

- a) In the Variable Token list, select the **{usertext}** variable and click **Add**.
- b) Enter "payroll.techco.com\_" as the host name and click **OK**.
- c) Click **Left** until the host name appears just after "smo" in the Format box.
- d) Click **Next**.

The Snapshot naming convention of *smo\_hostname\_smopprofile\_dbsid\_scope\_mode\_smid* becomes "smo\_payroll.techco.com\_payroll\_prod2\_payrolldb\_f\_a\_x" (where the "f" indicates a full backup, the "a" indicates the automatic mode, and the "x" represents the unique SMID).

9. Check **Protection Manager Protection Policy**, select the protection policy, **TechCo Payroll Data: Backup**, from the protection policies retrieved from Protection Manager, and click **Next**.

10. In the Perform Operation page, verify the information and click **Create**.

11. Click **Operation Details** to see information about the profile create operation and volume-based restore eligibility information.

- The assignment of a Protection Manager protection policy to the database profile automatically creates a nonconformant dataset, visible to the Protection Manager operator, with the name convention smo\_<hostname>\_<profilename>, or in this example: smo\_payroll.tech.com\_PAYDB.
- If the profile is not eligible for volume restore (also called "fast restore"), the following occurs:

- The Results tab indicates that the profile creation was successful and that warnings occurred during the operation.
- The Operation Details tab includes a WARNING log, which states the profile is not eligible for fast restore and explains why.

## Use Protection Manager to provision the new dataset

After the `smo_paydb` dataset is created, the storage administrator uses Protection Manager to assign storage system resources to provision the dataset's Backup node.

### Before You Begin

Before provisioning the newly created dataset, the storage administrator confers with the DBA partner for the following information:

- Name of the dataset specified in the profile  
In this case, the dataset name is `smo_payroll.tech.com_PAYDB`.

### Steps

1. Go to NetApp Management Console.
2. From the navigation pane, click **Data ► Datasets ► Overview**.

The Datasets tab of the **Datasets** window displays a list of datasets that includes the dataset that was just created through SnapManager.

3. Locate and select the **smo\_payroll.tech.com\_PAYDB** dataset.

When you select this dataset, the graph area displays the `smo_paydb` dataset with its backup node unprovisioned. Its conformance status is flagged as nonconformant.

4. With the `smo_paydb` dataset still highlighted, click **Edit**.

Protection Manager displays the **Edit Dataset** window for the **smo\_payroll.tech.com\_PAYDB** dataset. The window's navigation pane displays configuration options for the dataset's primary node, backup connection, and backup node.

5. From the navigation pane, locate the options for the dataset's backup node and select **provisioning/resource pools**.

The **Edit Dataset** window displays a setting for default provisioning policy and a list of available resource pools.

6. For this example, select the **paydb\_backup\_resource** resource pool and click >.

The selected resource pool is listed in the "Resource Pools for this node" field.

7. Click **Finish** to save your changes.

Protection Manager automatically provisions the secondary backup node with resources from the `paydb_backup_resource` resource pool.

## Use SnapManager for Oracle to create a protected backup

When creating a backup for this example, the DBA selects to create a full backup, sets backup options, and selects protection to secondary storage. Although the backup is initially made on local storage, because this backup is based on a protection-enabled profile, the backup is then transferred to secondary storage according to the protection policy's schedule as defined in Protection Manager.

### Steps

1. Go to the SnapManager for Oracle client.
2. From the SnapManager Repository tree, right-click the profile containing the database that you want to back up and select **Backup**.

The SnapManager for Oracle Backup Wizard starts.

3. Enter "Production\_payroll" as the label.
4. Enter "Production payroll Jan 19 backup" as the comment.
5. Select "Auto" as the type of backup that you want to create. This allows SnapManager to determine whether to perform an online or offline backup.
6. Select Daily or Weekly as the frequency of the backup.
7. To confirm that the backup is in a valid format for Oracle, check the box next to **Verify backup**.

This operation uses Oracle DBVerify to check the block format and structure.

8. To force the state of the database into the appropriate mode (for example, from open to mounted), check **Allow startup or shutdown of database, if necessary** and click **Next**.
9. In the Database, Tablespace or Datafiles to Backup page, select **Full Backup** and click **Next**.
10. To protect the backup on secondary storage, check **Protect the Backup** and click **Next**.
11. In the Perform Operation page, verify the information you supplied and click **Backup**.
12. In the progress page, view the progress and results of the backup creation.
13. To view the details of the operation, click **Operation Details**.

## Use SnapManager for Oracle to confirm backup protection

Using SnapManager for Oracle, you can view a list of backups associated with a profile, determine whether the backups were enabled for protection, and view the retention class (daily or weekly, in this example).

### Considerations

At first, the new backup in this example shows as scheduled for protection, but not yet protected (in the SnapManager graphical user interface and in the `backup show` command output). After the storage administrator ensures that the backup has been copied to secondary storage, SnapManager changes the backup protection state from "Not protected" to "Protected" in both the graphical user interface and with the `backup list` command.

### Steps

1. Go to the SnapManager for Oracle client.
2. In the SnapManager Repository tree, expand the profile to display its backups.
3. Click the **Backups/Clones** tab.
4. In the Reports pane, select **Backup Details**.
5. Look at the Protection column and ensure that the status is "Protected."

## Use SnapManager for Oracle to restore backups from secondary storage

Administrators can restore protected backups from secondary storage and can choose how they want to copy the data back to the primary storage.

### Before You Begin

Before you attempt to restore the backup, check the properties of the backup and ensure that the backup is freed on the primary storage system and is protected on secondary storage.

### Steps

1. From the SnapManager for Oracle Repository tree, right-click backup you want to restore and select **Restore**.
2. In the Restore and Recovery Wizard Welcome page, click **Next**.
3. In the Restore Configuration Information page, click **Complete Datafile/Tablespace Restore with Control Files**.

4. Click **Allow shutdown of database if necessary**. Then, click **Next**.

SnapManager changes the database state, if necessary. For example, if the database is offline and it needs to be online, SnapManager forces it online.

5. At the Recovery Configuration Information page, click **All Logs**. Then, click **Next**.

SnapManager restores and recovers the database to the last transaction and applies all required logs.

6. In the Restore Source Location Configuration page, select the ID of the protected backup source and click **Next**.
7. In the Volume Restore Configuration Information page, click **Attempt volume restore** to attempt volume restore.

8. Click **Fallback to file-based restore**.

This allows SnapManager to use the file-based restore method if the volume restore method cannot be completed.

9. To see the eligibility checks for fast restore and information about mandatory and overridable checks, click **Preview**.

10. At the Perform Operation page, verify the information you've supplied and click **Restore**.

11. To view details about the process, click **Operation Details**.



# Troubleshooting

---

This chapter describes how to address issues you might encounter while using Protection Manager and Provisioning Manager.

## Next topics

- [\*Data ONTAP 7.2 issues impacting protection on vFiler units\*](#) on page 159
- [\*Display issue in the Diagnose OSSV Host wizard\*](#) on page 160
- [\*Viewing Windows directories with Unicode characters in their names\*](#) on page 160
- [\*Backup of directory named with non-ASCII characters fails\*](#) on page 162
- [\*Adding directory to dataset fails with error\*](#) on page 162
- [\*Temporary conformance impact of deleting volumes or qtrees\*](#) on page 162
- [\*Deleting unnecessary secondary volumes\*](#) on page 163
- [\*Message: "qtree is not the source for the snapmirror destination"\*](#) on page 164
- [\*Number of bytes of data transferred during backup is not accurate\*](#) on page 164
- [\*Using the NetApp Management Console with DataFabric Manager prior to 3.5\*](#) on page 165
- [\*Provisioning failure despite sufficient space\*](#) on page 165
- [\*SnapMirror job fails with "process was aborted" message\*](#) on page 165
- [\*Ways to investigate problems with hosts\*](#) on page 166
- [\*Locating information about the client configuration\*](#) on page 167

## Data ONTAP 7.2 issues impacting protection on vFiler units

Data ONTAP versions earlier than 7.2 do not support SnapMirror and SnapVault commands on vFiler units. To create SnapMirror and SnapVault relationships, you must use the hosting storage system. The hosting storage system is used to create SnapMirror and SnapVault relationships.

For Data ONTAP 7.2 and later, SnapMirror and SnapVault relationships can be created using vFiler units. However, the server continues using the hosting storage system to create, monitor, and manage these relationships. As a result, you might encounter the following issues:

- If the snapvault.access and snapmirror.access options on the source storage system allow access only to the destination vFiler unit, the relationship creation, scheduled backups, on-demand backups, SnapMirror updates, and SnapMirror resync from the server fail with the following error message: "Request denied by the source filer. Check access permissions on the source."  
Workaround: To allow access to the destination hosting storage system, set the snapmirror.access and snapvault.access options on the source system.

- If the `ndmpd.preferred_interfaces` option is not set on the source hosting storage system, the backups might not use the correct network interface.  
Workaround: Set the `ndmpd.preferred_interfaces` option on the source hosting storage system.
- The backups and SnapMirror updates from the server fail with the error message “Source unknown.” This issue occurs when both of the following conditions are met:
  - A relationship between two vFiler units is imported into the server by autodiscovery or added manually.
  - The destination hosting storage system is not able to contact the IP address of the source vFiler unit.

Workaround: Ensure that the host name or IP address of the source system that is used to create relationships can be reached from the destination hosting storage system.

## Display issue in the **Diagnose OSSV Host** wizard

Open Systems SnapVault and NetApp Host Agent must be installed in proper sequence for the diagnostics wizard to display all pages properly.

If the Open Systems SnapVault client is down and you open the **Diagnose OSSV Host** wizard, the Enable OSSV option should be selected. From the page containing the Enable OSSV option, clicking Next should advance you to the next page of the wizard. However, sometimes the wizard does not advance when Next is clicked. An error message might also appear, stating "Unable to find API: ossv-query-service-status."

This problem occurs when the Open Systems SnapVault plugin is not installed with the NetApp Host Agent software. To prevent this problem, install the host agent within the Open Systems SnapVault installation sequence.

If this problem does occur, reinstall Open Systems SnapVault after NetApp Host Agent has been installed.

## Viewing Windows directories with Unicode characters in their names

If you cannot see the name of a Windows directory in NetApp Management Console and you know that the directory exists, check whether the name of the directory contains any multibyte characters. You may need to configure the Open Systems SnapVault agent running on Windows to display directories with names containing multibyte characters.



## Before You Begin

Ensure that you are assigned an administrator role that enables you to log in and perform administrative actions on the host that contains the problem directory.

You must also have administrator credentials for NetApp Host Agent on the host.

The host must be running Open Systems SnapVault 2.3 or later.

## Considerations

To use this procedure, you must be running Protection Manager, be logged into NetApp Management Console, and ensure that credentials for the host are configured in the DataFabric Manager database.

If you do not have access to NetApp Management Console, see the Operations Manager online Help for information about how to stop and start Open Systems SnapVault services.

## Steps

1. From the navigation pane, click **OSSV Hosts** window.

2. Determine which host contains the problem directory.

If you want to verify which host contains the problem directory, you can view the host's path area in the lower pane of the window. You might need to expand the directory hierarchy to view all directory names.

3. From the list of Open Systems SnapVault clients, select the host that contains the problem directory.

4. Click **Stop**.

The DataFabric Manager server stops the Open Systems SnapVault agent on the selected host, which stops the backup service.

5. Log in to the host that contains the problem directory.

6. In a text editor, open the `snapvault.cfg` file. The default location of this file is `C:\Program Files\netapp\snapvault\config\snapvault.cfg`.

7. In the `snapvault.cfg` file, edit the `[NDMP:ForceUTF8Encoding]` flag to read:  
`[NDMP:ForceUTF8Encoding] value=TRUE`

8. Save your changes and exit the `snapvault.cfg` file.

9. In Protection Manager, return to the **OSSV Hosts** window and select the host on which you stopped services in Step 4.

10. Click **Start**.

DataFabric Manager starts the Open Systems SnapVault agent on the selected host, which starts the backup service according to its schedule.

## Backup of directory named with non-ASCII characters fails

If the name of a directory in a dataset contains non-ASCII characters, the licensed protection application starts a job to back it up, but the job fails, issuing the following message: source qtree does not exist.

To work around this problem, add to the dataset the nearest directory ancestor that does not contain non-ASCII characters in its path.

## Adding directory to dataset fails with error

If you try to add a directory to a dataset and the licensed protection application issues an error indicating the directory does not exist or is not suitable for backup, the problem might be that the directory resides on a file system type that is not supported by Open Systems SnapVault.

You can use Open Systems SnapVault to back up supported file system types only. For example, Open Systems SnapVault supports only NTFS on systems running Windows.

To determine which file system types are supported by the version of Open Systems SnapVault that you are using, you can run the `svinstallcheck` utility on the Open Systems SnapVault host. See the Open Systems SnapVault documentation for details.

## Temporary conformance impact of deleting volumes or qtrees

If you delete a volume or qtree that is part of a dataset without deleting the volume or qtree from the DataFabric Manager server database, the deleted object is temporarily flagged in the database as “disappeared” for up to an hour before it is marked deleted.

The licensed protection application references the DataFabric Manager server database regarding objects used in protection implementations. Until a deleted object is marked as deleted in the database, the protection application attempts to create relationships for it, as specified in the policy applied to its dataset, generating conformance error messages. After a deleted object is marked as deleted in the database, the protection application no longer attempts to create relationships for it, and the conformance error messages are no longer generated.

To stop the conformance error messages, you can manually delete the volume or qtree from the DataFabric Manager server database. Alternatively, you can wait up to an hour for the DataFabric Manager server to mark the “disappeared” object as deleted, and the conformance error messages are no longer generated.

## Deleting unnecessary secondary volumes

You can search for and delete secondary volumes created by Protection Manager that used to contain backups but are now empty and no longer needed.

### Before You Begin

Ensure that you are assigned an administrator role that enables you to create and delete volumes.

### Considerations

Empty secondary volumes can occur when the aggregate containing the volume is low on available space and the licensed protection application creates a new secondary volume on another aggregate, then migrates the backup relationships to the new volume. The previous secondary volume is not deleted and still contains valid backups, but the backups expire according to their retention settings. After the backups expire, the previous secondary volume is not needed and can be deleted without impacting your data protection.

To perform this procedure, you must be running Protection Manager and be logged into the NetApp Management Console.

### Steps

1. In the management console, create a group composed of the datasets whose secondary volumes you want to review.

Since datasets can belong to more than one group, it can be more efficient to manage the secondary volumes by creating a group of the datasets you want to review.

2. Go to the Operations Manager user interface and, in the Group area, select the dataset group that you created in Step 1.

3. Select **Member Details** ► **File Systems**, then choose Volume Snapshot Counts from the View drop-down menu.

The Volume Snapshot Counts view displays the volumes that belong to datasets in the group and the current number of Snapshot copies each volume contains. The names of secondary volumes created by the protection application include a `dfpm_` prefix.

4. Evaluate which of the secondary volumes created by the protection application are volumes that you no longer need.

If a volume has a low number of Snapshot copies and a name prefixed by `dfpm_`, it might be a secondary volume you no longer need. To investigate, check the Snapshots area of the Volume Details page for the volume. The Snapshots area lists the Snapshot copies and the time that each copy was last accessed.

**Note:** The protection application keeps the last two successful backups, regardless of their retention settings. If backup relationships were migrated to a new secondary volume, it is unlikely that the last two successful backups are contained by the previous secondary volume. However, if you create an on-demand backup and there are no scheduled backups of the same retention type (for example, if you create an on-demand Monthly backup but there are no Monthly backups scheduled), the on-demand backup might be retained on the previous secondary volume as one of the last two successful backups.

5. After you identify the secondary volumes you no longer need, you can delete them as you normally would, without negatively impacting your data protection implementation.

For information about deleting volumes, see the Operations Manager online Help.

## Message: “qtree is not the source for the snapmirror destination”

If the licensed protection application generates the error message the qtree is not the source for the snapmirror destination, there are three possible causes:

- The SnapVault relationship was released manually from the source node.
- The base Snapshot copy was deleted manually from the source node.
- The source qtree for which the relationship was originally created was deleted and later re-created with the same name.

## Number of bytes of data transferred during backup is not accurate

When monitoring a backup job, the number of bytes of data transferred during the job does not match the number of bytes displayed in the **Jobs** window.

This is expected behavior. The number of bytes transferred is an approximation and does not reflect an exact count; it is always less than the actual number of bytes transferred. For jobs that take a short time to complete, the licensed protection application might report a data transfer size of zero.

## Using the NetApp Management Console with DataFabric Manager prior to 3.5

If you are using the NetApp Management Console and want to switch to an instance of NetApp Management Console earlier than version 3.5, you select Exit from the File menu, not Log Out.

The NetApp Management Console is backward compatible with versions of DataFabric Manager prior to 3.5. However, you must exit and restart the console to use a version of DataFabric Manager prior to 3.5.

## Provisioning failure despite sufficient space

An overcommitment threshold set for the DataFabric Manager server can impact the provisioning of flexible volumes in the resource pool.

The DataFabric Manager server allows you to set a `NearlyOvercommittedThreshold` parameter that reserves space on your system for projected future use. If this threshold is set too low, you can encounter problems provisioning volumes on destination storage systems. When such provisioning problems occur, you might see an inconsistency in which the dry run result reports insufficient space when the reported space available for the destination aggregate appears to be sufficient.

To resolve this problem, increase the `Nearly Overcommitted Threshold` in the DataFabric Manager server. By default, the `aggrNearlyOvercommittedThreshold` value is set to 95%. Increasing this value causes the DataFabric Manager server to allocate more storage in an aggregate before reporting it as full. Setting this value over 100% could result in an out of space condition. Note that other factors, such as Snapshot copy retention settings or resizing primary volumes, can also result in an out of space condition.

## SnapMirror job fails with "process was aborted" message

Problems on the data source node can prevent the licensed protection application from creating a mirror relationship, even though a preview of your dataset configuration detected no configuration problems. When the problem is with the data source node itself, the job that would have created the mirror relationship fails and the licensed protection application issues the message: `process was aborted`.

Problems with a data source node that can prevent the creation of a mirror relationship include the following:

- The maximum number of Snapshot copies that can be created on the source node has been reached, so no new Snapshot copies can be created.
- The Snapshot copy on the source node is locked, possibly by another operation.

You can find additional information about problems preventing the creation of a mirror relationship by checking two files on the SnapMirror destination node:

- /vol/vol0/etc/logs/snapmirror
- /vol/vol0/etc/logs/messages

## Ways to investigate problems with hosts

If you are investigating a policy failure, you can use the information displayed in the Hosts windows to determine whether the cause is a problem with a host. This information can also help determine the potential impact of any changes you might make to a host.

Most problems you might encounter with a host can be diagnosed and corrected by using the host diagnostics wizards. The diagnostics wizards are located on the **Storage Systems Hosts** window and the **OSSV Hosts** window. The wizards include steps to help you locate and fix issues with hosts. You can also use the Edit hosts property sheets to make changes to host licenses and host and NDMP credentials. You can access each of the wizards and property sheets in the following windows of the interface.

### **Storage Systems Hosts window**

Provides information about storage systems that can help you verify whether a host is up and accepting the NDMP credentials specified for it, as well as whether the appropriate licenses are assigned to it.

Allows you to review path and relationship information about storage systems, as well as to check host and NDMP status. The path and relationship information displayed for each individually selected storage system helps you see the interdependencies between hosts. For example, by reviewing the data flowing into and out of a selected storage system, you can evaluate the impact of temporarily removing that storage system from service for maintenance. You can also review information about input and output relationships to determine whether lag times are within specified thresholds and which datasets are impacted if the lag threshold has been or is about to be exceeded.

From this window, you can start the **Add Storage System** wizard and the **Diagnose Storage Systems** wizard, or you can open the Edit property sheet for storage systems. You can also refresh the information about a selected host in the window's host list.

### **vFiler Units window**

Allows you to review the status of vFiler units and to verify the IP address of the vFiler unit and the name of the storage system that is hosting it.

Allows you to review path and relationship information about vFiler units. The path and relationship information displayed for each individually selected vFiler unit helps you see the interdependencies between hosts and datasets. For example, by reviewing the data flowing into and out of a selected host, you can evaluate the impact of temporarily removing that host from service for maintenance.

From this window, you can start the Add vFiler Unit wizard or the Setup vFiler Unit wizard, and you can delete vFiler units.

### **OSSV Hosts window**

Allows you to review the status of Open Systems SnapVault hosts (including VMware ESX hosts) the port and credentials status of each NetApp Host Agent, and the status of NDMP connections and credentials.

Allows you to investigate problems with an Open Systems SnapVault client. Information in this window includes the host and NDMP status, the NDMP credentials status, the operating system and version each host is running, and path information for each host.

From this window, you can start the **Add OSSV Host** wizard and the **Diagnose OSSV Host** wizard, and open the Edit OSSV host property sheet for a host containing an Open Systems SnapVault agent.

From this window, you can also stop and start an Open Systems SnapVault 2.3 and later agent on which NetApp Host Agent is installed. Stopping and starting the agent stops and starts backup service on the selected client, which might resolve the problem. After you restart the backup service, you can click **Refresh** to display current data for the selected client and determine the effect of restarting the backup service.

**Note:** There is no Open Systems SnapVault plugin for Solaris, so the NetApp Host Agent can not talk to the Open Systems SnapVault agent. Therefore, the Host Agent Status displays as Not Detected and management tasks such as start and stop of the Open Systems SnapVault agent can not be performed from the management console.

## **Locating information about the client configuration**

Occasionally, you might want to locate the client configurations that are running on NetApp Management Console. This type of information is useful when troubleshooting problems or preparing to install software upgrades.

The About dialog box is accessed from the Help menu in the management console. This dialog box includes a Configuration button and a Licenses button. Click **Configuration** to get more information about the configuration of the client running NetApp Management Console, including:

- NetApp Management Console installation directory
- Operating system architecture, name and version
- Java version and associated memory
- DataFabric Manager version, serial number, host name, installation directory, and so forth.

Click **Licenses** to get a list of the data management applications installed on your system: Protection Manager, Disaster Recovery, or Provisioning Manager.





# NetApp Management Console

---

This chapter describes what NetApp Management Console is, the applications that run in the console, the console layout and navigational features, how to customize the console window, how to filter data displayed in the console, and how to download and install the console.

## Next topics

[What NetApp Management Console is](#) on page 169

[Applications that run in NetApp Management Console](#) on page 170

[NetApp Management Console window layout and navigation](#) on page 171

[NetApp Management Console window customization](#) on page 172

[NetApp Management Console data filtering](#) on page 173

[Printing Help topics](#) on page 174

## What NetApp Management Console is

NetApp Management Console is the client platform for NetApp Manageability Software applications. NetApp Management Console is used by administrators to carry out management tasks aided by DataFabric Manager, but it runs on a Windows or Linux system separate from the server on which DataFabric Manager is installed.

NetApp Management Console allows storage, application, and server administrators to perform management tasks such as data backup protection, space management, resource provisioning, data migration, and performance tuning, without having to switch between separate user interfaces.

The DataFabric Manager server provides infrastructure services (such as discovery, monitoring, role-based access control (RBAC), auditing, and logging for products in the storage and data suites) for NetApp Manageability Software client applications. The DataFabric Manager software runs on a separate server and is managed itself through Operations Manager, the Web-based user interface of DataFabric Manager. For more information about DataFabric Manager and Operations Manager, see the *Operations Manager Administration Guide*.

## Related information

[Operations Manager Administration Guide -](#)

[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)

## Applications that run in NetApp Management Console

The Performance Advisor and the licensed Protection Manager and Provisioning Manager applications run in NetApp Management Console.

**Performance Advisor** This application provides a single location from which you can view comprehensive information about storage system and MultiStore vFiler unit performance and perform short-trend analysis. This application also helps you identify in the data infrastructure causes and potential causes of reduced performance.

Performance Advisor is automatically enabled with the Operations Manager Core license. For more information, see the *Performance Advisor Administration Guide*.

**Protection Manager** This application provides a policy-based management tool to help you unify and automate backup and mirroring operations. The application uses a holistic approach to data protection. It provides end-to-end, workflow-based design and seamless integration of SnapVault, SnapMirror, and Open Systems SnapVault to enable you to manage large-scale deployments easily.

The disaster recovery feature of the licensed protection application enhances your data protection services by enabling you to continue to provide data access to your users, even in the event of mishap or disaster that disables or destroys the storage systems in your primary node. If disaster recovery protection is installed, you can quickly enable your secondary storage systems to provide primary data storage access to your users with little or no interruption, until your primary storage systems are reenabled or replaced.

To enable the protection features, you must purchase the protection license and install it on DataFabric Manager server. The disaster recovery feature is a licensed option for the Protection Manager.

**Provisioning Manager** This application helps you simplify and automate the tasks of provisioning and managing storage. The application provides policy-based provisioning and conformance of storage in datasets. The application also enables you to manually add volumes or qtrees to a dataset at any time, provides manual controls for space and capacity management of existing storage and newly provisioned storage, and allows you to migrate datasets offline to a new storage destination.

To enable the provisioning features, you must purchase the provisioning license and install it on DataFabric Manager server.

### Related information

*Performance Advisor Administration Guide -*  
[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)

## NetApp Management Console window layout and navigation

You can navigate NetApp Management Console to move within and between applications, to display Help, and to log out of the console.

### Learning about Protection Manager

The Get Started section of the user interface provides an overview of Protection Manager, a short tutorial that demonstrates how to set up protection, and a list of frequently asked questions (FAQs).

### Learning about disaster recovery

The Get Started section of the user interface provides an overview of disaster recovery, a short tutorial that demonstrates how to set up disaster recovery, and a list of frequently asked questions (FAQs).



### Learning about Provisioning Manager

The Get Started section of the user interface provides an overview of Provisioning Manager, a short tutorial that demonstrates how to set up provisioning, and a list of frequently asked questions (FAQs).

### Moving back and forth between panes


The Back and Forward arrow buttons toggle between your last and previous panes, even if the pane was in a different application.

### Toggling between applications

- To use Protection Manager or Provisioning Manager, select **Tasks** ➤ **Manage Data** or go to the Tasks Bar and click .
- To use Performance Advisor, select **Tasks** ➤ **Manage Performance** or go to the Tasks Bar and click .

The Tasks menu enables you to select and toggle between applications running in NetApp Management Console. To use Protection Manager or Provisioning Manager, select the Manage Data option. To use Performance Advisor, select the Manage Performance option. You can also go to the Tasks Bar and click the icon of the application you want to view.

### Displaying help


- To display the Help for all applications on NetApp Management Console, click **Help** ➤ **Help Contents**.
- To display Help for the specific window that is currently displayed, click **Help** ➤ **Help For This View** or click .

### Logging out

- To log out, select **File** ➤ **Log Out** or click the logout button.
- To log out and close NetApp Management Console, select **File** ➤ **Exit**.

**Viewing product license information** To view information about the product licenses you have installed, click **Help ► About ► Licenses**. Removed or added licenses are reflected in the license list after you restart NetApp Management Console.

Applications that run in NetApp Management Console vary in the specifics of their window layout. However, the windows are generally divided into two panes:

- Use the navigation pane on the left to move within an application.
- Use the content pane on the right to view and manage data. The content pane is generally divided into two areas: lists of selectable data and details of the selected data. Click , when it is displayed, for additional details.


**Note:** Specific applications might have additional navigation features not described in this section. In addition, software version incompatibility could result in some reduced functionality, causing some menu options or buttons to be disabled.

## NetApp Management Console window customization

NetApp Management Console includes features you can use to customize the application window layout. By customizing application windows, you can control which data is viewable or how it is displayed.


**Note:** Not all customization features are available for every application window.

**Hiding or redisplaying the Tasks Bar** You can hide the Tasks Bar to increase the space available for the content pane. (The overall width of the window remains the same when the bar is hidden.) You use the View menu to hide or display the bar.

**Selecting columns to display** In content panes that include a list divided into columns, you can choose which columns you want to display. To display or hide a column, click the column-selection icon in the upper-right corner above the scroll bar () , then click the name of a column heading from the selection list. Columns already displayed are identified with a check mark.

**Note:** The default version of a list does not necessarily include all available columns. You might find additional columns available in the column selection list.

**Readjusting column widths** In content panes that include a list divided into columns, you can adjust the width of individual columns by horizontally dragging the vertical line between column headings. If accommodating all the columns you want to include results in column widths that obscure data, you can still see the entire value of a column field by putting your cursor over the field. A tool tip pops up, displaying the entire value of the field. You can maximize data visibility

across all columns by going to the column selection icon () and choosing Pack All Columns.


- Rearranging column order** In content panes that include a list divided into columns, you can rearrange the column order for a session by dragging and dropping column headings horizontally within the table. The arrangement persists until you exit the console.
- Reapportioning a content pane** A splitter bar divides a content pane list area from its details area. You can move the splitter bar to increase or decrease the proportion of the content pane that displays the list of selectable data.

## NetApp Management Console data filtering

You can use data filtering features to display only data meeting the criteria you specify.


In large-scale environments, the content pane might list so much data that it becomes difficult to locate the information you want. Filtering the data by specified criteria helps you focus on the issues most important to you.


**Note:** Not all filtering features are available for every application window.

- Filtering by group** The Group selection list in the toolbar enables you to display only the data that pertains to objects in a selected group. This setting persists until you log out or choose a different group.
- Filtering by regular expression** You can filter columns displaying site-specific values, such as storage system names or dataset names, by regular expression. To filter a column by regular expression, click the filter icon in the column heading () and specify the regular expression to match against values in the column field. Headings of filtered columns are highlighted to remind you that some data is not currently displayed.

The NetApp Management Console uses Java regular expression syntax for filtering data, as shown in the following examples:

- To view only items beginning with the letters "sch," type **sch** in the filter field, which matches Schedule but not SnapMirror.
- To view only items containing "space" somewhere in their string, type **.\*space** in the filter field, which matches strings such as Volume Space Normal.
- To view only items ending with the string "ok," type **\*ok** in the filter field, which matches strings such as SnapMirror: Date Ok.

**Filtering by column values** When a column displays a set of predefined possible values, you can choose to display only the rows of data that include a selected value. To filter a column by a specific, predefined value, click the filter icon in the column heading (  ) and select the predefined value from the drop-down list. Headings of filtered columns are highlighted to remind you that some data is not currently displayed.

**Filtering by column view** You can click  in the upper-right corner of the list to select which columns you want displayed.

**Sorting by column values** You can click on the column header to change the sort order of the column entries. When you click the column header, the sort arrow appears for that column.

## Printing Help topics

You can print one or more topics from the online Help.

### Before You Begin

You must have the online Help displayed.

### Steps

1. In the online Help Table of Contents, select the topic or topics you want to print.

To print a single topic, select the topic.

To print multiple topics, use the **Shift** key to select multiple topics in a sequence. You can also use the **Ctrl** key to select multiple topics that are not in a sequence.

**Note:** Selecting a Table of Contents heading does not automatically select all the topics under that heading.

2. Click the print icon above the Help Table of Contents.

The print range in the Print dialog box indicates the number of print pages required for the selected topic or topics.

**Note:** For online Help, there is no distinction between the All and Pages options; both options print only the selected topic or topics.

# Administrator roles and capabilities

---

The administrator roles determine the tasks you can perform using applications in NetApp Management Console.

## Default and custom roles

One or more capabilities must be specified for every role, and you can assign multiple capabilities if you want the administrator to have more control than a specific role provides. For example, if you want an administrator to perform both the backup and restore operations, you must assign Back Up and Restore roles to the administrator.

The DataFabric Manager server and the client applications provide a set of default global roles described in the following list. You can customize these roles and the capabilities associated with them and you can create new ones using the Operations Manager Web-based user interface. For more information about configuring role-based access control (RBAC), see the *Operations Manager Administration Guide*.

<b>GlobalBackup</b>	You can initiate a backup to any secondary volume and ignore discovered hosts.
<b>GlobalDataProtection</b>	You can initiate a backup to any secondary volume; view backup configurations, events and alerts, and replication or failover policies; and import relationships into datasets.
<b>GlobalDataSet</b>	You can create, modify, and delete datasets.
<b>GlobalDelete</b>	You can delete information in the DataFabric Manager server database, including groups and members of a group, monitored objects, custom views, primary and secondary storage systems, and backup relationships, schedules, and retention policies.
<b>GlobalEvent</b>	You can view, acknowledge, and delete events and alerts.
<b>GlobalFullControl</b>	You can view and perform any operation on any object in the DataFabric Manager server database and configure administrator accounts. You cannot apply this role to accounts with group access control.
<b>GlobalMirror</b>	You can create, destroy, and can update replication or failover policies.
<b>GlobalRead</b>	You can view the DataFabric Manager server database, backup and provisioning configurations, events and alerts, performance data, and policies.
<b>GlobalRestore</b>	You can restore the primary data back to a point in time or restore to a new location.
<b>GlobalWrite</b>	You can view or write to the DataFabric Manager server database.

- GlobalResourceControl** You can add members to dataset nodes that are configured with provisioning policies.
- GlobalProvisioning** You can provision primary dataset nodes and can attach resource pools to secondary or tertiary dataset nodes. The GlobalProvisioning roles also includes all the capabilities of the GlobalResourceControl, GlobalRead, and GlobalDataset roles for dataset nodes that are configured with provisioning policies.
- GlobalPerfManagement** You can manage views, event thresholds, and alarms apart from viewing performance information in Performance Advisor.

**Related information**

*Operations Manager Administration Guide -*  
[http://now.netapp.com/NOW/knowledge/docs/DFM\\_win/dfm\\_index.shtml](http://now.netapp.com/NOW/knowledge/docs/DFM_win/dfm_index.shtml)



# List of events

---

These tables list events generated by Protection Manager, Provisioning Manager, and Operations Manager and the associated event severity types. Events are listed in alphabetical order by object type.

**Note:** Performance Advisor uses only the Normal and Error events.

## List of events

### Active/Active Configuration Controller

Event name	Severity
Can Take Over	Normal
Cannot Takeover	Error
Dead	Critical
Takeover	Warning

### Active/Active Configuration Interconnect

Event name	Severity
Down	Error
Not Present	Warning
Partial Failure	Error
Up	Normal

### Active/Active Configuration Partner

Event name	Severity
Dead	Warning
May Be Down	Warning
OK	Normal

### Active/Active Configuration Settings

Event name	Severity
Disabled	Normal
Enabled	Normal

Event name	Severity
Not Configured	Normal
Takeover Disabled	Normal
This Controller Dead	Warning

#### Agent

Event name	Severity
Down	Error
Login Failed	Warning
Login OK	Normal
Up	Normal

#### Aggregate

Event name	Severity
Almost Full	Warning
Almost Overcommitted	Warning
Deleted	Information
Discovered	Information
Failed	Error
Full	Error
Nearly Over Deduplicated	Warning
Not Over Deduplicated	Normal
Not Overcommitted	Normal
Offline	Error
Online	Normal
Overcommitted	Error
Over Deduplicated	Error
Restricted	Normal
Snapshot Reserve Almost Full	Warning
Snapshot Reserve Full	Warning

Event name	Severity
Snapshot Reserve OK	Normal
Space Normal	Normal

**Alarm**

Event name	Severity
Created	Information
Deleted	Information
Modified	Information

**CFO Interconnect**

Event name	Severity
Down	Error
Not Present	Warning
Partial Failure	Error
Up	Normal

**CFO Partner**

Event name	Severity
Dead	Warning
May Be Down	Warning
OK	Normal

**CFO Settings**

Event name	Severity
Disabled	Normal
Enabled	Normal
Not Configured	Normal
Takeover Disabled	Normal
This Node Dead	Warning

**CFO This Storage System**

Event name	Severity
Can Take Over	Normal
Cannot Take Over	Error
Dead	Critical
Takeover	Warning

#### **Configuration Changed**

Event name	Severity
Config Group	Information

#### **CPU**

Event name	Severity
Load Normal	Normal
Too Busy	Warning

#### **Data Protection**

Event name	Severity
Job Started	Information
Policy Created	Information
Policy Modified	Information
Schedule Created	Information
Schedule Modified	Information

#### **Database**

Event name	Severity
Backup Failed	Error
Backup Succeeded	Information
Restore Failed	Error
Restore Succeeded	Information

#### **Dataset**

Event name	Severity
Backup Aborted	Warning
Backup Completed	Normal
Backup Failed	Error
Created	Information
Deleted	Information
DR State Ready	Information
DR State Failover Over	Warning
DR State Failed Over	Information
DR State Failover Error	Error
DR Status Normal	Information
DR Status Warning	Warning
DR Status Error	Error
Initializing	Information
Job Failure	Warning
Member Clone Snapshot Discovered	Information
Member Clone Snapshot Status OK	Information
Member Dedupe Operation Failed	Error
Member Dedupe Operation Succeeded	Warning
Member Destroyed	Information
Member Destroy Operation Failed	Information
Member Resized	Information
Member Resize Operation Failed	Information
Modified	Information
Protected	Normal
Protection Failed	Error
Protection Lag Error	Error
Protection Lag Warning	Warning
Protection Suspended	Warning

Event name	Severity
Protection Uninitialized	Normal
Provisioning Failed	Error
Provisioning OK	Normal
Space Status: Normal	Normal
Space Status: Warning	Warning
Space Status: Error	Error
Write Guarantee Check - Member Resize Required	Warning
Write Guarantee Check - Member Size OK	Normal

#### Dataset Conformance

Event name	Severity
Conformant	Normal
Conforming	Information
Initializing	Information
Nonconformant	Warning

#### Disks

Event name	Severity
No Spares	Warning
None Failed	Normal
None Reconstructing	Normal
Some Failed	Error
Some Reconstructing	Warning
Spares Available	Normal

#### Enclosures

Event name	Severity
Active	Information
Disappeared	Warning

Event name	Severity
Failed	Error
Found	Normal
Inactive	Warning
OK	Normal

**Fans**

Event name	Severity
Many Failed	Error
Normal	Normal
One Failed	Error

**FC (Fibre Channel) Switch Port**

Event name	Severity
Faulty	Error
Offline	Warning
Online	Normal

**Filer Configuration**

Event name	Severity
Changed	Warning
OK	Normal
Push Error	Warning
Push OK	Normal

**Global Status**

Event name	Severity
Critical	Critical
Non Critical	Error
Non Recoverable	Emergency
OK	Normal

Event name	Severity
Other	Warning
Unknown	Warning

#### HBA Port

Event name	Severity
Offline	Warning
Online	Normal
Port Error	Error
Traffic High	Warning
Traffic OK	Normal

#### Host

Event name	Severity
Cluster Configuration Error	Error
Cluster Configuration OK	Normal
Cold Start	Information
Deleted	Information
Discovered	Information
Down	Critical
Identity Conflict	Warning
Identity OK	Normal
Login Failed	Warning
Login OK	Normal
Modified	Information
Name Changed	Information
SNMP Not Responding	Warning
SNMP OK	Normal
System ID Changed	Information
Up	Normal



**Host Agent**

Event name	Severity
Down	Error
Up	Normal
Host Agent: Login Failed	Warning

**Inodes**

Event name	Severity
Almost Full	Warning
Full	Error
Utilization Normal	Normal

**Interface Status**

Event name	Severity
Down	Error
Testing	Normal
Unknown	Normal
Up	Normal

**LUN**

Event name	Severity
Offline	Warning
Online	Normal
Snapshot Not Possible	Warning
Snapshot Possible	Normal

**Management Station**

Event name	Severity
Enough Free Space	Normal
File System File Size Limit Reached	Error
License Expired	Error

Event name	Severity
License Nearly Expired	Warning
License Not Expired	Normal
Load OK	Normal
Load Too High	Warning
Node Limit Nearly Reached	Warning
Node Limit OK	Normal
Node Limit Reached	Error
Not Enough Free Space	Error
Provisioning Manager Node Limit Nearly Reached	Warning
Provisioning Manager Node Limit Ok	Normal
Provisioning Manager Node Limit Reached	Error
Protection Manager Node Limit Nearly Reached	Warning
Protection Manager Node Limit Ok	Normal
Protection Manager Node Limit Reached	Error

## Migration

Event name	Severity
Dataset Not Migrating	Normal
Dataset Migrating	Normal
Dataset Migrated With Errors	Warning
Dataset Migrated	Normal
Dataset Migrate Failed	Error
vFiler Unit Not Migrating	Normal
vFiler Unit Migrating	Normal
vFiler Unit Migrated With Errors	Warning
vFiler Unit Migrated	Normal
vFiler Unit Migrate Failed	Error

## NDMP

Event name	Severity
Credentials Authentication Failed	Warning
Credentials Authentication Succeeded	Normal
Communication Initialization Failed	Warning
Communication Initialization Succeeded	Normal
Down	Warning
Up	Normal

**Network**

Event name	Severity
OK	Normal
Too Large	Warning

**Network Services**

Event name	Severity
CIFS Service - Up	Normal
CIFS Service - Down	Warning
NFS Service - Up	Normal
NFS Service - Down	Warning
iSCSI Service - Up	Normal
iSCSI Service - Down	Warning
FCP Service - Up	Normal
FCP Service - Down	Warning

**No Schedule Conflict**

Event name	Severity
Between Snapshot and SnapMirror Schedules	Normal
Between Snapshot and SnapVault Schedules	Normal

**NVRAM Battery**

Event name	Severity
Discharged	Error
Fully Charged	Normal
Low	Warning
Missing	Error
Normal	Normal
Old	Warning
Overcharged	Warning
Replace	Error
Unknown Status	Warning

#### OSSV (Open Systems SnapVault)

Event name	Severity
Host Discovered	Information

#### Performance Advisor

Event name	Severity
Enough Free Space	Normal
Not Enough Free Space	Error

#### Power Supplies

Event name	Severity
Many Failed	Error
Normal	Normal
One Failed	Error

#### Primary

Event name	Severity
Host Discovered	Information

#### Protection Policy

Event name	Severity
Created	Information
Deleted	Information
Modified	Information

**Protection Schedule**

Event name	Severity
Created	Information
Deleted	Information
Modified	Information

**Provisioning Policy**

Event name	Severity
Created	Information
Deleted	Information
Modified	Information

**Qtree**

Event name	Severity
Almost Full	Warning
Files Almost Full	Warning
Files Full	Error
Files Utilization Normal	Normal
Full	Error
Growth Rate Abnormal	Warning
Growth Rate OK	Information
Space Normal	Normal

**Remote Platform Management (RPM)**

Event name	Severity
Online	Normal

Event name	Severity
Unavailable	Critical

#### Resource Group

Event name	Severity
Created	Information
Deleted	Information
Modified	Information

#### Resource Pool

Event name	Severity
Created	Information
Deleted	Information
Modified	Information
Space Full	Error
Space Nearly Full	Warning
Space OK	Normal

#### SAN Host LUN Mapping

Event name	Severity
Changed	Warning

#### Script

Event name	Severity
Critical Event	Critical
Emergency Event	Emergency
Error Event	Error
Information Event	Information
Normal Event	Normal
Warning Event	Warning

#### SnapMirror

Event name	Severity
Abort Completed	Normal
Abort Failed	Error
Break Completed	Normal
Break Failed	Error
Date OK	Normal
Delete Aborted	Warning
Delete Completed	Information
Delete Failed	Error
Initialize Aborted	Warning
Initialize Completed	Normal
Initialize Failed	Error
Nearly Out of Date	Warning
Not Scheduled	Normal
Not Working	Error
Off	Normal
Out of Date	Error
Possible Problem	Warning
Quiesce Aborted	Warning
Quiesce Completed	Normal
Quiesce Failed	Error
Resume Completed	Normal
Resume Failed	Error
Resync Aborted	Warning
Resync Completed	Normal
Resync Failed	Error
Unknown State	Warning
Update Aborted	Warning
Update Completed	Normal

Event name	Severity
Update Failed	Error
Working	Normal

### Snapshot(s)

Event name	Severity
Age Normal	Normal
Age Too Old	Warning
Count Normal	Normal
Count OK	Normal
Count Too Many	Error
Created	Normal
Failed	Error
Full	Warning
Schedule Conflicts with the SnapMirror Schedule	Warning
Schedule Conflicts with the SnapVault Schedule	Warning
Schedule Modified	Information
Scheduled Snapshots Disabled	Warning
Scheduled Snapshots Enabled	Normal

### SnapVault

Event name	Severity
Backup Aborted	Warning
Backup Completed	Information
Backup Failed	Error
Host Discovered	Information
Relationship Create Aborted	Warning
Relationship Create Completed	Information
Relationship Create Failed	Error
Relationship Delete Aborted	Warning



Event name	Severity
Relationship Delete Completed	Information
Relationship Delete Failed	Error
Relationship Discovered	Information
Relationship Modified	Information
Replica Date OK	Normal
Replica Nearly Out of Date	Warning
Replica Out of Date	Error
Restore Aborted	Warning
Restore Completed	Normal
Restore Failed	Error

**SNMP Trap Listener**

Event name	Severity
Alert Trap Received	Information
Critical Trap Received	Information
Emergency Trap Received	Information
Error Trap Received	Information
Information Trap Received	Information
Notification Trap Received	Information
Warning Trap Received	Information
Start Failed	Warning
Start OK	Information

**Sync**

Event name	Severity
SnapMirror In Sync	Information
SnapMirror Out of Sync	Warning

**Temperature**

Event name	Severity
Hot	Critical
Normal	Normal

#### Unprotected Item

Event name	Severity
Discovered	Information

#### User

Event name	Severity
Disk Space Quota Almost Full	Warning
Disk Space Quota Full	Error
Disk Space Quota OK	Normal
Disk Space Soft Limit Exceeded	Warning
Disk Space Soft Limit Not Exceeded	Normal
E-mail Address OK	Normal
E-mail Address Rejected	Warning
Files Quota Almost Full	Warning
Files Quota Full	Error
Files Quota Utilization Normal	Normal
Files Soft Limit Exceeded	Warning
Files Soft Limit Not Exceeded	Normal

#### vFiler Unit

Event name	Severity
Deleted	Information
Discovered	Information
Hosting Storage System Login Failed	Warning
IP Address Added	Information
IP Address Removed	Information

Event name	Severity
Renamed	Information
Storage Unit Added	Information
Storage Unit Removed	Information

**vFiler Unit Template**

Event name	Severity
Created	Information
Deleted	Information
Modified	Information

**Volume**

Event name	Severity
Almost Full	Warning
Automatically Deleted	Information
Autosized	Information
Clone Deleted	Information
Clone Discovered	Information
Destroyed	Information
First Snapshot OK	Normal
Full	Error
Growth Rate Abnormal	Warning
Growth Rate OK	Normal
Maxdirsize Limit Nearly Reached	Information
Maxdirsize Limit Reached	Information
Nearly No Space for First Snapshot	Warning
Nearly Over Deduplicated	Warning
New Snapshot	Normal
Next Snapshot Not Possible	Warning
Next Snapshot Possible	Normal

Event name	Severity
No Space for First Snapshot	Warning
Not Over Deduplicated	Normal
Offline	Warning
Offline or Destroyed	Warning
Online	Normal
Over Deduplicated	Error
Quota Overcommitted	Error
Quota Almost Overcommitted	Warning
Restricted	Restricted
Snapshot Automatically Deleted	Information
Snapshot Deleted	Normal
Space Normal	Normal
Space Reserve Depleted	Error
Space Reservation Nearly Depleted	Error
Space Reservation OK	Normal

# Index

## A

administrator roles, list of [175](#)  
 aggregate overcommitment, defined [42](#)

## B

backups  
     multiple-to-single volume feature described [25](#)

## C

CLI commands, new and changed [31](#)  
 client platforms [169](#)  
 console  
     applications supported [170](#)  
     customizing [172](#)  
     using [171](#)  
 credentials, defined [43](#)  
 custom name prefix feature described [22](#)

## D

dashboards [48](#)  
 data management  
     change implementation [47](#)  
     concepts [40](#)  
     discovering data [45](#)  
     simplifying [44](#)  
     using datasets [45](#)  
 data transfer enhancements described [26](#)  
 DataFabric Manager clients [169](#)  
 dataset migration example  
     adding physical resources [74](#)  
     assumptions [73](#)  
     cleaning up the migration [78](#)  
     cutting over to new storage system [77](#)  
     manually deleting the old IPspace and VLAN [78](#)  
     setup [71](#)  
     starting the migration [75](#)  
     strategy [72](#)  
     updating SnapMirror relationships [76](#)  
 dataset migration feature described [22](#)

datasets  
     configuring for disaster recovery [51](#)  
     defined [41](#)  
     how to use [45](#)  
     migration overview [46](#)  
 deduplication  
     defined [52](#)  
     feature described [22](#)  
     process overview [53](#)  
 disaster recovery  
     configuring datasets for [51](#)  
     defined [49](#)  
     policies, defined [41](#)  
     terminology [49](#)  
 disaster recovery example  
     assign protection policy [133](#)  
     configuration assumptions [123](#)  
     configure hosts [125](#)  
     create dataset [131](#)  
     create failover script [127](#)  
     create protection policy [129](#)  
     create resource pools [126](#)  
     fail over [136](#)  
     failback manually [138](#)  
     perform unscheduled update [135](#)  
     prepare for recovery [137](#)  
     setup [121](#)  
     strategy [122](#)  
     test failover script [134](#)  
     verify disaster recovery protection [134](#)  
 dpDynamicSecondarySizing option [23](#)  
 dpMaxFanInRatio option [25](#)  
 dpReaperCleanupMode option [24](#)  
 dpReBaselineMode option [24](#)  
 dynamic secondary volume sizing feature described [23](#)

## E

events, complete list of [177](#)  
 events, new and changed [35](#)  
 export protocols  
     member-level settings [25](#)

## F

- failback
  - defined [49](#)
- failover
  - defined [49](#)
  - readiness, defined [49](#)
  - script, defined [49](#)
  - state, defined [49](#)

## G

- Get Started feature [171](#)

## H

- Help
  - accessing [171](#)
  - printing topics [174](#)
- host profiles, creating [152](#)
- hosts, investigating problems [166](#)

## I

- installation enhancements described [29](#)

## L

- licenses for NetApp Management Console applications [170](#)
- licensing enhancements described [28](#)
- limitations on protection and provisioning [36](#)
- logging out [171](#)

## M

- member-level export settings feature described [25](#)
- migration
  - overview [46](#)
  - See dataset migration example [71](#)
- monitoring
  - dashboards [48](#)
  - status [48](#)
- multiple volumes, backup [25](#)

## N

- name prefix feature described [22](#)

- NetApp Management Console
  - applications supported [170](#)
  - defined [169](#)
  - window layout and navigation [171](#)

## O

- offline migration feature described [22](#)

## P

- Performance Advisor application described [170](#)
- policies
  - consistency and conformance [44](#)
  - types of [41](#)
- printing Help topics [174](#)
- profiles
  - creating [152](#)
- protection
  - monitoring [47](#)
- protection example
  - assign policy [105](#)
  - configuration assumptions [83](#)
  - configure alarms [107](#)
  - configure host storage [86](#)
  - create datasets [103](#)
  - create groups [101](#)
  - create policy [93](#)
  - create resource pools [88](#)
  - evaluate policy settings for backup node [98](#)
  - evaluate policy settings for mirror connection [99](#)
  - import relationships [106](#)
  - schedules, determine for backup connection [91](#)
  - schedules, determine for mirror connection [93](#)
  - schedules, determine for primary data node [91](#)
  - schedules, evaluate and modify [90](#)
  - setup [81](#)
  - strategy [82](#), [111](#)
  - verify protection [107](#)
- Protection Manager
  - cleaning up relationships [24](#)
  - custom name prefixes [22](#)
  - defined [40](#)
  - dynamic secondary volume sizing [23](#)
  - new and changed features [21](#)
  - user interface changes [29](#)
- protection policies
  - defined [41](#)
- provisioning
  - monitoring [47](#)

- provisioning (*continued*)
  - overview for Protection Manager [46](#)
  - overview for Provisioning Manager [46](#)
- provisioning and protection example, NAS
  - configuration assumptions [112](#)
  - configure host storage [114](#)
  - create provisioning policies [118](#)
  - create resource pools [117](#)
  - setup [109](#)
  - strategy [82](#), [110](#), [111](#)
- provisioning example, SAN
  - configuration assumptions [58](#)
  - configure host storage [61](#)
  - create a dataset and provision a LUN [68](#)
  - create provisioning policy [66](#)
  - create resource pool [63](#)
  - create vFiler template [64](#)
  - create vFiler unit [65](#)
  - setup [55](#)
  - strategy [56](#)
- Provisioning Manager
  - deduplication [22](#)
  - defined [39](#)
  - member-level export protocol settings [25](#)
  - new and changed features [21](#)
  - user interface changes [29](#)
- provisioning policies
  - defined [41](#)

## Q

- Qtree SnapMirror, definition of [49](#)

## R

- RBAC (role-based access control)
  - described [54](#)
  - roles [175](#)
- rebaselining, definition of [49](#)
- relationship cleanup feature described [24](#)
- resource management, simplifying [44](#)

- resource pools
  - adding physical resources [74](#)
  - defined [42](#)
- retention class in profiles [152](#)
- roles, administrator (RBAC) [175](#)

## S

- SnapMirror relationship break, definition of [49](#)
- status monitoring [48](#)

## T

- troubleshooting
  - adding directory to dataset fails [162](#)
  - backup of directory with non-ASCII name fails [162](#)
  - deleting secondary volumes [163](#)
  - deleting volumes or qtrees, conformance impact [162](#)
  - Diagnose OSSV Host wizard display issue [160](#)
  - inaccurate number of bytes transferred [164](#)
  - locating client configuration information [167](#)
  - provisioning failure despite sufficient space [165](#)
  - qtree is not source for SnapMirror destination [164](#)
  - SnapMirror job aborts [165](#)
  - using console with earlier versions of server [165](#)
  - vFiler units, impact of Data ONTAP 7.2 [159](#)
  - viewing directories with Unicode names [160](#)
  - ways to investigate host problems [166](#)

## U

- Unicode characters [160](#)

## V

- vFiler unit enhancements described [27](#)
- vFiler unit migration feature described [22](#)
- vFiler units
  - defined [43](#)
  - investigating problems [166](#)
  - migration overview [46](#)
- Volume SnapMirror, definition of [49](#)

