Contents

Introduction to data protection ................................................................. 10
  Methods of protecting data ................................................................. 10
  Database protection ............................................................................. 11
  What a data loss disaster is ............................................................... 11
  Tools for protecting against data-loss disasters ................................. 12
  Data protection in a SAN environment ............................................... 13
  Types of data protection policies ....................................................... 13

Planning your data protection strategy .................................................. 15
  Working with Snapshot copies ......................................................... 15
    What a Snapshot copy is ............................................................... 15
    How Snapshot copies work ......................................................... 15
  Backup and recovery tasks you can perform with Snapshot copies .... 16
  Guidelines for working with Snapshot copies of Infinite Volumes .... 17
  How storage classes affect Snapshot copies of Infinite Volumes .... 18
  Maximum number of Snapshot copies ............................................. 18
  User access to Snapshot copies ..................................................... 19
  Creation of Snapshot copy schedules .............................................. 20
  Deleting Snapshot copies automatically ........................................... 23
  Viewing settings for the automatic deletion of Snapshot copies .......... 24
  What Snapshot disk consumption is ............................................... 24
  What the Snapshot copy reserve is .................................................. 26

Working with mirroring technology ....................................................... 28
  Components of a mirror relationship ................................................. 28
  Data protection mirror relationships for FlexVol volumes ................ 29
  Data protection mirror relationships for an Infinite Volume ............. 29
  When a destination volume grows automatically ............................ 30
  Path name pattern matching .......................................................... 30
  Language setting requirement ......................................................... 30
  User access to destination volumes ............................................... 31
  Guidelines for creating relationships between clusters or Vservers .... 31
  Limitations for data protection mirror relationships ....................... 33

Working with FlexVol volume SnapVault backups ............................... 35
What a SnapVault backup is ................................................................. 35
Which data gets backed up and restored from a SnapVault backup .......... 36
Which data does not get backed up to a SnapVault backup ...................... 36
How a SnapVault backup works ............................................................. 37
How SnapVault backups work with data compression ........................... 38
SnapVault backup limitations ................................................................. 38
Data protection for Vserver namespace and root information .................. 38
Guidelines for planning Snapshot copy schedule and retention for
SnapVault backups .................................................................................. 39
Supported data protection deployment configurations ............................ 40
What a basic backup deployment is ....................................................... 42
What source-to-destination-to-tape backup is ......................................... 42
How a mirror-mirror cascade works ....................................................... 43
How a mirror-SnapVault cascade works ................................................. 43
How a SnapVault-mirror cascade works ................................................. 44
How a mirror-SnapVault fanout works ................................................... 45
How a multiple-mirrors fanout works ..................................................... 46

Protecting data using Snapshot copies .................................................. 48
Managing Snapshot copies ....................................................................... 48
Commands for managing Snapshot copies ............................................. 48
Managing Snapshot policies ................................................................. 49
What the default Snapshot policy for an Infinite Volume is ...................... 49
How Snapshot policies are associated with volumes .............................. 49
Commands for managing Snapshot policies and schedules .................... 50
Strategies for creating a Snapshot copy policy ....................................... 51
Naming convention for scheduled Snapshot copies ............................... 51
What prefixes are .................................................................................. 52
Using prefixes to name automatic Snapshot copies ................................. 52
Restoring files from the Snapshot copy of a FlexVol volume .................. 53
Restoring a single file from a Snapshot copy of a FlexVol volume .......... 53
Restoring part of a file from a Snapshot copy of a FlexVol volume .......... 54
Restoring the contents of a volume from a Snapshot copy ..................... 54
Snapshot restoration using Shadow Copy Client tools ............................ 55
Managing Snapshot copy disk space ..................................................... 55
Monitoring Snapshot copy disk consumption ....................................... 55

Managing data protection using SnapMirror policies ............................. 57
Providing disaster recovery using mirroring technology ................. 61
Managing data protection mirror copies for FlexVol volumes ................ 61
Creating a data protection mirror copy for FlexVol volumes ............... 61
Managing mirror relationships ........................................................... 63
Commands for managing SnapMirror relationships ......................... 63
Using extended queries to operate on many SnapMirror relationships .... 66
What tape seeding is ........................................................................ 66
Performing tape seeding using SMTape ............................................. 67
Scalability limits for SMTape backup and restore sessions .................. 74
Listing the schedule state of a mirror relationship ............................ 74
Scheduling SnapMirror transfers ...................................................... 75
Changing mirror relationship schedules .......................................... 75
Manually updating data protection mirror copies on destination volumes ... 76
Deleting a mirror copy ..................................................................... 77
Reversing the data protection mirror relationship when disaster occurs .......... 78
Converting a data protection mirror destination to a writeable volume ........ 83
Testing database applications .......................................................... 83
Protecting data on FlexVol volumes by using SnapVault backups ...... 85
Creating SnapVault backups on FlexVol volumes .............................. 85
Guidelines for creating SnapVault relationships on FlexVol volumes .... 85
SnapVault updates fail if destination aggregate is full .......................... 87
Prepopulated SnapVault secondary scenarios .................................... 87
Creating a SnapVault backup in an empty FlexVol volume ............... 88
Creating the SnapVault relationship of a mirror-SnapVault cascade ....... 91
Preserving a Snapshot copy on the primary source volume .................. 92
Creating a SnapVault backup in a prepopulated FlexVol volume .......... 93
Creating a destination baseline using a tape backup .......................... 95
Converting a data protection destination to a SnapVault secondary ....... 96
Managing backup and restore operations for SnapVault backups .......... 97
Backing up from a Snapshot copy that is older than the base Snapshot copy .......................................................... 97
Backing up FlexVol volumes that contain the maximum limit of Snapshot copies ......................................................... 100
Managing the backup of a copied source volume ................................................................. 101
Guidelines for restoring the active file system .......................................................... 101
Guidelines for restoring LUNs in SAN environments ............................................. 101
How restore operations work from a SnapVault backup ..................................... 102
Restoring a volume from a SnapVault backup ......................................................... 103
Managing a SnapVault-mirror cascade when the SnapVault backup is unavailable ........................................................................................................ 104
Managing storage efficiency for SnapVault secondaries .................................. 107
Guidelines for managing storage efficiency for SnapVault backups ........ 107
Enabling storage efficiency on a SnapVault secondary volume ................ 108

Providing disaster recovery on Infinite Volumes using mirroring technology .......................................................... 110

Aggregate requirements for Infinite Volumes in a data protection mirror relationship ........................................................................................................ 110
Constituent size requirements for setting up data protection mirror relationships for Infinite Volumes ........................................................................................................ 111
Creating a data protection mirror copy for an Infinite Volume with dedicated aggregates ........................................................................................................ 111
Identifying the size of a source Infinite Volume and aggregate details ........ 112
Creating dedicated aggregates for a destination cluster (cluster administrators only) ........................................................................................................ 114
Creating a Vserver with Infinite Volume in a destination cluster (cluster administrators only) ........................................................................................................ 115
Assigning aggregates for all Vservers in a cluster (cluster administrators only) ........................................................................................................ 116
Creating cluster and Vserver peer relationships (cluster administrators only) ........................................................................................................ 117
Creating a destination Infinite Volume .................................................................................. 117
Creating and initializing a data protection mirror relationship .................................. 118
Creating a data protection mirror copy for an Infinite Volume with shared aggregates ........................................................................................................ 121
Identifying the size of a source Infinite Volume and constituent details .......... 122
Verifying aggregate space in a destination cluster (cluster administrators only) ....................................................................................................... 123
Creating a Vserver with Infinite Volume in a destination cluster (cluster administrators only) ....................................................................................................... 125
Creating cluster and Vserver peer relationships (cluster administrators only) ....................................................................................................... 126
Creating a destination Infinite Volume ....................................................................................................... 127
Creating and initializing a data protection mirror relationship ....................................................................................................... 127
Viewing information about Infinite Volumes ....................................................................................................... 130
When information is available about a destination Infinite Volume ....................................................................................................... 130
Viewing constituents in an Infinite Volume ....................................................................................................... 131
Managing mirror relationships for Infinite Volumes ....................................................................................................... 132
Commands for managing SnapMirror relationships ....................................................................................................... 132
How commands are run on Infinite Volumes ....................................................................................................... 135
Managing disaster recovery for Infinite Volumes ....................................................................................................... 136
How the snapmirror resync command works for Infinite Volumes and constituents ....................................................................................................... 136
Retrieving data from Infinite Volumes during disaster recovery ....................................................................................................... 136
Creating a namespace mirror constituent on a destination Infinite Volume ....................................................................................................... 139
Recovering individual failed constituents ....................................................................................................... 140
Expanding Infinite Volumes in data protection mirror relationships ....................................................................................................... 141
Adding disks to source and destination Infinite Volumes (cluster administrators only) ....................................................................................................... 141
Adding dedicated aggregates to the source and destination Infinite Volumes (cluster administrators only) ....................................................................................................... 142
Adding shared aggregates to the source and destination Infinite Volumes (cluster administrators only) ....................................................................................................... 143
Increasing the size of source and destination Infinite Volumes ....................................................................................................... 144
Reenabling SnapDiff after expanding a destination Infinite Volume onto new nodes ....................................................................................................... 146
How namespace mirror constituents affect source and destination Infinite Volumes ....................................................................................................... 147
What a namespace mirror constituent is ....................................................................................................... 147
When namespace mirror constituents are created ....................................................................................................... 147
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How modifying an Infinite Volume affects namespace mirror constituents</td>
<td>148</td>
</tr>
<tr>
<td>How namespace mirror constituents affect the state of an Infinite Volume</td>
<td>149</td>
</tr>
<tr>
<td>How Data ONTAP calculates the Infinite Volume size before the transfer of a mirror copy</td>
<td>150</td>
</tr>
<tr>
<td>How Data ONTAP selects aggregates for data protection of Infinite Volumes</td>
<td>151</td>
</tr>
<tr>
<td>When Data ONTAP selects aggregates for destination Infinite Volumes</td>
<td>151</td>
</tr>
<tr>
<td>How Data ONTAP automatically selects aggregates for destination Infinite Volumes</td>
<td>152</td>
</tr>
<tr>
<td>Examples of automatic aggregate selection for destination Infinite Volumes</td>
<td>156</td>
</tr>
<tr>
<td>How data protection mirror updates affect aggregate selection</td>
<td>158</td>
</tr>
<tr>
<td>Error messages and solutions for failed aggregate selection for destination Infinite Volumes</td>
<td>158</td>
</tr>
<tr>
<td>Insufficient space on destination for SnapMirror source Infinite Volume namespace constituent</td>
<td>159</td>
</tr>
<tr>
<td>Size exceeds maximum (namespace constituent)</td>
<td>159</td>
</tr>
<tr>
<td>Insufficient space for the following source data constituents on destination Vserver</td>
<td>160</td>
</tr>
<tr>
<td>Insufficient space on SnapMirror destination for source Infinite Volume data constituents</td>
<td>160</td>
</tr>
<tr>
<td>Size exceeds maximum (data constituents)</td>
<td>160</td>
</tr>
<tr>
<td>Providing disaster recovery on Infinite Volumes with storage classes using mirroring technology</td>
<td>162</td>
</tr>
<tr>
<td>What a storage class is</td>
<td>162</td>
</tr>
<tr>
<td>How storage classes affect data protection mirror relationships for Infinite Volumes</td>
<td>162</td>
</tr>
<tr>
<td>How storage classes affect which aggregates can be associated with Infinite Volumes</td>
<td>163</td>
</tr>
<tr>
<td>Tasks and tools for managing data protection mirror copies for Infinite Volumes with storage classes</td>
<td>163</td>
</tr>
<tr>
<td>Creating a data protection mirror copy for an Infinite Volume with storage classes</td>
<td>164</td>
</tr>
<tr>
<td>Exporting a data policy to a destination Vserver with Infinite Volume</td>
<td>165</td>
</tr>
</tbody>
</table>
Introduction to data protection

Data protection means backing up data and being able to recover it. You protect the data by making copies of it so that it is available for restoration even if the original is no longer available.

Businesses need data backup and protection for the following reasons:

- To protect data from accidentally deleted files, application crashes, data corruption, and viruses
- To archive data for future use
- To recover from a disaster

Methods of protecting data

Depending on your data protection and backup needs, Data ONTAP offers a variety of features and methods that enable you to protect data against accidental, malicious, or disaster-induced loss of data.

**Snapshot copies**

Enable you to manually or automatically create, schedule, and maintain multiple backups (also called *Snapshot copies*) of data on a volume. Snapshot copies use only a minimal amount of additional volume space, and do not have a performance cost.

If a user accidentally modifies or deletes crucial data on a volume with Snapshot technology enabled, that data can be easily and quickly restored from one of the latest Snapshot copies created. You can also create clones of FlexVol volumes using Snapshot copies.

This method is valid for FlexVol volumes and Infinite Volumes.

**SnapRestore** *(license required)*

Enables you to perform fast, space-efficient, on-request Snapshot recovery from Snapshot copies on an entire volume.

This method is valid for FlexVol volumes and Infinite Volumes.

**Data protection mirror copies** *(license required)*

Provide asynchronous disaster recovery. Data protection mirror relationships enable you to periodically create Snapshot copies of data on one volume; copy those Snapshot copies to a partner volume (the destination volume), usually on another cluster; and retain those Snapshot copies. The mirror copy on the destination volume ensures quick availability and restoration of data from the time of the latest Snapshot copy, if the data on the source volume is corrupted or lost.

If you conduct tape backup and archival operations, you can perform them on the data that is already backed up on the destination volume.

This method is valid for FlexVol volumes and Infinite Volumes.
**SnapVault backups** (SnapVault license required)

Provide storage-efficient and long-term retention of backups. SnapVault relationships enable you to back up selected Snapshot copies of volumes to a destination volume and retain the backups.

If you conduct tape backup and archival operations, you can perform them on the data that is already backed up on the SnapVault secondary volume.

This method is valid only for FlexVol volumes.

**volume copy**

Enables you to perform fast block-copy of data from one volume to another.

This method is valid only for FlexVol volumes.

**nvfail option to the volume modify command**

Provides protection against data corruption by failures of nonvolatile RAM (NVRAM).

This method is valid for FlexVol volumes and Infinite Volumes.

### Database protection

If NVRAM problems occur that compromise database validity, Data ONTAP can warn you and automatically rename the database so that it does not restart automatically. You can then ensure that the database is valid before restarting it.

Data ONTAP provides database protection using the `nvfail` option of the `volume create` or `volume modify` command.

For SnapVault relationships in SAN environments, the `nvfail` attribute of the LUN on a SnapVault secondary volume is always off.

For Infinite Volumes, it is recommended to leave the `nvfail` option disabled.

**Note:** You can use this feature only when there are databases on the storage system.

### What a data loss disaster is

A data loss disaster is a situation in which service from one physical site (for example, a building or a corporate campus) on the network is lost for an extended period of time.

The following are examples of disasters:

- Fire
- Earthquake
- Prolonged power outages at a site
- Prolonged loss of connectivity from clients to the storage system at a site
When a disaster occurs, it can affect all the computing infrastructure including storage systems, application servers, networking connectivity, and client connectivity. When you create a disaster plan, you should take your computing infrastructure into consideration.

**Tools for protecting against data-loss disasters**

Data ONTAP provides tools that enable you to back up or replicate data stored at a primary data storage site to an off-site network location. This ensures that you can restore data if data loss is caused by disaster at a primary data storage site.

**SnapVault backups for FlexVol volumes**

SnapVault is a Snapshot copy backup and restorability tool on FlexVol volumes. You can locate a SnapVault secondary volume on the same cluster or on a different cluster.

**Data recoverability**
If a data-loss disaster occurs at a source volume, you can restore data that is backed up to a SnapVault secondary volume. You can restore the data to the source volume after it is running again, or you can restore data to an alternate volume.

**Currency of restore data**
You can restore data from any Snapshot copy that was replicated to the destination system.

**Advantage**
A SnapVault backup provides an inexpensive backup solution.

**Data protection mirror copy**

A data protection mirror copy is a Snapshot copy replication, availability, and restorability tool. You can locate a data protection mirror destination on the same cluster or on a different cluster.

**Data availability**
If a source site experiences a data-loss disaster, you can quickly make available data at the data protection mirror copy destination site.

**Data recoverability**
If a data-loss disaster occurs at a source storage site, you can restore data from a data protection mirror copy destination volume. You can restore the data to the source volume after it is running again, or you can restore data to an alternate volume.

**Currency of restore data**
You can restore data from the last Snapshot copy that was replicated to the destination volume.

**Advantage**
Data protection mirror copies provide data protection and availability.
Data protection in a SAN environment

If FlexVol volumes contain logical units of storage (LUNs) created to enable integration into a storage area network (SAN) environment, the procedures to implement data protection might have to be modified. Infinite Volumes do not support SAN environments or LUNs.

Data protection mirror copies and SnapVault backups are achieved by the use of volume-to-volume relationships. Therefore, to protect data in a LUN, you back up the volume that contains the LUN.

Path-related metadata such as Persistent Reservations, are not replicated to a SnapVault backup. When you restore a volume from a SnapVault secondary volume, the LUNs in the SnapVault secondary volume are exported with a different identity from their counterparts in the source volume. Therefore, you must configure new access controls for the restored LUNs.

For more information about the descriptions of data backup and restore on volumes containing Data ONTAP LUNs, see the Clustered Data ONTAP SAN Administration Guide.

Types of data protection policies

You can assign Snapshot policies to FlexVol volumes and Infinite Volumes, and SnapMirror policies to data protection mirror relationships and SnapVault relationships.

| Snapshot policy | When you assign a Snapshot policy, the policy configures the Snapshot copy creation schedule and retention rules. You can assign the same Snapshot policy to multiple volumes. For example, you might configure a Snapshot policy to create a Snapshot copy every hour, at the end of every day, and at the end of every week, and then assign that same policy to more than one volume. You can assign only one Snapshot policy to a volume. You can assign Snapshot policies to FlexVol volumes and Infinite Volumes. Note: You cannot assign a Snapshot policy that contains the -snapmirror- label to an Infinite Volume. |
| SnapMirror policy | The SnapMirror policy specifies the configuration attributes of a relationship. A SnapMirror policy can be applied to a data protection mirror relationship or a SnapVault relationship. Whether the SnapMirror policy has rules determines if the policy is applied to a SnapVault relationship or applied to a data protection mirror copy. If the policy has rules that define which Snapshot copies are protected, then that policy can be applied to SnapVault relationships only. If the policy does not have rules, then that policy can be applied to data protection mirror copies only. |
Note: If no policy is assigned to a relationship, a default policy is assigned. If it is a data protection mirror relationship, the DPDefault policy is assigned. If it is a SnapVault relationship, the XDPDefault policy is assigned.
Planning your data protection strategy

Data ONTAP provides a variety of tools that you can use to build a comprehensive strategy to protect your company's data.

Vserver administrators can plan data protection for FlexVol volumes and Infinite volumes within their assigned Vservers. Cluster administrators can plan data protection for FlexVol volumes and Infinite Volumes within their assigned clusters.

Working with Snapshot copies

Snapshot copies are the first line of defense for data protection. Data ONTAP maintains a configurable Snapshot schedule that creates and deletes Snapshot copies automatically for each FlexVol volume and Infinite Volume. You can also create and delete Snapshot copies, and manage Snapshot schedules based on your requirements.

What a Snapshot copy is

A Snapshot copy is a read-only image of a FlexVol volume or Infinite Volume that captures the state of the file system at a point in time.

For information about FlexVol volumes, see the Clustered Data ONTAP Physical Storage Management Guide.

How Snapshot copies work

A Snapshot copy is a copy of a FlexVol volume representing the volume's contents at a particular point in time. You can view the contents of the Snapshot copy and use the Snapshot copy to restore data that you lost recently.

A Snapshot copy of a volume is located on the parent volume but has read-only access. It represents the contents of the original volume at a particular point in time. A parent volume and a Snapshot copy of it share disk space for all blocks that have not been modified between the creation of the volume and the time the Snapshot copy is made, thereby making Snapshot copies lightweight.

Similarly, two Snapshot copies share disk space for those blocks that were not modified between the times that the two Snapshot copies were created. You can create a chain of Snapshot copies to represent the state of a volume at a number of points in time. Users can access Snapshot copies online, enabling users to retrieve their own data from past copies, rather than asking a system administrator to restore data from tape. Administrators can restore the contents of a volume from a Snapshot copy.

Each volume has a .snapshot directory that is accessible to NFS users by using the ls command and to CIFS users by double-clicking the ~snapshot folder. The contents of the .snapshot directory are a set of subdirectories, labeled by type, date, and time, resembling the following:
Each subdirectory of the `.snapshot` directory includes a list of the parent volume's files and directories. If users accidentally delete or overwrite a file, they can locate it in the most recent Snapshot directory and restore it to their main read-write volume simply by copying it back to the main directory. The following example shows how an NFS user can locate and retrieve a file named `my.txt` from the `.snapshot` directory:

```
$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
daily.2006-05-14_0013/ hourly.2006-05-15_1306/
hourly.2006-05-15_1106/ weekly.2006-05-14_0019/
hourly.2006-05-15_1206/
$ ls .snapshot/hourly.2006-05-15_1506/my.txt
my.txt
$ ls my.txt
my.txt
```

The `.snapshot` directory is always visible to NFSv2 and NFSv3 clients and available from within the volume, and not visible but still available from any other volume. For NFSv4 clients, the `.snapshot` directory is not visible, but accessible in all paths of a volume.

**Backup and recovery tasks you can perform with Snapshot copies**

Snapshot copies enable system administrators and end users to perform important tasks in backup and recovery.

Snapshot copies enable system administrators to perform the following tasks:

- Create instantaneous backups
- Create a clone of a FlexVol volume
- Create a clone of a Data ONTAP LUN

For information about cloning a FlexVol volume, see the *Clustered Data ONTAP Logical Storage Management Guide*.

Snapshot copies enable end users to perform the following tasks:

- Recover older versions or sets of files that were accidentally changed or deleted
- Restore their own files without needing a system administrator to restore files from tape
Guidelines for working with Snapshot copies of Infinite Volumes

You can create, manage, and restore Snapshot copies of Infinite Volumes. However, you should be aware of the factors affecting the Snapshot creation process and the requirements for managing and restoring the copies.

Guidelines for creating Snapshot copies of Infinite Volumes

- The volume must be online. You cannot create a Snapshot copy of an Infinite Volume if the Infinite Volume is in a Mixed state because a constituent is offline.
- The Snapshot copy schedule should not be less than hourly. It takes longer to create a Snapshot copy of an Infinite Volume than of a FlexVol volume. If you schedule Snapshot copies of Infinite Volumes for less than hourly, Data ONTAP tries but might not meet the schedule. Scheduled Snapshot copies are missed when the previous Snapshot copy is still being created.
- Time should be synchronized across all the nodes that the Infinite Volume spans. Synchronized time helps schedules for Snapshot copies run smoothly and restoration of Snapshot copies function properly.
- The Snapshot copy creation job can run in the background. Creating a Snapshot copy of an Infinite Volume is a cluster-scoped job (unlike the same operation on a FlexVol volume). The operation spans multiple nodes in the cluster. You can force the job to run in the background by setting the -foreground parameter of the volume snapshot create command to false.
- After you create Snapshot copies of an Infinite Volume, you cannot rename the copy or modify the comment or SnapMirror label for the copy.

Guidelines for managing Snapshot copy disk consumption

- You cannot calculate the amount of disk space that can be reclaimed if Snapshot copies of an Infinite Volume are deleted.
- The size of a Snapshot copy for an Infinite Volume excludes the size of namespace mirror constituents.
- If you use the df command to monitor Snapshot copy disk consumption, it displays information about consumption of the individual data constituents in an Infinite Volume—not for the Infinite Volume as a whole.
- To reclaim disk space used by Snapshot copies of Infinite Volumes, you must manually delete the copies. You cannot use a Snapshot policy to automatically delete Snapshot copies of Infinite Volumes. However, you can manually delete Snapshot copies of Infinite Volumes, and you can run the delete operation in the background.

Guidelines for restoring Snapshot copies of Infinite Volumes

- You must restore the entire Snapshot copy of the Infinite Volume.
You cannot restore single files or parts of files. You also cannot restore a Snapshot copy of a single constituent.

- The Snapshot copy must be in a valid state.

You cannot use admin privilege to restore a Snapshot copy of an Infinite Volume if the copy is in a partial or invalid state because the commands require diagnostic privilege. However, you can contact technical support to run the commands for you.

For information about how efficiency settings work with restored Snapshot copies of volumes, see the *Clustered Data ONTAP Logical Storage Management Guide.*

### How storage classes affect Snapshot copies of Infinite Volumes

Snapshot copy creation and management is the same for an Infinite Volume with or without storage classes. You must create Snapshot copies for the entire Infinite Volume. You cannot create Snapshot copies for individual storage classes in Infinite Volumes.

**Related concepts**

- *What a storage class is* on page 162
- *How storage classes affect which aggregates can be associated with Infinite Volumes* on page 163

### Maximum number of Snapshot copies

You should know what the maximum number of Snapshot copies you can accumulate is to minimize the possibility that you do not have Snapshot copies available when you need them.

The maximum number of Snapshot copies follows:

- You can accumulate a maximum of 255 Snapshot copies of a FlexVol volume.
- If the FlexVol volume is in a data protection mirror relationship, the maximum number of Snapshot copies is 254 because one Snapshot copy is reserved for use by the relationship during recovery operations.
- If the FlexVol volume is in a disk to disk backup relationship, the maximum number of Snapshot copies is 251.
- If the Infinite Volume is in a data protection mirror relationship, the maximum number of Snapshot copies is reduced by two because two Snapshot copies are used for the data protection mirror relationship.

Over time, automatically generated hourly, weekly, and monthly Snapshot copies accrue. Having a number of Snapshot copies available gives you a greater degree of accuracy if you have to restore a file.

The number of Snapshot copies can approach the maximum if you do not remove older Snapshot copies. You can configure Data ONTAP to automatically delete older Snapshot copies of volumes as the number of Snapshot copies approaches the maximum.

The following data protection mirror copies affect the maximum number of Snapshot copies available to a volume:

- A FlexVol volume in a data protection mirror relationship
• A FlexVol volume with a load-sharing mirror copy
• An Infinite Volume with one or more namespace mirror constituents

Each namespace mirror constituent uses two Snapshot copies. By default, a read/write Infinite Volume contains one namespace mirror constituent. If you enable SnapDiff on an Infinite Volume, each additional namespace mirror uses two Snapshot copies.

An Infinite Volume also uses up to four Snapshot copies when technical support runs some commands that require diagnostic privilege. You must keep the number of Snapshot copies far enough below the limit to ensure that technical support can run commands.

User access to Snapshot copies

By default, every volume contains a directory named `.snapshot` through which users can access old versions of files in that directory. Users can gain access to Snapshot copies depending on the file-sharing protocol used—NFS or CIFS. Access to Snapshot copies can be turned off.

Snapshot files carry the same read permissions as the original file. A user who has permission to read a file in the volume can read that file in a Snapshot copy. A user without read permission to the volume cannot read that file in a Snapshot copy. Snapshot copies do not have write permissions.

What Snapshot copies you can access

The `.snapshot` directory on every FlexVol volume and Infinite Volume contains all of the Snapshot copies created for the volume. You can access only the Snapshot copies in the `.snapshot` directory that are displayed when you use the `volume snapshot show` command.

Some Snapshot copies in the `.snapshot` directory are used only to support internal system processes for the volume, such as data protection of the namespace constituent for an Infinite Volume, and you cannot access these Snapshot copies. You can access any of the Snapshot copies for a volume that are displayed when you use the `volume snapshot show` command. The command hides the types of Snapshot copies that you cannot access.

**Note:** If an NFS or CIFS client tries to access any of the Snapshot copies used for internal system processes, the client stops working.

When Snapshot copies of Infinite Volumes are accessible

Snapshot copies of an Infinite Volume are restorable and fully accessible to clients only when the Snapshot copies are in a valid state.

A Snapshot copy of an Infinite Volume consists of information spanning multiple constituents across multiple aggregates. Although a Snapshot copy cannot be created if a constituent is offline, a constituent might be deleted or taken offline after the Snapshot copy is created. If a Snapshot copy of an Infinite Volume references a constituent that is offline or deleted, the Snapshot copy might not be fully accessible to clients or restorable.

The availability of a Snapshot copy of an Infinite Volume is indicated by its state, as explained in the following table:
The validity of a Snapshot copy is not tied directly to the state of the Infinite Volume. A valid Snapshot copy can exist for an Infinite Volume with an offline state, depending on when the Snapshot copy was created compared to when the Infinite Volume went offline. For example, a valid Snapshot copy exists before a new constituent is created. The new constituent is offline, which puts the Infinite Volume in an offline state. However the Snapshot copy remains valid because it references its needed pre-existing constituents. The Snapshot copy does not reference the new, offline constituent.

To view the state of Snapshot copies, you can use the `volume snapshot show` command.

**When client access to Snapshot copies is temporarily disabled**

When a node in a cluster that contains an Infinite Volume loses quorum, client access to the Snapshot copies in the Infinite Volume is disabled.

When a node loses quorum, it cannot communicate with the cluster and receive updated information about the Snapshot copies of the Infinite Volume. While the node is out of quorum, client access to Snapshot copies in an Infinite Volume is temporarily disabled, and the storage system uses the following methods to indicate that it is inaccessible:

- You receive an event message from the Event Management System when client access to Snapshot copies is temporarily disabled.
- Clients become unresponsive when accessing Snapshot copies in an Infinite Volume.
- You receive an event message from the Event Management System when the node regains quorum and resumes communication with the cluster.

**Creation of Snapshot copy schedules**

Data ONTAP provides a default Snapshot copy schedule for each FlexVol volume and Infinite Volume. You can create schedules to fit your needs if the default Snapshot copy schedule is not adequate.

For FlexVol volumes, the default Snapshot copy schedule automatically creates one daily Snapshot copy Monday through Saturday at midnight, an hourly Snapshot copy five minutes past the hour, every hour, and a weekly Snapshot copy. Data ONTAP retains the two most recent nightly Snapshot copies and the six most recent hourly Snapshot copies, and deletes the oldest nightly and hourly Snapshot copies when new Snapshot copies are created.
Types of user-specified Snapshot copy schedules

Data ONTAP contains weekly, daily, and hourly Snapshot copy schedules that you can use to create Snapshot copy policies that retain the number and type of Snapshot copies you want.

The following table describes the available types of Snapshot copy schedules:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weekly</td>
<td>Data ONTAP creates these Snapshot copies every Sunday at 15 minutes after midnight. Weekly Snapshot copies are named <code>weekly.n</code>, where <code>n</code> is the date in year-month-day format followed by an underscore (_) and the time. For example, a weekly Snapshot copy created on 25 November 2012 is named <code>weekly.2012-11-25_0015</code>.</td>
</tr>
<tr>
<td>Daily</td>
<td>Data ONTAP creates these Snapshot copies every night at 10 minutes after midnight. Daily Snapshot copies are named <code>daily.n</code>, where <code>n</code> is the date in year-month-day format followed by an underscore (_) and the time. For example, a daily Snapshot copy created on 4 December 2012 is named <code>daily.2012-12-04_0010</code>.</td>
</tr>
<tr>
<td>Hourly</td>
<td>Data ONTAP creates these Snapshot copies five minutes after the hour. Hourly Snapshot copies are named <code>hourly.n</code>, where <code>n</code> is the date in year-month-day format followed by an underscore (_) and the time. For example, an hourly Snapshot copy created on 4 December 2012 at 1:00 (1300) is named <code>hourly.2012-12-04_1305</code>.</td>
</tr>
</tbody>
</table>

Creating a Snapshot copy schedule

If the default Snapshot copy schedule does not meet your needs, you can create a schedule that does.

**Step**

1. Create a Snapshot copy schedule by using the `job schedule cron create` command or the `job schedule interval create` command.

   The command you use depends on how you want to implement the schedule. See the man page for each command to determine the command that meets your needs.
If scheduled Snapshot copy creation fails

Scheduled Snapshot copy creation might fail for various reasons, such as a volume being unavailable. In such cases, Data ONTAP attempts to create a Snapshot copy when possible, outside the schedule.

If a scheduled Snapshot copy creation fails, Data ONTAP checks the Snapshot copies present in the volume. The checks performed and the actions taken depend on the type of scheduled Snapshot copy creation that failed. The process is described in the following list:

1. When a volume becomes available again for creating a Snapshot copy, Data ONTAP checks whether any Snapshot copies were created during a time period represented by `period_snap`. `period_snap` is a variable representing a time period that depends on the type of Snapshot copy schedule, as given in the following table:

<table>
<thead>
<tr>
<th>Type of Snapshot copy schedule</th>
<th>Value of the <code>period_snap</code> variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weekly</td>
<td>3 days</td>
</tr>
<tr>
<td>Nightly</td>
<td>3 days</td>
</tr>
<tr>
<td>Hourly</td>
<td>12 hours</td>
</tr>
</tbody>
</table>

*Note:* You cannot change the value of `period_snap`.

2. The check in the previous step returns one of the following values:

<table>
<thead>
<tr>
<th>If the check returns...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes (One or more Snapshot copies were created in the <code>period_snap</code> period.)</td>
<td>Data ONTAP performs step 3.</td>
</tr>
<tr>
<td>No (Snapshot copies were not created in the <code>period_snap</code> period.)</td>
<td>Data ONTAP performs step 4.</td>
</tr>
</tbody>
</table>

3. Data ONTAP checks whether any scheduled Snapshot copy creation failed after the most recent Snapshot copy. This check returns one of the following values:

<table>
<thead>
<tr>
<th>If the check returns...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes (One or more scheduled Snapshot copy creations were missed.)</td>
<td>Data ONTAP creates a Snapshot copy.</td>
</tr>
<tr>
<td>No (No scheduled Snapshot copy creation was missed.)</td>
<td>Data ONTAP does not create a Snapshot copy.</td>
</tr>
</tbody>
</table>

4. Data ONTAP checks whether any scheduled Snapshot copy creation have failed in the past 25 minutes. This check returns one of the following values:
<table>
<thead>
<tr>
<th>If the check returns...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes (A scheduled Snapshot copy creation was missed in the past 25 minutes.)</td>
<td>Data ONTAP creates a Snapshot copy.</td>
</tr>
<tr>
<td>No (No scheduled Snapshot copy creation was missed in the past 25 minutes.)</td>
<td>Data ONTAP does not create a Snapshot copy.</td>
</tr>
</tbody>
</table>

**Deleting Snapshot copies automatically**

You can define and enable a policy for automatically deleting Snapshot copies and FlexClone LUNs. Automatically deleting Snapshot copies and FlexClone LUNs can help you manage space utilization.

**About this task**

You can automatically delete Snapshot copies from read-write volumes and FlexClone LUNs from read-write parent volumes. You cannot set up automatic deletion of Snapshot copies from Infinite Volumes or from read-only volumes, for example, SnapMirror destination volumes.

**Step**

1. You define and enable a policy for automatically deleting Snapshot copies by using the `volume snapshot autodelete modify` command.

   See the `volume snapshot autodelete modify` man page for information about the parameters that you can use with this command to define a policy that meets your needs.

**Example**

The following command enables the automatic deletion of Snapshot copies and sets the trigger to `snap_reserve` for the `vol3` volume, which is part of the `vs0` Vserver:

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol3 -enabled true -trigger snap_reserve
```

**Example**

The following command enables the automatic deletion of Snapshot copies and of FlexClone LUNs for the `vol3` volume, which is part of the `vs0` Vserver:

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol3 -enabled true -trigger volume -commitment try -delete-order oldest_first -destroy-list lun_clone,file_clone
```
Viewing settings for the automatic deletion of Snapshot copies

You can view the settings for the automatic deletion of Snapshot copies to help you when you are deciding if the settings are meeting your needs.

Step

1. View the settings for the automatic deletion of Snapshot copies by using the `volume snapshot autodelete show` command.

See the `volume snapshot autodelete show` command man pages for information about parameters shown by this command.

Example

The following command displays the automatic deletion settings of Snapshot copies for the vol3 volume, which is part of the vs0 Vserver:

```bash
cluster1::> volume snapshot autodelete show -vserver vs0 -volume vol3

Vserver | Volume | Option Name | Option Value
---------|--------|-------------|------------------
         | vol3   | Enabled     | false
         |        | Commitment  | try
         |        | Trigger     | volume
         |        | Target Free Space | 20%
         |        | Delete Order | oldest_first
         |        | Defer Delete | user_created
         |        | Defer Delete Prefix | (not specified)
         |        | Destroy List | none
```

What Snapshot disk consumption is

Data ONTAP preserves pointers to all the disk blocks currently in use at the time the Snapshot copy is created. When a file is changed, the Snapshot copy still points to the disk blocks where the file existed before it was modified, and changes are written to new disk blocks.

How Snapshot copies consume disk space

Snapshot copies minimize disk consumption by preserving individual blocks rather than whole files. Snapshot copies begin to consume extra space only when files in the active file system are changed...
or deleted. When this happens, the original file blocks are still preserved as part of one or more Snapshot copies.

In the active file system the changed blocks are rewritten to different locations on the disk or removed as active file blocks entirely. As a result, in addition to the disk space used by blocks in the modified active file system, disk space used by the original blocks is still reserved to reflect the status of the active file system before the change.

The following illustration shows disk space usage for a Snapshot copy:

![Disk space usage for a Snapshot copy](image)

**How changing file content consumes disk space**

A given file might be part of a Snapshot copy. The changes to such a file are written to new blocks. Therefore, the blocks within the Snapshot copy and the new (changed or added) blocks both use space within the volume.

Changing the contents of the `myfile.txt` file creates a situation where the new data written to `myfile.txt` cannot be stored in the same disk blocks as the current contents because the Snapshot copy is using those disk blocks to store the old version of `myfile.txt`. Instead, the new data is written to new disk blocks. As the following illustration shows, there are now two separate copies of `myfile.txt` on disk—a new copy in the active file system and an old one in the Snapshot copy:
What the Snapshot copy reserve is

The Snapshot copy reserve sets a specific percent of the disk space for Snapshot copies. For FlexVol volumes, the default Snapshot copy reserve is set to 5 percent of the disk space. By default, the Snapshot copy reserve is 5 percent of the disk space for a FlexVol volume and 0 percent for aggregates.

The active file system cannot consume the Snapshot copy reserve space, but the Snapshot copy reserve, if exhausted, can use space in the active file system.

How Data ONTAP uses deleted active file disk space

When enough disk space is available for Snapshot copies in the Snapshot copy reserve, deleting files in the active file system frees disk space for new files, while the Snapshot copies that reference those files consume only the space in the Snapshot copy reserve.

If Data ONTAP created a Snapshot copy when the disks were full, deleting files from the active file system does not create any free space because everything in the active file system is also referenced by the newly created Snapshot copy. Data ONTAP has to delete the Snapshot copy before it can create any new files.

The following example shows how disk space being freed by deleting files in the active file system ends up in the Snapshot copy:
If Data ONTAP creates a Snapshot copy when the active file system is full and there is still space remaining in the Snapshot reserve, the output from the `df` command—which displays statistics about the amount of disk space on a volume—is as follows:

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>kbytes</th>
<th>used</th>
<th>avail</th>
<th>capacity</th>
<th>Mounted</th>
</tr>
</thead>
<tbody>
<tr>
<td>/vol/vol0/</td>
<td>3000000</td>
<td>3000000</td>
<td>0</td>
<td>100%</td>
<td>vs1</td>
</tr>
<tr>
<td>/vol/vol0/.snapshot</td>
<td>1000000</td>
<td>500000</td>
<td>500000</td>
<td>50%</td>
<td>vs1</td>
</tr>
</tbody>
</table>

If you delete 100,000 KB (0.1 GB) of files, the disk space used by these files is no longer part of the active file system, so the space is reassigned to the Snapshot copies instead.

Data ONTAP reassigns 100,000 KB (0.1 GB) of space from the active file system to the Snapshot reserve. Because there was reserve space for Snapshot copies, deleting files from the active file system freed space for new files. If you enter the `df` command again, the output is as follows:

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>kbytes</th>
<th>used</th>
<th>avail</th>
<th>capacity</th>
<th>Mounted</th>
</tr>
</thead>
<tbody>
<tr>
<td>/vol/vol0/</td>
<td>3000000</td>
<td>2900000</td>
<td>100000</td>
<td>97%</td>
<td>vs1</td>
</tr>
<tr>
<td>/vol/vol0/.snapshot</td>
<td>1000000</td>
<td>600000</td>
<td>400000</td>
<td>60%</td>
<td>vs1</td>
</tr>
</tbody>
</table>

**Example of what happens when Snapshot copies exceed the reserve**

Because there is no way to prevent Snapshot copies from consuming disk space greater than the amount reserved for them, it is important to reserve enough disk space for Snapshot copies so that the active file system always has space available to create new files or modify existing ones.

Consider what happens in the following example if all files in the active file system are deleted. Before the deletion, the `node run -node nodename df` output is as follows:

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>kbytes</th>
<th>used</th>
<th>avail</th>
<th>capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>/vol/vol0/</td>
<td>3000000</td>
<td>3000000</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>/vol/vol0/.snapshot</td>
<td>1000000</td>
<td>500000</td>
<td>500000</td>
<td>50%</td>
</tr>
</tbody>
</table>

After the deletion, the `node run -node nodename df` command generates the following output:

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>kbytes</th>
<th>used</th>
<th>avail</th>
<th>capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>/vol/vol0/</td>
<td>3000000</td>
<td>2500000</td>
<td>500000</td>
<td>83%</td>
</tr>
<tr>
<td>/vol/vol0/.snapshot</td>
<td>1000000</td>
<td>3500000</td>
<td>0</td>
<td>350%</td>
</tr>
</tbody>
</table>
The output shows that the entire 3,000,000 KB (3 GB) in the active file system is still being used by Snapshot copies in addition to the 500,000 KB (0.5 GB) that was used by Snapshot copies before the deletion. Therefore, a total of 3,500,000 KB (3.5 GB) is being used by Snapshot copy data, which is 2,500,000 KB (2.5 GB) more than the space reserved for Snapshot copies. This means that 2.5 GB of space that would be available to the active file system is now unavailable to it. The post-deletion output of the `node run -node nodename df` command lists this unavailable space as `used` even though no files are stored in the active file system.

Recovery of disk space for file system use

Whenever Snapshot copies consume more than 100% of the Snapshot reserve, they begin to occupy the active file system space. This process is called Snapshot spill. When the Snapshot copies continue to occupy the active file system space, the system is in danger of becoming full. If the system becomes full due to Snapshot spill, you can create files only after you delete enough Snapshot copies.

If 500,000 KB (0.5 GB) of data is added to the active file system, a `node run -node nodename df` command generates the following output:

```
<table>
<thead>
<tr>
<th>Filesystem</th>
<th>kbytes</th>
<th>used</th>
<th>avail</th>
<th>capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>/vol/vol0</td>
<td>3000000</td>
<td>3000000</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>/vol/vol0/.snapshot</td>
<td>1000000</td>
<td>3500000</td>
<td>0</td>
<td>350%</td>
</tr>
</tbody>
</table>
```

As soon as Data ONTAP creates a new Snapshot copy, every disk block in the file system is referenced by some Snapshot copy. Therefore, no matter how many files you delete from the active file system, there is still no room to add any more. The only way to recover from this situation is to delete enough Snapshot copies to free more disk space.

**Working with mirroring technology**

Before using mirroring technology, you should understand the components of a mirror relationship, types of mirror copies, where mirror copies are located, path naming and language requirements, and what mirror relationships are not intended to do.

**Components of a mirror relationship**

In its simplest configuration, a mirror relationship is between a source volume and a destination volume and data is replicated to the destination volume using Snapshot copies.

Typically, the source volume is a read-write volume that clients can access and modify. The destination volume is a read-only volume that exports a Snapshot copy to clients for read-only access. The only time the source volume is not a read-write volume is in a cascade configuration where the source volume is a destination of one mirror relationship and the source of another mirror relationship.
Snapshot copies are used by the source volume to update destination volumes. Snapshot copies are transferred from the source volume to the destination volume using an automated schedule or manually; therefore, mirror copies are updated asynchronously. You use the set of `snapmirror` commands to create and manage mirror relationships.

**Related concepts**

*Supported data protection deployment configurations* on page 40

**Data protection mirror relationships for FlexVol volumes**

You can create a mirror relationship to a destination within a cluster to protect your data or, for greater disaster protection, you can create a mirror relationship to a destination in a different cluster in a different location. A data protection mirror configuration consists of a source volume that can be replicated to one or more destination volumes. Each data protection mirror relationship is independent from the other.

**Note:** The version of Data ONTAP that is running on the destination volume must be the same or a later version than the one running on the source volume.

You can create data protection mirror relationships to destinations on the same aggregate as the source volume, and on the same Vserver or on a different Vserver. For greater protection, you can create the relationships to destinations on a different aggregate, which enables you to recover from the failure of the source volume’s aggregate. Neither of these two configurations protects against a cluster failure.

To protect against a cluster failure, you can create a data protection mirror relationship in which the source volume is on one cluster and the destination volume is on a different cluster. If the cluster on which the source volume resides experiences a disaster, you can direct user clients to the destination volume on the cluster peer until the source volume is available again.

You can also use mirror relationships for limited disaster recovery, off-loading tape backup, data distribution, and making offline copies of production data for research, such as data mining.

**Data protection mirror relationships for an Infinite Volume**

You can create a data protection mirror relationship from a source Infinite Volume on one cluster to a destination Infinite Volume on a different cluster to provide asynchronous disaster recovery. Infinite Volumes support bidirectional data exchange between two sites and multiple-mirror fanout deployments.

You cannot create a data protection mirror relationship between two Infinite Volumes on the same cluster, and you cannot create a data protection mirror relationship between a FlexVol volume and an Infinite Volume.
When a destination volume grows automatically

During a data protection mirror transfer, the destination volume grows to ensure the success of the transfer.

At the start of a data protection mirror transfer, the destination volume grows in size if the source volume has grown. This occurs irrespective of any automatic growth setting on the destination volume. The automatic growth of the destination volume occurs as long as there is available space in the aggregate that contains the destination volume. You cannot prevent Data ONTAP from growing or limiting it growth.

Path name pattern matching

You can use pattern matching when you use snapmirror commands to have the command work on selected mirroring relationships.

The snapmirror commands use fully qualified path names in the following format: `vserver:volume`. You can abbreviate the path name by not entering the Vserver name. If you do this, the snapmirror command assumes the local Vserver context of the user.

Assuming that the Vserver is called “vserver1” and the volume is called “vol1”, the fully qualified path name is `vserver1:vol1`.

You can use the asterisk (*) in paths as a wildcard to select matching, fully qualified path names. The following table provides examples of using the wildcard to select a range of volumes.

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Matches all paths.</td>
</tr>
<tr>
<td>vs*</td>
<td>Matches all Vservers and volumes with Vserver names beginning with <code>vs</code>.</td>
</tr>
<tr>
<td>*:<em>src</em></td>
<td>Matches all Vservers with volume names containing the <code>src</code> text.</td>
</tr>
<tr>
<td><em>:vol</em></td>
<td>Matches all Vservers with volume names beginning with <code>vol</code>.</td>
</tr>
</tbody>
</table>

Language setting requirement

The source and destination FlexVol volumes or Infinite Volumes of a mirror relationship must have the same language setting; otherwise, NFS or CIFS clients might not be able to access data.

For FlexVol volumes, it is not a problem if the source and destination volumes are located on the same Vserver because the language is set on the Vserver. For FlexVol volumes and Infinite Volumes
with mirror relationships between volumes on two different Vservers, the language setting on the Vservers must be the same.

**User access to destination volumes**

Users have read-only access to the active file system on the destination FlexVol volume or Infinite Volume. The active file system on the destination volume is an exported Snapshot copy of the active file system from the source volume.

**Protocols supported on destination Infinite Volumes**

You can use the NFSv3 protocol to access the active file system on the destination Infinite Volume. Other protocols are not supported because the destination Infinite Volume does not support locks. However, you can use CIFS and NFS protocols to access Snapshot copies on the destination Infinite Volume.

For CIFS access to Snapshot copies on a destination Infinite Volume, you should create a share at or below `/NS/.snapshot`.

**When clients can access the active file system on the destination volume**

The active file system on a destination volume is available to clients after the system transfers one or more Snapshot copies of the source volume to the destination volume. The number of Snapshot copies transferred and the time required to transfer the Snapshot copies differ between FlexVol volumes and Infinite Volumes.

For a FlexVol volume in a mirror relationship, the storage system automatically directs clients to use the active file system in the latest Snapshot copy on the destination FlexVol volume. For FlexVol volumes that are secondary volumes of a SnapVault relationship, the active file system on the secondary volume is available after the baseline transfer. Attributes of the file system, such as the number of files or the amount of space consumed, are refreshed after the Snapshot copy for the volume is transferred.

For an Infinite Volume in a data protection mirror relationship, the storage system automatically directs clients to use the active file system in the latest coordinated Snapshot copy on the destination Infinite Volume. A coordinated Snapshot copy means that Snapshot copies exist for the namespace constituent and all of the data constituents in the Infinite Volume. The latest coordinated Snapshot copy must be transferred before a consistent view of the active file system is available on the destination Infinite Volume. Because the mirror relationship between Infinite Volumes integrates multiple, separate Snapshot copy transfers, attributes of the file system are updated incrementally as each Snapshot copy transfer is complete.

**Guidelines for creating relationships between clusters or Vservers**

Before you create a mirror or SnapVault relationship between volumes in different clusters or Vservers, you should ensure that the relationship follows the supported configurations. Mirror
relationships are supported by FlexVol volumes and Infinite Volumes. SnapVault relationships are supported only by FlexVol volumes.

**Relationships between volumes in different clusters**

Before you can create a relationship between volumes in different clusters, there must be a cluster peer relationship established between the two clusters and a Vserver peer relationship established between the two Vservers.

**Mirror relationships between clusters running different versions of Data ONTAP**

The version of Data ONTAP that is running on the destination volume must be the same or a later version than the one running on the source volume.

For example, you can create a mirror relationship between a source volume running Data ONTAP 8.1.x and a destination volume running Data ONTAP 8.2.x but not vice versa. Data ONTAP 8.1 commands are supported only for creating and managing these relationships, and you must specify the cluster names.

The `snapmirror show` command displays mixed-version relationships in addition to same-version relationships.

SnapVault relationships are supported only between clusters running Data ONTAP 8.2 or later.

For more information about mirror relationships between clusters running different versions of Data ONTAP, see the Upgrade and Revert/Downgrade Guide.

**SnapVault relationships between clusters running different versions of Data ONTAP**

A mixed cluster has at least one node that is running Data ONTAP 8.1.x and other nodes running Data ONTAP 8.2.x. data protection mirror relationships created in Data ONTAP 8.1.x are supported in Data ONTAP 8.2.x, but only the cluster administrator can manage and modify them. Only Data ONTAP 8.1 commands are supported for managing these data protection mirror relationships.

For SnapVault relationships, the version of Data ONTAP that is running on the primary and secondary volumes must be Data ONTAP 8.2 or later. You cannot create a SnapVault relationship with a secondary volume that is running a later version of Data ONTAP than the source volume.

**Relationships between volumes in different Vservers**

Before you can create a relationship between volumes in different Vservers, there must be a peer relationship established between the two Vservers. You can only establish a Vserver peer relationship between Vservers with unique names. You should use unique, fully qualified domain names for each Vserver.

You can create a peer relationship between two Vservers with FlexVol volumes or between two Vservers with Infinite Volume, but you cannot create a peer relationship between a Vserver with FlexVol volume and a Vserver with Infinite Volume.
Limitations for data protection mirror relationships

When working with data-protection mirror relationships, you should be aware that there are limitations to data protection mirror relationships.

The following limitations apply to data-protection mirror relationships:

- Snapshot copies cannot be deleted on destination volumes.
- An empty junction path on a destination FlexVol volume is not accessible from CIFS clients.
- A volume can have a maximum of 255 Snapshot copies.
- A FlexClone volume cannot be the source of a data-protection mirror relationship.

Mirror relationship fanout limits

When you are planning the number and types of mirror relationships for a single source volume, you should remember that the source volume is limited in the number of destination volumes that it can have.

The fanout limits depend on the type of mirror relationship that you want to fan out from a single source volume:

- For load-sharing mirror relationships, you can fan out a maximum of one destination volume on a node for a single source volume.
  The maximum number of nodes within a cluster depends on the platform model and licensed protocols. For details about cluster size limits, see the Hardware Universe (formerly the System Configuration Guide) at support.netapp.com/knowledge/docs/hardware/NetApp/syscfg/index.shtml.
- For data protection mirror relationships, you can fan out a maximum of four destination volumes from a single source volume.
- A single source volume can have both one load-sharing destination volume on a node and four data protection destination volumes.

Snapshot copies cannot be deleted automatically on destination volumes

You cannot automatically delete old Snapshot copies on destination FlexVol volumes or Infinite Volumes of mirror relationships because the destination volume is a read-only version of the source volume and should contain the same data as the source.

This is not true of Snapshot copies on destination FlexVol volumes of SnapVault relationships. You can delete old Snapshot copies on SnapVault secondary volumes.

**Note:** Using the `snap autodelete` command to automatically delete Snapshot copies from a destination volume to remove older Snapshot copies will fail.
Empty junction path on a destination volume is not accessible from CIFS clients

If internally mounted FlexVol volumes form a namespace and you have a mirror relationship, CIFS clients on a destination volume that attempt to view mirrored volumes not at the highest level of the namespace are denied access.

This occurs when you create a namespace using more than one volume, in which one volume is the source volume of a mirror relationship and the other volumes are members of the namespace. For example, assume that you have two volumes: vol x, which has a junction path /x, and vol y, which has a junction path /x/y. When a SnapMirror transfer occurs, a directory under vol x is created for vol y on the destination volume. From an NFS client, you can see that the directory is empty, but from a CIFS client, you get the following message:

access is denied.

Maximum number of Snapshot copies for volumes that are mirrored

The maximum number of Snapshot copies that a FlexVol volume in a mirror relationship can contain is 251. The maximum number of Snapshot copies that an Infinite Volume in a data protection mirror relationship can contain is 250.

For FlexVol volumes, whenever an update to a data protection mirror copy or set of load-sharing mirror copies occurs, Data ONTAP creates one new Snapshot copy. For Infinite Volumes, whenever an update to a data protection mirror copy occurs, Data ONTAP creates one new Snapshot copy. You should consider this as you manage the number of Snapshot copies on the source volume. You must keep the number of Snapshot copies far enough below the limit that updates to the mirror copy do not exceed the limit.

Related concepts

Maximum number of Snapshot copies on page 18

Unsupported SnapMirror features in Infinite Volumes

Infinite Volumes do not support all the SnapMirror features. Awareness of the unsupported features helps you understand how you can use SnapMirror technology to protect data in Infinite Volumes.

Infinite Volumes do not support the following SnapMirror features:

- Load-sharing mirror copies
- Vault relationships
- NAS protocols other than NFSv3 for the active file system on the destination Infinite Volume

You can use supported NFS and CIFS protocols to access Snapshot copies on destination Infinite Volumes. For more information about protocols supported for Infinite Volumes, see the Clustered Data ONTAP File Access and Protocols Management Guide.
You cannot use NDMP-based backup for an Infinite Volume. You can use other non-NDMP methods to back up and restore data in an Infinite Volume to tape. For more information, see the Clustered Data ONTAP Data Protection Tape Backup and Recovery Guide.

Working with FlexVol volume SnapVault backups

Before using SnapVault technology, you should understand how SnapVault backups work, where SnapVault volumes are located, and what SnapVault relationships are not intended to do.

What a SnapVault backup is

A SnapVault backup is a collection of Snapshot copies on a FlexVol volume that you can restore data from if the primary data is not usable. Snapshot copies are created based on a Snapshot policy. The SnapVault backup backs up Snapshot copies based on its schedule and SnapVault policy rules.

A SnapVault backup is a disk-to-disk backup solution that you can also use to offload tape backups. In the event of data loss or corruption on a system, backed-up data can be restored from the SnapVault secondary volume with less downtime and uncertainty than is associated with conventional tape backup and restore operations.

The following terms are used to describe SnapVault backups:

- **baseline transfer**: An initial complete backup of a primary storage volume to a corresponding volume on the secondary system.
- **secondary volume**: A volume to which data is backed up from a primary volume. Such a volume can be a secondary or tertiary (and onward) destination in a cascade or fanout backup configuration. The SnapVault secondary system maintains Snapshot copies for long-term storage and possible restore operations.
- **incremental transfer**: A follow-up backup to the secondary system that contains only the changes to the primary data since the last transfer action.
- **SnapMirror label**: An attribute that identifies Snapshot copies for the purpose of selection and retention in SnapVault backups. Each SnapVault policy configures the rules for selecting Snapshot copies on the primary volume and transferring the Snapshot copies that match a given SnapMirror label.
- **Snapshot copy**: The backup images on the source volume that are created manually or automatically as scheduled by an assigned policy. Baseline Snapshot copies contain a copy of the entire source data being protected; subsequent Snapshot copies contain differential copies of the source data. Snapshot copies can be stored on the source volume or on a different destination volume in a different Vserver or cluster.

Snapshot copies capture the state of volume data on each source system. For SnapVault and mirror relationships, this data is transferred to destination volumes.
**primary volume**
A volume that contains data that is to be backed up. In cascade or fanout backup deployments, the primary volume is the volume that is backed up to a SnapVault backup, regardless of where in the chain the SnapVault source is. In a cascade chain configuration in which A has a mirror relationship to B and B has a SnapVault relationship to C, B serves as the source for the SnapVault backup even though it is a secondary destination in the chain.

**SnapVault relationship**
A backup relationship, configured as a SnapVault relationship, between a primary volume and a secondary volume.

---

**Which data gets backed up and restored from a SnapVault backup**

You create SnapVault relationships to back up and restore volumes. You can select the Snapshot copies that the SnapVault relationship uses to backup and restore volumes.

The SnapVault operation backs up a specified volume on the primary system to the associated volume on the SnapVault secondary system. If necessary, data is restored from the SnapVault secondary volume back to the associated primary volume or to a different volume.

The Snapshot policy assigned to the source volume specifies when Snapshot copies are performed. The SnapVault policy assigned to the SnapVault relationship specifies which of the source volume Snapshot copies are replicated to the SnapVault backup.

If the destination volume is a FlexClone volume, the volume retains two more Snapshot copies than the number you configure in the policy. This occurs because the volume retains the FlexClone Snapshot copy and an exported Snapshot copy. For example, if your policy specifies to retain three Snapshot copies, five Snapshot copies are retained (three specified Snapshot copies, one FlexClone Snapshot copy, and one exported Snapshot copy).

In SAN environments, LUN identifiers are preserved on the SnapVault secondary volume.

The secondary system uses slightly more disk space and directories than the source system.

**Related concepts**

*Which data does not get backed up to a SnapVault backup* on page 36

*Guidelines for restoring the active file system* on page 101

---

**Which data does not get backed up to a SnapVault backup**

If you back up an entire Vserver to a SnapVault backup by establishing a SnapVault relationship for each volume in the Vserver, namespace and root information is not backed up. To protect namespace and root information for a Vserver, you must manually create the namespace and root on the SnapVault secondary volume. When backing up LUNs to a SnapVault secondary volume, not all LUN information is replicated.

In SAN environments, the following LUN attributes are not replicated to the secondary volume:

- Path
The LUN in the SnapVault secondary volume can be in a different Vserver or volume from the source LUN. Path-related metadata, such as persistent reservations, are not replicated to the SnapVault primary volume.

- Serial number
- Device ID
- UUID
- Mapped status
- Read Only state
  The Read Only state is always set to true on the destination LUN.
- NVFAIL attribute
  The NVFAIL attribute is always set to false on the destination LUN.

You can set persistent reservations for LUNs on the SnapVault secondary volume.

**Related concepts**

*Which data gets backed up and restored from a SnapVault backup* on page 36

**How a SnapVault backup works**

Backing up volumes to a SnapVault backup involves starting the baseline transfers, making scheduled incremental transfers, and restoring data upon request.

**Baseline transfers**

In general, baseline transfers work as follows:

A baseline transfer occurs when you initialize the SnapVault relationship. When you do this, Data ONTAP creates a new Snapshot copy. Data ONTAP transfers the Snapshot copy from the primary volume to the secondary volume. This Snapshot copy is the baseline of the volume at the time of the transfer and is a complete transfer, not an incremental transfer. As a result, none of the other Snapshot copies on the primary volume are transferred as part of the initial SnapVault transfer, regardless of whether they match rules specified in the SnapVault policy.

**Incremental transfers**

The source system creates incremental Snapshot copies of the source volume as specified by the Snapshot policy that is assigned to the primary volume. Each Snapshot copy for a specific volume contains a label that is used to identify it.

The SnapVault secondary system selects and retrieves specifically labeled incremental Snapshot copies, according to the rules that are configured for the SnapVault policy that is assigned to the SnapVault relationship. The Snapshot label is retained to identify the backup Snapshot copies.

Snapshot copies are retained in the SnapVault backup for as long as is needed to meet your data protection requirements. The SnapVault relationship does not configure a retention schedule, but the SnapVault policy does specify number of Snapshot copies to retain.
SnapVault backup updates

At the end of each Snapshot copy transfer session, which can include transferring multiple Snapshot copies, the most recent incremental Snapshot copy in the SnapVault backup is used to establish a new common base between the primary and secondary volumes and is exported as the active file system.

Data restore

If data needs to be restored to the primary volume or to a new volume, the SnapVault secondary transfers the specified data from the SnapVault backup.

How SnapVault backups work with data compression

SnapVault relationships preserve storage efficiency when replicating data from the source to the SnapVault secondary volume except when additional data compression is enabled.

If additional compression is enabled on the SnapVault secondary volume, storage efficiency is affected as follows:

- Storage efficiency is not preserved for data transfers between the primary and secondary volumes.
- You do not have the option of returning to replicating data while preserving storage efficiency.

Related tasks

Managing storage efficiency for SnapVault secondaries on page 107

SnapVault backup limitations

When planning SnapVault relationships, you must keep in mind what is supported and what is not supported.

The following limitations apply to SnapVault backups:

- 32-bit aggregates are not supported.
  Clustered Data ONTAP systems do not support the SnapVault backup feature for volumes in 32-bit aggregates.
- A SnapVault secondary volume cannot be the secondary volume for multiple primary volumes. A volume can be the secondary for one SnapVault relationship only. However, that same volume can be the source for other relationships.
- SnapVault backups are not supported on Infinite Volumes.

Data protection for Vserver namespace and root information

Backups to secondary volumes in SnapVault relationships between FlexVol volumes replicate only volume data, not the Vserver namespace or root information.

SnapVault relationships replicate only volume data. If you want to back up an entire Vserver to a SnapVault secondary volume, you must first create SnapVault relationships for every volume in the Vserver.
To provide data protection of the Vserver namespace information, you must manually create the namespace on the SnapVault secondary immediately after the first data transfer is completed for all of the volumes in the Vserver and while the source Vserver volumes are still active. When subsequent changes are made to the namespace on the source Vserver, you must manually update the namespace on the destination Vserver.

You cannot create the namespace for a Vserver on a SnapVault secondary volume if only a subset of the Vserver volumes are in a SnapVault relationship, or if only a subset of the Vserver volumes have completed the first data transfer.

Guidelines for planning Snapshot copy schedule and retention for SnapVault backups

It is important to plan the Snapshot copy transfer schedule and retention for your SnapVault backups. When planning SnapVault relationships, consider the following guidelines:

- Before you create a SnapVault policy, you should create a table to plan which Snapshot copies you want replicated to the SnapVault secondary volume and how many of each you want to keep. For example:
  
  - Hourly (periodically throughout the day)
    Does the data change often enough throughout the day to make it worthwhile to replicate a Snapshot copy every hour, every two hours, or every four hours?
  
  - Nightly
    Do you want to replicate a Snapshot copy every night or just workday nights?
  
  - Weekly
    How many weekly Snapshot copies is it useful to keep in the SnapVault secondary volume?

- The primary volume should have an assigned Snapshot policy that creates Snapshot copies at the intervals you need, and labels each Snapshot copy with the appropriate snapmirror-label attribute name.

- The SnapVault policy assigned to the SnapVault relationship should select the Snapshot copies you want from the primary volume, identified by the snapmirror-label attribute name, and specify how many Snapshot copies of each name you want to keep on the SnapVault secondary volume.

<table>
<thead>
<tr>
<th>snapmirror-label attribute value</th>
<th>Source volume: Snapshot copy schedule</th>
<th>Primary volume: Snapshot copies retained</th>
<th>SnapVault secondary volume: Snapshot copies retained</th>
</tr>
</thead>
<tbody>
<tr>
<td>weekly</td>
<td>Every Saturday at 19:00</td>
<td>4</td>
<td>8</td>
</tr>
</tbody>
</table>
## Supported data protection deployment configurations

A simple data protection deployment consists of a FlexVol volume or Infinite Volume in a single mirror relationship or a FlexVol volume in a SnapVault relationship. More complex deployment configurations that provide additional data protection consist of a cascade chain of relationships between FlexVol volumes or a set of fanout relationships for a FlexVol volume or Infinite Volume.

Although a single volume-to-volume relationship does provide data protection, your data protection needs might require the additional protection that is provided by more complex cascade and fanout configurations.

An example of a cascade chain is an A to B to C configuration. In this example, A is the source that is replicated to B as a data protection mirror, and B is the primary that is backed up to C as a SnapVault backup. Cascade chains can be more complex than A to B to C, but the more relationships that are involved in the chain, the greater the number of temporary locks on volumes while replication or update operations are in progress.

An example of a fanout is an A to B and A to C backup or mirror replication configuration. In this example, A is the primary source that is replicated to both B (either in a mirror or SnapVault relationship) and C.

**Note:** Only one SnapVault relationship is supported in a cascade chain configuration, but many SnapVault relationships are supported in a fanout configuration; multiple mirror relationships are supported.

**Attention:** The longer you configure a chain of relationships or the more you add fanout destinations, the greater the risk of Snapshot copies being locked on the source. Depending on the update schedule, the worst case is when one Snapshot copy is locked for each cascade or fanout destination.

The types of supported deployment configurations are as follows:

- Basic data protection configuration (for FlexVol volumes and Infinite Volumes)

---

<table>
<thead>
<tr>
<th>snapmirror-label attribute value</th>
<th>Source volume: Snapshot copy schedule</th>
<th>Primary volume: Snapshot copies retained</th>
<th>SnapVault secondary volume: Snapshot copies retained</th>
</tr>
</thead>
<tbody>
<tr>
<td>nightly</td>
<td>Every Monday through Friday at 19:00</td>
<td>10</td>
<td>60</td>
</tr>
<tr>
<td>hourly</td>
<td>Every hour from 07:00 through 18:00</td>
<td>11</td>
<td>120</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>n/a</td>
<td><strong>25</strong></td>
<td><strong>188</strong></td>
</tr>
</tbody>
</table>
A FlexVol volume or Infinite Volume is in a single relationship with another volume as the source or the destination of mirror replication operations, or a FlexVol volume is in a single relationship with another volume as the primary or the secondary of SnapVault operations.

- **Cascade** (one-to-one-to-one relationship)
  The three types of cascade chain relationships that you can configure are as follows:
  
  - **Mirror-mirror cascade** (for FlexVol volumes only)
    A chain of at least two mirror relationships in which a volume is the source for replication operations to a secondary volume, and the secondary volume is the source for replication operations to a tertiary volume. This configuration might be described as follows: A mirror to B mirror to C.
  
  - **Mirror-SnapVault cascade** (for FlexVol volumes only)
    A chain of a mirror relationship followed by a SnapVault relationship in which a volume is the source for replication operations to a secondary volume, and the secondary volume is the primary for SnapVault operations to a tertiary volume. This configuration might be described as follows: A mirror to B SnapVault backup to C.
  
  - **SnapVault-mirror cascade** (for FlexVol volumes only)
    A chain of a SnapVault relationship followed by a mirror relationship in which a volume is the primary for SnapVault operations to a secondary volume, and the secondary volume is the source for replication operations to a tertiary volume. This configuration might be described as follows: A SnapVault backup to B mirror to C.

A load-sharing mirror source volume or destination volume cannot be a part of any cascade relationship. See the *Clustered Data ONTAP Logical Storage Management Guide* for information about load-sharing mirror relationships.

- **Fanout** (one-to-many relationship)
  In a fanout relationship structure, the source is replicated to multiple destinations, which can be mirror or SnapVault destinations. Only one SnapVault relationship is allowed in a fanout.
  
  - **Mirror-SnapVault fanout** (for FlexVol volumes only)
    A volume is the source for replication operations to a secondary volume and also the source for SnapVault operations to a different secondary volume. This configuration might be described as follows: A mirror to B and A also SnapVault backup to C.
  
  - **Multiple-mirrors fanout** (for FlexVol volumes and Infinite Volumes)
    A volume is the source for replication operations to a destination volume and also the source for replication operations to another, different destination volume. This configuration might be described as follows: A mirror to B and A also mirror to C.

**Related concepts**

- *Components of a mirror relationship* on page 28
- *What source-to-destination-to-tape backup is* on page 42
- *How a mirror-mirror cascade works* on page 43
- *How a mirror-SnapVault cascade works* on page 43
- *How a SnapVault-mirror cascade works* on page 44
- *How a mirror-SnapVault fanout works* on page 45
What a basic backup deployment is

A basic data protection deployment consists of two volumes, either FlexVol volumes or Infinite Volumes, in a one-to-one, source-to-destination relationship. This deployment backs up data to one location, which provides a minimal level of data protection.

In a data protection configuration, source volumes are the data objects that need to be replicated. Typically, users can access and write to source volumes.

Destination volumes are data objects to which the source volumes are replicated. Destination volumes are read-only. Destination FlexVol volumes are usually placed on a different Vserver from the source Vserver. Destination Infinite Volumes must be placed on a different Vserver from the source Vserver. Destination volumes can be accessed by users in case the source becomes unavailable. The administrator can use SnapMirror commands to make the replicated data at the destination accessible and writeable.

The following illustration depicts a basic data protection deployment:

![Basic Data Protection Deployment Diagram]

What source-to-destination-to-tape backup is

A common variation of the basic data protection backup deployment adds a tape backup of a destination FlexVol volume. By backing up to tape from the destination volume, you do not subject the heavily accessed source volume to the performance degradation and complexity of a direct tape backup.

The following illustration depicts a data protection chain deployment with a tape backup:

![Data Protection Chain with Tape Backup Diagram]

NDMP is required for this configuration, and Infinite Volumes do not support NDMP. However, you can use other methods to create a tape backup of an Infinite Volume. For more information, see the *Clustered Data ONTAP Data Protection Tape Backup and Recovery Guide.*
How a mirror-mirror cascade works

A mirror-mirror cascade deployment is supported on FlexVol volumes and consists of a chain of mirror relationships in which a volume is replicated to a secondary volume and the secondary is replicated to a tertiary volume. This deployment adds one or more additional backup destinations without degrading performance on the source volume.

By replicating source A (as shown in the following illustration) to two different volumes (B and C) in a series of mirror relationships in a cascade chain, you create an additional backup. The base for the B-to-C relationship is always locked on A to ensure that the backup data in B and C always stay synchronized with the source data in A.

If the base Snapshot copy for the B-to-C relationship is deleted from A, the next update operation from A to B fails and an error message is generated that instructs you to force an update from B to C. The forced update establishes a new base Snapshot copy and releases the lock, which enables subsequent updates from A to B to finish successfully.

If the volume on B becomes unavailable, you can synchronize the relationship between C and A to continue protection of A without performing a new baseline transfer. After the resynchronize operation finishes, A is in a direct mirror relationship with C, bypassing B.

The following illustration depicts a mirror-mirror cascade chain:

![Mirror-mirror cascade chain illustration](image)

How a mirror-SnapVault cascade works

A mirror-SnapVault cascade deployment is supported on FlexVol volumes and consists of a chain of relationships in which a volume is replicated to a destination volume and then the destination volume becomes the primary for a SnapVault backup on a tertiary volume. This deployment adds a SnapVault backup, which fulfills more strict protection requirements.

In a typical mirror-SnapVault cascade, only the exported Snapshot copies from the mirror destination are transferred to the SnapVault secondary when the SnapVault update occurs. These exported Snapshot copies are created by Data ONTAP and have a prefix of snapmirror and a hidden snapmirror-label called sm_created. The SnapVault backup, using a SnapVault policy and applying a rule that identifies Snapshot copies with the sm_created snapmirror-label, backs up the exported Snapshot copies. Only in the case of mirror-SnapVault cascades is the snapmirror-label sm_created used.
**Note:** A cascade chain can contain multiple mirror relationships but only one SnapVault relationship. The SnapVault relationship can occur anywhere in the chain, depending on your data protection requirements.

The following illustration depicts a mirror-SnapVault cascade chain:

![Diagram of a mirror-SnapVault cascade chain]

**Related references**

*Creating the SnapVault relationship of a mirror-SnapVault cascade* on page 91

**How a SnapVault-mirror cascade works**

A SnapVault-mirror cascade consists of a chain of relationships in which a volume has a SnapVault backup on a secondary volume, and then that secondary volume data is replicated to a tertiary volume. In effect, this deployment provides two SnapVault backups.

A SnapVault-mirror cascade deployment is only supported on FlexVol volumes if the first leg in the cascade is a SnapVault backup. In cascade chains that include a SnapVault relationship, updates to the SnapVault backup always include the Snapshot copy base of the SnapVault relationship in addition to the Snapshot copies that are selected in conformance with the SnapVault policy that is assigned to the relationship. This ensures that the common Snapshot copy for B is always available on A (as shown in the following illustration), which enables you to establish a direct relationship for A to C, if necessary. The extra base Snapshot copy is replaced with a newer common Snapshot copy at every subsequent SnapVault update.
The following illustration depicts a SnapVault-to-mirror cascade chain:

![Diagram of SnapVault-to-mirror cascade chain](image)

**Related concepts**

*Managing a SnapVault-mirror cascade when the SnapVault backup is unavailable* on page 104

**How a mirror-SnapVault fanout works**

A mirror-SnapVault fanout deployment is supported on FlexVol volumes and consists of a source volume that has a direct mirror relationship to a secondary volume and also a direct SnapVault relationship to a different secondary volume.

**Note:** A fanout deployment might not provide as much data protection as a cascade chain.
The following illustration depicts a mirror and SnapVault fanout:

How a multiple-mirrors fanout works

A multiple-mirrors fanout deployment is supported on FlexVol volumes and Infinite Volumes, and consists of a source volume that has a direct mirror relationship to multiple secondary volumes.

The volume on A (as shown in the following illustration) always contains the base Snapshot copies for both B and C. Because updates to B or C automatically include the base Snapshot copy of the other relationship, B and C always have a common Snapshot copy.

**Note:** A fanout deployment might not provide as much data protection as a cascade chain.
The following illustration depicts a mirror and mirror fanout:
Protecting data using Snapshot copies

You can use Snapshot copies to restore data that is lost because of accidental deletion to FlexVol volumes and Infinite Volumes.

Data ONTAP maintains a configurable Snapshot schedule that creates and deletes Snapshot copies automatically for each volume. You can also create and delete Snapshot copies, and manage Snapshot schedules based on your requirements.

If you lose data due to a disaster, you use data protection mirror copies to restore data.

Managing Snapshot copies

You can create multiple schedules that create and delete Snapshot copies, as desired.

Commands for managing Snapshot copies

Cluster administrators can use the `volume snapshot` commands to create and manage all Snapshot copies. Vserver administrators can use the same commands to create and manage Snapshot copies within Vservers.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about Snapshot copies</td>
<td><code>volume snapshot show</code></td>
</tr>
<tr>
<td>Create a Snapshot copy of a volume</td>
<td><code>volume snapshot create</code></td>
</tr>
<tr>
<td>If you are using Infinite Volumes, you must ensure that the Infinite Volume is in an online state. You cannot create a Snapshot copy if the Infinite Volume is in a mixed state due to a offline constituent.</td>
<td></td>
</tr>
<tr>
<td>Modify the attributes of a Snapshot copy</td>
<td><code>volume snapshot modify</code></td>
</tr>
<tr>
<td>If you are using Infinite Volumes, you cannot change the comment or name associated with a Snapshot copy of an Infinite Volume.</td>
<td></td>
</tr>
<tr>
<td>Rename a Snapshot copy of a FlexVol volume</td>
<td><code>volume snapshot rename</code></td>
</tr>
<tr>
<td>You cannot rename a Snapshot copy that is created as a reference copy during execution of the <code>volume copy</code> or <code>volume move</code> commands.</td>
<td></td>
</tr>
<tr>
<td>If you are using Infinite Volumes, you cannot rename a Snapshot copy of an Infinite Volume.</td>
<td></td>
</tr>
</tbody>
</table>
If you want to... | Use this command...
---|---
Delete a Snapshot copy | `volume snapshot delete`
If you are using Infinite Volumes, the Infinite Volume must be online. You cannot delete a Snapshot copy of an Infinite Volume when the Infinite Volume is in a mixed state without assistance from technical support.
If you are using SnapMirror, base Snapshot copies must exist and at least one common Snapshot copy must exist between the source and destination volume to use the `snapmirror resync` command.

See the man page for each command for more information.

**Managing Snapshot policies**

Snapshot policies automatically manage Snapshot copy schedules and retention on FlexVol volumes or Infinite Volumes. You must be a cluster administrator or Vserver administrator to perform most of the Snapshot policy commands.

**What the default Snapshot policy for an Infinite Volume is**

The default Snapshot policy for an Infinite Volume is named `default-1weekly`, and the Snapshot policy includes a default schedule for creating Snapshot copies of the Infinite Volume. You can modify the default Snapshot policy, or you can assign a custom Snapshot policy to an Infinite Volume.

The default schedule automatically creates a Snapshot copy every hour, once a day, and once a week. A maximum of six hourly, two daily, and one weekly Snapshot copies are retained. Older Snapshot copies are automatically deleted to free up space. You can modify the schedule, or you can add more schedules to the Snapshot policy.

**How Snapshot policies are associated with volumes**

Unless you specify a Snapshot policy when you create a FlexVol volume or an Infinite Volume, a volume inherits the Snapshot policy associated with its containing Vserver.

When you create a Vserver, you can specify a Snapshot policy. If you do not specify a Snapshot policy when you create a Vserver, a default Snapshot policy is associated with the Vserver. The default Snapshot policy for a Vserver with FlexVol volume is named `default`, and the default Snapshot policy for a Vserver with Infinite Volume is named `default-1weekly`.

**Note:** When you upgrade a Vserver with Infinite Volume from Data ONTAP 8.1.x, the default Snapshot policy changes from `default` to `default-1weekly`. 
When you create a volume, you can specify a Snapshot policy. If you do not specify a Snapshot policy when you create a volume, the volume inherits the Snapshot policy associated with its containing Vserver.

**Note:** A Snapshot policy is not associated with each constituent in an Infinite Volume, and you cannot associate a Snapshot policy with constituents. A Snapshot policy is only associated with an Infinite Volume.

### Commands for managing Snapshot policies and schedules

Cluster administrators can use the `volume snapshot policy` commands to create and manage all Snapshot copy policies. Vserver administrators can use the same commands to create and manage Snapshot policies within Vservers.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about Snapshot copy policies</td>
<td><code>volume snapshot policy show</code></td>
</tr>
<tr>
<td>Create a new Snapshot copy policy</td>
<td><code>volume snapshot policy create</code></td>
</tr>
<tr>
<td>Create a schedule that can be used in Snapshot copy policies</td>
<td><code>job schedule cron create</code></td>
</tr>
<tr>
<td>Add a schedule to an existing Snapshot copy policy</td>
<td><code>volume snapshot policy add-schedule</code></td>
</tr>
<tr>
<td>A Snapshot policy can have up to five schedules. If you are using Infinite Volumes, scheduled Snapshot copies cannot occur more often than hourly. Cluster administrator only</td>
<td></td>
</tr>
<tr>
<td>Remove a schedule from a Snapshot copy policy</td>
<td><code>volume snapshot policy remove-schedule</code></td>
</tr>
<tr>
<td>Cluster administrator only</td>
<td></td>
</tr>
<tr>
<td>Modify the maximum number of Snapshot copies for a Snapshot copy policy schedule</td>
<td><code>volume snapshot policy modify-schedule</code></td>
</tr>
<tr>
<td>Cluster administrator only</td>
<td></td>
</tr>
<tr>
<td>Modify the description of a Snapshot copy policy</td>
<td><code>volume snapshot policy modify</code></td>
</tr>
<tr>
<td>Dissociate a Snapshot copy policy from a volume</td>
<td><code>volume modify</code></td>
</tr>
<tr>
<td>Cluster administrator only</td>
<td></td>
</tr>
<tr>
<td>Delete a Snapshot copy policy</td>
<td><code>volume snapshot policy delete</code></td>
</tr>
<tr>
<td>Cluster administrator only</td>
<td></td>
</tr>
</tbody>
</table>
Strategies for creating a Snapshot copy policy

You should create a Snapshot copy policy that meets the needs of your organization and users. Following are some strategies for using policies and schedules to schedule and retain Snapshot copies:

- If users rarely lose files or typically notice lost files right away, you can use the default Snapshot copy policy. This policy uses the weekly schedule to create two weekly Snapshot copies; the daily schedule to create a Snapshot copy every day and keeps two; and the hourly schedule to create hourly Snapshot copies and keeps six.

- If users commonly lose files or do not typically notice lost files right away, you should delete the Snapshot copies less often than you would if you used the default policy. Following is the recommended Snapshot copy policy for this situation. It uses the weekly schedule to keep two weekly Snapshot copies, the daily schedule to keep six daily Snapshot copies, and the hourly schedule to keep eight hourly Snapshot copies:

  ```bash
  snapshot policy create -vserver vs1 -policy keep-more-snapshot -enabled true -schedule1 weekly -count1 2 -prefix1 weekly -schedule2 daily -count2 6 -prefix2 daily -schedule3 hourly -count3 8 -prefix3 hourly
  ```

On many systems, only 5 to 10 percent of the data changes each week, so the Snapshot copy schedule of six daily and two weekly Snapshot copies consumes 10 to 20 percent of disk space. Considering the benefits of Snapshot copies, it is worthwhile to reserve this amount of disk space for Snapshot copies.

- You can create different Snapshot copy policies for different volumes on a Vserver. On a very active volume, you should schedule Snapshot copies every hour and keep them for just a few hours, or turn off Snapshot copies. For example, the following schedule creates a Snapshot copy every hour and keeps the last three:

  ```bash
  snapshot policy create -vserver vs1 -policy hourly-keep-3 -enabled true -schedule1 hourly -count1 3 -prefix1 hourly
  ```

- When you create a new volume, the new volume inherits the Snapshot copy schedule from the root volume. After you use the volume for a while, you should check how much disk space the Snapshot copies consume and how often users need to recover lost files, and then adjust the schedule as necessary.

Naming convention for scheduled Snapshot copies

The scheduled Snapshot copy name is composed of an optional prefix or the schedule name specified in the Snapshot policy, and the timestamp. Snapshot names cannot be longer than 255 characters.

If prefix is specified, the Snapshot name is made up of prefix and the timestamp.

If you do not specify the prefix, by default, the schedule name is prepended with the timestamp to form a Snapshot name.
What prefixes are
A prefix is an optional string that you can specify to be used in creating automatic Snapshot copies. Using prefixes in Snapshot names provides more flexibility than using schedule names in naming automatic Snapshot copies.

Prefix names must be unique within a policy. The length of the prefix cannot exceed the maximum allowable length for Snapshot names; that is, Snapshot names cannot be longer than 255 characters. Prefix names must follow the character encoding rules used by Snapshot names.

If a prefix is specified in the Snapshot schedule, then the schedule name is not used to name Snapshot copies. If the prefix is not specified for a Snapshot schedule within a Snapshot policy, then the schedule name is used.

Using prefixes to name automatic Snapshot copies
You can use prefixes to provide flexibility to the naming convention for scheduled Snapshot copies. It removes the dependency on using the schedule names in naming scheduled Snapshot copies.

About this task
• A schedule cannot have more than one prefix.
• Prefixes within a policy should be unique.

Step
1. You can specify prefixes when you create a Snapshot policy or when you add a schedule to the Snapshot policy.

Example
The following command creates a Snapshot policy “test”, which contains the schedule named “5min” having the temp prefix:

```
cluster1::> volume snapshot policy create -policy test -enabled true -schedule1 5min -count1 2 -prefix1 temp
```

Example
The following command adds the “6min” schedule with the “test” prefix to the default policy:

```
cluster1::> volume snapshot policy add-schedule -policy default -schedule 6min -count 4 -prefix test
```
Restoring files from the Snapshot copy of a FlexVol volume

You might have to restore a file from the Snapshot copy of a FlexVol volume if the file was accidentally erased or corrupted. You can use the SnapRestore feature to automatically restore files from the Snapshot copy of a FlexVol volume.

Steps

1. If the original file still exists and you do not want it overwritten by the file in a Snapshot copy, then use your UNIX or Windows client to rename the original file or move it to a different directory.

2. Locate the Snapshot copy that contains the version of the file that you want to restore.

3. Copy the file from the .snapshot directory to the directory in which the file originally existed.

Restoring a single file from a Snapshot copy of a FlexVol volume

You can restore a single file to the required version from a Snapshot copy of a FlexVol volume.

Before you begin

- The volume to which you want to restore the file should be online and writeable.
- The volume to which you want to restore the file should have enough space for the restore operation to be completed successfully.

About this task

The restored file can replace an existing file with the same name in the active file system or become a new file if there is data in the existing file that you want to retain. You can also restore LUNs, but you cannot restore a single file from a Snapshot copy of an Infinite Volume.

If you are restoring an existing LUN, a LUN clone is created and is backed up in the form of a Snapshot copy. During the restore operation, you can read to and write from the LUN.

Step

1. To restore a single file or LUN, use the `volume snapshot restore-file` command.

   The restore operation might take a long time, depending on the size of the file or LUN that you are restoring.

   If you want to display the number of in-progress single file restore operations, use the `volume snapshot restore-file-info` command.
Restoring part of a file from a Snapshot copy of a FlexVol volume

You can restore a range of data from a file in a Snapshot copy to an existing file in the active file system. Partial file restores can only be used to restore specific pieces of a LUN, and NFS or CIFS container files.

Before you begin

- You must understand the metadata of the host LUN or container file so that you know which bytes belong to the object that you want to restore.
- Write operations are not allowed on the object that you are restoring. Otherwise, it might result in an inconsistent data.
- The volume where the LUN or the container file is to be restored must be online and writable.

Steps

1. To restore part of a file, use the `volume snapshot partial-restore-file` command.
   
   To get the settings for partial file restore on a cluster, use the `volume snapshot partial-restore-file-list-info` command.
   
   After the restore is complete, you must purge operating system or application buffers so that the stale data is cleaned.

2. After the restore is complete, purge operating system or application buffers so that the stale data is cleaned.

Restoring the contents of a volume from a Snapshot copy

You can restore the contents of a FlexVol volume or Infinite Volume from a Snapshot copy to quickly recover lost or damaged data.

Before you begin

- You must have the advanced privilege level or higher to run the command.
- If you are working with a Snapshot copy of an Infinite Volume, the Snapshot copy must be valid and the Infinite Volume must be online.

Steps

1. If the volume is an Infinite Volume, use the `volume unmount` command to unmount it.

2. Use the `volume snapshot restore` command to restore the contents of a volume from a Snapshot copy.
Example

The following command restores data to a volume named src_os from a Snapshot copy named src_os_snap_3 on a Vserver named vs0:

```
vs1::> volume snapshot restore -vserver vs0 -volume src_os -snapshot src_os_snap_3
```

3. If the volume is an Infinite Volume, use the `volume mount` command to mount it.

After you finish

You should manually replicate all mirror copies of a volume immediately after you restore from a Snapshot copy. Not doing so can result in unusable mirror copies that must be deleted and re-created.

Snapshot restoration using Shadow Copy Client tools

You can access and restore Data ONTAP Snapshot files using the Windows Shadow Copy Client. The Shadow Copy Client provides a Previous Versions tab in the Properties menu from which you can view and restore Data ONTAP Snapshot images.

The Shadow Copy Client software for Windows 2003 is called the Previous Versions Client. Downloads available from Microsoft allow you to use Shadow Copy client tools on most older versions of Windows. For more information about Shadow Copy Client or Previous Versions Client software, consult the Microsoft documentation.

Managing Snapshot copy disk space

The data referenced by a Snapshot copy cannot be accidentally deleted because of the Snapshot feature's design.

Monitoring Snapshot copy disk consumption

You can monitor Snapshot copy disk consumption using the `df` command, which displays the amount of free space on a disk.

About this task

For an Infinite Volume, the `df` command displays information about all of the data constituents, not about the Infinite Volume as a whole.

Step

1. To display information about Snapshot copy disk consumption, use the `df` command.
Example

The `df` command treats Snapshot copies as a partition different from the active file system. The following example shows a volume with these characteristics:

- The total volume capacity (`kbytes` column) is 4,000,000 KB (4 GB): 3,000,000 KB (75 percent) for the active file system, and 1,000,000 KB (25 percent) for Snapshot copies.
- The active file system is using 2,000,000 KB of its 3,000,000 KB capacity (66 percent, rounded to 65 percent in the `capacity` column), leaving 1,000,000 KB (34 percent) available.
- Snapshot copies are using 500,000 KB of their 1,000,000 KB capacity (50 percent in the `capacity` column), leaving 500,000 KB (50 percent of the space allotted for Snapshot copies, not 50 percent of disk space) available.

**Note:** It is important to understand that the `/vol/vol0/.snapshot` line counts data that exists only in a Snapshot copy. The Snapshot copy calculation does not include Snapshot copy data that is shared with the active file system.
Managing data protection using SnapMirror policies

To manage a data protection mirror or SnapVault relationship, you must assign a policy to the relationship. You use the policy to maximize the efficiency of the transfers to the backup secondaries and manage the update operations for SnapVault backups.

FlexVol volumes support data protection mirror and SnapVault relationships and policies. Infinite Volumes support only data protection mirror relationships and policies.

Commands for managing mirror and SnapVault policies

Cluster administrators can use the `snapmirror policy` commands to create and manage all data protection mirror and SnapVault policies. Vserver administrators can use the same commands to create and manage all data protection mirror and SnapVault policies within Vservers.

- All policy-management commands (except for the `snapmirror policy show` command) must be run on the Vserver that contains the destination volume.
- Commands for SnapVault policies are supported only by FlexVol volumes.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a new rule to a SnapVault policy</td>
<td><code>snapmirror policy add-rule</code></td>
</tr>
<tr>
<td>Create a new mirror or SnapVault policy</td>
<td><code>snapmirror policy create</code></td>
</tr>
<tr>
<td>Delete a mirror or SnapVault policy</td>
<td><code>snapmirror policy delete</code></td>
</tr>
<tr>
<td>Modify a mirror or SnapVault policy</td>
<td><code>snapmirror policy modify</code></td>
</tr>
<tr>
<td>Modify an existing rule in a SnapVault policy</td>
<td><code>snapmirror policy modify-rule</code></td>
</tr>
<tr>
<td>Remove a rule in a SnapVault policy</td>
<td><code>snapmirror policy remove-rule</code></td>
</tr>
<tr>
<td>Display a list of mirror and SnapVault policies</td>
<td><code>snapmirror policy show</code></td>
</tr>
</tbody>
</table>

See the man page for each command for more information.

How SnapMirror policies work with clusters and Vservers

A SnapMirror policy in which the `vserver` parameter contains the cluster name is a cluster-wide policy. You can assign cluster-wide SnapMirror policies to relationships in a cluster. Cluster-wide policies can be configured only by a cluster administrator.
A SnapMirror policy in which the `vserver` parameter contains a Vserver name is a Vserver-wide policy. You can assign Vserver-wide SnapMirror policies to relationships within the Vserver in which the policy was created. Vserver policies can be configured by either a cluster administrator or a Vserver administrator.

**Comparison of what cluster administrators and Vserver administrators can manage**

Cluster administrators and Vserver administrators have different privileges for creating, managing, and assigning policies to mirror and SnapVault relationships.

Cluster administrators can do the following:

- Create and manage any policy in a cluster or Vserver
  - For cluster-wide policies, the `vserver` parameter contains the cluster name. For Vserver-wide policies, the `vserver` parameter contains the Vserver name.
- View, modify, or delete policies in a cluster or Vserver
- Assign a cluster-wide or Vserver-wide policy to a relationship

Vserver administrators can do the following:

- Create and manage policies within a Vserver
  - Policies created by a Vserver administrator are automatically configured with the Vserver name in the `vserver` parameter.
- View cluster-wide policies and Vserver-wide policies created in a specified Vserver
  - Although Vserver administrators can view cluster-wide policies, they cannot modify or delete them. Vserver administrators can view only the Vserver-wide policies that were created within the Vserver on which the `snapmirror policy show` command is executed.
- Assign a cluster-wide or Vserver-wide policy to a relationship

Vserver administrators cannot access Vserver-wide policies of another Vserver.

**Guidelines for naming Snapmirror and SnapVault policies**

Before you create a SnapMirror or SnapVault policy, you should ensure that the policy name is unique.

Cluster-wide policy names must be unique within the cluster and must not conflict with any Vserver-wide policy names.

Vserver-wide policy names must be unique within the Vserver in which the policy is created. However, a Vserver policy name can be the same as a policy name created in a different Vserver, as long as the name does not conflict with any cluster-wide policy name.
Example of creating a tiered backup policy

Data ONTAP uses the `snapmirror-label` attribute to identify Snapshot copies between primary and secondary FlexVol volumes in a SnapVault relationship. When you configure rules in a SnapVault policy, you enter the `snapmirror-label` name that you want to use to identify the Snapshot copies to which the rule applies.

In a tiered backup strategy, a SnapVault policy might have several rules, each one identifying a different set of Snapshot copies. In this example, you have a volume to which you have assigned a Snapshot policy that specifies the following schedule:

- **An hourly Snapshot copy**
  Every two hours, a Snapshot copy is created and is assigned the attribute `-snapmirror-label hourly`.

- **A daily Snapshot copy**
  Every day at 5:00 p.m., a Snapshot copy is created and is assigned the attribute `-snapmirror-label daily`.

- **A weekly Snapshot copy**
  Every Friday at 6:00 p.m., a Snapshot copy is created and is assigned the attribute `weekly`.

In addition, the volume is part of an Oracle database. Using the online management tool for Host Services Agent for Oracle, you set up a schedule that creates a Snapshot copy every day at 5:00 p.m. These Snapshot copies are assigned the attribute `-snapmirror-label Oracle-consistent`.

To set up tiered, disk-to-disk data protection for this volume, in which only the Snapshot copies labeled `daily`, `weekly`, and `Oracle-consistent` are replicated to the SnapVault backup, you do the following:

1. **Create a separate rule for each of the three types of Snapshot copies that you want replicated to the SnapVault secondary volume.**
   You should have three rules. Each rule must specify the retention count. For this example, you configure a retention count of 20 for the daily Snapshot copies, 24 for the weekly Snapshot copies, and 100 for the Oracle-consistent Snapshot copies.

2. **Create a new “TieredOracle” SnapVault policy by using the `snapmirror policy create` command, and add the rules you created in Step 1.**

3. **Assign the new SnapVault policy to the SnapVault relationship that exists between the primary and secondary volumes.**

The new SnapVault policy configuration is as follows:

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Policy</th>
<th>Number Of Rules</th>
<th>Transfer Tries</th>
<th>Priority</th>
<th>Restart</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>TieredOracle 3</td>
<td>8</td>
<td>normal</td>
<td>default</td>
<td>default</td>
<td>Example of a tiered backup policy</td>
</tr>
<tr>
<td></td>
<td>SnapMirror-label: daily</td>
<td>Keep: 20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>weekly</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Oracle-consistent</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Related concepts

Commands for managing mirror and SnapVault policies on page 57

Related references

Commands for managing mirror and SnapVault policies on page 57
Providing disaster recovery using mirroring technology

Stored data is susceptible to disaster, either through hardware failure or environmental catastrophe. You can use mirroring technology to create an identical second set of data to replace the primary set of data, should something happen to the primary set of data.

Managing data protection mirror copies for FlexVol volumes

Data protection mirror management for FlexVol volumes consists of activities such as creating data protection mirror copies for source volumes, modifying data protection mirror copies, and monitoring the status of data protection mirror copies.

Creating a data protection mirror copy for FlexVol volumes

You can protect data by replicating it to data protection mirror copies. You can use data protection mirror copies to recover data when a disaster occurs.

Before you begin

- You must have installed a SnapMirror license on both the source and destination cluster.
- You must have created the cluster and Vserver peering relationship.
  To learn about creating cluster and Vserver peering, see the Clustered Data ONTAP System Administration Guide for Cluster Administrators.

About this task

You can create data protection mirror copies in a cluster using FlexVol volumes only.

Steps

1. Create a destination volume on the destination Vserver that will become the data protection mirror copy by using the `volume create` command.

Example

The following command creates a data protection mirror volume named `dept_eng_dr_mirror1` on a Vserver named `vs1`. The destination volume is located on an aggregate named `aggr3`. The destination volume is also on Vserver `vs1`.

```
vs1::> vol create -volume dept_eng_dr_mirror1 -aggregate aggr3 -size 20MB -type DP
```
If you are creating a data protection mirror copy on a Vserver peer, the destination volume is created on the Vserver peer:

```
vs2::> volume create -volume dept_eng_dr_mirror1
       -aggregate aggr3 -size 20MB -type DP
```

2. Create a data protection mirror relationship by using the `snapmirror create` command.

**Example**

The following command creates a data protection relation with the destination volume named `dept_eng_dp_mirror2` of the source volume named `dept_eng` within a Vserver. The Vserver is named `vs1`.

```
vs1::> snapmirror create -destination-path vs1:dept_eng_dp_mirror2
       -source-path vs1:dept_eng -type DP -schedule 5min
```

If you are creating the data protection mirror relationship with the destination volume on a Vserver peer, you create the data protection mirror relationship from the Vserver that contains the destination volume. For example, if the destination volume were on the Vserver peer named `vs2`, the command to create the data protection mirror relationship is as follows:

```
vs2::> snapmirror create -destination-path vs2:dept_eng_dp_mirror2
       -source-path vs1:dept_eng -type DP -schedule 5min
```

Data ONTAP creates the data protection mirror relationship, but the relationship is left in an uninitialized state.

3. Initialize the data protection mirror copy by using the `snapmirror initialize` command.

**Example**

The following command initializes a data protection mirror copy named `dept_eng_dp_mirror2` of a source volume named `dept_eng`. The source volume and the data protection mirror copy are on the same Vserver named `vs1`.

```
vs1::> snapmirror initialize -destination-path vs1:dept_eng_dp_mirror2
```

If you are initializing the data protection mirror relationship with the destination volume on a Vserver peer, you must initialize the data protection mirror relationship from the Vserver that contains the destination volume. For example, if the destination volume of the single Vserver example were on a Vserver peer named `vs2`, the command to create the data protection mirror relationship is as follows:

```
vs2::> snapmirror initialize -destination-path vs2:dept_eng_dp_mirror2
```
Managing mirror relationships

You manage mirror relationships to optimize the performance of those relationships.

Commands for managing SnapMirror relationships

There are Data ONTAP commands for managing SnapMirror relationships of FlexVol volumes and Infinite Volumes.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abort an active transfer. Use the <code>snapmirror show</code> command to determine the status of the abort operation.</td>
<td><code>snapmirror abort</code></td>
</tr>
<tr>
<td><strong>Note:</strong> Management tasks must be performed on the Infinite Volume and not its individual constituents.</td>
<td></td>
</tr>
<tr>
<td>Make a data protection mirror copy destination writable. This command must be used from the destination Vserver.</td>
<td><code>snapmirror break</code></td>
</tr>
<tr>
<td>When you use this command, the common Snapshot copy between your source and destination is not protected on your source and can be deleted. If you use this command, you should create your own Snapshot copy on the source that will not get auto-deleted and replicate it to the destination volume before breaking the relationship.</td>
<td></td>
</tr>
<tr>
<td>Create a new data protection mirror relationship. This command must be used from the destination Vserver.</td>
<td><code>snapmirror create</code></td>
</tr>
<tr>
<td><strong>Note:</strong> If you are using Infinite Volumes, you can create data protection mirror relationships between clusters only, not within a cluster.</td>
<td></td>
</tr>
<tr>
<td>Delete a data protection mirror relationship. This command must be used from the destination Vserver.</td>
<td><code>snapmirror delete</code></td>
</tr>
<tr>
<td><strong>Note:</strong> Management tasks must be performed on the Infinite Volume and not its individual constituents.</td>
<td></td>
</tr>
<tr>
<td>If you want to...</td>
<td>Use this command...</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Start a baseline transfer. This command must be used from the destination Vserver.</td>
<td>snapmirror initialize</td>
</tr>
<tr>
<td>Display a list of data protection mirror relationships whose source endpoints are in the current Vserver.</td>
<td>snapmirror list-destinations</td>
</tr>
<tr>
<td>Modify a data protection mirror relationship. This command must be used from the destination Vserver.</td>
<td>snapmirror modify</td>
</tr>
<tr>
<td>Display a list of data protection and load-sharing mirror relationships or display the state of a scheduled transfer for a SnapMirror relationship. The information that this command shows is updated periodically; therefore, any changes to a relationship might not show immediately.</td>
<td>snapmirror show</td>
</tr>
<tr>
<td>Disable future transfers for a mirror relationship. This command must be used from the destination Vserver.</td>
<td>snapmirror quiesce</td>
</tr>
<tr>
<td>Enable future transfers for a mirror relationship. This command must be used from the destination Vserver.</td>
<td>snapmirror resume</td>
</tr>
<tr>
<td>Start a resynchronize operation. This command must be used from the destination Vserver.</td>
<td>snapmirror resync</td>
</tr>
<tr>
<td><strong>Attention:</strong> A resynchronize operation can cause data loss on the destination volume because the command can remove the exported Snapshot copy on the destination volume.</td>
<td></td>
</tr>
<tr>
<td>Add an owner to prevent premature deletion of a user created Snapshot copy for a SnapMirror mirror-to-SnapVault cascade configuration. A typical use case is to preserve an application-consistent Snapshot copy.</td>
<td>snapmirror snapshot-owner create</td>
</tr>
<tr>
<td><strong>Note:</strong> This task is not supported for Infinite Volumes.</td>
<td></td>
</tr>
<tr>
<td>If you want to...</td>
<td>Use this command...</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>Delete an owner used to preserve a user created Snapshot copy for a SnapMirror mirror-to- SnapVault cascade configuration.</td>
<td>snapmirror snapshot-owner delete</td>
</tr>
<tr>
<td><strong>Note:</strong> This task is not supported for Infinite Volumes.</td>
<td></td>
</tr>
<tr>
<td>Show all the Snapshot copies with owners that were added using the <code>snapmirror snapshot-owner create</code> command.</td>
<td>snapmirror snapshot-owner show</td>
</tr>
<tr>
<td><strong>Note:</strong> This task is not supported for Infinite Volumes.</td>
<td></td>
</tr>
<tr>
<td>Start an incremental transfer. This command must be used from the destination cluster.</td>
<td>snapmirror update</td>
</tr>
<tr>
<td><strong>Note:</strong> If you are using Infinite Volumes, aggregate requirements must be met before performing the incremental transfer. Management tasks must be performed on the Infinite Volume and not its individual constituents.</td>
<td></td>
</tr>
<tr>
<td>You can disregard error messages that result from updating a SnapMirror relationship from a Snapshot copy that exists on the destination volume. The message is for support use.</td>
<td></td>
</tr>
<tr>
<td>Create a new policy for a data protection mirror relationship.</td>
<td>snapmirror policy create</td>
</tr>
<tr>
<td>Delete a policy of a data protection mirror relationship.</td>
<td>snapmirror policy delete</td>
</tr>
<tr>
<td>Add a new rule to a SnapVault relationship.</td>
<td>snapmirror policy add-rule</td>
</tr>
<tr>
<td>Modify an existing rule in the policy of a SnapVault relationship.</td>
<td>snapmirror policy modify-rule</td>
</tr>
<tr>
<td>Modify a policy of a data protection mirror relationship.</td>
<td>snapmirror policy modify</td>
</tr>
<tr>
<td>Remove a rule from the policy of a data protection mirror relationship.</td>
<td>snapmirror policy remove-rule</td>
</tr>
<tr>
<td>Show the policy of a data protection mirror relationship.</td>
<td>snapmirror policy show</td>
</tr>
</tbody>
</table>
If you want to... | Use this command...
---|---
Copy data to a volume. | snapmirror restore

**Note:** This task is not supported for Infinite Volumes.

Remove the SnapMirror relationship information from the source Vserver. This command must be used from the source Vserver. | snapmirror release

See the man page for each command for more information.

**Using extended queries to operate on many SnapMirror relationships**

You can use extended queries to perform SnapMirror operations on many SnapMirror relationships at one time. For example, you might have many uninitialized SnapMirror relationships that you want to initialize using one command.

**About this task**

You can apply extended queries to the following SnapMirror operations:

- Initializing many **Uninitialized** SnapMirror relationships
- Resuming many **Quiesced** SnapMirror relationships
- Resynchronizing many **Broken** SnapMirror relationships
- Updating many **Idle** SnapMirror relationships
- Aborting many currently **Transferring** SnapMirror relationships

**Step**

1. You perform a SnapMirror operation on many SnapMirror relationships by using the following syntax: `snapmirror command {-state state } *`

**Example**

The following command initializes only SnapMirror relationships that are in an **Uninitialized** state:

```
vs1::> snapmirror initialize {-state Uninitialized} *
```

**What tape seeding is**

Tape seeding is an SMTape functionality that helps you initialize a destination FlexVol volume in a data protection mirror relationship.

Tape seeding enables you to establish a data protection mirror relationship between a source system and a destination system over a low-bandwidth connection. Incremental mirroring of Snapshot copies
from the source to the destination is feasible over a low bandwidth connection. However, an initial mirroring of the base Snapshot copy would take a long time over a low-bandwidth connection. In such a case, you can perform an SMTape backup of the source volume to a tape and use the tape to transfer the initial base Snapshot copy to the destination. You can then set up incremental SnapMirror updates to the destination system using the low-bandwidth connection.

Performing tape seeding using SMTape

Using SMTape, cluster administrators can perform tape seeding to initialize a destination FlexVol volume in a data protection mirror relationship. The time taken to initialize this destination volume over a low bandwidth connection using SMTape is faster when compared to using the `snapmirror initialize` command.

**Before you begin**

Volume and tape must be located on the same node.

**About this task**

To perform tape seeding successfully, you must ensure that all nodes in a cluster are running clustered Data ONTAP 8.2 and later. You can view the event log files at any point in time. For more information about accessing and viewing event log files, see *Clustered Data ONTAP Data Protection Tape Backup and Recovery Guide*. For more information about SMTape commands or other commands, see the man pages.

**Note:** Both source and destination volumes must be located on clustered Data ONTAP storage systems.

**Steps**

1. Determine which Snapshot copy you want to use for tape seeding by using the `volume snapshot show` command.

**Example**

The following example lists the Snapshot copies:

```
clus1::> vol snapshot show -vserver vs1 -volume voll
(volume snapshot show)
<table>
<thead>
<tr>
<th>Vserver</th>
<th>Volume</th>
<th>Snapshot</th>
<th>State</th>
<th>Size</th>
<th>Total%</th>
<th>Used%</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>voll</td>
<td>hourly.2013-01-25_0005</td>
<td>valid</td>
<td>224KB</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>daily.2013-01-25_0010</td>
<td>valid</td>
<td>92KB</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hourly.2013-01-25_0105</td>
<td>valid</td>
<td>228KB</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hourly.2013-01-25_0205</td>
<td>valid</td>
<td>236KB</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hourly.2013-01-25_0305</td>
<td>valid</td>
<td>244KB</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hourly.2013-01-25_0405</td>
<td>valid</td>
<td>244KB</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hourly.2013-01-25_0505</td>
<td>valid</td>
<td>244KB</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>
```
2. If you do not have an existing Snapshot copy, manually make a Snapshot copy of a source volume by using the `volume snapshot create` command.

You must specify a Vserver name, source volume name, and Snapshot copy name.

**Attention:** You must not delete this Snapshot copy until tape seeding is over.

**Example**

The following example shows how to create a Snapshot copy named `mysnap` of a source volume named `src1` on a Vserver named `vs1`. You can view the details of the Snapshot copy `mysnap` by using the `volume snapshot show` command:

```bash
clus1::> volume snapshot create -vserver vs1 -volume src1 -snapshot mysnap
clus1::> volume snapshot show -vserver vs1 -volume src1 -snapshot mysnap
```

```
Vserver: vs1
Volume: src1
Snapshot: mysnap
Creation Time: Thu Aug 09 12:03:46 2012
Snapshot Busy: false
List of Owners: -
Snapshot Size: 52KB
Percentage of Total Blocks: 0%
Percentage of Used Blocks: 1%
Comment: 
7-Mode Snapshot: false
Label for SnapMirror Operations: -
Snapshot State: valid
Constituent Snapshot: false
```

3. Move and position the tape correctly by using the `run -node <node_name> mt` command at the nodeshell.

**Note:** For more information about the `mt` command, see the man pages.

**Example**

The following example moves and positions a no rewind tape device `st0l`:

```bash
clus1::> run -node clus1-01 "mt -t nrst0l rewind"
clus1::> run -node clus1-01 "mt -t nrst0l status"
```

```
Tape drive: Hewlett-Packard LTO-4
Status: ready, write enabled
Format: LTO-2(ro)/3 2/400GB
fileno = 0 blockno = 0 resid = 0
```
4. Use the `smtape backup` command to copy all volume Snapshot copies including the base Snapshot copy to tape.

**Example**

The following example backs up Snapshot copy `mysnap` to the tape device `st01`:

```
clus1::> system smtape backup -vserver vs1 -volume src1 -backup-snapshot mysnap -tape /clus1-01/nrst01
Session 35 created successfully
```

5. Use the `smtape status show` command to see the progress of the baseline transfer.

**Example**

The following example shows the progress and status of the SMTape backup operation triggered in the previous step:

```
clus1::> system smtape status show -session 35 -instance
Session Identifier: 35
   Node Name: clus1-01
Operation Type: backup
Session Status: ACTIVE
   Path Name: /vs1/src1
   Device Name: /clus1-01/nrst01
Bytes Transferred: 0B
   Start Time: 8/9/2012 12:03:55
   End Time: -
Snapshot Name: mysnap
Tape Block Size: 240
Error Description: None
clus1::> smtape status show
(system smtape status show)
```

6. Depending upon the status of the SMTape backup operation, you can perform one of the following actions:

<table>
<thead>
<tr>
<th>If the Status shows...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPLETED</td>
<td>Baseline transfer is complete; go to step 7.</td>
</tr>
</tbody>
</table>
If the Status shows... Then...

**WAITING**

a. Load and position the new tape by using the `run -node <node_name> mt` command.

b. Continue the SMTape backup operation by using the `smtape continue` command.

7. Physically transport the tapes to the destination node.

8. Optional: View the data backed up on a tape by using the `smtape showheader` command.

9. Create a destination volume of type `DP` and appropriate size (same or greater than the source volume size) on the destination cluster that will become the data protection mirror by using the `volume create` command and restrict the volume.

**Example**

The following example creates a data protection mirror volume named `dst1` on a Vserver named `vs1`. The destination volume is located on an aggregate named `aggr5`. Destination volume `dst1` is in the restricted state:

```
clus1::> volume create -vserver vs1 -volume dst1 -aggregate aggr5 -size 400m -type DP -state restricted

[Job 83] Job is queued: Create dst1.
[Job 83] Initializing
[Job 83] Job succeeded: Successful
```

10. Move and position the tape correctly by using the `run -node <node_name> mt` command at the nodeshell.

   **Note:** For more information about the `mt` command, see the man pages.

**Example**

The following example moves and positions a no rewind tape device `st0l` at the destination volume:

```
clus1::> run -node clus1-01 "mt -t nrst0l rewind"
clus1::> run -node clus1-01 "mt -t nrst0l status"

Tape drive: Hewlett-Packard LTO-4
Status: ready, write enabled
Format: LTO-2(ro)/3 2/400GB
fileno = 0  blockno = 0  resid = 0
```

11. Use the `smtape restore` command to restore all the volume Snapshot copies including the base Snapshot copy from tape to the destination volume.
Example

The following example restores all the data from tape to the destination volume dst1 on Vserver vs1:

```
clus1::> system smtape restore -vserver vs1 -volume dst1 -tape /clus1-01/nrst01
Session 36 created successfully
```

12. Use the `smtape status show` command to see the progress of the baseline transfer.

Example

The following example shows the progress and status of the SMTape restore operation triggered in the previous step:

```
clus1::> system smtape status show -session 36 -instance
Session Identifier: 36
    Node Name: clus1-01
Operation Type: restore
Session Status: ACTIVE
    Path Name: /vs1/dst1
    Device Name: /clus1-01/nrst01
Bytes Transferred: 0B
    Start Time: 8/9/2012 12:04:15
    End Time: -
    Snapshot Name: None
    Tape Block Size: 240
    Error Description: None
clus1::> system smtape status show
```

```
<table>
<thead>
<tr>
<th>Session Type</th>
<th>Status</th>
<th>Progress</th>
<th>Path</th>
<th>Device</th>
<th>Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
<td>restore</td>
<td>ACTIVE</td>
<td>0B</td>
<td>/vs1/dst1</td>
<td>clus1-01</td>
</tr>
<tr>
<td>35</td>
<td>backup</td>
<td>COMPLETED</td>
<td>6.01MB</td>
<td>/vs1/src1</td>
<td>clus1-01</td>
</tr>
</tbody>
</table>
```

2 entries were displayed.

13. Depending upon the status of the SMTape restore operation, you can perform one of the following actions:

<table>
<thead>
<tr>
<th>If the Status shows...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPLETED</td>
<td>Baseline transfer is complete; go to step 14.</td>
</tr>
</tbody>
</table>
| WAITING                | a. Load and position the new tape by using the `run -node <node_name>` `mt` command.  
                            b. Continue the SMTape restore operation by using the `smtape continue` command. |

14. Use the `smtape break` command to break the volume and tape relationship.

Note: This command is available for the Vserver administrators also.
Example

The following example breaks the SMTape relationship between the tape and the volume dst1:

clus1::> system smtape break -vserver vs1 -volume dst1

[Job 84] Job is queued: snapmirror break for destination vs1:dst1.
[Job 84] Job succeeded: SnapMirror Break Succeeded

This makes the destination volume writeable and a mirror relationship can be reestablished.

15. Establish the SnapMirror or SnapVault relationship by using the snapmirror resync command.

A SnapMirror relationship creates a data protection copy of the source volume; a SnapVault relationship creates a backup copy. The -type parameter determines the type of relationship established. The value of the -type parameter for a SnapMirror relationship is DP and the value for a SnapVault relationship is XDP.

Example

The following example reestablishes a SnapMirror relationship between the destination volume dst1 and the source volume src1:

clus1::> snapmirror resync -destination-path vs1:dst1 -source-path vs1:src1 -type DP

[Job 85] Job is queued: initiate snapmirror resync to destination "vs1:dst1".
[Job 85] [Job 85] Job succeeded: SnapMirror Resync Transfer Queued

16. Use the snapmirror show command to see the progress of the data protection mirror relationship reestablished between the destination volume and source volume in the previous step.

Example

The following example shows the data protection mirror relationship established between the source volume vs1 and destination volume dst1. The data protection mirror relationship type established is DP:

clus1::> snapmirror show -destination-path vs1:dst1

Source Path: vs1:src1
Destination Path: vs1:dst1
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: -
Relationship Status: Transferring
Transfer Snapshot: snapmirror.58621f01-
When the relationship status shows idle, the data protection mirror relationship is established and tape seeding is complete.

Example

c1s1::> snapmirror show -destination-path vs1:dst1

Source Path: vs1:src1
Destination Path: vs1:dst1
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.58621f01-e214-11e1-833d-123478563412_2147484708.2012-08-09_120444
Newest Snapshot Timestamp: 08/09 12:04:44
Exported Snapshot: snapmirror.58621f01-e214-11e1-833d-123478563412_2147484708.2012-08-09_120444
Exported Snapshot Timestamp: 08/09 12:04:44
Healthy: true
Constituent Relationship: false
Relationship ID: 6485d262-e21a-11e1-833d-123478563412
Transfer Type: resync
Transfer Error: -
Current Throttle: 103079214
Current Transfer Priority: normal
Last Transfer Type: resync
Last Transfer Error: -
Last Transfer Size: 72KB
Scalability limits for SMTape backup and restore sessions

While performing tape seeding, you must be aware of the maximum number of SMTape backup and restore sessions that can be performed simultaneously on storage systems of different system memory capacities. This maximum number depends on the system memory of a storage system.

<table>
<thead>
<tr>
<th>System memory of a storage system</th>
<th>Maximum number of NDMP sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 16 GB</td>
<td>6</td>
</tr>
<tr>
<td>Greater than or equal to 16 GB but less than 24 GB</td>
<td>16</td>
</tr>
<tr>
<td>Greater than or equal to 24 GB</td>
<td>32</td>
</tr>
</tbody>
</table>

You can obtain the system memory of your storage system by using the `sysconfig -a` command (available through the nodeshell). For more information about using this command, see the man pages.

Listing the schedule state of a mirror relationship

You might want to see what state a scheduled transfer for a mirror relationship is in to ensure that jobs are running as they should.

About this task

The state of a scheduled job might be dormant. The dormant state means that the job is waiting for the scheduled start time to begin the transfer. There is nothing wrong with the job and you do not need to do anything.

Step

1. To see the state of scheduled jobs, use the `snapmirror show` command.
Scheduling SnapMirror transfers

If you want scheduled SnapMirror transfers, you can add a schedule to a mirror relationship after you initially create the relationship.

About this task

Unless you create and implement a schedule for SnapMirror transfers, you are limited to manually updating destination FlexVol volumes or Infinite Volumes with mirror relationships. The following are characteristics of adding a SnapMirror transfer schedule:

• When you add a schedule for a data protection mirror copy of Infinite Volumes, do not schedule updates for less than one hour intervals.
  
  If you schedule updates for less than one hour intervals, Data ONTAP tries but cannot meet the schedule for Infinite Volumes, and the data protection mirror relationship is displayed as unhealthy.

• Scheduled SnapMirror transfers (or even manual updates) can disrupt Snapshot copy schedules when a transfer lasts longer than the full retention period of the schedule.

Steps

1. Create the schedule you want to implement by using the `job schedule cron create` command.

2. Apply the schedule to the mirror relationship by using the `-schedule` option of the `snapmirror modify` command.

   See the `snapmirror modify` command man page for more information about the command.

Changing mirror relationship schedules

You can change a schedule that updates mirror relationships for FlexVol volumes and Infinite Volumes if the schedule impacts other backups or updates.

Before you begin

• You must have created the cluster and Vserver peering relationship.

  To know about creating cluster and Vserver peering, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

About this task

Changing a schedule affects load-sharing mirror copies differently than it does for data-protection mirror copies. If you change a schedule to a load-sharing mirror relationship, Data ONTAP makes the change to the relationships of all the load-sharing mirror copies in the group. Data ONTAP determines the load-sharing mirror group by the Vserver and source volume specified by the command. See the *Clustered Data ONTAP Logical Storage Management Guide* for more information about load-sharing mirror copies.
Steps

1. Create the new schedule by using the `job schedule cron create` command.

   Creating a schedule is described in the cron job creation section of the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*. See the man page for details about the `job schedule cron create` command.

2. Change the schedule for a mirror relationship by using the `snapmirror modify -schedule` command.

   This command must be used from the destination Vserver.

Example

The following command changes the update schedule used by a data protection mirror relationship for destination volume named “dept_eng_ls1” to a schedule named “dept_eng_mirror_sched”:

```
vs2::> snapmirror modify -source-path vs1:dept_eng
       -destination-path vs2:dept_eng_ls1 -schedule dept_eng_mirror_sched
```

Manually updating data protection mirror copies on destination volumes

You can schedule updates to data protection mirror copies for destination FlexVol volumes or Infinite Volumes, or you can manually update a data protection mirror copy to transfer Snapshot copies between the source and destination volume. However, for Infinite Volumes, you cannot choose which Snapshot copies to transfer.

Before you begin

- A base Snapshot copy must exist on the source volume and the destination volume.
- The destination volume must be the same size or bigger than the source volume.

About this task

You can have cluster administrator or Vserver administrator privileges to perform this task.

When you update a destination volume, all of the Snapshot copies from the source volume are transferred to the destination volume. In addition, any Snapshot copies deleted from the source volume are deleted from the destination volume during the update. Similarly, any new Snapshot copies on the source volume are transferred to the destination volume.

Step

1. On the destination cluster, manually update a destination volume by using the `snapmirror update` command.
Example

The following command updates the data protection mirror relationship for a destination volume named repo_vol_dest on a Vserver named vs0_dest:

```
vs2::> snapmirror update -destination-path vs0_dest:repo_vol_dest
```

Related concepts

*How Data ONTAP calculates the Infinite Volume size before the transfer of a mirror copy* on page 150
*How data protection mirror updates affect aggregate selection* on page 158

Deleting a mirror copy

You can delete a mirror relationship and the destination FlexVol volume or Infinite Volume if you no longer want the mirror copy.

About this task

When you delete a mirror copy, you must delete the mirror relationship and the destination volume. Deleting the mirror relationship does not delete SnapMirror created Snapshot copies on either the source or destination volumes. Deleting the mirror relationship attempts to delete Snapshot copy owners for the SnapMirror created Snapshot copies on both source and destination volumes.

When you delete a load-sharing mirror copy from a set of load-sharing mirror copies, the destination volume of the deleted load-sharing mirror relationship cannot be used again as a destination volume of a load-sharing relationship if it contains any data or Snapshot copies.

Steps

1. Optional: On the source Vserver, use the `snapmirror list-destination` command to view the list of destination volumes for that source volume.

```
vs1::> snapmirror list-destinations
```

<table>
<thead>
<tr>
<th>Source Path</th>
<th>Type</th>
<th>Destination Path</th>
<th>Status</th>
<th>Transfer Progress</th>
<th>Progress Last Updated</th>
<th>Relationship Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1:src_ui</td>
<td>DP</td>
<td>vs2:vsrsrc_ui ls mir2</td>
<td>Idle</td>
<td>-</td>
<td>-</td>
<td>3672728c-</td>
</tr>
<tr>
<td>ad06-11e2-981e-123478563412</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Use the `snapmirror delete` command to delete a mirror relationship.
Example

The following command deletes a mirror relationship between a destination volume named src_ui_ls_mir2 and a source volume named src_ui:

```
vs2::> snapmirror delete -source-path vs1:src_ui -destination-path vs2:src_ui_ls_mir2
```

The command deletes the mirror relationship, but does not delete the destination volume. In the case of a load-sharing mirror copy, the destination volume will be in the restricted state. If you want to use it as a destination volume of a data protection relationship, you must wait at least 10 minutes. This is the amount of time required to refresh internal caches and place the volume back online.

3. Use the `snapmirror release` command from the source Vserver to remove the configuration information and Data ONTAP created Snapshot copies on the source volume.

Example

The following command removes the DP or XDP relationship from the source Vserver named vs1:

```
vs1::> snapmirror release -source-path vs1:src_ui -destination-path vs2:src_ui_ls_mir2
```

This command removes the DP or XDP relationship information from the source Vserver and does not delete any volumes. This command deletes the base Snapshot copies for the destination volume named src_ui_ls_mir2 from the source volume named src_ui.

4. Optional: Use the `volume delete` command to delete the destination volume.

Delete the destination volume if you no longer need the volume.

Reversing the data protection mirror relationship when disaster occurs

When disaster disables the source FlexVol volume of a data protection mirror relationship, you can use the destination FlexVol volume to serve data while you repair or replace the source, update the source, and reestablish the original configuration of the systems.

About this task

The following procedure describes a data protection mirror relationship that has the source volume on one Vserver and the destination volume on another Vserver. The source and the destination clusters and source and destination Vservers are in peer relationships. The original source (the one disabled by the disaster) is vs1:volA and the original destination is vs2:volB.
All data from the last scheduled SnapMirror Snapshot copy before the source was disabled and all the data written to vs2:volB after it was made writeable is preserved. Any data written to vs1:volA between the last SnapMirror Snapshot copy and the time that vs1:volA was disabled is not preserved.

**Steps**

1. Temporarily make the original source volume a read-only destination volume and reverse the data protection mirror relationship to continue to serve data.

   If the source vs1:volA is recoverable and its data is intact, complete the following steps:

   a) After the source volume (in this case, vs1:volA) is disabled, use the `snapmirror break` command on the destination volume, vs2:volB, to make the destination volume, vs2:volB, writeable.

   **Example**

   ```
   vs2::> snapmirror break vs2:volB
   ```

   b) Redirect the clients of the source volume vs1:volA to the new source volume vs2:volB.

   The former clients of vs1:volA access and write to vs2:volB.

   c) On the destination volume, vs2:volB, use the `snapmirror delete` command to remove the data protection mirror relationship between the source vs1:volA and the destination vs2:volB.

   **Example**

   ```
   vs2::> snapmirror delete vs2:volB
   ```

   d) On the source volume, vs1:volA, use the `snapmirror release` command to remove relationship information from the source.

   **Example**

   ```
   vs1::> snapmirror release vs2:volB
   ```

   e) On the new destination volume, vs1:volA, use the `snapmirror create` command to create the mirror relationship, but with vs2:volB as the new source and vs1:volA as the new destination.

   **Example**

   ```
   vs1::> snapmirror create vs2:volB vs1:volA -type DP
   ```
f) If there are LUNs on the original source volume, vs1:volA, remove the mapping by using the **lun unmap** command.

g) On the new destination volume, vs1:volA, use the **snapmirror resync** command to resynchronize vs1:volA with vs2:volB.

**Example**

```
vs1::> snapmirror resync vs1:volA
```

h) If there were LUNs, map the LUNs on the new source vs2:volB by using the **lun map** command.

If the source vs1:volA is unrecoverable, complete the following steps:

a) After the source volume (in this case, vs1:volA) is disabled, use the **snapmirror break** command on the destination volume, vs2:volB, to make the destination volume, vs2:volB, writeable.

**Example**

```
vs2::> snapmirror break vs2:volB
```

b) Redirect the clients of the source volume vs1:volA to the new source volume vs2:volB.

The former clients of vs1:volA access and write to vs2:volB.

c) On the destination volume, vs2:volB, use the **snapmirror delete** command to remove the data protection mirror relationship between the source vs1:volA and the destination vs2:volB.

**Example**

```
vs2::> snapmirror delete vs2:volB
```

d) On the source Vserver, vs1, use the **snapmirror release** command to remove relationship information from the source.

Even though the source volume is unrecoverable, the data protection mirror relationship still exists and must be removed.

**Example**

```
vs1::> snapmirror release vs2:volB
```

e) Delete the old volume volA and use the **volume create** command to create a new data protection destination volume called vs1:volA.

**Note:** Remember to use the **-type DP** parameter when creating the destination volume.
Example

```
vs1::> volume delete -volume vs1:volA
```

```
vs1::> volume create -volume volA -aggr aggr1 -type DP -vserver vs1
```

f) On the new destination volume, vs1:volA, use the `snapmirror create` command to create the data protection mirror relationship with vs2:volB as the new source volume and vs1:volA as the new destination volume.

Example

```
vs1::> snapmirror create vs2:volB vs1:volA -type DP
```

g) On the new destination volume, vs1:volA, use the `snapmirror initialize` command to create the baseline on the data protection mirror copy. This command also makes vs1:volA a read-only destination.

Example

```
vs1::> snapmirror initialize vs1:volA
```

h) If there were LUNs, map the LUNs on the new source vs2:volB by using the `lun map` command.

You can keep this configuration or, after resolving the problem with the original source volume, you can complete the following steps to reestablish the original data protection mirror relationship.

2. On the new destination volume, vs1:volA, update the new destination volume vs1:volA to transfer the latest data from the new source volume vs2:volB by using the `snapmirror update` command.

Example

```
vs1::> snapmirror update vs1:volA
```

3. On the new destination volume, vs1:volA, use the `snapmirror break` command to make vs1:volA writeable.

Example

```
vs1::>> snapmirror break -source-path vs2:volB -destination-path vs1:volA
```
4. On the new destination volume, \texttt{vs1:volA}, use the \texttt{snapmirror delete} command to remove the data protection mirror relationship between the new source \texttt{vs2:volB} and the new destination \texttt{vs1:volA}.

   \textbf{Example}

   \begin{verbatim}
   vs1::> snapmirror delete vs1:volA
   \end{verbatim}

5. On the new source volume, \texttt{vs2:volB}, use the \texttt{snapmirror release} command to remove the data protection mirror relationship between the new source \texttt{vs2:volB} and the new destination \texttt{vs1:volA}.

   \textbf{Example}

   \begin{verbatim}
   vs2::> snapmirror release vs1:volA
   \end{verbatim}

6. On the original destination volume, \texttt{vs2:volB}, use the \texttt{snapmirror create} command to recreate the original data protection mirror relationship with \texttt{vs1:volA} as the source and \texttt{vs2:volB} as the destination.

   \textbf{Example}

   \begin{verbatim}
   vs2::> snapmirror create vs1:volA vs2:volB -type DP
   \end{verbatim}

7. If there are LUNs on the source \texttt{vs2:volB}, remove the mapping by using the \texttt{lun unmap} command.

8. On the original destination volume, \texttt{vs2:volB}, use the \texttt{snapmirror resync} command to resynchronize the original source and original destination volumes.

   \textbf{Example}

   \begin{verbatim}
   vs2::> snapmirror resync vs2:volB
   \end{verbatim}

9. Redirect the clients from \texttt{vs2:volB} back to their original source volume \texttt{vs1:volA}.

10. If there were LUNs, map them back to the original source \texttt{vs1:volA}.
Converting a data protection mirror destination to a writeable volume

You can convert the destination volume of a data protection mirror relationship to a writeable volume if you want to use that volume to serve data. For example, you might do this if you want to migrate a volume.

Steps

1. On the destination Vserver, make the destination volume writeable by using the `snapmirror break` command.
2. Remove the data protection mirror relationship that the destination volume has with the source volume by using the `snapmirror delete` command.
3. On the source Vserver, remove the configuration information and Data ONTAP created Snapshot copies by using the `snapmirror release` command.

Testing database applications

You can use data protection mirror relationships to create a copy of database data on which to test software applications that run on a database, to avoid the possibility of changing or corrupting the database.

Before you begin

The volume that contains the database must be in a data protection mirror relationship.

About this task

Although you can use this method to test database applications, the preferred method is to create a FlexCache volume. See the *Clustered Data ONTAP Logical Storage Management Guide* for information about creating FlexCache volumes.

Steps

1. On the destination Vserver, use the `snapmirror break` command to make the destination volume writeable.

Example

```
vs2::>> snapmirror break -destination-path vs2:Test_vol
```

2. Run the application on the data in the former destination volume (Test_vol).
3. Check the data in the former destination volume (Test_vol).

4. If testing results in alterations to the data that you do not want, use the `snapmirror resync` command to reestablish the mirror relationship.

5. Repeat Steps 2, 3, and 4, until you are satisfied with the testing.

**After you finish**

After completing the test, you can resynchronize the source and the destination volumes.
Protecting data on FlexVol volumes by using SnapVault backups

You can create a SnapVault relationship between FlexVol volumes and assign a SnapVault policy to it to create a SnapVault backup. A SnapVault backup contains a set of read-only backup copies, located on a secondary volume.

**Note:** SnapVault relationships are supported on clusters running Data ONTAP 8.2 or later. SnapVault relationships are not supported on Infinite Volumes.

A SnapVault backup differs from a set of Snapshot copies or a set of mirror copies on a destination volume. In a SnapVault backup, the data in the secondary volume is periodically updated to keep the data in the secondary volume up to date with changes made in the primary data.

Creating SnapVault backups on FlexVol volumes

You configure a SnapVault relationship and assign a SnapVault policy to the relationship to establish a SnapVault backup.

**About this task**

The commands you use to create SnapVault backups are the same commands you use to create data protection mirrors. For a list of commands, see *Commands for managing data protection mirror copies* on page 63.

**Related concepts**

*Supported data protection deployment configurations* on page 40

Guidelines for creating SnapVault relationships on FlexVol volumes

You must follow certain guidelines when creating SnapVault relationships.

**General guidelines for creating a SnapVault relationship**

The following guidelines apply to all SnapVault relationships:

- A volume can be in multiple relationships, either as the secondary or the primary.
  A volume can be the primary for multiple secondaries and also the secondary for another primary.
- A volume can be the secondary for only one SnapVault relationship.
- You cannot configure SnapVault relationships from multiple primary volumes to a single SnapVault secondary volume.
For example, if you want to back up an entire Vserver to a SnapVault backup, then you must create a separate secondary volume for each volume in the Vserver, and create a separate SnapVault relationship for each primary volume.

- You can configure SnapVault relationships to be used simultaneously with data protection mirror relationships.
- Primary or secondary volumes cannot be 32-bit volumes.
- The primary of a SnapVault backup should not be a FlexClone volume. The relationship will work, but the efficiency provided by FlexClone volumes is not preserved.
- A SnapVault secondary volume cannot be the primary volume of FlexCache volumes.
- Primary and secondary volumes must have the same vol lang settings.
- After you establish a SnapVault relationship, you cannot change the language assigned to the secondary volume.
- A SnapVault relationship can be only one leg of a cascade chain.
- After you establish a SnapVault relationship, you can rename primary or secondary volumes. If you rename a primary volume, it can take a few minutes for the relationship to recover from the name change.

Guidelines for creating a SnapVault relationship to a prepopulated secondary

Typically, you create a prepopulated secondary volume when you copy a primary volume to a secondary volume using tape. This process is known as tape seeding.

If the SnapVault secondary volume already contains data, you can create a SnapVault relationship by using the snapmirror resync command with the -type XDP option.

Before creating a SnapVault relationship to a prepopulated secondary, you must use the following guidelines:

- The primary and secondary volumes must have a common Snapshot copy.
- Snapshot copies on the secondary volume that are newer than the common Snapshot copy are deleted.
  
  When a SnapVault relationship is created, all Snapshot copies on the secondary volume that are more recent than the common Snapshot copy and that are not present on the primary volume are deleted. Newer Snapshot copies on the primary volume that match the configured SnapVault policy are transferred to the secondary volume according to the SnapVault policy.
  
  You can use the -preserve option to keep any Snapshot copies that are more recent than the common Snapshot copy on the SnapVault secondary volume and that are not present on the primary volume.
  
  When you use the -preserve option, data on the secondary volume is logically made the same as the common Snapshot copy. All newer Snapshot copies on the primary volume that match the SnapVault policy are transferred to the secondary volume.
  
  This option is useful when the latest common Snapshot copy is deleted from the primary volume but another, older common Snapshot copy between the primary and secondary volumes still exists.
SnapVault updates fail if destination aggregate is full

If the aggregate that contains the secondary volume of the SnapVault backup is out of space, SnapVault updates fail, even if the secondary volume has space.

Ensure that there is free space in the aggregate and the volume for transfers to succeed.

Prepopulated SnapVault secondary scenarios

There are several ways in which a secondary FlexVol volume for a SnapVault relationship might be prepopulated with data.

The following are some scenarios in which a SnapVault secondary might be populated before a SnapVault relationship is created:

• You used tape backups to provide a baseline transfer to a secondary volume.

   Note: Disk seeding to establish a baseline is not supported for SnapVault backups.

• A SnapVault primary volume in a cascade becomes unavailable.
You have a data protection mirror relationship between a source and a destination volume (a mirror relationship from A to B) and a SnapVault relationship between the secondary destination volume and a tertiary destination volume (a SnapVault relationship from B to C). The backup cascade chain is A mirror to B and B SnapVault backup to C. If the volume on B becomes unavailable, you can configure a SnapVault relationship directly from A to C. The cascade chain is now A SnapVault backup to C, where C was prepopulated with data.

• You created a SnapVault relationship between two flexible clones.
You create a SnapVault relationship between two flexible clones for which their respective parent volumes are already in a SnapVault relationship.

• You extended the SnapVault backup protection beyond 251 Snapshot copies.
To extend the SnapVault backup protection beyond the volume limit of 251 Snapshot copies, you can clone the secondary volume. The original SnapVault secondary volume is the parent volume for the new flexible clone.

• You restored data from a SnapVault secondary to a new primary volume.
You have a SnapVault relationship from A to B. A becomes inaccessible, so the SnapVault secondary volume (B) is used for a baseline restore operation to a new SnapVault secondary volume (C).

After the restore operation finishes, you establish a new SnapVault relationship from the new secondary volume (C), which now becomes the primary volume, and the original SnapVault secondary volume (in other words, C to B). The disk to disk backup relationship is now C to B, where B was prepopulated with data.

• You deleted the base Snapshot copy from the primary volume.
You deleted the base Snapshot copy from the primary volume that was used for a SnapVault transfer, but another, older Snapshot copy exists that is common between the primary and secondary volumes.
Creating a SnapVault backup in an empty FlexVol volume

You can protect data that has long-term storage requirements on a FlexVol volume by replicating selected Snapshot copies to a SnapVault backup on another Vserver or cluster.

Before you begin

- You must have cluster administrator privileges to perform this task for a cluster, and Vserver administrator privileges to perform this task for a Vserver.
- If the primary and secondary volumes are in different Vservers, the Vservers must be in a peer relationship.
  If the primary and secondary volumes are in different clusters, the clusters must be in a peer relationship.
  For information about creating peer relationships, see the Clustered Data ONTAP System Administration Guide for Cluster Administrators.
- A SnapVault policy must exist.
  You must either create one or accept the default SnapVault policy (named XDPDefault) that is automatically assigned.
  Only Snapshot copies with the labels configured in the SnapVault policy rules are replicated in SnapVault operations.
- The Snapshot policy assigned to the primary volume must include the snapmirror-label attribute.
  You can create a new Snapshot policy by using the volume snapshot policy add-schedule command, or you can modify an existing policy by using the volume snapshot policy modify-schedule command to set the snapmirror-label attribute for the set of Snapshot copies that you want backed up to the SnapVault secondary volume. Other Snapshot copies on the primary volume are ignored by the SnapVault relationship.
- Your work environment must be able to accommodate the time it might take to transfer a baseline Snapshot copy with a large amount of data.

Steps

1. On the destination Vserver, create a SnapVault secondary volume with a volume type DP.
   For information about creating a FlexVol volume, see the Clustered Data ONTAP System Administration Guide for Cluster Administrators.

2. Create a schedule that Data ONTAP uses to update the SnapVault relationship by using the job schedule cron create command.
   For more information, see Scheduling SnapMirror transfers on page 75.

Example

The following command creates a schedule that runs on the weekend at 3 a.m.:
3. On the source Vserver, create a Snapshot copy policy that contains the schedule of when Snapshot copies with snapmirror-label attributes occur by using the `volume snapshot policy create` command with the `snapmirror-label` parameter, or use the default Snapshot copy policy called `default`.

**Example**

The following command creates a Snapshot copy policy called “keep-more-snapshot”:

```
vserverB::> snapshot policy create -vserver vs1 -policy keep-more-snapshot
-enabled true -schedule1 weekly -count1 2 -prefix1 weekly -schedule2
daily -count2 6 -prefix2 daily -schedule3 hourly -count3 8 -prefix3 hourly```

The name specified in the `snapmirror-label` attribute for the new Snapshot policy must match the `snapmirror-label` attribute that is specified in the SnapVault policy. This ensures that all subsequent Snapshot copies created on the primary volume have labels that are recognized by the SnapVault policy.

The default Snapshot copy policy has two `snapmirror-label` attributes associated with it, daily and weekly.

4. Create a SnapVault policy by using the `snapmirror policy create` command, or use the default SnapVault policy called `XDPDefault`.

**Example**

The following command creates a SnapVault policy called “vserverB-vault-policy”:

```
vserverB::> snapmirror policy create -vserver vserverB -policy
class vserverB-vault-policy```

5. Add the `snapmirror-label` attribute to the SnapVault policy you created by using the `snapmirror policy add-rule` command.

If you used the XDPDefault SnapMirror policy, you do not need to perform this step. The XDPDefault SnapVault policy uses the daily and weekly `snapmirror-label` attributes specified by the default Snapshot copy policy.

**Example**

The following command adds a rule to the vserverB-vault-policy to transfer Snapshot copies with the “weekly” `snapmirror-label` attribute and to keep 40 Snapshot copies:
vserverB::> snapmirror policy add-rule -vserver vserverB -policy vserverB-vault-policy -snapmirror-label weekly -keep 40

6. On the destination Vserver, create a SnapVault relationship and assign a SnapVault policy by using the `snapmirror create` command with the `type XDP` parameter and the `policy` parameter.

In the path specification, a single name is interpreted as a volume name in the Vserver from which the command is executed. To specify a volume in a different Vserver or in a different cluster, you must specify the full path name.

**Example**

The following command creates a SnapVault relationship between the primary volume “srcvolA” on Vserver “vserverA” and the empty secondary volume “dstvolB” on Vserver “vserverB”. It assigns the SnapVault policy named “vserverB-vault-policy” and uses the “weekendcron” schedule:

vserverB::> snapmirror create -source-path vserverA:srcvolA -destination-path vserverB:dstvolB -type XDP -policy vserverB-vault-policy -schedule weekendcron

7. On the destination Vserver, initialize the SnapVault relationship by using the `snapmirror initialize` command to start a baseline transfer.

The command creates a new Snapshot copy that is transferred to the secondary volume and used as a baseline for subsequent incremental Snapshot copies. The command does not use any Snapshot copies that currently exist on the primary volume.

**Note:** Creating a baseline for a large amount of data might take a while.

**Example**

The following command begins the relationship initialization by creating and transferring a baseline Snapshot copy to the destination volume “dstvolB” on Vserver “vserverB”:

vserverB::> snapmirror initialize -destination-path vserverB:dstvolB

**Related concepts**

*Guidelines for creating SnapVault relationships on FlexVol volumes* on page 85

**Related references**

*Commands for managing mirror and SnapVault policies* on page 57
Creating the SnapVault relationship of a mirror-SnapVault cascade

The SnapVault relationship of a mirror-SnapVault cascade requires a different configuration from a SnapVault relationship that is not a part of a mirror-SnapVault cascade.

Before you begin

- You must have cluster administrator privileges to perform this task for a cluster, and Vserver administrator privileges to perform this task for a Vserver.
- If the primary and secondary volumes are in different Vservers, the Vservers must be in a peer relationship.
  If the primary and secondary volumes are in different clusters, the clusters must be in a peer relationship.
  For information about creating peer relationships, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators.*

About this task

The Snapshot copies that are exported to the mirror destination are ones that are created by Data ONTAP. These Snapshot copies have a snapmirror-label called sm_created associated with them. Only these Snapshot copies are replicated from the mirror to the SnapVault backup. To configure the SnapVault relationship of the mirror-SnapVault cascade, the SnapVault policy associated with the SnapVault relationship must have the sm_created snapmirror-label in a rule to restrict the number of Snapshot copies retained on the SnapVault backup.

Steps

1. On the destination Vserver, create a SnapVault secondary volume with a volume type DP.
   For information about creating a FlexVol volume, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators.*

2. Create a SnapVault policy by using the `snapmirror policy create` command, or use the default SnapVault policy called XDPDefault.

   Example
   
   This procedure uses the XDPDefault policy in the examples.

3. Add the sm_created snapmirror-label to the SnapVault policy by using the `snapmirror policy add-rule` command.
   
   Only the sm_created rule will be observed. Any other rules associated with the SnapVault policy, like the daily or weekly rule, will be disregarded.

   Example
   
   The following command adds a rule to the XDPDefault policy to transfer Snapshot copies with the “sm_created” snapmirror-label and to keep 40 Snapshot copies:
4. On the destination Vserver, create a SnapVault relationship and assign a SnapVault policy by using the `snapmirror create` command with the type XDP parameter and the policy parameter.

Example

The following command creates a SnapVault relationship between the primary volume `srcvolB` on Vserver `vserverB` and the empty secondary volume `dstvolC` on Vserver `vserverC`. It assigns the SnapVault policy named `XDPDefault`:

```
vserverC::> snapmirror create -source-path vserverB:srcvolB -destination-path vserverC:dstvolC -type XDP -policy XDPDefault
```

5. On the destination Vserver, initialize the SnapVault relationship by using the `snapmirror initialize` command to start a baseline transfer.

Note: Creating a baseline for a large amount of data might take a while.

Example

The following command begins the relationship initialization by creating and transferring a baseline Snapshot copy to the secondary volume `dstvolC` on Vserver `vserverC`:

```
vserverC::> snapmirror initialize -destination-path vserverC:dstvolC
```

Related tasks

*How a mirror-SnapVault cascade works* on page 43

Preserving a Snapshot copy on the primary source volume

In a mirror-SnapVault cascade, you must preserve a Snapshot copy on the primary source volume until it transfers to the secondary volume of the SnapVault backup. For example, you want to ensure that application-consistent Snapshot copies are backed up.

**Before you begin**

You must have created the mirror-SnapVault cascade.

**Steps**

1. Ensure that the Snapshot copy you want to preserve has a snapmirror-label by using the `volume snapshot show` command.
2. If the Snapshot copy does not have a snapmirror-label associated with it, add one by using the `volume snapshot modify` command.

   **Example**

   The following command adds a snapmirror-label called “exp1” to the Snapshot copy called “snapappa”:

   ```
   clust1::> volume snapshot modify -volume vol1 -snapshot snapappa -snapmirror-label exp1
   ```

3. Preserve the Snapshot copy on the source volume by using the `snapmirror snapshot-owner create` command to add an owner name to the Snapshot copy.

   **Example**

   The following command adds ApplicationA as the owner name to the snap1 Snapshot copy in the testvol volume on the vs1 Vserver:

   ```
   clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1 -snapshot snapappa -owner ApplicationA
   ```

4. Update the destination volume of the data protection mirror relationship by using the `snapmirror update` command.

   Alternatively, you can wait for the scheduled update of the data protection mirror relationship to occur.

5. Update the secondary volume of the SnapVault relationship to transfer the specific Snapshot copy from the SnapMirror destination volume to the SnapVault secondary volume by using the `snapmirror update` command with the `-source-snapshot` parameter.

6. Remove the owner name from the primary source volume by using the `snapmirror snapshot-owner delete` command.

   **Example**

   The following command removes ApplicationA as the owner name to the snap1 Snapshot copy in the testvol volume on the vs1 Vserver:

   ```
   clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1 -snapshot snapappa -owner ApplicationA
   ```

**Creating a SnapVault backup in a prepopulated FlexVol volume**

You can protect data that has long-term storage requirements on a FlexVol Volume by replicating selected Snapshot copies to a SnapVault backup on another Vserver or cluster. The SnapVault
secondary volume might contain data that already exists from a previous data protection mirror or SnapVault relationship or has been loaded from a tape backup.

**Before you begin**

- You must have cluster administrator privileges to perform this task for a cluster, and you must have Vserver administrator privileges to perform this task for a Vserver.
- If the primary and secondary volumes are in different Vservers, the Vservers must be in a peer relationship.
  - If the primary and secondary volumes are in different clusters, the clusters must be in a peer relationship.
  - For information about creating peer relationships, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.
- The secondary volume must be prepopulated with data.
- A SnapVault policy must exist.
  - You must either create one or accept the default SnapVault policy (named XDPDefault) that is automatically assigned.
  - The SnapVault policy configuration includes the snapmirror-label attribute that is used to select Snapshot copies on the primary volume and match Snapshot copies between the primary and secondary volumes. Only Snapshot copies with the labels configured in the SnapVault policy rules are replicated in SnapVault operations.
  - The Snapshot policy assigned to the primary volume must include the snapmirror-label attribute.
    - The name specified in the snapmirror-label attribute for the new Snapshot policy must match the snapmirror-label attribute that is specified in the SnapVault policy. This ensures that all subsequent Snapshot copies created on the primary volume have labels that are recognized by the SnapVault policy.
    - You can create a new Snapshot policy by using the `volume snapshot policy add-schedule` command, or you can modify an existing Snapshot policy by using the `volume snapshot policy modify-schedule` command to set the snapmirror-label attribute for the set of Snapshot copies that you want replicated to the SnapVault secondary volume. Other Snapshot copies on the primary volume are ignored by the SnapVault relationship.
- Your work environment must be able to accommodate the time it might take to transfer a baseline Snapshot copy with a large amount of data.

**Step**

1. On the destination Vserver, establish the relationship by using the `snapmirror resync` command and the `-type XDP` parameter.

   If the most recent common Snapshot copy between the primary and the secondary is deleted from the primary but there exists another, older common Snapshot copy, you can also use the `-preserve` option. This option performs a logical local rollback to make the data in the primary and the secondary the same, and then it replicates all newer Snapshot copies from the source that match the SnapVault policy.
Example

The following command creates a SnapVault relationship between the primary volume srcvolA on Vserver vserverA and the prepopulated secondary volume dstvolB on Vserver vserverB:

```
vserverB::> snapmirror resync -source-path vserverA:srcvolA -destination-path vserverB:dstvolB -type XDP
```

Related concepts

- Guidelines for creating SnapVault relationships on FlexVol volumes on page 85
- Prepopulated SnapVault secondary scenarios on page 87

Related tasks

- Creating a destination baseline using a tape backup on page 95

Related references

- Commands for managing mirror and SnapVault policies on page 57

Creating a destination baseline using a tape backup

You can perform a baseline transfer from local tape copies to a SnapVault secondary volume to manage your bandwidth or timing constraints over a network.

Before you begin

- You must have cluster administrator privileges to perform this task for a cluster.
- You must have Vserver administrator privileges to perform this task for a Vserver.
- The destination volume must not contain data.

About this task

This operation physically copies data from tape to one or more secondary volumes. When the operation finishes, the secondary volume contains all the Snapshot copies that existed on the primary volume at the time the tape copy was created.

Steps

1. Create a copy of the primary volume on the tape by using the `system smtape backup` command.

   For information about backing up and restoring from tape, see Performing tape seeding using SMTape on page 67.

2. Restore the data to the empty secondary volume from the tape copy.

   For information about backing up and restoring from tape, see Performing tape seeding using SMTape on page 67.
3. Initialize the SnapVault relationship by using the `snapmirror resync` command with the `-type XDP` parameter on the secondary volume, and enable incremental updates.

Converting a data protection destination to a SnapVault secondary

You convert a data protection destination volume to a SnapVault secondary volume after a tape seeding operation or after you lose a SnapVault secondary volume in a backup to disaster protection mirror cascade.

Before you begin

- You must have cluster administrator privileges to perform this task for a cluster.
- You must have Vserver administrator privileges to perform this task for a Vserver.

About this task

In the case of tape seeding, after you transfer the data from the tape to the volume, the volume is a data protection destination volume.

In the case of a SnapVault secondary volume to disaster protection volume cascade, if the SnapVault secondary volume is lost, you can resume SnapVault protection by creating a direct relationship between the SnapVault primary volume and the disaster protection destination volume. You must make the disaster protection destination volume a SnapVault secondary volume to do this.

Steps

1. Break the data protection mirror relationship by using the `snapmirror break` command.
   
   The relationship is broken and the disaster protection volume becomes a read-write volume.

2. Delete the existing data protection mirror relationship, if one exists, by using the `snapmirror delete` command.

3. Remove the relationship information from the source Vserver by using the `snapmirror release` command.
   
   This also deletes the Data ONTAP created Snapshot copies from the source volume.

4. Create a SnapVault relationship between the primary volume and the read-write volume by using the `snapmirror create` command with the `-type XDP` parameter.

5. Convert the destination volume from a read-write volume to a SnapVault volume and establish the SnapVault relationship by using the `snapmirror resync` command.
Managing backup and restore operations for SnapVault backups

You configure SnapVault relationships on FlexVol volumes to establish SnapVault backups. You manage SnapVault relationships to optimize the performance of the relationships.

Backing up from a Snapshot copy that is older than the base Snapshot copy

You might want to replicate a special, manually initiated Snapshot copy to the SnapVault backup. The Snapshot copy is one that is not in the sequence scheduled by the SnapVault policy assigned to the SnapVault relationship.

Before you begin

You must have cluster administrator privileges to perform this task for a cluster. You must have Vserver administrator privileges to perform this task for a Vserver.

Step

1. Begin the backup transfer of the older Snapshot copy by using the `snapmirror update` command.

   Example

   The following command starts an out-of-order transfer of Snapshot copy SC3 from the source volume `srcvolA` on Vserver `vserverA` and the secondary volume `dstvolB` on Vserver `vserverB`:

   ```
   vserverA::> snapmirror update -source-path vserverA:srcvolA -destination-path vserverB:dstvolB -snapshot SC3
   ```

   Result

   After the backup finishes, the transferred Snapshot copy becomes the base.

How an out-of-order Snapshot copy transfer works

The transfer of a Snapshot copy that does not conform to the usual sequence scheduled by a SnapVault policy is an out-of-order Snapshot copy transfer.

In SnapVault relationships, Snapshot copies are selected and transferred from the primary volume to the secondary volume, according to the configured SnapVault policy. Only Snapshot copies that are newer than the common Snapshot copy between the primary and secondary volume are transferred. However, you can use the `snapmirror update` command to initiate the transfer of a Snapshot copy that was not originally selected and transferred.
When you initiate an out-of-order transfer, an older Snapshot copy is used to establish the base. To avoid subsequent transfers of Snapshot copies that already exist on the SnapVault secondary volume, the list of Snapshot copies that are selected for transfer in this update cycle are reconciled against the Snapshot copies that are already present on the secondary volume. Snapshot copies that are already present on the secondary volume are discarded from the transfer list.

**Example of a new base that is established from an out-of-order Snapshot copy transfer**

In this example, the SnapVault policy has a schedule in which only the even-numbered Snapshot copies on the primary volume are transferred to the secondary volume. Before the out-of-order transfer begins, the primary volume contains Snapshot copies 2 through 6; the secondary volume contains only the even-numbered Snapshot copies (noted as “SC” in the figures). Snapshot copy 4 is the common Snapshot copy that is used to establish the base, as shown in the following figure:

After Snapshot copy 3 is transferred to the secondary volume, out of order, it becomes the new common Snapshot copy that is used to establish the base, as shown in the following figure:
Note: Although Snapshot copy 3 is now the base, the exported Snapshot copy is still Snapshot copy 4.

When Snapshot copies are selected for subsequent updates according to the SnapVault policy, the policy selects Snapshot copy 4 and Snapshot copy 6 for transfer to the secondary volume. When the transfer list is reconciled, Snapshot copy 4 is removed from the transfer list because it already exists on the secondary volume. Only Snapshot copy 6 is transferred, which becomes the new common Snapshot copy that is used to establish the base, as shown in the following figure:
Backing up FlexVol volumes that contain the maximum limit of Snapshot copies

To work around the limit of 251 Snapshot copies per volume, you can create a new destination volume clone, then establish a SnapVault relationship with the new clone.

Before you begin

You must have cluster administrator privileges to perform this task for a cluster. You must have Vserver administrator privileges to perform this task for a Vserver.

About this task

Creating a new SnapVault relationship to a new volume clone enables you to continue SnapVault protection with minimum disruption on the clone volume and without starting a new baseline transfer. Because the source clone and the volume clone share the latest common Snapshot copy, subsequent updates are performed as usual, according to the policy assigned to the SnapVault relationship.

Steps

1. Quiesce the SnapVault relationship between the primary volume and the secondary volume by using the `snapmirror quiesce` command.
   This step prevents updates from starting until after the task is complete.

2. Verify that there are no active transfers on the relationship by using the `snapmirror show` command.
   The Relationships field should be Idle.

3. Create a volume clone based on the most recent common Snapshot copy between the SnapVault primary volume and the SnapVault secondary volume by using the `volume clone create` command with the `-type DP` parameter.

4. Establish the SnapVault relationship between the primary volume and the newly created secondary volume clone by using the `snapmirror resync` command and the `-type XDP` parameter.

5. Delete the SnapVault relationship between the primary volume and the original SnapVault secondary volume by using the `snapmirror delete` command.
Managing the backup of a copied source volume

If you use the volume copy command to copy the primary volume of a SnapVault relationship to a different volume, Data ONTAP does not copy SnapMirror labels for Snapshot copies, and you lose the capability to back up from the primary volume copy.

About this task

You must add the SnapMirror labels back before you can back up the volume copy.

Step

1. Add the SnapMirror labels to the copied volume by using the volume snapshot modify command or by using the snapmirror update -s command.

Guidelines for restoring the active file system

The restore operation from a SnapVault backup copies a single, specified Snapshot copy from a SnapVault secondary volume to a specified volume. Restoring a volume from a SnapVault secondary volume changes the view of the active file system but preserves all earlier Snapshot copies in the SnapVault backup.

Before restoring a volume, you must shut down any application that accesses data in a volume to which a restore is writing data. Therefore, you must dismount the file system, shut down any database, and deactivate and quiesce the Logical Volume Manager (LVM) if you are using an LVM.

The restore operation is disruptive. When the restore operation finishes, the cluster administrator or Vserver administrator must remount the volume and restart all applications that use the volume.

The restore destination volume must not be the destination of another mirror or the secondary of another SnapVault relationship.

You can restore to the following volumes:

- Original source volume
  You can restore from a SnapVault secondary volume back to the original SnapVault primary volume.
- New, empty secondary volume
  You can restore from a SnapVault secondary volume to a new, empty secondary volume. You must first create the volume as a data protection (DP) volume.
- New secondary that already contains data
  You can restore from a SnapVault secondary volume to a volume that is prepopulated with data. The volume must have a Snapshot copy in common with the restore primary volume and must not be a DP volume.

Guidelines for restoring LUNs in SAN environments

The restore operation from a SnapVault backup copies a single, specified LUN from a SnapVault secondary volume to a specified volume. Restoring a LUN from a SnapVault secondary volume
changes the view of the active system on the volume to which data is being restored, preserving all earlier Snapshot copies.

The following guidelines apply only to SAN environments:

- You can restore a single file or single LUN from a SnapVault secondary volume by using the NetApp OnCommand management software online management tools.
- When LUNs are restored to existing LUNs, new access controls do not need to be configured. You must configure new access controls for the restored LUNs only when restoring LUNs as newly created LUNs on the volume.
- If LUNs on the SnapVault secondary volume are online and mapped before the restore operation begins, they remain so for the duration of the restore operation and after the operation finishes.
- The host system can discover the LUNs and issue non-media access commands for the LUNs, such as inquiries or commands to set persistent reservations, while the restore operation is in progress.
- You cannot create new LUNs in a volume during a restore operation with the `lun create` command.
- Restore operations from tape and from a SnapVault backup are identical.
- You cannot restore a single LUN from a SnapVault secondary volume that is located on a system that is running in 7-Mode.

For more information about backing up and restoring data in a SAN environment, see the *Clustered Data ONTAP SAN Administration Guide*.

**How restore operations work from a SnapVault backup**

A restore operation from a SnapVault backup consists of a series of actions performed on a temporary restore relationship and on the secondary volume.

During a restore operation, the following actions occur:

1. A new temporary relationship is created from the restore source (which is the original SnapVault relationship secondary volume) to the restore destination. The temporary relationship is a restore type (RST). The `snapmirror show` command displays the RST type while the restore operation is in progress. The restore destination might be the original SnapVault primary or might be a new SnapVault secondary.

2. During the restore process, the restore destination volume is changed to read-only.

3. When the restore operation finishes, the temporary relationship is removed and the restore destination volume is changed to read-write.
Restoring a volume from a SnapVault backup

If the data on a volume becomes unavailable, you can restore the volume to a specific time by copying a Snapshot copy in the SnapVault backup. You can restore data to the same primary volume or to a new location. This is a disruptive operation.

Before you begin

- You must have cluster administrator privileges to perform this task for a cluster.
- You must have Vserver administrator privileges to perform this task for a Vserver.
- CIFS traffic must not be running on the SnapVault primary volume when a restore operation is running.

About this task

This task describes how to restore a whole volume from a SnapVault backup. To restore a single file or LUN, you can restore the whole volume to a different, non-primary volume, and then select the file or LUN, or you can use the NetApp OnCommand management software online management tools.

Steps

1. If the volume to which you are restoring has compression enabled and the secondary volume from which you are restoring does not have compression enabled, disable compression.
   
   You disable compression to retain storage efficiency during the restore.

2. Restore a volume by using the `snapmirror restore` command.

   Example

   ```
   vs1::> snapmirror restore -destination-path vs1:vol1
   vs1:vol1
   -source-path vs2:vol1_dp_mirror2 -source-snapshot snap3
   Warning: All data newer than Snapshot copy snap6 on volume vs1:vol1
   will be deleted.
   Do you want to continue? {y|n}:
   y
   [Job 34] Job is queued: snapmirror restore from source vs2:vol1_dp_mirror2 for the snapshot snap3.
   ```

   For more information about the `snapmirror restore` command, see the man pages.

3. Remount the restored volume and restart all applications that use the volume.

4. If you previously disabled compression, reenable compression on the volume.
Managing a SnapVault-mirror cascade when the SnapVault backup is unavailable

You can manipulate relationships in a SnapVault-mirror cascade to maintain data backup relationships if the secondary of the SnapVault relationship becomes unavailable.

Before you begin

You must have a SnapVault-mirror cascade already configured.

About this task

The destination of the SnapVault relationship is the middle of the SnapVault-mirror cascade. If it becomes unavailable, you might have the following issues:

• You cannot update the SnapVault backup.
• You cannot update the mirror copy of the SnapVault secondary.

To manage this issue, you can temporarily remove the SnapVault secondary volume from the cascade and establish a SnapVault relationship to the mirror copy of the SnapVault secondary volume. When the unavailable secondary volume becomes available, you can reestablish the original cascade configuration.

In the following steps, the primary volume of the cascade is called “A”, the secondary volume of the SnapVault relationship is called “B”, and the destination volume of the data protection mirror relationship is called “C”.

Steps

1. Identify the current exported Snapshot copy on C by using the `volume snapshot show` command with the `-fields busy` parameter.
   
   The busy field is set to true for the exported Snapshot copy.

   **Example**
   
   `volume snapshot show C -fields busy`

2. Break the data protection mirror relationship by using the `snapmirror break` command on C.

   **Example**
   
   `snapmirror break C`
3. Create a dummy snapmirror-label on the exported Snapshot copy you previously identified by using the `volume snapshot modify` command with the `-snapmirror-label` parameter.

If a snapmirror-label already exists for the exported Snapshot copy, you do not need to perform this step.

**Example**
```
volume snapshot modify -volume C -snapshot name -snapmirror-label exp1
```

4. Create a Snapshot owner on the exported Snapshot copy of C by using the `snapmirror snapshot-owner create` command.

This prevents clustered Data ONTAP from deleting the Snapshot copy.

**Example**
```
snapmirror snapshot-owner create -volume C -snapshot exported -owner admin1
```

5. Delete the data protection mirror relationship between B and C by using the `snapmirror delete` command.

**Example**
```
snapmirror delete C
```

6. Create the SnapVault relationship between A and C by using the `snapmirror resync` command and the `-type XDP` parameter.

**Example**
```
snapmirror resync -source-path A -destination-path C -type XDP
```

You can maintain this SnapVault relationship until you recover the original SnapVault secondary volume. At that time, you can reestablish the original cascade relationship by using the steps that follow this step.

7. Delete the data protection mirror relationship between A and B by using the `snapmirror delete` command.

8. Perform a disaster recovery resynchronization from C to B by using the `snapmirror resync` command.

**Example**
```
snapmirror resync -source-path C -destination-path B
```

This step copies from C to B, all of the Snapshot copies made after B became unavailable.

9. Identify the current exported Snapshot copy on B by using the `volume snapshot show` command with the `-fields busy` parameter.
Example

```
volume snapshot show B -fields busy
```

The *busy* field is set to *true* for the exported Snapshot copy.

10. Break the data protection mirror relationship by using the `snapmirror break` command on B.

Example

```
snapmirror break B
```

11. Create a dummy snapmirror-label on the exported Snapshot copy you previously identified by using the `volume snapshot modify` command with the `-snapmirror-label` parameter.

Example

```
volume snapshot modify -volume B -snapshot name -snapmirror-label exp2
```

If a snapmirror-label already exists for the exported Snapshot copy, you do not need to perform this step.

12. Create a Snapshot owner on the exported Snapshot copy of B by using the `snapmirror snapshot-owner create` command.

This prevents clustered Data ONTAP from deleting the Snapshot copy.

Example

```
snapmirror snapshot-owner create -volume B -snapshot exported -owner admin1
```

13. Delete the data protection mirror relationship between C and B by using the `snapmirror delete` command.

14. Perform a SnapVault resynchronization from A to B by using the `snapmirror resync` command and the `-type XDP` parameter.

Example

```
snapmirror resync -source-path A -destination-path B -type XDP
```

New Snapshot copies that meet the Snapshot policy of the SnapVault relationship are transferred from A to B.

15. Delete the data protection mirror relationship between A and C by using the `snapmirror delete` command.

16. Perform a disaster recovery resynchronization from B to C by using the `snapmirror resync` command.

This step copies from B to C, all of the Snapshot copies made after reestabishing the A to B relationship without deleting any Snapshot copies on C.
Example

`snapmirror resync -source-path B -destination-path C`

17. Remove the Snapshot copy owner from volumes B and C by using the `snapmirror snapshot-owner delete` command.

Example

`snapmirror snapshot-owner delete -volume B -snapshot exported_snap`

18. Remove SnapMirror labels that you created from volumes B and C by using the `snapshot modify` command.

Example

`snapshot modify -volume B -snapshot exported_snap -snapmirror-label text`

Example

`snapshot modify -volume C -snapshot exported_snap -snapmirror-label text`

Managing storage efficiency for SnapVault secondaries

SnapVault relationships preserve storage efficiency when backing up data from the primary volume to the secondary volume, with one exception: if post-process and optionally inline compression are enabled on the secondary volume, storage efficiency is not preserved for data transfers between the primary and secondary volumes.

Guidelines for managing storage efficiency for SnapVault backups

If both the primary and secondary volumes in a SnapVault relationship have storage efficiency enabled, then data transfers to the SnapVault secondary volume preserve storage efficiency. If the primary volume does not have storage efficiency enabled, you might want to enable storage efficiency only on the secondary volume.

Because SnapVault secondary volumes typically contain a large amount of data, storage efficiency on SnapVault secondary volumes can be very important.

If storage efficiency is enabled on the primary volumes

If the primary volume in a SnapVault relationship is enabled for storage efficiency, all data backup operations preserve the storage efficiency.

If storage efficiency is enabled only on the secondary volume

If the primary volume in a SnapVault relationship does not have storage efficiency enabled, you might want to enable storage efficiency for the secondary volume because it is likely to contain a large amount of data over time.
You can use the `volume efficiency` command to start a scan on the volume if there is already data on the volume from transfers. If this is a new relationship with no transfers, then there is no need to run the scan manually.

Changes to the volume's efficiency schedule do not take effect for a SnapVault secondary volume. Instead, when storage efficiency is enabled, the SnapVault relationship manages the schedule. When a data transfer begins, the storage efficiency process automatically pauses until the transfer is finished, and then automatically begins again after the data transfer is complete. Because data transfers to a SnapVault secondary volume might include more than one Snapshot copy, the storage efficiency process is paused for the entire duration of the update operation. After the transfer is finished and the post-transfer storage efficiency process is complete, the last Snapshot copy created in the secondary volume is replaced by a new, storage-efficient Snapshot copy.

If the last Snapshot copy that is created in the secondary volume is locked before it can be replaced by a new, storage-efficient Snapshot copy, then a new, storage-efficient Snapshot copy is still created, but the locked Snapshot copy is not deleted. That Snapshot copy is deleted later during the storage-efficient cleanup process after a subsequent update to the SnapVault secondary volume and after the lock is released. A Snapshot copy in a SnapVault secondary volume might be locked because the volume is the source in another relationship, such as a data protection mirror relationship.

**If the secondary volume has additional compression enabled, storage efficiency is not preserved**

Storage efficiency on all data transfers in SnapVault relationships is not preserved when the secondary volume has additional compression enabled. Because of the loss of storage efficiency, a warning message is displayed when you enable compression on a SnapVault secondary volume. After you enable compression on the secondary volume, you can never have storage-efficient transfers.

**Related tasks**

`Enabling storage efficiency on a SnapVault secondary volume` on page 108

**Enabling storage efficiency on a SnapVault secondary volume**

If the primary volume does not have storage efficiency enabled, you can enable storage efficiency on a SnapVault secondary volume by enabling storage efficiency on the volume.

**Before you begin**

You must have cluster administrator privileges to perform this task for a cluster. You must have Vserver administrator privileges to perform this task for a Vserver.

**About this task**

For information about increasing storage efficiency using deduplication and compression, see the *Clustered Data ONTAP Logical Storage Management Guide*. 
Steps

1. Use the `volume efficiency` command with the `-on` parameter to enable storage efficiency.

2. If the volume already has data which you want to make storage efficient, use the `volume efficiency` command with the `-start` and `-scan-old-data` parameters to start a scan of the volume.

Related concepts

*Guidelines for managing storage efficiency for SnapVault backups* on page 107
Providing disaster recovery on Infinite Volumes using mirroring technology

Stored data is susceptible to disaster, either through hardware failure or environmental catastrophe. You can use mirroring technology on Infinite Volumes to create an identical second set of data to replace the primary set of data, in case something happens to the primary set of data.

Aggregate requirements for Infinite Volumes in a data protection mirror relationship

Before you create a destination Infinite Volume, you must create enough aggregate space in the destination cluster for the destination Infinite Volume to use.

An Infinite Volume spans several aggregates, and aggregates are automatically selected for a destination Infinite Volume when you initialize a data protection mirror relationship. If the data protection mirror relationship cannot be initialized because of insufficient aggregate space, you receive an error message that informs you how to adjust aggregate space before trying the operation again.

You should use the following guidelines to create aggregates for destination Infinite Volumes:

- The destination Infinite Volume and source Infinite Volume should have the same number of aggregates.
  For example, if the source Infinite Volume uses four aggregates, you should create four aggregates for the destination Infinite Volume. The same number of aggregates for the source and destination Infinite Volumes is recommended, but not required. The key requirement is that aggregates associated with a destination Infinite Volume have enough space to contain a mirror copy of the source Infinite Volume.
- The aggregates for the destination Infinite Volume must have enough space to contain a mirror copy of the source Infinite Volume.
  You should compare the sizes in KB.

Note: The size of the destination Infinite Volume must be equal to or larger than the size of the source Infinite Volume to successfully create a data protection mirror relationship.

Related concepts

How Data ONTAP selects aggregates for data protection of Infinite Volumes on page 151
Error messages and solutions for failed aggregate selection for destination Infinite Volumes on page 158
Constituent size requirements for setting up data protection mirror relationships for Infinite Volumes

When the source and destination Infinite Volumes are on platforms that support different maximum data constituent sizes, you must know the maximum data constituent sizes for the different platforms to successfully set up a data protection mirror relationship for Infinite Volumes.

The maximum data constituent size for an Infinite Volume corresponds to the maximum FlexVol volume size for the platform. You must correctly set the maximum data constituent size when you create the source and the destination Infinite Volumes. For example, if you want to create a data protection mirror relationship between a source Infinite Volume on a platform with a large data constituent size and a destination Infinite Volume on a platform with a small data constituent size, the size of the constituents in the source and destination Infinite Volumes are restricted to the smaller maximum data constituent size. You must set the maximum data constituent size for the source and destination Infinite Volumes to be the size of the smaller maximum data constituent size for the two platforms.

You should set the maximum data constituent size when you create the source and destination Infinite Volumes. You can modify the maximum data constituent size for an Infinite Volume. However, you cannot use the setting to shrink the size of existing data constituents. If the current data constituent size is larger than the size that you want to specify, the setting cannot shrink the existing data constituents to the smaller size.

For information about the maximum FlexVol volume size for each platform, see the Hardware Universe.

Related references

- Size exceeds maximum (namespace constituent) on page 159
- Size exceeds maximum (data constituents) on page 160

Creating a data protection mirror copy for an Infinite Volume with dedicated aggregates

When source and destination Infinite Volumes do not share aggregates with other Infinite Volumes or FlexVol volumes in the same cluster, you can create the same number and size of aggregates for the destination volume as are used by the source volume before you create a data protection mirror relationship.

About this task

Cluster administrators can perform all data protection tasks, and Vserver administrators can perform only the following data protection tasks:
Creating destination Infinite Volumes
Creating and initializing data protection mirror relationships

This workflow applies only to an Infinite Volume without storage classes. If you want to create a data protection mirror copy of an Infinite Volume with storage classes, you cannot use the command-line interface; you must use OnCommand Workflow Automation instead.

Steps
1. Identifying the size of a source Infinite Volume and aggregate details on page 112
2. Creating dedicated aggregates for a destination cluster (cluster administrators only) on page 114
3. Creating a Vserver with Infinite Volume in a destination cluster (cluster administrators only) on page 115
4. Assigning aggregates for all Vservers in a cluster (cluster administrators only) on page 116
5. Creating cluster and Vserver peer relationships (cluster administrators only) on page 117
6. Creating a destination Infinite Volume on page 117
7. Creating and initializing a data protection mirror relationship on page 118

Related tasks
Creating a data protection mirror copy for an Infinite Volume with storage classes on page 164

Identifying the size of a source Infinite Volume and aggregate details

You must identify the size of the source Infinite Volume to create a destination Infinite Volume of the same size or bigger. You must also identify the number and size of aggregates used by the source volume to create the same number and size of aggregates for the destination volume.

Steps
1. Identify the size of the source Infinite Volume by using the volume show command.
   The destination Infinite Volume must be equal to or larger than the size of the source Infinite Volume.

   Example
   The following command shows that the source volume repo_vol is 2 GB in size:

```
cluster1::> volume show -volume repo_vol
Vserver  Volume  Aggregate  State  Type  Size  Available  Used%
-----------  --------  ---------  -----  ----  ------  ---------  -----
vs0        repo_vol  -        online  RW    2GB    1.90GB    5%
```

2. Identify the number of aggregates the source Infinite Volume uses by using the volume show command with the -is-constituent parameter.
   The destination Infinite Volume should have the same number of aggregates.
Example

The following command shows that the source volume repo_vol uses four aggregates: aggr1, aggr2, aggr3, and vs_aggr:

```
cluster1::> volume show -is-constituent true

Vserver       Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- ----- 
vs0          repo_vol_1024_data0001 aggr1 online  RW        384MB    364.6MB    5%     
vs0          repo_vol_1024_data0002 aggr2 online  RW        384MB    364.6MB    5%     
vs0          repo_vol_1024_data0003 aggr3 online  RW        384MB    364.6MB    5%     
vs0          repo_vol_1024_data0004 vs_aggr online  RW        384MB    364.6MB    5%     
6 entries were displayed.
```

3. Set units to KB by using the `set` command.

You must view aggregate sizes in KB to have the most accurate size information.

Example

```
cluster1::> set -units KB
```

4. Identify the size of each aggregate that the source Infinite Volume uses by using the `storage aggregate show` command.

The destination Infinite Volume should have the same number and size of aggregates as the source Infinite Volume.

Example

The following command shows that aggr1 is 1843200 KB, aggr2 is 1843200 KB, aggr3 is 1843200 KB, and vs_aggr is 1843200 KB in size:

```
cluster1::> storage aggregate show

Aggregate     Size     Available Used% State   #Vols  Nodes     RAID Status
---------     -------- --------- ----- ------- ------ --------- ------------ 
aggr0         921600KB  43664KB   95%  online    1    node2     raid_dp,
aggr0_node1_0 921600KB  43680KB   95%  online    1    node1     raid_dp,
aggr0_node3_0 921600KB  43680KB   95%  online    1    node3     raid_dp,
aggr0_node4_0 921600KB  43680KB   95%  online    1    node4     raid_dp,
aggr1         1843200KB 1180496KB 36%  online    2    node1     raid4,
aggr2         1843200KB 1180488KB 36%  online    2    node2     raid4,
aggr3         1843200KB 1446400KB 22%  online    1    node3     raid4,
vs_aggr       1843200KB 1425664KB 23%  online    2    node4     raid4,
8 entries were displayed.
```

Result

You have the following numbers that you require to create dedicated aggregates for the destination Infinite Volume:

- Size of the source Infinite Volume
Number of aggregates used by the source Infinite Volume
Size of each aggregate (in KB) used by the source Infinite Volume

Creating dedicated aggregates for a destination cluster (cluster administrators only)

You can create the same number of aggregates for the destination Infinite Volume as are used by the source Infinite Volume. The aggregates should be the same size or larger than the aggregates used by the source Infinite Volume.

Before you begin

- You must have cluster administrator privileges to perform this task.
- You must know the number and size of aggregate in KB used by the source Infinite Volume.

About this task

Aggregates are dedicated when only one Vserver in a cluster uses the aggregates. You use the aggregate list for a Vserver to control which aggregates a Vserver uses. For more information about creating aggregates, see the _Clustered Data ONTAP Physical Storage Management Guide_.

Step

1. On the destination cluster, create the same number of aggregates for the destination Infinite Volume as are used by the source Infinite Volume by using the `storage aggregate create` command.

   The aggregates for the destination cluster should be the same size or larger than the aggregates used for the source Infinite Volume. If you cannot create the same number and size of aggregates, ensure that the overall aggregate space for the destination Infinite Volume is large enough to fit a mirror copy of the source Infinite Volume.

After you finish

You must create a Vserver with Infinite Volume and modify its aggregate list to specify the aggregates to use. You must also ensure that aggregate lists for other Vservers in the cluster do not reference the dedicated aggregates.

Related information

_Documentation on the NetApp Support Site: support.netapp.com_
Creating a Vserver with Infinite Volume in a destination cluster (cluster administrators only)

You must create a Vserver with Infinite Volume in the destination cluster and specify an aggregate list for the Vserver with Infinite Volume to control how volumes in the cluster use the aggregates.

Before you begin

- You must have cluster administrator privileges to perform this task.
- You must have created aggregates in the destination cluster to specify in the aggregate list for the destination Vserver with Infinite Volume.

About this task

Each Vserver name in all the clusters should be unique because you can set up Vserver peer relationships only between Vservers with unique names. You should use a fully qualified domain name for each Vserver.

Steps

1. On the destination cluster, create a Vserver with Infinite Volume by using the `vserver create` command with the `-is-repository` parameter.

   **Example**

   In the following example, a Vserver with Infinite Volume named vs0_dest is created:

   ```bash
   cluster2::> vserver create -vserver vs0_dest -rootvolume root_vs0 -aggregate aggr1 -ns-switch file -rootvolume-security-style mixed -is-repository true
   ```

2. Modify the Vserver with Infinite Volume to specify the aggregate list by using the `vserver modify` command with the `-aggr-list` parameter:

   **Example**

   In the following example, a Vserver with Infinite Volume named vs0_dest is modified to specify aggr1, aggr2, aggr3, and vs_aggr in the aggregate list for the Vserver:

   ```bash
   cluster2::> vserver modify -vserver vs0_dest -aggr-list aggr1,aggr2,aggr3,vs_aggr
   ```

Result

A Vserver with Infinite Volume is created in the cluster, and the aggregate list specifies which aggregates to use.
Assigning aggregates for all Vservers in a cluster (cluster administrators only)

You can ensure that no other Vservers use the aggregates that you want to dedicate to an Infinite Volume by specifying the aggregate lists for all Vservers in the cluster. If the aggregate list of a Vserver is not specified, the Vserver might potentially use the aggregates that you want to dedicate to the Infinite Volume.

About this task

This procedure applies when the cluster already contains Vservers. If the cluster does not yet contain any Vservers, you can skip this procedure.

Steps

1. For each Vserver in the cluster, specify the aggregates that will be used by the Vserver by using `vserver modify` command with the `-aggr-list` parameter.

   **Example**
   
   The following command assigns the aggregates aggr1 and aggr4 to the Vserver vs1, ensuring that any new FlexVol volumes created on the Vserver vs1 can be created only on the aggregates aggr1 or aggr4:
   
   ```
   cluster::> vserver modify -vserver vs1 -aggr-list aggr1,aggr4
   ```

2. Verify that all the data Vservers in the cluster have a specified aggregate list by using the `vserver show` command with the `-type data` and `-fields aggr-list,aggregate` parameters.

   A specified aggregate list contains the name of an aggregate. An unspecified aggregate list is displayed as a dash ("-").

   **Example**
   
   The following output displays one data Vserver with a specified aggregate list:
   
   ```
   cluster::> vserver show -type data -fields aggr-list,aggregate
   vserver aggregate aggr-list
   --------- ----------- -------------------------
   vs1  aggr1  aggr1,aggr4
   ```

After you finish

Make a note that each time that a Vserver is created in the future, its aggregates must be specified.
Creating cluster and Vserver peer relationships (cluster administrators only)

You must create a cluster peer relationship between the source and destination clusters and a Vserver peer relationship between the source and destination Vservers with Infinite Volume before you can create a data protection mirror relationship for two Infinite Volumes.

Before you begin

- You must have cluster administrator privileges to perform this task.
- The Vservers with Infinite Volume must have unique names.

About this task

You cannot create a Vserver peer relationship between a Vserver with FlexVol volume and a Vserver with Infinite Volume.

Steps

1. Create a cluster peer relationship between the source and destination clusters.

   For information about cluster peering, see the Clustered Data ONTAP System Administration Guide for Cluster Administrators.

2. Create a Vserver peer relationship between the Vserver with Infinite Volume in the source cluster and the Vserver with Infinite Volume in the destination cluster.

   For information about Vserver peering, see the Clustered Data ONTAP System Administration Guide for Cluster Administrators.

Related information

Documentation on the NetApp Support Site: support.netapp.com

Creating a destination Infinite Volume

You must create a destination Infinite Volume that is the same size as or bigger than the source Infinite Volume to create a data protection mirror relationship between the source and destination volumes.

Before you begin

- You must know the size of the source Infinite Volume.
- If you want to specify an aggregate for the namespace constituent, you must have advanced privilege.
Step

1. On the destination cluster in the Vserver with Infinite Volume, create a destination Infinite Volume with a type of DP by using the `volume create` command with the `-type` parameter.

Example

In the following example, a destination Infinite Volume named `repo_vol_dest` of 2 GB size is created:

```bash
cluster2::> volume create -vserver vs0_dest -volume repo_vol_dest -type dp -size 2GB
```

A destination Infinite Volume is created. However, constituents are not created yet.

After you finish

Create and initialize a data protection mirror relationship between the source and destination Infinite Volumes.

Creating and initializing a data protection mirror relationship

You must create and initialize the data protection mirror relationship between the source and destination Infinite Volumes to mirror all constituents from the source volume to the destination volume.

Before you begin

- A cluster peer relationship must exist between the source and destination clusters.
- A Vserver peer relationship must exist between the source and destination Vservers with Infinite Volume.
- A SnapMirror license must be installed on the source and destination clusters.

About this task

You can have cluster administrator or Vserver administrator privileges to perform this task. However, if you see an error message about insufficient aggregate space, you require cluster administrator privileges to add or modify aggregates.

The following illustration shows what constituents are mirrored from the source Infinite Volume to the destination Infinite Volume after you initialize the data protection mirror relationship. In this example, SnapDiff is disabled on the source and destination Infinite Volumes. Notice how the namespace mirror constituent from the source Infinite Volume is not mirrored to the destination Infinite Volume.
The following illustration shows what constituents are mirrored from the source Infinite Volume to the destination Infinite Volume after you initialize the data protection mirror relationship when SnapDiff is enabled on the source Infinite Volume. Notice how the namespace mirror constituents from the source Infinite Volume are not mirrored to the destination Infinite Volume.

The following illustration shows what constituents are mirrored from the source Infinite Volume to the destination Infinite Volume after you initialize the data protection mirror relationship when SnapDiff is enabled on the source Infinite Volume. Notice how the namespace mirror constituents from the source Infinite Volume are not mirrored to the destination Infinite Volume.
Steps

1. On the destination Infinite Volume, create a data protection mirror relationship between the source and destination Infinite Volumes by using the `snapmirror create` command.

   **Example**

   In the following example, a data protection mirror relationship is created between the destination Infinite Volume named `repo_vol_dest` and the source Infinite Volume named `repo_vol`:

   ```
   cluster2::> snapmirror create -destination-path vs0_dest:repo_vol_dest -source-path vs0:repo_vol -type DP
   ```

   A data protection mirror relationship is created between the two Infinite Volumes, but no constituents exist yet for the destination Infinite Volume.

2. On the destination Infinite Volume, initialize the data protection mirror relationship by using the `snapmirror initialize` command.

   **Example**

   In the following example, a data protection mirror relationship is initialized between the destination Infinite Volume named `repo_vol_dest` and the source Infinite Volume named `repo_vol`:

   ```
   cluster2::> snapmirror initialize -destination-path vs0_dest:repo_vol_dest
   ```

   Aggregates are automatically identified and evaluated for available space. If aggregates have enough space, the namespace constituent and all of the data constituents from the source Infinite Volume are mirrored to the destination Infinite Volume. If aggregates lack enough space, an error message is displayed, and the data protection mirror relationship is not initialized.

   **Note:** Namespace mirror constituents are not mirrored from the source to the destination Infinite Volume because they are intracluster data protection mirror copies for the source Infinite Volume.

3. You can view constituents in the destination Infinite Volume by using the `volume show` command with the `-is-constituent` parameter.

   In the following example, the destination Infinite Volume named `repo_vol_dest` contains four data constituents (`repo_vol_dest_1024_data0001`, `repo_vol_dest_1024_data0002`, `repo_vol_dest_1024_data0003`, and `repo_vol_dest_1024_data0004`) and one namespace constituent (`repo_vol_dest_ns`) after the data protection mirror relationship is initialized:

   ```
   cluster2::> volume show -is-constituent true
   ```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Volume</th>
<th>Aggregate</th>
<th>State</th>
<th>Type</th>
<th>Size</th>
<th>Available</th>
<th>Used%</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs0_dest</td>
<td>repo_vol_dest_1024_data0001</td>
<td>aggr3</td>
<td>online</td>
<td>DP</td>
<td>384MB</td>
<td>364.7MB</td>
<td>5%</td>
</tr>
<tr>
<td>vs0_dest</td>
<td>repo_vol_dest_1024_data0002</td>
<td>vs_aggr</td>
<td>online</td>
<td>DP</td>
<td>384MB</td>
<td>364.7MB</td>
<td>5%</td>
</tr>
<tr>
<td>vs0_dest</td>
<td>repo_vol_dest_1024_data0003</td>
<td>aggr2</td>
<td>online</td>
<td>DP</td>
<td>384MB</td>
<td>364.7MB</td>
<td>5%</td>
</tr>
<tr>
<td>vs0_dest</td>
<td>repo_vol_dest_1024_data0004</td>
<td>aggr1</td>
<td>online</td>
<td>DP</td>
<td>384MB</td>
<td>364.7MB</td>
<td>5%</td>
</tr>
</tbody>
</table>
Creating a data protection mirror copy for an Infinite Volume with shared aggregates

When source and destination Infinite Volumes share aggregates with other Infinite Volumes or FlexVol volumes in the same cluster, you must ensure that enough shared aggregate space is available for the destination Infinite Volume before you create a data protection mirror relationship.

About this task
Cluster administrators can perform all data protection tasks, and Vserver administrators can perform only the following data protection tasks:

- Creating destination Infinite Volumes
- Creating and initializing data protection mirror relationships

This workflow applies only to an Infinite Volume without storage classes. If you want to create a data protection mirror copy of an Infinite Volume with storage classes, you cannot use the command-line interface; you must use OnCommand Workflow Automation instead.

Steps

1. Identifying the size of a source Infinite Volume and constituent details on page 122
2. Verifying aggregate space in a destination cluster (cluster administrators only) on page 123
3. Creating a Vserver with Infinite Volume in a destination cluster (cluster administrators only) on page 125
4. Creating cluster and Vserver peer relationships (cluster administrators only) on page 126
5. Creating a destination Infinite Volume on page 127
6. Creating and initializing a data protection mirror relationship on page 127

Related tasks

Creating a data protection mirror copy for an Infinite Volume with storage classes on page 164
Identifying the size of a source Infinite Volume and constituent details

You must identify the size of the source Infinite Volume to create a destination Infinite Volume that is the same size as or larger than the source volume. You must also identify the size of constituents in the source volume to help identify the aggregate space that is required for the destination volume.

About this task

Each source Infinite Volume has one namespace constituent, and its default maximum size is 10 TB.

Steps

1. Identify the size of the source Infinite Volume by using the `volume show` command:

   The destination Infinite Volume must be equal to or larger in size than the source Infinite Volume.

   **Example**

   In the following example, the source volume is named repo_vol, and it is 2 GB in size:

   ```
   cluster1::> volume show -volume repo_vol
   Vserver   Volume       Aggregate    State      Type       Size  Available Used%
    --------- ------------ ------------ ---------- ---- ---------- ---------- ----- 
    vs0       repo_vol     -            online     RW          2GB     1.90GB    5% 
   ```

2. Identify how many data constituents exist in the source Infinite Volume by using the `volume show` command with the `-is-constituent` parameter.

   **Example**

   In the following example, the volume named repo_vol has four data constituents named `repo_vol_1024_data0001`, `repo_vol_1024_data0002`, `repo_vol_1024_data0003`, and `repo_vol_1024_data0004`:

   ```
   cluster1::> volume show -is-constituent true
   Vserver Volume                 Aggregate State  Type    Size   Available Used%
    ------- ------------           --------- ------ ------- ------ --------- ----- 
    vs0     repo_vol_1024_data0001 aggr1     online RW   384MB  364.7MB    5% 
    vs0     repo_vol_1024_data0002 aggr2     online RW   384MB  364.7MB    5% 
    vs0     repo_vol_1024_data0003 aggr3     online RW   384MB  364.7MB    5% 
    vs0     repo_vol_1024_data0004 vs_aggr   online RW   384MB  364.7MB    5% 
    vs0     repo_vol_ns            aggr1     online RW   256MB  243.0MB    5% 
    vs0     repo_vol_ns_mirror0001 aggr2     online DP   256MB  243.1MB    5% 
    6 entries were displayed. 
   ```

3. Identify the maximum data constituent size for the source Infinite Volume:

   a) Identify the smallest system for the nodes that the source Infinite Volume spans.
For example, if the source Infinite Volume spans a node for a 6280 system and a node for a 3270 system, the 3270 system is the smaller system.

b) Identify either the 64-bit maximum FlexVol volume size or the maximum data constituent size for the smaller system by using the *Hardware Universe*.

4. Identify the overall aggregate space required for all of the data constituents in the source Infinite Volume by multiplying the number of data constituents by the maximum FlexVol volume size.

**Example**

For example, if the source Infinite Volume has four data constituents, and the maximum FlexVol volume size is 40 TB, you require 160 TB of available space on the destination Infinite Volume for mirror copies of the data constituents.

**Result**

You have the following numbers that you require to create shared aggregates for the destination Infinite Volume:

- Size of the source Infinite Volume
- Aggregate space required for a mirror copy of the namespace constituent
  The aggregate space required for a mirror copy of the namespace constituent is based on the default maximum size, which is 10 TB.
- Aggregate space required for mirror copies of all data constituents
  The aggregate space required for mirror copies of the data constituents is the number of data constituents multiplied by the maximum data constituent size for the source Infinite Volume.

**Note:** Namespace mirror constituents are not mirrored to the destination Infinite Volume. You do not have to identify information about namespace mirror constituents.

**Related information**

*Documentation on the NetApp Support Site: support.netapp.com*

**Verifying aggregate space in a destination cluster (cluster administrators only)**

When an Infinite Volume shares aggregates with other volumes in the cluster, you must have enough available aggregate space in the destination cluster to create a data protection mirror copy of the source Infinite Volume.

**Before you begin**

- You must have cluster administrator privileges to perform this task.
- You must know the following information about the source Infinite Volume:
  - Size of the Infinite Volume
  - Aggregate space required for a mirror copy of the namespace constituent
• Aggregate space required for mirror copies of all of the data constituents

Steps

1. Set units to KB by using the `set` command.

   You must view aggregate sizes in KB to have the most accurate size information.

   **Example**

   The following command sets the unit to KB:

   ```
   cluster1::> set -units KB
   ```

2. On the destination cluster, view the available aggregate space by using the `storage aggregate show-space` command.

   The space available in the aggregates must be large enough to fit the following items:

   • The size of the source Infinite Volume
   • A mirror copy of the namespace constituent from the source Infinite Volume
   • Mirror copies of all of the data constituents from the source Infinite Volume

   **Note:** When you initialize the data protection mirror relationship, a mirror copy of the namespace constituent and each data constituent in the source Infinite Volume is transferred to the destination Infinite Volume. The size of each mirror copy reflects the current size of each constituent (not the maximum size of each constituent). For example, if the maximum constituent size for data constituents is 70 TB, but the current size of each data constituent is 40 TB, the size of each mirror copy of a data constituent is 40 TB, not 70 TB.

   **Example**

   The following example displays the available space for all aggregates in cluster1:

   ```
   cluster2::> storage aggregate show
   
   Aggregate    Size     Available  Used%  State   #Vols Nodes       RAID Status
   ---------     --------  ---------   ----- ------- ------ -------- ------------
   aggr0         921600KB  43664KB    95%  online    1    node2     raid_dp, normal
   aggr0_node1_0 921600KB  43680KB    95%  online    1    node1     raid_dp, normal
   aggr0_node3_0 921600KB  43680KB    95%  online    1    node3     raid_dp, normal
   aggr0_node4_0 921600KB  43680KB    95%  online    1    node4     raid_dp, normal
   aggr1         1843200KB 1180496KB  36%  online    2    node1     raid_dp, normal
   aggr2         1843200KB 1180488KB  36%  online    2    node2     raid_dp, normal
   aggr3         1843200KB 1446400KB  22%  online    1    node3     raid_dp, normal
   vs_aggr       1843200KB 1425664KB  23%  online    2    node4     raid_dp, normal
   ```
3. If more aggregate space is required in the destination cluster, add disks or aggregates to the cluster by using the `storage aggregate create` command.

For information about adding aggregates, see the *Clustered Data ONTAP Physical Storage Management Guide*.

**Result**

The available aggregate space in the destination cluster is large enough to fit a mirror copy of the source Infinite Volume.

### Creating a Vserver with Infinite Volume in a destination cluster (cluster administrators only)

You must create a Vserver with Infinite Volume in the destination cluster and specify an aggregate list for the Vserver with Infinite Volume to control how volumes in the cluster use the aggregates.

**Before you begin**

- You must have cluster administrator privileges to perform this task.
- You must have created aggregates in the destination cluster to specify in the aggregate list for the destination Vserver with Infinite Volume.

**About this task**

Each Vserver name in all the clusters should be unique because you can set up Vserver peer relationships only between Vservers with unique names. You should use a fully qualified domain name for each Vserver.

**Steps**

1. On the destination cluster, create a Vserver with Infinite Volume by using the `vserver create` command with the `-is-repository` parameter.

   **Example**

   In the following example, a Vserver with Infinite Volume named vs0_dest is created:

   ```bash
   cluster2::> vserver create -vserver vs0_dest -rootvolume root_vs0 -aggregate aggr1 -ns-switch file -rootvolume-security-style mixed -is-repository true
   ```

2. Modify the Vserver with Infinite Volume to specify the aggregate list by using the `vserver modify` command with the `-aggr-list` parameter:
Example
In the following example, a Vserver with Infinite Volume named vs0_dest is modified to specify aggr1, aggr2, aggr3, and vs_aggr in the aggregate list for the Vserver:

```shell
cluster2::> vserver modify -vserver vs0_dest -aggr-list aggr1,aggr2,aggr3,vs_aggr
```

Result
A Vserver with Infinite Volume is created in the cluster, and the aggregate list specifies which aggregates to use.

Creating cluster and Vserver peer relationships (cluster administrators only)
You must create a cluster peer relationship between the source and destination clusters and a Vserver peer relationship between the source and destination Vservers with Infinite Volume before you can create a data protection mirror relationship for two Infinite Volumes.

Before you begin
- You must have cluster administrator privileges to perform this task.
- The Vservers with Infinite Volume must have unique names.

About this task
You cannot create a Vserver peer relationship between a Vserver with FlexVol volume and a Vserver with Infinite Volume.

Steps
1. Create a cluster peer relationship between the source and destination clusters.
   For information about cluster peering, see the Clustered Data ONTAP System Administration Guide for Cluster Administrators.

2. Create a Vserver peer relationship between the Vserver with Infinite Volume in the source cluster and the Vserver with Infinite Volume in the destination cluster.
   For information about Vserver peering, see the Clustered Data ONTAP System Administration Guide for Cluster Administrators.

Related information
Documentation on the NetApp Support Site: support.netapp.com
Creating a destination Infinite Volume

You must create a destination Infinite Volume that is the same size as or bigger than the source
Infinite Volume to create a data protection mirror relationship between the source and destination
volumes.

Before you begin

- You must know the size of the source Infinite Volume.
- If you want to specify an aggregate for the namespace constituent, you must have advanced
  privilege.

Step

1. On the destination cluster in the Vserver with Infinite Volume, create a destination Infinite
   Volume with a type of DP by using the `volume create` command with the `-type` parameter.

   Example

   In the following example, a destination Infinite Volume named `repo_vol_dest` of 2 GB size is
   created:

   ```
   cluster2::> volume create -vserver vs0_dest -volume repo_vol_dest -type dp -size 2GB
   ```

   A destination Infinite Volume is created. However, constituents are not created yet.

   After you finish

   Create and initialize a data protection mirror relationship between the source and destination Infinite
   Volumes.

Creating and initializing a data protection mirror relationship

You must create and initialize the data protection mirror relationship between the source and
destination Infinite Volumes to mirror all constituents from the source volume to the destination
volume.

Before you begin

- A cluster peer relationship must exist between the source and destination clusters.
- A Vserver peer relationship must exist between the source and destination Vservers with Infinite
  Volume.
- A SnapMirror license must be installed on the source and destination clusters.
About this task

You can have cluster administrator or Vserver administrator privileges to perform this task. However, if you see an error message about insufficient aggregate space, you require cluster administrator privileges to add or modify aggregates.

The following illustration shows what constituents are mirrored from the source Infinite Volume to the destination Infinite Volume after you initialize the data protection mirror relationship. In this example, SnapDiff is disabled on the source and destination Infinite Volumes. Notice how the namespace mirror constituent from the source Infinite Volume is not mirrored to the destination Infinite Volume.

The following illustration shows what constituents are mirrored from the source Infinite Volume to the destination Infinite Volume after you initialize the data protection mirror relationship when SnapDiff is enabled on the source Infinite Volume. Notice how the namespace mirror constituents from the source Infinite Volume are not mirrored to the destination Infinite Volume.
Steps

1. On the destination Infinite Volume, create a data protection mirror relationship between the source and destination Infinite Volumes by using the `snapmirror create` command.

Example

In the following example, a data protection mirror relationship is created between the destination Infinite Volume named `repo_vol_dest` and the source Infinite Volume named `repo_vol`:

```
cluster2::> snapmirror create -destination-path vs0_dest:repo_vol_dest -source-path vs0:repo_vol -type DP
```

A data protection mirror relationship is created between the two Infinite Volumes, but no constituents exist yet for the destination Infinite Volume.

2. On the destination Infinite Volume, initialize the data protection mirror relationship by using the `snapmirror initialize` command.

Example

In the following example, a data protection mirror relationship is initialized between the destination Infinite Volume named `repo_vol_dest` and the source Infinite Volume named `repo_vol`:

```
cluster2::> snapmirror initialize -destination-path vs0_dest:repo_vol_dest
```
Aggregates are automatically identified and evaluated for available space. If aggregates have enough space, the namespace constituent and all of the data constituents from the source Infinite Volume are mirrored to the destination Infinite Volume. If aggregates lack enough space, an error message is displayed, and the data protection mirror relationship is not initialized.

**Note:** Namespace mirror constituents are not mirrored from the source to the destination Infinite Volume because they are intracluster data protection mirror copies for the source Infinite Volume.

3. You can view constituents in the destination Infinite Volume by using the `volume show` command with the `-is-constituent` parameter.

In the following example, the destination Infinite Volume named repo_vol_dest contains four data constituents (repo_vol_dest_1024_data0001, repo_vol_dest_1024_data0002, repo_vol_dest_1024_data0003, and repo_vol_dest_1024_data0004) and one namespace constituent (repo_vol_dest_ns) after the data protection mirror relationship is initialized:

```
cluster2::> volume show -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
vs0_dest  repo_vol_dest_1024_data0001 aggr3 online DP    384MB    364.7MB    5%
vs0_dest  repo_vol_dest_1024_data0002 vs_aggr online DP  384MB    364.7MB    5%
vs0_dest  repo_vol_dest_1024_data0003 aggr2 online DP    384MB    364.7MB    5%
vs0_dest  repo_vol_dest_1024_data0004 aggr1 online DP    384MB    364.7MB    5%
vs0_dest  repo_vol_dest_ns    aggr3    online     DP        256MB    243.1MB    5%
5 entries were displayed.
```

### Viewing information about Infinite Volumes

After you initialize a data protection mirror relationship for an Infinite Volume, you can view data protection information about the Infinite Volume. You can also view namespace mirror constituents in an Infinite Volume.

### When information is available about a destination Infinite Volume

Some information about a destination Infinite Volume is available only after constituents exist. Constituents exist on a destination Infinite Volume after you initialize a data protection mirror relationship between the source and destination Infinite Volumes.

The following table identifies the information that is displayed by some commands and parameters for a destination Infinite Volume before and after you initialize a data protection mirror relationship by using the `snapmirror initialize` command:
Before you initialize a data protection mirror relationship

<table>
<thead>
<tr>
<th>Command</th>
<th>Before you initialize a data protection mirror relationship</th>
<th>After you initialize a data protection mirror relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>volume show command with the <code>-state</code> parameter</td>
<td>Displays a temporary expected value</td>
<td>Displays the current value based on the setting for each constituent in the destination Infinite Volume. The current value can only be derived after constituents exist in the destination Infinite Volume.</td>
</tr>
<tr>
<td>volume show command with the <code>-space-guarantee</code> parameter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>volume show command with the <code>-language</code> parameter (requires advanced privilege)</td>
<td>Displays a dash (-)</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** For information about how thin and thick provisioning work on Infinite Volumes with storage classes, see the *Clustered Data ONTAP Logical Storage Management Guide.*

### Viewing constituents in an Infinite Volume

You can view constituents in an Infinite Volume to see the number of namespace mirror constituents or data constituents and the size of each constituent.

#### Step

1. View constituents in an Infinite Volume by using the `volume show` command with the `-is-constituent` parameter.

#### Example

In the following example, the Infinite Volume contains the following constituents:

- Data constituents named `repo_vol_1024_data0001`, `repo_vol_1024_data0002`, `repo_vol_1024_data0003`, and `repo_vol_1024_data0004`
- Namespace constituent named `repo_vol_ns`
- Namespace mirror constituent named `repo_vol_ns_mirror0001`

```
cluster1::> volume show -is-constituent true

Vserver  Volume          Aggregate  State   Type   Size  Available  Used%
--------- ---------------           --------  ------  ---- ----- ---------- ----
vs0       repo_vol_1024_data0001 aggr1  online  RW   384MB 364.7MB    5%
vs0       repo_vol_1024_data0002 aggr2  online  RW   384MB 364.7MB    5%
vs0       repo_vol_1024_data0003 aggr3  online  RW   384MB 364.7MB    5%
vs0       repo_vol_1024_data0004 vs_aggr online  RW   384MB 364.7MB    5%
vs0       repo_vol_ns            aggr1  online  RW   256MB 243.0MB    5%
vs0       repo_vol_ns_mirror0001 aggr2  online  DP   256MB 243.1MB    5%
6 entries were displayed.
```

### Related concepts

*What a namespace mirror constituent is* on page 147
Managing mirror relationships for Infinite Volumes

You can use the `snapmirror` commands to manage mirror relationships for Infinite Volumes. The commands are run as jobs.

Commands for managing SnapMirror relationships

There are Data ONTAP commands for managing SnapMirror relationships of FlexVol volumes and Infinite Volumes.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abort an active transfer. Use the <code>snapmirror show</code> command to determine the status of the abort operation. Note: Management tasks must be performed on the Infinite Volume and not its individual constituents.</td>
<td><code>snapmirror abort</code></td>
</tr>
<tr>
<td>Make a data protection mirror copy destination writable. This command must be used from the destination Vserver. When you use this command, the common Snapshot copy between your source and destination is not protected on your source and can be deleted. If you use this command, you should create your own Snapshot copy on the source that will not get auto-deleted and replicate it to the destination volume before breaking the relationship.</td>
<td><code>snapmirror break</code></td>
</tr>
<tr>
<td>Create a new data protection mirror relationship. This command must be used from the destination Vserver. Note: If you are using Infinite Volumes, you can create data protection mirror relationships between clusters only, not within a cluster.</td>
<td><code>snapmirror create</code></td>
</tr>
<tr>
<td>If you want to...</td>
<td>Use this command...</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Delete a data protection mirror relationship. This</td>
<td>snapmirror delete</td>
</tr>
<tr>
<td>command must be used from the destination Vserver.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> Management tasks must be performed on the</td>
<td></td>
</tr>
<tr>
<td>Infinite Volume and not its individual constituents.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Start a baseline transfer. This command must be</td>
<td>snapmirror initialize</td>
</tr>
<tr>
<td>used from the destination Vserver.</td>
<td></td>
</tr>
<tr>
<td>Display a list of data protection mirror relationships whose source endpoints are in the current Vserver.</td>
<td>snapmirror list-destinations</td>
</tr>
<tr>
<td>Modify a data protection mirror relationship. This</td>
<td>snapmirror modify</td>
</tr>
<tr>
<td>command must be used from the destination Vserver.</td>
<td></td>
</tr>
<tr>
<td>Display a list of data protection and load-sharing</td>
<td>snapmirror show</td>
</tr>
<tr>
<td>mirror relationships or display the state of a</td>
<td></td>
</tr>
<tr>
<td>scheduled transfer for a SnapMirror relationship.</td>
<td></td>
</tr>
<tr>
<td>The information that this command shows is updated</td>
<td></td>
</tr>
<tr>
<td>periodically; therefore, any changes to a relationship might not show immediately.</td>
<td></td>
</tr>
<tr>
<td>Disable future transfers for a mirror relationship.</td>
<td>snapmirror quiesce</td>
</tr>
<tr>
<td>This command must be used from the destination Vserver.</td>
<td></td>
</tr>
<tr>
<td>Enable future transfers for a mirror relationship.</td>
<td>snapmirror resume</td>
</tr>
<tr>
<td>This command must be used from the destination Vserver.</td>
<td></td>
</tr>
<tr>
<td>Start a resynchronize operation. This command</td>
<td>snapmirror resync</td>
</tr>
<tr>
<td>must be used from the destination Vserver.</td>
<td></td>
</tr>
<tr>
<td><strong>Attention:</strong> A resynchronize operation can cause</td>
<td></td>
</tr>
<tr>
<td>data loss on the destination volume because the</td>
<td></td>
</tr>
<tr>
<td>command can remove the exported Snapshot copy on the destination volume.</td>
<td></td>
</tr>
<tr>
<td>If you want to...</td>
<td>Use this command...</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| Add an owner to prevent premature deletion of a user created Snapshot copy for a SnapMirror mirror-to-SnapVault cascade configuration. A typical use case is to preserve an application-consistent Snapshot copy.  
**Note:** This task is not supported for Infinite Volumes. | `snapmirror snapshot-owner create` |
| Delete an owner used to preserve a user created Snapshot copy for a SnapMirror mirror-to-SnapVault cascade configuration.  
**Note:** This task is not supported for Infinite Volumes. | `snapmirror snapshot-owner delete` |
| Show all the Snapshot copies with owners that were added using the `snapmirror snapshot-owner create` command.  
**Note:** This task is not supported for Infinite Volumes. | `snapmirror snapshot-owner show` |
| Start an incremental transfer. This command must be used from the destination cluster.  
**Note:** If you are using Infinite Volumes, aggregate requirements must be met before performing the incremental transfer. Management tasks must be performed on the Infinite Volume and not its individual constituents.  
You can disregard error messages that result from updating a SnapMirror relationship from a Snapshot copy that exists on the destination volume. The message is for support use. | `snapmirror update` |
| Create a new policy for a data protection mirror relationship. | `snapmirror policy create` |
| Delete a policy of a data protection mirror relationship. | `snapmirror policy delete` |
| Add a new rule to a SnapVault relationship. | `snapmirror policy add-rule` |
If you want to... | Use this command...
---|---
Modify an existing rule in the policy of a SnapVault relationship. | `snapmirror policy modify-rule`
Modify a policy of a data protection mirror relationship. | `snapmirror policy modify`
Remove a rule from the policy of a data protection mirror relationship. | `snapmirror policy remove-rule`
Show the policy of a data protection mirror relationship. | `snapmirror policy show`
Copy data to a volume. | `snapmirror restore`
Note: This task is not supported for Infinite Volumes.
Remove the SnapMirror relationship information from the source Vserver. This command must be used from the source Vserver. | `snapmirror release`

See the man page for each command for more information.

**How commands are run on Infinite Volumes**

You must run most commands sequentially on an Infinite Volume to allow one job to complete before you start the next job. However, you can run the `snapshot delete` and the `snapmirror abort` commands simultaneously with other commands on Infinite Volumes.

When you run a command on an Infinite Volume, the Infinite Volume uses a job to run the command on all of the constituents that it contains. As a result, you only have to run Snapshot and SnapMirror commands on the Infinite Volume, not the individual constituents. Because the Infinite Volume takes each command, creates a job, and runs the command on all of its constituents, it can take some time for each command to complete the operation. If you try to run two commands on the same Infinite Volume, you can create a conflict that results in an error. To avoid conflicts, you must wait for each command to complete the operation before you run the next command.

However, you can run the following commands while other commands are running:

- `snapshot delete`
  You can run multiple `snapshot delete` commands at the same time, as long as the commands are not operating on the same Snapshot copy.
- `snapmirror abort`
  You can run a `snapmirror abort` command when another command is running, as long as you run the `snapmirror abort` command after you run the other command. If you run the `snapmirror abort` command first, you cannot run another command. The `snapmirror abort` command must complete its operation before you run the next command.
Managing disaster recovery for Infinite Volumes

When an Infinite Volume is in a data protection mirror relationship, you can use the SnapMirror commands on the Infinite Volume to recover the entire Infinite Volume and its constituents. However, you cannot use the SnapMirror commands on individual constituents in an Infinite Volume.

Related tasks

Retrieving data from Infinite Volumes with storage classes during disaster recovery on page 165

How the snapmirror resync command works for Infinite Volumes and constituents

You can use the `snapmirror resync` command on an Infinite Volume, and the system recovers the Infinite Volume and its constituents—including the namespace constituent and data constituents—from the destination Infinite Volume. However, you cannot use the `snapmirror resync` command on individual constituents.

**Note:** A data protection mirror relationship between two Infinite Volumes excludes the namespace mirror constituent. The namespace mirror constituent is an intracluster data protection mirror copy of the namespace constituent in an Infinite Volume. The data protection mirror relationship for the namespace constituent is in addition to and separate from the data protection mirror relationship for the Infinite Volume.

You can use the `snapmirror resync` command on the Infinite Volume to recover the entire volume and its constituents. When you use the `snapmirror resync` command, the system uses the current Infinite Volume configuration to determine whether a constituent is newly added, deleted, or failed. The system creates and initializes data protection mirror relationships for newly added constituents during the resynchronization. Deleted constituents are not resynchronized. Failed constituents are not recovered, and you must contact technical support to recover failed constituents.

Retrieving data from Infinite Volumes during disaster recovery

If disaster disables the source Infinite Volume of a data protection mirror relationship, you can use the destination Infinite Volume to serve data while you repair or replace the source, update the source, and reestablish the original configuration of the systems.

**About this task**

You can have cluster administrator or Vserver administrator privileges to perform this task.

In the following example, a data protection mirror relationship exists between a source Infinite Volume on one cluster and a destination Infinite Volume on another cluster. The clusters are in a peer relationship, and the Vservers are in a peer relationship. The original source volume (the one
you want to make unavailable) is `cluster1://vs1/volA`, and the original destination volume is `cluster2://vs2/volB`.

---

**Data Protection Mirror Relationship with Offline Constituent**

In this example, a data constituent 3 is offline. All data from the last scheduled data protection mirror update before the source was disabled is preserved, and all the data written to `cluster2://vs2/volB` after you made the volume writable is preserved. Any data written to `cluster1://vs1/volA` between the last data protection mirror copy update and the time that `cluster1://vs1/volA` was disabled is not preserved. You must use SnapMirror commands in this procedure on the destination Vserver with Infinite Volume, unless otherwise specified.

**Steps**

1. After the source volume A (`cluster1://vs1/volA`) is disabled, break the data protection mirror relationship between volume A and volume B (`cluster2://vs2/volB`) by using the `snapmirror break` command.

   **Example**

   ```
   cluster2::> snapmirror break -destination-path vs2:volB
   ```

   The data protection mirror relationship is broken. Volume B changes from read-only to read/write. The system stores the base Snapshot copy for the data protection mirror relationship for later use.

2. Redirect the clients to volume B (`cluster2://vs2/volB`).
The former clients of volume A (cluster1://vs1/volA) access and write to volume B (cluster2://vs2/volB).

3. Ensure that volume B has a namespace mirror constituent to provide data protection for its namespace constituent.

4. Temporarily make volume A (cluster1://vs1/volA) a read-only destination volume.

You must perform this operation on the original source cluster (cluster1).

<table>
<thead>
<tr>
<th>If...</th>
<th>Then...</th>
</tr>
</thead>
</table>
| You can return the constituent in volume A (cluster1://vs1/volA) to an online state, and data is intact | a. Return the constituent in volume A (cluster1://vs1/volA) to an online state, and make volume A available again.  

b. Remove the old data protection mirror relationship between volume A (cluster1://vs1/volA) and volume B (cluster2://vs2/volB) by using the snapmirror delete command.  

c. Create a new data protection mirror relationship by using the snapmirror create command.  

In this configuration, volume B (cluster2://vs2/volB) is the source volume, and volume A (cluster1://vs1/volA) is the destination volume.  

d. Mirror the latest information from volume B (cluster2://vs2/volB) to volume A (cluster1://vs1/volA) by using the snapmirror resync command.  

The base Snapshot copy is used to resynchronize the data protection mirror relationship.  

**Note:** If the resynchronization process fails, create and resynchronize the data protection mirror relationship again. |
| You cannot return the constituent in volume A (cluster2://vs2/volB) to an online state | a. Create a new data protection Infinite Volume called //vs1/volA on cluster1 by using the volume create command.  

b. Create a data protection mirror relationship by using the snapmirror create command.  

In this configuration, volume B (cluster2://vs2/volB) is the source volume, and volume A (cluster1://vs1/volA) is the destination volume.  

c. Initialize the data protection mirror relationship by using the snapmirror initialize command.  

Volume A (cluster1://vs1/volA) becomes read-only. |

Volume B operates as the read/write source volume, and volume A operates as the read-only destination volume. You can keep this configuration, or you can return the volumes to their original data protection configuration by completing the following steps.
5. Redirect the clients from volume B (cluster2://vs2/volB) to volume A (cluster1://vs1/volA).

After redirecting the clients, clients temporarily cannot access or write to either volume.

6. Transfer the latest data from volume B (cluster2://vs2/volB) to volume A (cluster1://vs1/volA) by using the snapmirror update command.

7. Break the data protection mirror relationship by using the snapmirror break command on vserver1.

Example

```
vs1::>>snapmirror break -source-path vs2:volB -destination-path vs1:volA
```

Volume A (cluster1://vs1/volA) changes from read-only to read/write.

8. Remove the old data protection mirror relationship between volume B (cluster2://vs2/volB) and volume A (cluster1://vs1/volA) by using the snapmirror delete command.

9. Re-create the original data protection mirror relationship with volume A (cluster1://vs1/volA) as the source and volume B (cluster2://vs2/volB) as the destination by using the snapmirror create command.

10. On vserver2, resynchronize the original source and original destination volumes by using the snapmirror resync command.

Related concepts

- What a namespace mirror constituent is on page 147
- Aggregate requirements for Infinite Volumes in a data protection mirror relationship on page 110

Related tasks

- Creating a namespace mirror constituent on a destination Infinite Volume on page 139

Creating a namespace mirror constituent on a destination Infinite Volume

After you break a data protection mirror relationship for two Infinite Volumes, the destination Infinite Volume changes from read-only to read/write. You should create a namespace mirror constituent on the Infinite Volume to provide data protection for the namespace constituent.

Before you begin

The Infinite Volume must not contain storage classes. If you want to create a namespace mirror constituent for an Infinite Volume with storage classes, you cannot use the command-line interface; you must use OnCommand Workflow Automation instead.
About this task

You do not have to create a namespace mirror constituent when SnapDiff is enabled on the destination Infinite Volume because one or more namespace mirror constituents already exist on the destination volume. However, if SnapDiff is disabled on the destination Infinite Volume, no namespace mirror constituents exist on the destination volume, and you should create a namespace mirror constituent.

Steps

1. Identify the size of the namespace constituent in the Infinite Volume by using the `volume show` command with the `-is-constituent` parameter.

Example

In the following example, the namespace constituent named volB_ns is 256 MB and no namespace mirror constituent exists:

```
cluster2::> volume show -is-constituent true
Vserver Volume                Aggregate State  Type Size  Available Used%
------- ------------       --------- ------ ---- ----- --------- ----- 
vs2     volB_1024_data0001 aggr1     online RW   384MB 364.7MB    5%  
vs2     volB_1024_data0002 aggr2     online RW   384MB 364.7MB    5%  
vs2     volB_1024_data0003 aggr3     online RW   384MB 364.7MB    5%  
vs2     volB_1024_data0004 vs_aggr online RW   384MB 364.7MB    5%  
vs2     volB_ns             aggr1     online RW   256MB 243.0MB    5%  
5 entries were displayed.
```

2. Increase the size of the Infinite Volume by using the `volume modify` command.

At a minimum, you must increase the size of the volume by the size of the namespace constituent. The namespace mirror constituent is automatically created when you increase the size of the Infinite Volume.

Example

In the following example, the size of the volume named volB is increased by the size of the namespace constituent, which is 256 MB:

```
cluster2::> volume modify -vserver vs2 -volume volB -size +256MB
```

A namespace mirror constituent is created for the Infinite Volume.

Recovering individual failed constituents

If a constituent in an Infinite Volume fails and the Infinite Volume is in a data protection mirror relationship, you can use the SnapMirror commands to recover the entire Infinite Volume. You
cannot use the SnapMirror commands to recover individual constituents. You must contact technical support to recover only constituents.

**About this task**

Following are examples of when a constituent in an Infinite Volume can fail:

- An aggregate or shelf used by an Infinite Volume fails.
- The active file system in an Infinite Volume becomes corrupt, and clients cannot read data.

For example, if the namespace constituent fails and you want to recover only the namespace constituent, you must contact technical support.

**Step**

1. Contact technical support to recover individual, failed constituents.

**Expanding Infinite Volumes in data protection mirror relationships**

You can add more aggregate space to source and destination Vservers with Infinite Volume and increase the size of Infinite Volumes in data protection mirror relationships. Cluster administrators can perform all of the expansion tasks. The Vserver administrator can only increase the size of Infinite Volumes to use newly added aggregate space.

**Note:** If you want to increase the size of an Infinite Volume with storage classes, you cannot use the command-line interface; you must use OnCommand Workflow Automation instead.

**Related concepts**

*How storage classes affect which aggregates can be associated with Infinite Volumes* on page 163

**Related tasks**

*Increasing the size of source and destination Infinite Volumes with storage classes* on page 166

**Adding disks to source and destination Infinite Volumes (cluster administrators only)**

When Infinite Volumes are in a data protection mirror relationship, you should add the same amount of disk space to the aggregates used by the source volume and the aggregates used by the destination volume to provide the same amount of aggregate space to each volume for expansion.

**Before you begin**

- You must have cluster administrator privileges to perform this task.
About this task

For an Infinite Volume with storage classes, you must add disks that meet the requirements of the storage class definitions. For storage class definitions, see OnCommand Workflow Automation.

Steps

1. Add disks to the aggregates used by the source Infinite Volume.
2. Add the same amount of disk space to the aggregates used by the destination Infinite Volume.

   For information about adding disks to aggregates, see the *Clustered Data ONTAP Physical Storage Management Guide*.

After you finish

You must increase the size of the source and destination Infinite Volumes. You should increase the size of destination volume before you increase the size of the source volume.

Related tasks

*Increasing the size of source and destination Infinite Volumes* on page 144

Related information

*Documentation on the NetApp Support Site: support.netapp.com*

Adding dedicated aggregates to the source and destination Infinite Volumes (cluster administrators only)

When Infinite Volumes are in a data protection mirror relationship and use dedicated aggregates, you should add the same number of new aggregates to the source and destination Vservers with Infinite Volume to provide the same amount of aggregate space to each volume for expansion.

Before you begin

- You must have cluster administrator privileges to perform this task.
- For the aggregates to be dedicated to the Vserver with Infinite Volume, no other Vservers must reference the aggregates.

About this task

For an Infinite Volume with storage classes, you must add aggregates that meet the requirements of the storage class definitions. For storage class definitions, see OnCommand Workflow Automation.

Step

1. Add new aggregates to the source and destination cluster:
   a) Create aggregates by using the `storage aggregate create` command.
b) Add the new aggregates to the aggregate list for the Vserver with Infinite Volume by using the `vserver modify` command.

For information about adding aggregates, see the *Clustered Data ONTAP Physical Storage Management Guide*.

**Result**

The same number of aggregates is available to the source and destination Infinite Volumes.

**After you finish**

You must increase the size of the source and destination Infinite Volumes. You should increase the size of destination volume before you increase the size of the source volume.

**Related tasks**

*Increasing the size of source and destination Infinite Volumes* on page 144

**Related information**

*Documentation on the NetApp Support Site: support.netapp.com*

**Adding shared aggregates to the source and destination Infinite Volumes (cluster administrators only)**

When Infinite Volumes are in a data protection mirror relationship and use shared aggregates, you should add the same amount of aggregate space to the source and destination Vservers with Infinite Volume to allow for expansion.

**Before you begin**

- You must have cluster administrator and advanced privileges to perform this task.

**About this task**

For an Infinite Volume with storage classes, you must add aggregates that meet the requirements of the storage class definitions. For storage class definitions, see OnCommand Workflow Automation.

**Step**

1. Add the same amount of aggregate space to the source and destination Infinite Volumes:
   - Add more disks to existing aggregates.
   - Add more aggregates, and add the new aggregates to the aggregate list for the Vserver with Infinite Volume by using the `vserver modify` command.
     Other Vservers in the cluster can reference the aggregates and share space on the aggregates.

For information about adding aggregates, see the *Clustered Data ONTAP Physical Storage Management Guide*. 
After you finish

You must increase the size of the source and destination Infinite Volumes. You should increase the size of destination volume before you increase the size of the source volume.

Related tasks

*Increasing the size of source and destination Infinite Volumes* on page 144

Related information

*Documentation on the NetApp Support Site: support.netapp.com*

Increasing the size of source and destination Infinite Volumes

When Infinite Volumes are in a data protection mirror relationship, you must increase the size of both the source and destination volumes, and the data protection mirror copy must be updated to transfer mirror copies of existing and new constituents from the source to the destination volume.

Before you begin

- The Infinite Volume must not contain storage classes.
  
  If you want to increase the size of an Infinite Volume with storage classes, you cannot use the command-line interface; you must use OnCommand Workflow Automation instead.

- The destination Infinite Volume must have the same amount of or more available aggregate space as the source Infinite Volume.

About this task

You can have cluster administrator or Vserver administrator privileges to perform this task. However, if you require more aggregate space, you must have cluster administrator privileges to add and modify aggregates.

**Note:** You must increase the size of both the source and destination Infinite Volumes before the next scheduled update of the data protection mirror copy. Otherwise, the next scheduled update of the data protection mirror copy will fail. You can modify the schedule if required to allow time for increasing the size of the source and destination Infinite Volumes. You should increase the size of the destination Infinite Volume before you increase the size of the source Infinite Volume.

Steps

1. Increase the size of the destination Infinite Volume by using the `volume modify` command.

   The destination Infinite Volume must be equal to or larger than the source Infinite Volume.

   **Example**

   In the following example, a destination Infinite Volume named `repo_vol_dest` is increased to a size of 3 GB:
The size of the destination Infinite Volume is increased, but mirror copies of the constituents are not yet transferred from the source to the destination volume.

2. Increase the size of the source Infinite Volume by using the `volume modify` command.

**Example**

In the following example, a source Infinite Volume named `repo_vol` is increased to a size of 3 GB:

```
cluster1::> volume modify -vserver vs0 -volume repo_vol -size 3GB
```

The size of the source Infinite Volume and the existing constituents is increased. If required, new data constituents are created on new aggregates.

3. Perform one of the following actions:
   - Wait for the next scheduled update of the data protection mirror copy.
   - Manually update the data protection mirror copy.

**Example**

In the following example, the data protection mirror relationship is manually updated for a Vserver with Infinite Volume named `vs0_dest:repo_vol_dest`:

```
cluster2::> snapmirror update -destination-path vs0_dest:repo_vol_dest
```

Mirror copies of the namespace constituent and all of the data constituents—including any new data constituents—are transferred from the source Infinite Volume to the destination Infinite Volume. Namespace mirror constituents are not transferred.

**Related concepts**

- *Error messages and solutions for failed aggregate selection for destination Infinite Volumes* on page 158
- *How data protection mirror updates affect aggregate selection* on page 158

**Related tasks**

- *Increasing the size of source and destination Infinite Volumes with storage classes* on page 166
- *Reenabling SnapDiff after expanding a destination Infinite Volume onto new nodes* on page 146
Reenabling SnapDiff after expanding a destination Infinite Volume onto new nodes

If you are using SnapDiff for incremental tape backup of a Snapshot copy on a destination Infinite Volume, you must manually reenable SnapDiff after you expand the destination volume onto a new node to automatically create namespace mirror constituents on the new node. Otherwise, tape backup operations might fail.

Before you begin

- The Infinite Volume must not contain storage classes.
  If you want to expand an Infinite Volume with storage classes, you cannot use the command-line interface; you must use OnCommand Workflow Automation instead. When an Infinite Volume with storage classes is in a data protection mirror relationship, the expansion workflow provided by OnCommand Workflow Automation reenables SnapDiff if necessary.
- SnapDiff must be enabled on the destination Infinite Volume.
- You must have increased the size of the destination Infinite Volume to expand the volume onto one or more new nodes.
- You must have updated the data protection mirror relationship to transfer new data constituents from the source Infinite Volume to the new nodes for the destination Infinite Volume.

About this task

When Infinite Volumes are in a data protection mirror relationship, you can use SnapDiff for incremental tape backup of a Snapshot copy on the destination Infinite Volume. When you increase the size of the source and destination Infinite Volumes in a data protection mirror relationship to expand onto new nodes, you must also manually reenable SnapDiff on the destination Infinite Volume to create namespace mirror constituents on the new nodes for SnapDiff to use.

Step

1. On the destination Infinite Volume, reenable SnapDiff by using the `volume modify` command with the `-enable-snapdiff` parameter.

   Example

   In the following example, SnapDiff is reenabled for the Infinite Volume repo_vol:

   ```
   cluster2::> volume modify repo_vol_dest -enable-snapdiff true
   ```

   Namespace mirror constituents are automatically created on the new nodes for SnapDiff to use for incremental tape backup of Infinite Volumes.
How namespace mirror constituents affect source and destination Infinite Volumes

Namespace mirror constituents are automatically created for different purposes on the source Infinite Volume and the destination Infinite Volume, and the namespace mirror constituents use aggregate space. Understanding when namespace mirror constituents are automatically created on Infinite Volumes helps you better understand aggregate usage.

Note: The namespace mirror constituents work the same way for an Infinite Volume with or without storage classes.

What a namespace mirror constituent is

A namespace mirror constituent is an intracluster data protection mirror copy of the namespace constituent in an Infinite Volume. The namespace mirror constituent performs two roles: It provides data protection of the namespace constituent, and it supports SnapDiff for incremental tape backup of Infinite Volumes.

Related tasks

Viewing constituents in an Infinite Volume on page 131

When namespace mirror constituents are created

When you create an Infinite Volume, one namespace mirror constituent is automatically created to provide data protection for the namespace constituent. When you enable SnapDiff for an Infinite Volume, additional namespace mirror constituents are automatically created for SnapDiff for incremental tape backup of Infinite Volumes.

When you create a read/write Infinite Volume that spans two or more nodes in a cluster, one namespace mirror constituent is automatically created, and a data protection mirror relationship is automatically created between the namespace constituent and the namespace mirror constituent. The data protection mirror relationship is updated every five minutes. The data protection mirror relationship is an automatic process for an Infinite Volume. You cannot use SnapMirror commands to modify or manage the data protection mirror relationship between the namespace constituent and the namespace mirror constituent.

When you enable SnapDiff on an Infinite Volume that spans three or more nodes, additional namespace mirror constituents are automatically created for SnapDiff to use for incremental tape backup of Infinite Volumes. A namespace mirror constituent is created on each node with a data constituent, except the node with the namespace constituent and the node with the namespace mirror constituent that was created to provide data protection for the namespace constituent. Namespace mirror constituents created to support SnapDiff are updated daily or as configured for SnapDiff. A SnapMirror license is not required to enable SnapDiff.
When you create a destination Infinite Volume for a data protection mirror relationship, a namespace mirror constituent is not created on the destination Infinite Volume. However, if you enable SnapDiff on a destination Infinite Volume, namespace mirror constituents are automatically created for use by SnapDiff. You must initialize the data protection mirror relationship between the source and destination Infinite Volumes before you can enable SnapDiff.

The following illustration shows an Infinite Volume in a data protection mirror relationship. SnapDiff is disabled on the source and the destination Infinite Volumes. With SnapDiff disabled, a namespace mirror constituent is created on the source Infinite Volume to provide data protection for the namespace constituent, and no other namespace mirror constituents are created.

### Data Protection Mirror Relationship

<table>
<thead>
<tr>
<th>Source Infinite Volume</th>
<th>Destination Infinite Volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>Namespace constituent</td>
<td>Data constituent 1</td>
</tr>
<tr>
<td>Namespace mirror constituent</td>
<td>Data constituent 2</td>
</tr>
<tr>
<td></td>
<td>Data constituent 3</td>
</tr>
<tr>
<td></td>
<td>Data constituent 4</td>
</tr>
<tr>
<td></td>
<td>Data constituent 1</td>
</tr>
<tr>
<td></td>
<td>Data constituent 2</td>
</tr>
<tr>
<td></td>
<td>Data constituent 3</td>
</tr>
<tr>
<td></td>
<td>Data constituent 4</td>
</tr>
</tbody>
</table>

### How modifying an Infinite Volume affects namespace mirror constituents

Namespace mirror constituents are automatically created or deleted when you modify Infinite Volumes, depending on the SnapDiff setting for the volume. The behavior differs slightly between a read/write Infinite Volume and a read-only destination Infinite Volume in a data protection mirror relationship.

When you modify a read/write Infinite Volume to increase its size and create data constituents on new nodes, and SnapDiff is already enabled on the Infinite Volume, namespace mirror constituents are automatically created on new nodes as required. When you modify a read/write or read-only Infinite Volume, and SnapDiff is already disabled, all namespace mirror constituents—except one namespace mirror constituent—are automatically deleted. One namespace mirror constituent is retained to provide data protection for the namespace constituent.

The following table summarizes when namespace mirrors are automatically created and deleted when you modify a read/write or read-only Infinite Volume:
<table>
<thead>
<tr>
<th>Infinite Volume</th>
<th>SnapDiff setting</th>
<th>Task</th>
<th>Result</th>
</tr>
</thead>
</table>
| Read/write Infinite Volume                          | Enabled          | Add new nodes to the cluster and increase volume size by using `volume modify`  
**Note:** You must increase the size enough to create new data constituents on the new nodes. | Namespace mirror constituents are automatically created on new nodes as required. |
| Read-only destination Infinite Volume in a data protection mirror relationship |                  |                                                                     | Namespace mirror constituents are not automatically created on new nodes, although SnapDiff is enabled on the destination Infinite Volume. You must expand the destination Infinite Volume onto new nodes and update the data protection mirror relationship before you reenable SnapDiff to automatically create namespace mirror constituents on new nodes. |
| Read/write Infinite Volume and read-only destination Infinite Volume in a data protection mirror relationship | Disabled         | Modify the volume by using `volume modify`                                | All namespace mirror constituents—except one namespace mirror constituent—are automatically deleted. |

**How namespace mirror constituents affect the state of an Infinite Volume**

Infinite Volumes with SnapDiff enabled temporarily display a mixed state while namespace mirror constituents are created. After the namespace mirror constituents are created, Infinite Volumes automatically display an online state. You cannot start new operations until the namespace mirror constituents are created, and the Infinite Volume displays an online state.

The amount of time required to create all of the namespace mirror constituents depends on the size of the namespace constituent and the number of nodes an Infinite Volumes spans.

If you enable SnapDiff when you create an Infinite Volume, the namespace constituent is empty, and little time is required to create namespace mirror constituents on all of the nodes that an Infinite Volume spans. As a result, the Infinite Volume displays a mixed state for a small amount of time.
If you enable SnapDiff after an Infinite Volume has existed for some time, the namespace constituent contains data, and more time is required to create namespace mirror constituents. The Infinite Volume displays a mixed state until all of the namespace mirror constituents are created and initialized on all of the nodes with data constituents. The number of nodes that the Infinite Volume spans also affects the amount of time it takes to create and initialize namespace mirror constituents.

When you resize an Infinite Volume with SnapDiff enabled, namespace mirror constituents are created and initialized on all the new nodes with data constituents. Depending on the size of the namespace constituent and the number of new nodes, it can take some time to create and initialize a namespace mirror constituent on each new node. The Infinite Volume displays a mixed state while the namespace mirror constituents are being initialized.

Before you start a tape backup operation, you should wait until all of the namespace mirror constituents are created and initialized, and the Infinite Volume displays an online state.

How Data ONTAP calculates the Infinite Volume size before the transfer of a mirror copy

A mirror copy of a source Infinite Volume is only transferred to the destination Infinite Volume when the mirrored volume size of the destination volume is equal to or bigger than the mirrored volume size of the source volume. How the mirrored volume size is calculated differs between the source and destination volumes.

You must understand the difference between the specified volume size and the mirrored volume size. The specified volume size is identified when you create an Infinite Volume. The specified size of the destination Infinite Volume must be equal to or bigger than the source Infinite Volume to create and initialize a data protection mirror relationship.

The mirrored volume size is calculated when the system determines whether the destination Infinite Volume has enough space for a mirror copy of the source volume. The mirrored volume size is calculated as follows for the source and destination Infinite Volumes:

- For the source Infinite Volume, the mirrored volume size = (current size of the namespace constituent) + (current sizes of all data constituents).
  For example, a source Infinite Volume contains a 10 TB namespace constituent, a 10 TB namespace mirror constituent, and three 40 TB data constituents. The mirrored volume size of the Infinite Volume is calculated as 130 TB, which is the sum of the namespace constituent and three data constituents.

- For the destination Infinite Volume, the mirrored volume size = (specified volume size) - (the sum of all the namespace mirror constituents sizes on the destination Infinite Volume).
  For example, a destination Infinite Volume has a specified size of 150 TB and contains a 10 TB namespace constituent, two 10 TB namespace mirror constituents (for SnapDiff and tape backup), and three 40 TB data constituents. The mirrored size of the destination Infinite Volume is calculated as 130 TB, which is the size of the destination Infinite Volume (150 TB) minus the size of all the namespace mirror constituents (20 TB).
**Note:** The size of the namespace mirror constituents is excluded from the mirrored volume size of the source and destination Infinite Volumes because only the namespace constituent and the data constituents are mirrored from the source Infinite Volume to the destination Infinite Volume.

A mirror copy transfer can fail when the specified size of a destination Infinite Volume is bigger than the source Infinite Volume, but namespace mirror constituents on the destination Infinite Volume consume so much space that the destination Infinite Volume lacks enough space for a mirror copy of the source Infinite Volume. This can happen when you enable SnapDiff on the destination Infinite Volume, and the namespace mirror constituents created for SnapDiff consume so much space that a mirror copy of the source Infinite Volume cannot fit on the destination Infinite Volume.

**How Data ONTAP selects aggregates for data protection of Infinite Volumes**

Aggregates are automatically selected for a destination Infinite Volume when you initialize a data protection mirror relationship. You must understand the factors that affect aggregate selection and how aggregates are selected to correctly create constituents for a destination Infinite Volume.

**Related concepts**

*Processes used to select aggregates for destination Infinite Volumes with and without storage classes* on page 166

**When Data ONTAP selects aggregates for destination Infinite Volumes**

Data ONTAP automatically selects aggregates for a destination Infinite Volume when you initialize a data protection mirror relationship, and not when you create a destination Infinite Volume. When you
create a destination Infinite Volume, no aggregates are selected for the destination Infinite Volume because no constituents exist yet.

A pool of available aggregates is identified for the destination Infinite Volume and evaluated for available space. If aggregates have enough space, constituents are mirrored from the source Infinite Volume to aggregates on the destination Infinite Volume, and the data protection mirror relationship is initialized. If aggregates lack enough space, an error message is displayed, and the data protection mirror relationship is not initialized.

Related concepts

*Error messages and solutions for failed aggregate selection for destination Infinite Volumes* on page 158

How Data ONTAP automatically selects aggregates for destination Infinite Volumes

Data ONTAP automatically selects aggregates for destination Infinite Volumes. Understanding how aggregates are automatically selected helps you better plan and create aggregates for a destination Infinite Volume.

Methods to control aggregate selection for destination Infinite Volumes

You can use the aggregate list for a destination Vserver with Infinite Volume to specify which aggregates in the destination cluster are considered available for automatic selection for a destination Infinite Volume.

You can use the following methods to affect aggregate selection for a destination Infinite Volume:

<table>
<thead>
<tr>
<th>Method</th>
<th>Privilege</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify an aggregate list for the destination Vserver with Infinite Volume by using the <code>vserver modify</code> command.</td>
<td>Cluster administrator</td>
<td>Specifies the aggregates in the destination cluster that Data ONTAP should consider available when selecting aggregates for destination Infinite Volume. When the aggregate list is unspecified for a Vserver with Infinite Volume, all aggregates available to the destination cluster are considered available for cluster administrators to create an Infinite Volume. You must specify an aggregate list to allow Vserver administrators to create an Infinite Volume.</td>
</tr>
<tr>
<td>Method</td>
<td>Privilege</td>
<td>Result</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Specify an aggregate to use for the namespace constituent when you create an Infinite Volume by using the <code>volume create</code> command.</td>
<td>Cluster or Vserver administrator with advanced privilege</td>
<td>Specifies which aggregate from the aggregate list to use for the namespace constituent in the destination Infinite Volume. When you do not specify an aggregate for the namespace constituent, all aggregates available to the destination Vserver are considered for a mirror copy of the namespace constituent on the destination Infinite Volume.</td>
</tr>
</tbody>
</table>

**How aggregates are selected for constituents in a destination Infinite Volume**

When you initialize a data protection mirror relationship for a destination Infinite Volume, Data ONTAP automatically selects aggregates for constituents in a destination Infinite Volume. Understanding how aggregates are selected helps you create the required number and size of aggregates for destination Infinite Volumes.

When you initialize a data protection mirror relationship for a destination Infinite Volume, Data ONTAP uses the following process to choose aggregates for the namespace constituent and all of the data constituents from the source Infinite Volume that will be mirrored to the destination Infinite Volume:

1. Identifies the pool of aggregates available to the destination Vserver with Infinite Volume:
   - If you specified an aggregate for the namespace constituent when you created the destination Infinite Volume, aggregates are divided into two temporary, internal lists: the aggregate specified for the namespace constituent and the aggregates available for all data constituents. The aggregates available for the data constituents are from the aggregate list for the destination Vserver with Infinite Volume.
   - If you did not specify an aggregate for the namespace constituent, one temporary, internal list of available aggregates is created from the aggregate list for the destination Vserver with Infinite Volume.

2. Chooses an aggregate for the namespace constituent
   If you specified an aggregate for the namespace constituent, Data ONTAP uses it. Otherwise, Data ONTAP chooses the best aggregate for the namespace constituent. If the aggregate is too small, the initialization operation fails and you receive an error message that informs you how to adjust aggregate space before using the `snapmirror initialize` command again.

3. Chooses aggregates for all of the data constituents
   The best available aggregates are used for the bigger data constituents. Data ONTAP can place more than one data constituent on the same aggregate, if the aggregate has enough available space.
   The result of this step determines what happens next:
   - If all data constituents can fit on the chosen aggregates, constituents from the source Infinite Volume are mirrored to the chosen aggregates, and the data protection mirror relationship is initialized.
• If all data constituents cannot fit on the chosen aggregates, Data ONTAP returns to step 2. The aggregate that was previously considered for the namespace constituent is returned to the pool of available aggregates. Data ONTAP considers the second best aggregate for the namespace constituent and tries to fit the data constituents on the remaining available aggregates. Data ONTAP continues to try and fit the namespace constituent and all data constituents on the available aggregates until all constituents fit, or until Data ONTAP determines that the constituents cannot fit.

**Note:** If you specified an aggregate for the namespace constituent and the aggregate is too small, the initialization operation fails because Data ONTAP cannot use any other aggregates for the namespace constituent.

**Related concepts**

*How the best available aggregate is identified* on page 155

*Error messages and solutions for failed aggregate selection for destination Infinite Volumes* on page 158

**How space guarantee for a destination Infinite Volume affects aggregate selection**

The space guarantee for a destination Infinite Volume affects which aggregates are selected for its constituents.

When you create a destination Infinite Volume, you can specify the space guarantee for the Infinite Volume by using the `volume create` command with the `-space-guarantee` parameter as follows:

• When you set `-space-guarantee` to `volume`, the Infinite Volume is thick-provisioned.
• When you set `-space-guarantee` to `none`, the Infinite Volume is thin-provisioned.

The space guarantee for the Infinite Volume applies to all of its data constituents, but not to its namespace constituent. The namespace constituent is always thick-provisioned.

The following space requirements apply to thick-provisioned and thin-provisioned data constituents:

• When data constituents are thick-provisioned, the space available on the aggregate must be equal to or greater than the size of the data constituents.

  You can view the size of a data constituent by using the `volume show` command with the `-is-constituent` and `-size` parameters.

• When data constituents are thin-provisioned, the space available on the aggregate must be equal to or greater than the current used size of the data constituents.

  You can view the size of the data constituent by using the `volume show` command with the `-is-constituent` and `-used` parameters.
How the best available aggregate is identified

Whether a constituent is thin-provisioned or thick-provisioned for a destination Infinite Volume affects which aggregates are considered the best choice and selected for its constituents.

For thin-provisioned constituents in a destination Infinite Volume, the best aggregate has the least overcommitment ratio. If two or more aggregates have the same overcommitment ratio, the aggregate with the larger available space is the better aggregate for the constituent.

For thick-provisioned constituents in a destination Infinite Volume, the best aggregate has the largest available size. If two or more aggregates have the same large available size, the larger aggregate is considered better.

How multiple constituents are placed on one aggregate

Data ONTAP uses a calculation to verify the space required to place more than one data constituent on the same aggregate for a destination Infinite Volume.

An aggregate for a destination Infinite Volume has enough space for multiple data constituents when the available space on the aggregate minus $n$ multiplied by the maximum data constituent size is greater than zero. Where $n$ is the number of existing data constituents on the aggregate. The aggregate that contains a namespace constituent can also contain one or more data constituents.

Restrictions on automatic aggregate selection

Shared aggregate space and aggregate overhead affect automatic aggregate selection for destination Infinite Volumes. You should keep these restrictions in mind when creating aggregates for destination Infinite Volumes.

The following restrictions apply to the automatic aggregate selection process:

- Multiple volumes in a destination cluster can share aggregate space.
  When you create a destination Infinite Volume in a cluster, the aggregate selection process selects aggregates that allow constituents to grow to the maximum size. However, until the constituents grow to their maximum size and consume space in the aggregates, the space appears available for other volumes to use. As a result, aggregate space that was expected to be available can be consumed by volumes in the cluster, leaving the destination Infinite Volume without enough aggregate space for its constituents to grow.

- Only 91% of the total size of an aggregate can be used to create constituents for an Infinite Volume.
  The remaining space is required for overhead.

  **Note:** The available space is rounded down to the nearest 4K.
Examples of automatic aggregate selection for destination Infinite Volumes

The examples illustrate how Data ONTAP selects aggregates on the destination Infinite Volume for mirror copies of constituents from the source Infinite Volume, and initializes a data protection mirror relationship.

Note: For simplicity, the following examples exclude overhead space requirements for aggregates.

Typical constituent layout for a destination Infinite Volume

This example represents a typical constituent layout on a destination Infinite Volume. In this example, constituents from the source Infinite Volume are mirrored to aggregates for the destination Infinite Volume, and the data protection mirror relationship is initialized.

The source Infinite Volume contains the following constituents:

- Namespace constituent of 10 TB
- Data constituent 1 of 35 TB
- Data constituent 2 of 20 TB

The aggregate list for the destination Vserver with Infinite Volume contains the following aggregates:

- Aggregate 1 has 50 TB of available aggregate space.
- Aggregate 2 has 25 TB of available aggregate space.

Constituents from the source Infinite Volume are mirrored to aggregates for the destination Infinite Volume as follows:

- Namespace constituent is created on aggregate 1.
- Data constituent 1 is created on aggregate 1.
- Data constituent 2 is created on aggregate 2.

Each constituent for a destination Infinite Volume is placed on a different aggregate

In this example, constituents from the source Infinite Volume are mirrored to aggregates for the destination Infinite Volume, and the data protection mirror relationship is initialized.

The source Infinite Volume contains the following constituents:

- Namespace constituent of 5 TB
- Data constituent 1 of 30 TB
- Data constituent 2 of 20 TB

The aggregate list for the destination Vserver with Infinite Volume contains the following aggregates, and no aggregate is specified for the namespace constituent:

- Aggregate 1 has 10 TB of available aggregate space.
- Aggregate 2 has 20 TB of available aggregate space.
- Aggregate 3 has 30 TB of available aggregate space.
The constituents from the source Infinite Volume are mirrored to aggregates for the destination Infinite Volume as follows:

- Aggregate 1 (10 TB) contains the namespace constituent (5 TB).
- Aggregate 2 (20 TB) contains data constituent 2 (20 TB).
- Aggregate 3 (30 TB) contains data constituent 1 (30 TB).

**Multiple constituents for a destination Infinite Volume are placed on one aggregate**

In this example, constituents from the source Infinite Volume are mirrored to aggregates for the destination Infinite Volume, and the data protection mirror relationship is initialized. Multiple data constituents are placed on the same aggregate in the destination Infinite Volume.

The source Infinite Volume contains the following constituents:

- Namespace constituent of 10 TB
- Data constituent 1 of 20 TB
- Data constituent 2 of 20 TB

For the destination Infinite Volume, the maximum data constituent size is 20 TB. The aggregate list for the destination Vserver with Infinite Volume contains 50 TB of available aggregate space on one aggregate, and no aggregate is specified for the namespace constituent. All of the constituents from the source Infinite Volume are mirrored to the single aggregate for the destination Infinite Volume.

**Constituents for a destination Infinite Volume are too big for the available aggregate space**

In this example, constituents from the source Infinite Volume are not mirrored to aggregates for the destination Infinite Volume, and the data protection mirror relationship is not initialized. Although aggregates for the destination Infinite Volume contain enough overall available space, you have specified an aggregate for the namespace constituent, and the remaining aggregates lack enough space for the data constituents.

The source Infinite Volume contains the following constituents:

- Namespace constituent of 10 TB
- Data constituent 1 of 35 TB
- Data constituent 2 of 20 TB

The aggregate list for the destination Vserver with Infinite Volume contains 70 TB of available aggregate space on the following aggregates, and aggregate 1 (40 TB) is specified for the namespace constituent:

- Aggregate 1 has 40 TB of available aggregate space.
- Aggregate 2 has 10 TB of available aggregate space.
- Aggregate 3 has 20 TB of available aggregate space.

The constituents from the source Infinite Volume are not mirrored to aggregates for the destination Infinite Volume. Because you specified aggregate 1 (40 TB) for the namespace constituent in the
destination Infinite Volume, the remaining aggregates are too small for the two data constituents. As a result, you cannot initialize the data protection mirror relationship.

**How data protection mirror updates affect aggregate selection**

During manual or scheduled updates of a data protection mirror relationship for two Infinite Volumes, additional aggregate space is used, and sometimes new aggregates are automatically selected for a destination Infinite Volume.

When you increase the size of a source Infinite Volume, you must also increase the size of the destination Infinite Volume. The destination volume must be the same size or bigger than the source volume. It is recommended that you increase the size of the destination Infinite Volume before you increase the size of the source Infinite Volume to avoid a scheduled data protection mirror update starting before you finished increasing the size of the destination Infinite Volume.

When you increase the size of the source Infinite Volume, and new data constituents are created, aggregates must be selected on the destination Infinite Volume for mirror copies of the new data constituents. Before the next manual or scheduled update to the data protection mirror copy, you must increase the size of the destination volume by using the `volume modify` command to provide enough space for the mirror copies to transfer from the source to the destination Infinite Volume.

During manual or scheduled updates to the data protection mirror relationship, mirror copies of the namespace constituent and all data constituents—including new data constituents—are transferred to the destination volume, and aggregate space is selected for the new data constituents. New aggregates are automatically selected from the aggregate list assigned to the destination Vserver with Infinite Volume. Alternatively, previously selected aggregates can be used for the new data constituents when the aggregates have enough space.

**Note:** During a data protection mirror update, constituents are not moved between different aggregates. When an aggregate is selected for a namespace constituent or a data constituent, the constituent remains on the aggregate.

For more information about resizing and expanding Infinite Volumes, see *Clustered Data ONTAP Logical Storage Management Guide*.

**Related concepts**

*How Data ONTAP calculates the Infinite Volume size before the transfer of a mirror copy* on page 150

**Error messages and solutions for failed aggregate selection for destination Infinite Volumes**

When you initialize a data protection mirror relationship for a destination Infinite Volume, aggregates are automatically selected for constituents. If aggregates lack enough space, an error message is displayed that identifies the problem and provides a solution. Cluster administrators can adjust aggregate space to correct the problem.
**Insufficient space on destination for SnapMirror source Infinite Volume namespace constituent**

**Message**

Error: command failed: [Job number] Job failed: Insufficient space on destination for SnapMirror source Infinite Volume namespace constituent "Vserver name:namespace constituent name" (Destination aggregate "aggregate name" needs numberunit more to store snapmirror source Infinite Volume constituent "Vserver name:namespace constituent name".).

**Cause**
The aggregate is too small for the namespace constituent.

**Corrective action**
Add more disks to the existing aggregate to create more space for the namespace constituent.

**Size exceeds maximum (namespace constituent)**

**Message**

Error: command failed: [Job number] Job failed: Size exceeds maximum. The Infinite Volume namespace constituent "Vserver name:namespace constituent name" on SnapMirror source is larger than the maximum allowed size for the namespace constituent as determined by the configuration of the destination Infinite Volume. Source namespace constituent size: numberunit. Maximum allowed: numberunit.

**Cause**
The platform for the destination Infinite Volume is smaller than the platform for the source Infinite Volume. The two platforms support different maximum constituent sizes. The maximum constituent size for an Infinite Volume corresponds to the maximum FlexVol volume size for a platform. Because the maximum constituent size for the destination Infinite Volume is smaller than the maximum constituent size for the source Infinite Volume, the namespace constituent from the source Infinite Volume is too big for the destination Infinite Volume. The namespace constituent cannot fit into the aggregates for the destination Infinite Volume. You would only encounter this error if you set the -max-namespace-constituent-size parameter to greater than 10 TB.

**Corrective action**
Choose one of the following options:

- Choose a different cluster with a bigger platform for the destination Infinite Volume.
- Contact technical support for help with setting up the destination Infinite Volume.

**Related concepts**

Constituent size requirements for setting up data protection mirror relationships for Infinite Volumes on page 111
Insufficient space for the following source data constituents on destination Vserver

**Message**  
Error: command failed: [Job number] Job failed: Insufficient space for the following source data constituents on destination Vserver "Vserver name": data constituent name(sizeunit). Add aggregates of sufficient size for each constituent, or increase the size of existing aggregates for the Vserver.

**Cause**  
The Vserver with Infinite Volume in the destination cluster specifies too few aggregates to mirror all of the data constituents from the source Infinite Volume to the destination Infinite Volume.

**Corrective action**  
Choose one of the following options:

- Add more disks to the existing aggregate to create enough space to fit two or more data constituents on one aggregate.
- Add more aggregates to the destination cluster for the Vserver with Infinite Volume. Add an aggregate for each data constituent in the source Infinite Volume to allow each data constituent to be mirrored to its own aggregate on the destination Infinite Volume.

Insufficient space on SnapMirror destination for source Infinite Volume data constituents

**Message**  
Error: command failed: [Job number] Job failed: Insufficient space on SnapMirror destination for source Infinite Volume data constituent "Vserver name: data constituent name". Destination aggregate "aggregate name" needs sizeunit more to store snapmirror source Infinite Volume constituent "Vserver name: data constituent name".

**Cause**  
The aggregates being considered for data constituents have some space, but not enough space.

**Corrective action**  
Add more disks to the existing aggregates to create more space.

Size exceeds maximum (data constituents)

**Message**  
Error: command failed: [Job number] Job failed: Size exceeds maximum. The Infinite Volume data constituent "Vserver name: data constituent name" on SnapMirror source is larger than the maximum allowed size for a single data constituent as determined by the configuration of the destination Infinite Volume. Source data constituent size: numberunit. Maximum allowed: numberunit.
Cause
The platform for the destination Infinite Volume is smaller than the platform for the source Infinite Volume. The two platforms support different maximum constituent sizes. The maximum constituent size for an Infinite Volume corresponds to the maximum FlexVol volume size for a platform. Because the maximum constituent size for the destination Infinite Volume is smaller than the maximum constituent size for the source Infinite Volume, the data constituents from the source Infinite Volume are too big for the destination Infinite Volume. The data constituents cannot fit into the aggregates for the destination Infinite Volume.

Corrective action
Choose one of the following options:
• Choose a different cluster with a bigger platform for the destination Infinite Volume.
• Contact technical support for help with setting up the destination Infinite Volume.

Related concepts
Constituent size requirements for setting up data protection mirror relationships for Infinite Volumes on page 111
Providing disaster recovery on Infinite Volumes with storage classes using mirroring technology

You can use mirroring technology on Infinite Volumes with storage classes to create an identical second set of data to replace the primary set of data, in case something happens to the primary set of data. However, you must use OnCommand Workflow Automation to perform most operations.

What a storage class is

A storage class is a definition of aggregate characteristics and volume settings. You can define different storage classes and associate one or more storage classes with an Infinite Volume. You must use OnCommand Workflow Automation to define workflows for your storage class needs and to assign storage classes to Infinite Volumes.

You can define the following characteristics for a storage class:

- Aggregate characteristics, such as the type of disks to use
- Volume settings, such as compression, deduplication and volume guarantee

For example, you can define a performance storage class that uses only aggregates with SAS disks and the following volume settings: thin provisioning with compression and deduplication enabled.

How storage classes affect data protection mirror relationships for Infinite Volumes

Setup of data protection mirror relationships differs between Infinite Volumes with and without storage classes. For Infinite Volumes without storage classes, you can use the command-line interface, but for Infinite Volumes with storage classes, you cannot use the command-line interface; you must use OnCommand Workflow Automation instead.

Storage classes affect data protection mirror relationships as follows for Infinite Volumes with and without storage classes:

<table>
<thead>
<tr>
<th>For an Infinite Volume...</th>
<th>Operations...</th>
<th>Tools supported...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without storage classes</td>
<td>Create and initialize manage data protection mirror relationships</td>
<td>Command-line interface</td>
</tr>
<tr>
<td></td>
<td>Increase the size of Infinite Volumes in data protection mirror relationships</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recover from disaster</td>
<td></td>
</tr>
</tbody>
</table>
For an Infinite Volume... | Operations... | Tools supported...
---|---|---
With storage classes | Create and initialize data protection mirror relationships | OnCommand Workflow Automation
| Increase the size of Infinite Volumes in data protection mirror relationships | |
| Recover from disaster | |

How storage classes affect which aggregates can be associated with Infinite Volumes

Each storage class definition specifies an aggregate type. When you create an Infinite Volume with a storage class, only the type of aggregate specified for the storage class can supply storage for the volume. You must understand storage class definitions to create aggregates that are appropriate for the storage class.

Storage class definitions are available only in OnCommand Workflow Automation. After you understand the aggregate requirements for each storage class, you can use the command-line interface or OnCommand Workflow Automation to create aggregates for storage classes. However, you must use OnCommand Workflow Automation, not the command-line interface, to create an Infinite Volume with one or more storage classes.

When you use OnCommand Workflow Automation to create an Infinite Volume with a storage class, OnCommand Workflow Automation automatically filters the aggregates available in the cluster based on the storage class that you want to use. If no aggregates meet the requirements of the storage class, you cannot create an Infinite Volume with that storage class.

Tasks and tools for managing data protection mirror copies for Infinite Volumes with storage classes

You must use OnCommand Workflow Automation and OnCommand Unified Manager to perform operations for Infinite Volumes with storage classes in a data protection mirror relationship.

<table>
<thead>
<tr>
<th>To...</th>
<th>Use this tool or command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create and initialize data protection mirror relationships for an Infinite Volume with one or more storage classes</td>
<td>OnCommand Workflow Automation</td>
</tr>
<tr>
<td>Manually transfer the data policy for the source Infinite Volume with storage classes to the destination Infinite Volume with storage classes</td>
<td>OnCommand Unified Manager</td>
</tr>
</tbody>
</table>
### Creating a data protection mirror copy for an Infinite Volume with storage classes

You can create a data protection mirror copy for an Infinite Volume with storage classes by using OnCommand Workflow Automation to set up the mirror relationship. You cannot use the command-line interface.

**Before you begin**

- You must have created aggregates for the destination Infinite Volume that meet the requirements of the storage classes used by the source Infinite Volume because the source and destination Infinite Volumes must use the same type and number of storage classes.
  
  For example, if the source Infinite Volume uses a performance storage class and a capacity storage class, the workflow must be able to create a destination Infinite Volume with a performance storage class and a capacity storage class. For storage class definitions, see OnCommand Workflow Automation.

**About this task**

You cannot create a data protection mirror copy between an Infinite Volume without storage classes and an Infinite Volume with storage classes.

**Steps**

1. Create a destination Infinite Volume in another cluster by using the workflow in OnCommand Workflow Automation.
   
   The Infinite Volume is created but no storage classes are created yet.

2. Create a data protection mirror relationship between the two Infinite Volumes in different clusters by using the workflow in OnCommand Workflow Automation.
   
   The data protection mirror relationship is created, and the workflow creates the same number and type of storage classes for the destination Infinite Volume as are used by the source Infinite Volume.

3. Export the data policy from the source Vserver with Infinite Volume, and import the data policy to the destination Vserver with Infinite Volume by using OnCommand Unified Manager.
Exporting a data policy to a destination Vserver with Infinite Volume

The destination Vserver with Infinite Volume should always reference the same data policy as the source Vserver with Infinite Volume. Therefore, you should manually export the data policy after you create a data protection mirror relationship and at any time that you modify the policy in the source Vserver.

Steps

1. Export the data policy from the source Vserver with Infinite Volume by using OnCommand Unified Manager.
   See the OnCommand Unified Manager Online Help.
2. Import the data policy to the destination Vserver with Infinite Volume by using OnCommand Unified Manager.
   See the OnCommand Unified Manager Online Help.

Both Infinite Volumes reference the same data policy and its rules.

Retrieving data from Infinite Volumes with storage classes during disaster recovery

If disaster disables the source Infinite Volume with storage classes of a data protection mirror relationship, you can use the destination Infinite Volume for recovery by using a workflow in OnCommand Workflow Automation.

Step

1. Recover an Infinite Volume with storage classes from disaster by using a workflow in OnCommand Workflow Automation.
Increasing the size of source and destination Infinite Volumes with storage classes

You must use OnCommand Workflow Automation to increase the size of Infinite Volumes with storage classes that are in a data protection mirror relationship. You cannot use the command-line interface.

Steps

1. Increase the size of source and destination Infinite Volumes with storage classes by using a workflow in OnCommand Workflow Automation.

2. If you added new storage classes to the source Infinite Volume, modify the data policy for the source Vserver with Infinite Volume to add rules for filtering data into the new storage classes.

   See the OnCommand Unified Manager Online Help.

3. If you updated the data policy for the source Vserver with Infinite Volume, export the updated data policy from the source Vserver with Infinite Volume, and import the data policy to the destination Vserver with Infinite Volume by using OnCommand Unified Manager.

   See the OnCommand Unified Manager Online Help.

Processes used to select aggregates for destination Infinite Volumes with and without storage classes

The aggregate selection process that is used depends on whether the Infinite Volume uses storage classes and on the tool that is used to create the data protection mirror relationship for the Infinite Volume.

For Infinite Volumes without storage classes, you can use the command-line interface or OnCommand Workflow Automation to create and initialize data protection mirror relationships. In this case, the aggregate selection process provided by Data ONTAP is used.

For Infinite Volumes with storage classes, you must use OnCommand Workflow Automation to create and initialize data protection mirror relationships. You cannot use the command-line interface. In this case, the aggregate selection process provided by OnCommand Workflow Automation is used because it can factor storage classes into its aggregate selection process.

Related concepts

How Data ONTAP selects aggregates for data protection of Infinite Volumes on page 151
Copyright information

Copyright © 1994–2013 NetApp, Inc. All rights reserved. Printed in the U.S.

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. 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

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, CyberSnap, Data Center Fitness, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, ExpressPod, FAServer, FastStak, FilerView, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Mars, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, Snap Creator, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, VelocityStak, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

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 www.ibm.com/legal/copytrade.shtml.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States 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 United States 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.
How to send your comments

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

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

You can also contact us in the following ways:

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

A

about
- snapshot copy reserve 26
active file disk space
how Data ONTAP uses deleted 26
active file systems
- access on destination volumes 31
- guidelines for restoring from SnapVault backups 101
- protocols supported on destination Infinite Volumes 31
- when available on destination volumes 31
aggregate lists
- specifying for a Vserver with Infinite Volume 115, 125
aggregates
- adding disks for Infinite Volumes to use 141
- adding more space for Infinite Volumes 141
- adding space to shared aggregates for Infinite Volumes 143
- adding to a destination cluster 114, 123
- adding to Infinite Volumes, dedicated 142
- associating with Vservers 116
- automatically selected during mirror copy updates 158
- automatically selected for destination Infinite Volumes 152
- calculation used to very space to fit multiple constituents 155
- error messages for destination Infinite Volumes, examples of 158
- examples of automatic selection for Infinite Volumes 156
- expanding Infinite Volumes to use more space 144
- how automatically selected for destination Infinite Volumes 153
- how provisioning of constituents affects aggregate selection for Infinite Volumes 155
- how storage classes use for Infinite Volumes 163
- identifying how many a source Infinite Volume uses 112
- identifying number required for destination Infinite Volumes 112
- identifying space required for destination Infinite Volumes 122
- impact of space guarantee for destination Infinite Volumes on 154
- methods to control selection for destination Infinite Volumes 152
- methods used to select for destination Infinite Volumes 152
- requirements for Infinite Volumes and data protection mirror relationships 110
- requirements for storage classes 163
- restrictions for automatic selection 155
- setting up data protection for Infinite Volumes using dedicated aggregates 111
- setting up data protection for Infinite Volumes using shared aggregates 121
- understanding selection for destination Infinite Volumes 151
- when automatically selected for destination Infinite Volumes 151
- automatic Snapshot copies
  - using prefixes to name 52
- automatically deleting
  - Snapshot copies 23

B

backup policies
- example of creating tiered 59
backup tasks
- Snapshot copy 16
backups
- guidelines for managing storage efficiency for SnapVault 107
- guidelines for restoring active file system from SnapVault 101
- how restore operations work from SnapVault 102
- managing copied source volume, in SnapVault relationships 101
- SnapVault, how they work 37
baseline transfers
- defined 35

C

cascades
- creating SnapVault backup in mirror-SnapVault 91
managing SnapVault-mirror, when SnapVault backup is unavailable 104
mirror-SnapVault, how they work 43
SnapVault-mirror, how they work 44
CIFS clients
  destination volume not accessible 34
  client access
to active file systems on destination volumes 31
to Snapshot copies of Infinite Volumes, temporarily disabled 20
what Snapshot copies to access 19
cluster administrators
  mirror and SnapVault relationship management capabilities 58
cluster peering
  creating peer relationships between clusters 117, 126
clusters
  guidelines for creating mirror or SnapVault relationships between 31
  how SnapMirror policies work with 57
command line
  aggregate selection process for destination Infinite Volumes 166
commands
  for managing mirror and SnapVault policies 57
  for managing SnapMirror relationships 63, 132
  for managing Snapshot copy policies and schedules 50
  for monitoring Snapshot copy disk consumption) 55
  for scheduling when SnapMirror transfers occur 75
  job show 74
  managing mirror relationships for Infinite Volumes 132
  run sequentially on Infinite Volumes 135
  snapmirror break 83
  snapmirror create 61
  snapmirror delete 83
  snapmirror delete, when deleting mirror relationships 77
  snapmirror initialize 61
  volume create 61
  volume delete, when deleting mirror relationships 77
  volume snapshot partial-restore-file 54
  volume snapshot partial-restore-file-list-info 54
  volume snapshot restore 54
  volume snapshot restore-file 53
  volume snapshot restore-file-info 53
configurations
  deployment, how mirror-SnapVault cascades work 43
  supported data protection deployment 40
  constituents
    and Snapshot copies 19
  creating for destination Infinite Volumes 117, 118, 127
  data constituents, recovering after failure 140
  effect on information availability about destination Infinite Volumes 130
  how provisioning affects aggregate selection 155
  identifying how many a source Infinite Volume uses 122
  identifying size of 122
  managing disaster recovery 136
  namespace constituent, recovering after failure 140
  size requirements for setting up data protection mirror copies for Infinite Volumes 111
  viewing for an Infinite Volume 131
copied source volumes
  managing SnapVault backup of 101
D
data compression
  how SnapVault backups work with 38
data constituents
  calculation used to verify space for multiple constituents on one aggregate 155
  viewing in an Infinite Volume 131
data loss
tools to protect against 12
data loss disaster 11
data policies
  exporting from a source to a destination Vserver with Infinite Volume 165
data protection
  creating a namespace mirror constituent, Infinite Volumes 139
  creating mirror copies for Infinite Volumes with storage classes 164
  in SAN environments 13
  levels of provided by mirror relationships 29
  overview of methods for 10
  setting up for Infinite Volume with shared aggregates 121
  setting up for Infinite Volumes with dedicated aggregates 111
data protection mirror copies
  Infinite Volumes with storage classes, impact on 162
  namespace constituent in Infinite Volumes, of 147
  providing disaster recovery for Infinite Volumes 110
data protection mirror relationship
initialization errors for Infinite Volumes 158
adding space to shared aggregates for Infinite Volumes 143
aggregate requirements for Infinite Volumes 110
between volumes on platforms of different sizes 111
destination Infinite Volumes, when information is available 130
error messages for Infinite Volumes, examples of 158
expanding Infinite Volumes 141
expanding Infinite Volumes to use more aggregate space 144
how maximum constituent size affects Infinite Volumes 111
how updates affect aggregate selection 158
increasing the size of Infinite Volumes with storage classes 166
retrieving data from Infinite Volumes during a disaster 136
troubleshooting errors for Infinite Volumes 158
when aggregates are selected for Infinite Volumes 151
data protection mirrors
active file systems for 31
creating 61
creating relationships for Infinite Volumes 118, 127
FlexVol volumes, support of 29
Infinite Volume size requirements for mirror copy transfers 150
Infinite Volume support of 29
initializing data protection mirror relationships for Infinite Volumes 118, 127
making a destination volume writeable 83
reestablishing the relationship after disaster 78
reversing the relationship after disaster 78
support limitations for Infinite Volumes 34
understanding aggregate selection for destination Infinite Volumes 151
using to test databases 83
data protection policies
types of 13
data protection strategy
planning 15
databases
protection of 11
deleting
Snapshot copies automatically 23
deployment configurations
basic, defined 42
how mirror-mirror cascades work 43
how mirror-SnapVault cascades work 43
how SnapVault-mirror cascades work 44
mirror-SnapVault fanout, defined 45
multiple-mirrors fanout, how they work 46
source-to-destination-to-tape, defined 42
supported data protection 40
destination Infinite Volumes
adding dedicated aggregates to a cluster for 114
adding shared aggregates to a cluster for 123
aggregates are automatically selected for 152
aggregates, method used to select for 166
availability of information about 130
client access to Snapshot copies on 31
creating 117, 127
creating a data protection mirror relationship for 118, 127
creating constituents for 118, 127
destinations of 118, 127
examples of automatic aggregate selection for 156
expanding by adding disks 141
how mirror copy updates affect aggregate selection 158
identifying aggregate space required for 122
identifying number of aggregates required for 112
identifying size required 112
namespace mirror constituents on 147
protocols supported for client access 31
understanding aggregate selection for 151
when aggregates are automatically selected for 151
destination volumes
access to active file systems on 31
CIFS clients cannot access 34
components of a mirror relationship 28
correcting to SnapVault secondary 96
matching source volume size 30
directories
for Snapshot copies of volumes 19
disaster recovery
Infinite Volumes with storage classes, for 165
reestablishing the original data protection mirror relationship 78
reversing the data protection mirror relationship 78
disasters
managing recovery for Infinite Volumes 136
tools to protect against data-loss 12
disk consumption
monitoring Snapshot copy 55
disk space
  recovery of 28
disks
  adding to Infinite Volumes 141
monitoring Snapshot copy consumption 55

E
error messages
  for failed aggregate selection 158
  insufficient space for the following source data constituents on destination Vserver 160
  insufficient space on destination for namespace constituent 159
  insufficient space on SnapMirror destination for source Infinite Volume data constituents 160
  size exceeds maximum, data constituents 160
  size exceeds maximum, namespace constituent 159
extended queries
  using to operate on many SnapMirror relationships 66

F
fanout limits
  mirror relationship 33
fanouts
  multiple-mirrors, how they work 46
file system
  recovery of disk space for use by the 28
file systems
  guidelines for restoring active, from SnapVault backups 101
files
  restoring from Snapshot copies of FlexVol volumes 53
FlexVol volumes
  creating SnapVault backup in prepopulated 93
  creating SnapVault backups in empty 88
  guidelines for creating SnapVault relationships on 85
  how maximum size affects Infinite Volumes in data protection mirror relationships 111
  mirror relationships for 29
  restoring part of a file 54
  SnapVault backup limitations 38
  which data gets backed up and restored from 36
  which data is not backed up to SnapVault backups 36

I
incremental transfers
  defined 35
Infinite Volumes
  adding new (dedicated) aggregates 142
  adding space to shared aggregates for 143
  aggregate requirements for data protection mirror relationships 110
  calculation used to verify space on one aggregate for multiple constituents 155
  commands for managing mirror relationships 132
  commands run sequentially 135
  constituents
    how you can recover 136
    creating a namespace mirror constituent for 139
    creating cluster peer relationships 117, 126
    creating Vserver peer relationships 117, 126
  data protection mirror update errors for 158
  data protection mirrors
    adding dedicated aggregates to Infinite Volumes 142
  data protection mirrors supported for 29
  default Snapshot policy for 49
  effect of namespace mirror constituents on the state of 149
  error messages for failed aggregate selection 158
  examples of automatic aggregate selection 156
  expanding by adding disks 141
  expanding onto more aggregate space 144
  expanding when in data protection mirror relationships 141
  guidelines for Snapshot copies 17
  how aggregates are automatically selected 153
  how constituents are recovered 136
  how maximum constituent size affects data protection mirror relationships 111
  how namespace mirror constituents provide data protection 147
  how namespace mirror constituents support tape backup 147
  how provisioning affects aggregate selection 155
  how Snapshot policies are associated with 49
  how storage classes use aggregates for 163
  identifying aggregates used by 112
  identifying number of data constituents used by 122
  identifying size the size 112
  information about destination, when available 130
  initialization errors for 158
  managing disaster recovery 136
maximum number of Snapshot copies for namespace mirror constituents on protocols supported for the active file system providing disaster recovery using mirroring technology recovering failed constituents reenabling SnapDiff restrictions for automatic aggregate selection retrieving data during a disaster setting up data protection using dedicated aggregates setting up data protection using shared aggregates Snapshot copies clients can access storage classes, definition of storage classes, with See also Infinite Volumes with storage classes support limitations for SnapMirror troubleshooting updating data protection mirror copies manually viewing constituents in viewing information about data protection mirror relationships volume size calculation for mirror copy transfer when active file system is available on the destination Infinite Volumes with storage classes creating a data protection mirror copy for data protection mirror relationships, impact on expanding to use more aggregate space exporting a data policy increasing the size when in a mirror relationship retrieving data during disaster recovery Snapshot copies, impact on tools for creating mirror copies using mirroring technology invalid state Snapshot copies

L
language settings requirement between Vservers limitations mirror relationship of Infinite Volume support for SnapMirror SnapVault backup

limits mirror relationship fanout

load-sharing mirrors modifying relationship schedules locks supported for the active file system on destination Infinite Volumes
LUNs guidelines for restoring in SAN environments protecting data

M
methods overview of data protection manually updating data protection, on volumes mirror policies commands for managing description of mirror relationships components of creating for Infinite Volumes with storage classes differences between cluster administrator and Vserver administrator policy management privileges fanout limits on guidelines for creating limitations tools for creating for Infinite Volumes with storage classes mirror-SnapVault cascades creating SnapVault backup for how they work preserving Snapshot copies on primary source volume of mirrors creating data protection deleting modifying load-sharing relationship schedules reestablishing the relationship after disaster reversing the relationship after disaster scheduling when transfers occur Snapshot copy limit using to test databases multiple-mirrors fanout deployments how they work
namespace constituent  
viewing in an Infinite Volume 131  
namespace mirror constituents  
creating for destination Infinite Volumes 139  
definition of 147  
effect of modifying the Infinite Volume 148  
effect on Infinite Volume state 149  
impact on source and destination Infinite Volumes 147  
viewing in an Infinite Volume 131  
viewing in Infinite Volumes 130  

namespaces  
protecting Vserver 38  
naming guidelines  
SnapMirror and SnapVault policy 58  
naming guidelines for SnapMirror 58  
nodes  
losing quorum affects Snapshot copies of Infinite Volumes 20  

NVRAM  
warning of database validity 11  

O  
older-than-base Snapshot copies  
backing up from 97  
out-of-order Snapshot copies  
how they work 97  

P  
partial state  
Snapshot copies 19  
path names  
abbreviating 30  
pattern matching of 30  
 wildcard use for 30  
pattern matching path names 30  
permissions  
for Snapshot copies 19  
policies  
commands for managing mirror and SnapVault 57  
commands for managing Snapshot copy 50  
 differences between cluster administrator and Vserver administrator management privileges 58  
example of creating tiered backup 59  

introduction to managing data protection using SnapMirror 57  
naming guidelines for SnapVault 58  
SnapMirror, how they work with clusters and Vservers 57  
Snapshot copy schedule and retention planning guidelines for SnapVault backups 39  
types of data protection 13  
 prefixes  
using to name automatic Snapshot copies 52  
primary volumes  
defined 35  
 protection deployments  
See deployment configurations  
 protection policies  
types of data 13  
 protocols  
supported on destination Infinite Volumes 31  

R  
recovery tasks  
Snapshot copy 16  
 relationships  
components of mirror 28  
creating SnapVault backup, in a prepopulated FlexVol volume 93  
creating SnapVault backup, in empty FlexVol volumes 88  
guidelines for creating mirror or SnapVault, between clusters or Vservers 31  
guidelines for creating SnapVault, on FlexVol volumes 85  
prepopulated SnapVault secondary scenarios 87  
SnapVault, creating baseline from tape 95  
transition (TDP) 10  

requirements  
Vserver language setting 30  
reserve  
 example of what happens when exceeding Snapshot copy 27  
restore operations  
guidelines for LUNs in SAN environments 101  
guidelines for restoring active file system from SnapVault backups 101  
how they work from a SnapVault backup 102  
restoring volumes from SnapVault backups 103  
restoring Snapshot copies  
Shadow Copy Client tools 55  
root information
protection Vserver 38

S

SAN (storage area network)
  data protection of volumes containing LUNs 13
SAN environments
  guidelines for restoring LUNs in 101
  which LUN data is backed up to SnapVault backups 36
  which LUN data is not backed up to SnapVault backups 36
schedules
  commands for managing Snapshot copy 50
  creating a Snapshot copy 21
  for default Snapshot copies 20
  guidelines for planning Snapshot copy 39
  Snapshot copies of Infinite Volumes, default for 49
  strategies for Snapshot copies 51
secondary volumes
  defined 35
  enabling storage efficiency on SnapVault 108
SMtape
  performing tape seeding using 67
SMtape backup and restore sessions
  scalability limits for 74
SnapDiff
  namespace mirror constituents creation for tape
  backup of Infinite Volumes 147
  namespace mirror constituents for 147
  reenabling it after expanding destination Infinite Volume 146
SnapMirror
  creating a data protection 61
  data protection mirrors supported for Infinite Volumes 29
  deleting a mirror relationship 77
  how destination volumes match source volume size 30
  listing the state of a scheduled transfer 74
  modifying relationship schedules 75
  scheduling when transfers occur 75
  support limitations for Infinite Volume 34
  using extended queries 66
SnapMirror commands
  for managing mirror and SnapVault policies 57
SnapMirror labels
  defined 35
SnapMirror policies
  how they work with clusters and Vservers 57

introduction to managing data protection using 57
Snapshot copies
  backing up FlexVol volumes with over 251 100
  backing up from older than base 97
  backup and recovery tasks you can perform with 16
  client access on destination Infinite Volumes 31
  commands for managing 48
  commands for managing policies and schedules 50
  creating a schedule 21
  default schedule 20
  default schedule for Infinite Volumes 49
  defined 35
  defining 15
  deleting automatically 23
  directory for 19
  example of what happens when the reserve is exceeded 27
  guidelines for Infinite Volumes 17
  how out-of-order transfers work 97
  how they work 15
  Infinite Volumes 19, 31
  Infinite Volumes with storage classes, impact on 18
  limit on source volume 34
  maximum number 18
  monitoring disk consumption of) 55
  preserving on primary source volume in mirror-SnapVault cascades 92
  protecting data, about 48
  restoring a single file from 53
  restoring part of a file 54
  restoring volume contents 54
  states 19
  types of user-specified schedules 21
  using prefixes to name automatic 52
  viewing automatic deletion settings for 24
  what copies to access 19
Snapshot copies of Infinite Volumes
  client access is temporarily disabled 20
  guidelines for 17
Snapshot copy reserve
  how deleted active file disk space consumes 26
Snapshot policies
  description of 13
  how volumes inherit from Vservers 49
  Infinite Volumes, default for 49
SnapVault
  backing up FlexVol volumes with over 255 Snapshot copies 100
  backing up from older-than-base Snapshot copy 97
converting data protection destination to secondary 96
creating a baseline from tape 95
creating backup, in a prepopulated FlexVol volume 93
differences between cluster administrator and Vserver administrator policy management privileges 58
which data is backed up and restored from FlexVol volume 36
which data is not backed up to 36
SnapVault backups
creating in empty FlexVol volumes 88
creating in mirror-SnapVault cascades 91
guidelines for managing storage efficiency for 107
guidelines for planning Snapshot copy schedule and retention for 39
guidelines for restoring active file system from 101
guidelines for restoring LUNs in SAN environments 101
how restore operations work from 102
how they work 37
how they work with data compression 38
introduction to protecting FlexVol volume date using 85
limitations for FlexVol volume backup 38
managing SnapVault-mirror cascade when unavailable 104
preserving Snapshot copies on primary source volume in mirror-SnapVault cascades 92
restoring volumes from 103
Vserver namespace 38
SnapVault policies
commands for managing 57
description of 13
how out-of-order Snapshot copy transfers work with 97
SnapVault relationships
defined 35
example of creating tiered backup policy for 59
guidelines for creating 31
guidelines for creating on FlexVol volumes 85
managing backup of copied source volumes in 101
prepopulated secondary scenarios 87
SnapVault secondary volumes
enabling storage efficiency on 108
introduction to managing storage efficiency for 107
SnapVault updates
no space on destination aggregate failure 87
SnapVault-mirror cascades
how they work 44
managing when SnapVault backup is unavailable 104
source Infinite Volumes
namespace mirror constituents on 147
source volumes
components of a mirror relationship 28
managing SnapVault backup of copied 101
space guarantee
how affects aggregate selection for destination Infinite Volumes 154
states
Snapshot copies 19
storage classes
creating mirror copies of Infinite Volumes with 164
data protection mirror relationships for Infinite Volumes, impact on 162
definition of 162
increasing the size of Infinite Volumes when in a mirror relationship 166
retrieving data from Infinite Volumes with 165
Snapshot copies of Infinite Volumes, impact on 18
tools for creating mirror relationships for Infinite Volumes with 163
using mirroring technology on Infinite Volumes with 162
See also Infinite Volumes with storage classes
storage efficiency
enabling on SnapVault secondary volume 108
guidelines for managing, for SnapVault backups 107
how SnapVault backups work with data compression 38
introduction to managing, for SnapVault secondary volumes 107

T
tape backup
how namespace mirror constituents support SnapDiff for 147
tape seeding 66
tiered backup policies
example of creating 59
tools
for data-loss protection 12
transfers
mirror copy, size calculation of Infinite Volumes for 150
scheduling SnapMirror 75
V

valid state
  Snapshot copies
  volumes
volume snapshot commands
  for managing Snapshot copies
volume snapshot policy commands
  for managing Snapshot copy policies and schedules
volumes
  components of a mirror relationship
  converting data protection destination to SnapVault secondary
  creating SnapVault backup in prepopulated FlexVol
  creating SnapVault backups in empty FlexVol
  enabling storage efficiency on SnapVault secondary
  guidelines for creating SnapVault relationships on FlexVol
  how Snapshot policies are associated with
  manually updating data protection mirror copies on
  maximum number of Snapshot copies for
  restoring from SnapVault backup
  SnapVault copies clients can access
  SnapVault backup limitations for FlexVol

which data gets backed up and restored from FlexVol
Vserver administrators
  mirror and SnapVault relationship management capabilities
Vserver peering
  creating peer relationships between Vservers with Infinite Volume
Vservers
  assigning aggregates for
  default Snapshot policies associated with
  guidelines for creating mirror or SnapVault relationships between
  how SnapMirror policies work with
  mirror language setting requirement
  namespace, protecting
  root information, protecting
Vservers with Infinite Volume
  creating
  exporting a data policy
  methods of aggregate selection for destination
Infinite Volumes
  specifying an aggregate list

W

wildcards
  path names using