Protect and restore data

Active IQ Unified Manager 9.10

NetApp
October 22, 2024

Table of Contents

Protect and restore data

Creating, monitoring, and troubleshooting protection relationships

Unified Manager enables you to create protection relationships, to monitor and troubleshoot mirror protection and backup vault protection of data stored on managed clusters, and to restore data when it is overwritten or lost.

Types of SnapMirror protection

Depending on the deployment of your data storage topology, Unified Manager enables you to configure multiple types of SnapMirror protection relationships. All variations of SnapMirror protection offer failover disaster recovery protection, but offer differing capabilities in performance, version flexibility, and multiple backup copy protection.

Traditional SnapMirror Asynchronous protection relationships

Traditional SnapMirror Asynchronous protection provides block replication mirror protection between source and destination volumes.

In traditional SnapMirror relationships, mirror operations execute faster than they would in alternative SnapMirror relationships because the mirror operation is based on block replication. However, traditional SnapMirror protection requires that the destination volume run under the same or later minor version of ONTAP software as the source volume within the same major release (for example, version 8.x to 8.x, or 9.x to 9.x). Replication from a 9.1 source to a 9.0 destination is not supported because the destination is running an earlier major version.

SnapMirror Asynchronous protection with version-flexible replication

SnapMirror Asynchronous protection with version-flexible replication provides logical replication mirror protection between source and destination volumes, even if those volumes are running under different versions of ONTAP 8.3 or later software (for example, version 8.3 to 8.3.1, or 8.3 to 9.1, or 9.2.2 to 9.2).

In SnapMirror relationships with version-flexible replication, mirror operations do not execute as quickly as they would in traditional SnapMirror relationships.

Because of slower execution, SnapMirror with version-flexible replication protection is not suitable to implement in either of the following circumstances:

- The source object contains more than 10 million files to protect.
- The recovery point objective for the protected data is two hours or less. (That is, the destination must always contain mirrored, recoverable data that is no more than two hours older than data at the source.)

In either of the listed circumstances, the faster block-replication based execution of default SnapMirror protection is required.

SnapMirror Asynchronous protection with version-flexible replication and backup option

SnapMirror Asynchronous protection with version-flexible replication and backup option provides mirror

protection between source and destination volumes and the capability to store multiple copies of the mirrored data at the destination.

The storage administrator can specify which Snapshot copies are mirrored from source to destination and can also specify how long to retain those copies at the destination, even if they are deleted at the source.

In SnapMirror relationships with version-flexible replication and backup option, mirror operations do not execute as quickly as they would in traditional SnapMirror relationships.

SnapMirror Unified Replication (mirror and vault)

SnapMirror unified replication allows you to configure disaster recovery and archiving on the same destination volume. As with SnapMirror, unified data protection performs a baseline transfer the first time you invoke it. A baseline transfer under the default unified data protection policy “MirrorAndVault” makes a Snapshot copy of the source volume, then transfers that copy and the data blocks it references to the destination volume. Like SnapVault, unified data protection does not include older Snapshot copies in the baseline.

SnapMirror Synchronous protection with strict synchronization

SnapMirror Synchronous protection with “strict” synchronization ensures that the primary and secondary volumes are always a true copy of each other. If a replication failure occurs when attempting to write data to the secondary volume, then the client I/O to the primary volume is disrupted.

SnapMirror Synchronous protection with regular synchronization

SnapMirror Synchronous protection with “regular” synchronization does not require that the primary and secondary volume are always a true copy of each other; thereby ensuring availability of the primary volume. If a replication failure occurs when attempting to write data to the secondary volume, the primary and secondary volumes fall out of sync and client I/O will continue to the primary volume.

The Restore button and the Relationship operation buttons are not available when monitoring synchronous protection relationships from the Health: All Volumes view or the Volume / Health details page.

SnapMirror Synchronous Business Continuity

The SnapMirror Business Continuity (SM-BC) feature is available with ONTAP 9.8 and later, and you can use it to protect applications with LUNs, enabling applications to fail over transparently, ensuring business continuity in case of a disaster.

It allows you to discover and monitor the synchronous SnapMirror relationships for Consistency Groups (CGs) available on clusters and storage virtual machines from Unified Manager. SM-BC is supported on AFF clusters or All SAN Array (ASA) clusters, where the primary and secondary clusters can be either AFF or ASA. SM-BC protects applications with iSCSI or FCP LUNs.

When you view the volumes and LUNs protected by the SM-BC relationship, you can get a unified view for protection relationships, Consistency Groups in volume inventory, view protection topology for Consistency Group relationships, view historical data for Consistency Group relationships up to a year. You can also download the report. You can also view the summary of Consistency Group relationships, search support for Consistency Group relationships, and gain information about volumes that are protected by the Consistency Group.

On the Relationships page, you can also sort, filter, and extend protection on the source and destination storage objects and their relationship that are protected by the Consistency Group.

To know more about SnapMirror Synchronous Business Continuity, refer to ONTAP 9 Documentation for SM-BC.

Setting up protection relationships in Unified Manager

There are several steps that you must perform to use Unified Manager and OnCommand Workflow Automation to set up SnapMirror and SnapVault relationships to protect your data.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have established peer relationships between two clusters or two storage virtual machines (SVMs).
- OnCommand Workflow Automation must be integrated with Unified Manager:
  - Set up OnCommand Workflow Automation
  - Verifying Unified Manager data source caching in Workflow Automation

Steps

1. Depending on the type of protection relationship you want to create, do one of the following:
   - Create a SnapMirror protection relationship.
   - Create a SnapVault protection relationship.
2. If you want to create a policy for the relationship, depending on the relationship type you are creating, do one of the following:
   - Create a SnapVault policy.
   - Create a SnapMirror policy.
3. Create a SnapMirror or SnapVault schedule.

Configuring a connection between Workflow Automation and Unified Manager

You can configure a secure connection between OnCommand Workflow Automation (WFA) and Unified Manager. Connecting to Workflow Automation enables you to use protection features such as SnapMirror and SnapVault configuration workflows, as well as commands for managing SnapMirror relationships.

What you'll need

- The installed version of Workflow Automation must be 5.1 or greater.

  The "WFA pack for managing Clustered Data ONTAP" is included in WFA 5.1 so there is no need to download this pack from the NetAppStorage Automation Store and install it separately onto your WFA server as was required in the past. WFA pack for managing ONTAP

- You must have the name of the database user that you created in Unified Manager to support WFA and Unified Manager connections.

This database user must have been assigned the Integration Schema user role.

- You must be assigned either the Administrator role or the Architect role in Workflow Automation.
- You must have the host address, port number 443, user name, and password for the Workflow Automation setup.
- You must have the Application Administrator or Storage Administrator role.

Steps

1. In the left navigation pane, click **General** > **Workflow Automation**.
2. In the **Database User** area of the **Workflow Automation page**, select the name, and enter the password for the database user that you created to support Unified Manager and Workflow Automation connections.
3. In the **Workflow Automation Credentials** area of the page, enter the host name or IP address (IPv4 or IPv6), and the user name and password for the Workflow Automation setup.

   You must use the Unified Manager server port (port 443).

4. Click **Save**.
5. If you use a self-signed certificate, click **Yes** to authorize the security certificate.

   The Workflow Automation page displays.

6. Click **Yes** to reload the web UI, and add the Workflow Automation features.

Related information

NetApp Documentation: OnCommand Workflow Automation (current releases)

Verifying Unified Manager data source caching in Workflow Automation

You can determine whether Unified Manager data source caching is working correctly by checking if data source acquisition is successful in Workflow Automation. You might do this when you integrate Workflow Automation with Unified Manager to ensure that Workflow Automation functionality is available after the integration.

What you'll need

You must be assigned either the Administrator role or the Architect role in Workflow Automation to perform this task.

Steps

1. From the Workflow Automation UI, select **Execution** > **Data Sources**.
2. Right-click the name of the Unified Manager data source, and then select **Acquire Now**.
3. Verify that the acquisition succeeds without errors.

   Acquisition errors must be resolved for Workflow Automation integration with Unified Manager to succeed.

What happens when OnCommand Workflow Automation is reinstalled or upgraded

Before reinstalling or upgrading OnCommand Workflow Automation, you must first remove the connection between OnCommand Workflow Automation and Unified

Manager, and ensure that all OnCommand Workflow Automation currently running or scheduled jobs are stopped.

You must also manually delete Unified Manager from OnCommand Workflow Automation.

After you reinstall or upgrade OnCommand Workflow Automation, you must set up the connection with Unified Manager again.

Removing OnCommand Workflow Automation setup from Unified Manager

You can remove the OnCommand Workflow Automation setup from Unified Manager when you no longer want to use Workflow Automation.

What you'll need

You must have the Application Administrator or Storage Administrator role.

Steps

1. In the left navigation pane, click **General** > **Workflow Automation** in the left Setup menu.
2. In the **Workflow Automation** page, click **Remove Setup**.

Performing a protection relationship failover and failback

When a source volume in your protection relationship is disabled because of a hardware failure or a disaster, you can use the protection relationship features in Unified Manager to make the protection destination read/write accessible and fail over to that volume until the source is online again; then, you can fail back to the original source when it is available to serve data.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up OnCommand Workflow Automation to perform this operation.

Steps

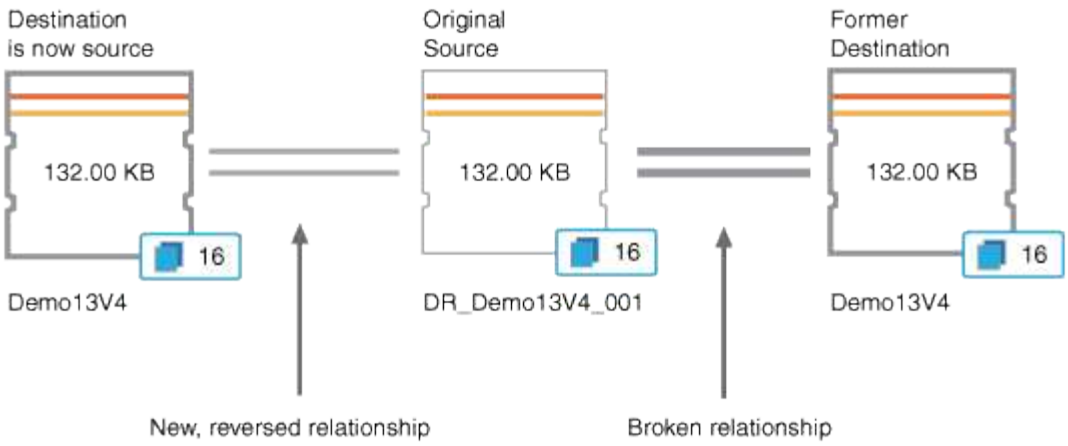
1. Break the SnapMirror relationship.

   You must break the relationship before you can convert the destination from a data protection volume to a read/write volume, and before you can reverse the relationship.

2. Reverse the protection relationship.

   When the original source volume is available again, you might decide to reestablish the original protection relationship by restoring the source volume. Before you can restore the source, you must synchronize it with the data written to the former destination. You use the reverse resync operation to create a new protection relationship by reversing the roles of the original relationship and synchronizing the source volume with the former destination. A new baseline Snapshot copy is created for the new relationship.

   The reversed relationship looks similar to a cascaded relationship:



3. Break the reversed SnapMirror relationship.

   When the original source volume is resynchronized and can again serve data, use the break operation to break the reversed relationship.

4. Remove the relationship.

   When the reversed relationship is no longer required, you should remove that relationship before reestablishing the original relationship.

5. Resynchronize the relationship.

   Use the resynchronize operation to synchronize data from the source to the destination and to reestablish the original relationship.

Breaking a SnapMirror relationship from the Volume / Health details page

You can break a protection relationship from the Volume / Health details page and stop data transfers between a source and destination volume in a SnapMirror relationship. You might break a relationship when you want to migrate data, for disaster recovery, or for application testing. The destination volume is changed to a read-write volume. You cannot break a SnapVault relationship.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.

Steps

1. In the **Protection** tab of the **Volume / Health** details page, select from the topology the SnapMirror relationship you want to break.
2. Right-click the destination and select **Break** from the menu.

   The Break Relationship dialog box is displayed.

3. Click **Continue** to break the relationship.
4. In the topology, verify that the relationship is broken.

Reversing protection relationships from the Volume / Health details page

When a disaster disables the source volume in your protection relationship, you can use the destination volume to serve data by converting it to read/write while you repair or replace the source. When the source is again available to receive data, you can use the reverse resynchronization operation to establish the relationship in the reverse direction, synchronizing the data on the source with the data on the read/write destination.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.
- The relationship must not be a SnapVault relationship.
- A protection relationship must already exist.
- The protection relationship must be broken.
- Both the source and destination must be online.
- The source must not be the destination of another data protection volume.
- When you perform this task, data on the source that is newer than the data on the common Snapshot copy is deleted.
- Policies and schedules created on the reverse resynchronization relationship are the same as those on the original protection relationship.

  If policies and schedules do not exist, they are created.

Steps

1. From the **Protection** tab of the **Volume / Health** details page, locate in the topology the SnapMirror relationship on which you want to reverse the source and destination, and right-click it.
2. Select **Reverse Resync** from the menu.

   The Reverse Resync dialog box is displayed.

3. Verify that the relationship displayed in the **Reverse Resync** dialog box is the one for which you want to perform the reverse resynchronization operation, and then click **Submit**.

   The Reverse Resync dialog box is closed and a job link is displayed at the top of the Volume / Health details page.

4. **Optional:** Click **View Jobs** on the **Volume / Health** details page to track the status of each reverse resynchronization job.

   A filtered list of jobs is displayed.

5. **Optional:** Click the **Back** arrow on your browser to return to the **Volume / Health** details page.

   The reverse resynchronization operation is finished when all job tasks are completed successfully.

Removing a protection relationship from the Volume / Health details page

You can remove a protection relationship to permanently delete an existing relationship between the selected source and destination: for example, when you want to create a relationship using a different destination. This operation removes all metadata and cannot be undone.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.

Steps

1. In the **Protection** tab of the **Volume / Health** details page, select from the topology the SnapMirror relationship you want to remove.
2. Right-click the name of the destination and select **Remove** from the menu.

   The Remove Relationship dialog box is displayed.
3. Click **Continue** to remove the relationship.

   The relationship is removed from the Volume / Health details page.

Resynchronizing protection relationships from the Volume / Health details page

You can resynchronize data on a SnapMirror or SnapVault relationship that was broken and then the destination was made read/write so that data on the source matches the data on the destination. You might also resynchronize when a required common Snapshot copy on the source volume is deleted causing SnapMirror or SnapVault updates to fail.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up OnCommand Workflow Automation.

Steps

1. From the **Protection** tab of the **Volume / Health** details page, locate in the topology the protection relationship that you want to resynchronize and right-click it.
2. Select **Resynchronize** from the menu.

   Alternatively, from the **Actions** menu, select **Relationship** > **Resynchronize** to resynchronize the relationship for which you are currently viewing the details.

   The Resynchronize dialog box is displayed.
3. In the **Resynchronization Options** tab, select a transfer priority and the maximum transfer rate.
4. Click **Source Snapshot Copies**; then, in the **Snapshot Copy** column, click **Default**.

   The Select Source Snapshot Copy dialog box is displayed.

5. If you want to specify an existing Snapshot copy rather than transferring the default Snapshot copy, click **Existing Snapshot Copy** and select a Snapshot copy from the list.
6. Click **Submit**.

   You are returned to the Resynchronize dialog box.

7. If you selected more than one source to resynchronize, click **Default** for the next source for which you want to specify an existing Snapshot copy.
8. Click **Submit** to begin the resynchronization job.

   The resynchronization job is started, you are returned to the Volume / Health details page and a jobs link is displayed at the top of the page.

9. **Optional:** Click **View Jobs** on the **Volume / Health details** page to track the status of each resynchronization job.

   A filtered list of jobs is displayed.

10. **Optional:** Click the **Back** arrow on your browser to return to the **Volume / Health** details page.

    The resynchronization job is finished when all job tasks successfully complete.

Resolving a protection job failure

This workflow provides an example of how you might identify and resolve a protection job failure from the Unified Manager dashboard.

What you'll need

Because some tasks in this workflow require that you log in using the Administrator role, you must be familiar with the roles required to use various functionality.

In this scenario, you access the Dashboard page to see if there are any issues with your protection jobs. In the Protection Incident area, you notice that there is a Job Terminated incident, showing a Protection Job Failed error on a volume. You investigate this error to determine the possible cause and potential resolution.

Steps

1. In the Protection Incidents panel of the Dashboard Unresolved Incidents and Risks area, you click the **Protection job failed** event.

   The linked text for the event is written in the form `object_name:/object_name - Error Name`, such as `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`.

   The Event details page for the failed protection job displays.

2. Review the error message in the Cause field of the **Summary** area to determine the problem and evaluate potential corrective actions.

   See Identifying the problem and performing corrective actions for a failed protection job.

Identifying the problem and performing corrective actions for a failed protection job

You review the job failure error message in the Cause field on the Event details page and determine that the job failed because of a Snapshot copy error. You then proceed to the Volume / Health details page to gather more information.

What you'll need

You must have the Application Administrator role.

The error message provided in the Cause field on the Event details page contains the following text about the failed job:

```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure.)
Job Details
```

This message provides the following information:

- A backup or mirror job did not complete successfully.

  The job involved a protection relationship between the source volume `cluster2_src_vol2` on the virtual server `cluster2_src_svm` and the destination volume `managed_svc2_vol3` on the virtual server named `cluster3_dst_svm`.

- A Snapshot copy job failed for `0426cluster2_src_vol2snap` on the source volume `cluster2_src_svm:/cluster2_src_vol2`.

In this scenario, you can identify the cause and potential corrective actions of the job failure. However, resolving the failure requires that you access either the System Manager web UI or the ONTAP CLI commands.

Steps

1. You review the error message and determine that a Snapshot copy job failed on the source volume, indicating that there is probably a problem with your source volume.

   Optionally, you could click the **Job Details** link at the end of the error message, but for the purposes of this scenario, you choose not to do that.

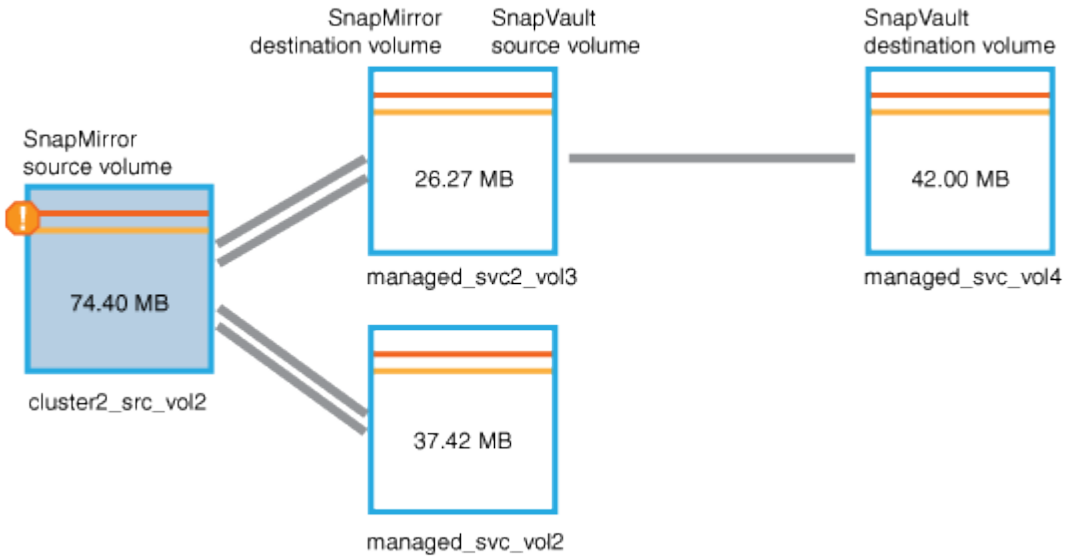
2. You decide that you want to try to resolve the event, so you do the following:
   a. Click the **Assign To** button and select **Me** from the menu.
   b. Click the **Acknowledge** button so that you do not continue to receive repeat alert notifications, if alerts were set for the event.
   c. Optionally, you can also add notes about the event.
3. Click the **Source** field in the **Summary** pane to see details about the source volume.

The **Source** field contains the name of the source object: in this case, the volume on which the Snapshot copy job was scheduled.

The Volume / Health details page displays for `cluster2_src_vol2`, showing the content of the Protection tab.

4. Looking at the protection topology graph, you see an error icon associated with the first volume in the topology, which is the source volume for the SnapMirror relationship.

   You also see the horizontal bars in the source volume icon, indicating the warning and error thresholds set for that volume.



5. You place your cursor over the error icon to see the pop-up dialog box that displays the threshold settings and see that the volume has exceeded the error threshold, indicating a capacity issue.
6. Click the **Capacity** tab.

   Capacity information about volume `cluster2_src_vol2` displays.

7. In the **Capacity** panel, you see that there is an error icon in the bar graph, again indicating that the volume capacity has surpassed the threshold level set for the volume.
8. Below the capacity graph, you see that volume autogrow has been disabled and that a volume space guarantee has been set.

   You could decide to enable autogrow, but for the purposes of this scenario, you decide to investigate further before making a decision about how to resolve the capacity problem.

9. You scroll down to the **Events** list and see that Protection Job Failed, Volume Days Until Full, and Volume Space Full events were generated.
10. In the **Events** list, you click the **Volume Space Full** event to get more information, having decided that this event seems most relevant to your capacity issue.

    The Event details page displays the Volume Space Full event for the source volume.

11. In the **Summary** area, you read the Cause field for the event: `The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.`

12. Below the Summary area, you see Suggested Corrective Actions.

    The Suggested Corrective Actions display only for some events, so you do not see this area for all types of events.

    You click through the list of suggested actions that you might perform to resolve the Volume Space Full event:

    - Enable autogrow on this volume.
    - Resize the volume.
    - Enable and run deduplication on this volume.
    - Enable and run compression on this volume.

13. You decide to enable autogrow on the volume, but to do so, you must determine the available free space on the parent aggregate and the current volume growth rate:
    a. Look at the parent aggregate, `cluster2_src_aggr1`, in the **Related Devices** pane.

       You can click the name of the aggregate to get further details about the aggregate.

       You determine that the aggregate has sufficient space to enable volume autogrow.

    b. At the top of the page, look at the icon indicating a critical incident and review the text below the icon.

       You determine that "Days to Full: Less than a day | Daily Growth Rate: 5.4%".

14. Go to System Manager or access the ONTAP CLI to enable the `volume autogrow` option.

    Make note of the names of the volume and aggregate so you have them available when enabling autogrow.

15. After resolving the capacity issue, return to the Unified Manager **Event** details page and mark the event as resolved.

Resolving lag issues

This workflow provides an example of how you might resolve a lag issue. In this scenario, you are an administrator or operator accessing the Unified ManagerDashboard page to see if there are any problems with your protection relationships and, if they exist, to find solutions.

What you'll need

You must have the Application Administrator or Storage Administrator role.

In the Dashboard page, you look at the Unresolved Incidents and Risks area and see a SnapMirror Lag error in the Protection pane under Protection Risks.

Steps

1. In the **Protection** pane on the **Dashboard** page, locate the SnapMirror relationship lag error and click it.

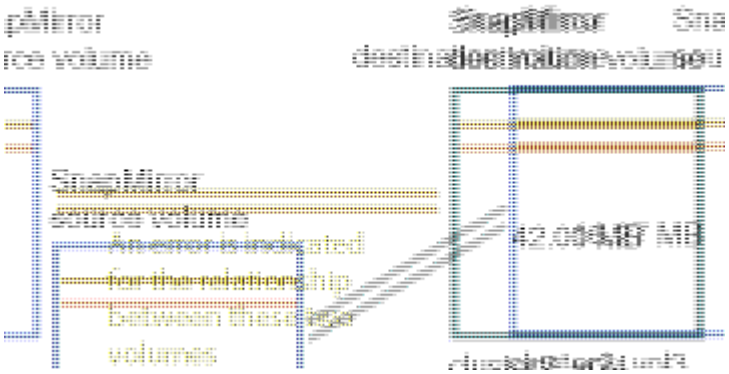
The Event details page for the lag error event is displayed.

2. From the **Event** details page you can perform one or more of the following tasks:
   - Review the error message in the Cause field of the Summary area to determine if there is any suggested corrective action.
   - Click the object name, in this case a volume, in the Source field of the Summary area to get details about the volume.
   - Look for notes that might have been added about this event.
   - Add a note to the event.
   - Assign the event to a specific user.
   - Acknowledge or resolve the event.
3. In this scenario, you click the object name (in this case, a volume) in the Source field of the **Summary** area to get details about the volume.

   The Protection tab of the Volume / Health details page is displayed.

4. In the **Protection** tab, you look at the topology diagram.

   You note that the volume with the lag error is the last volume in a three-volume SnapMirror cascade. The volume you selected is outlined in dark gray, and a double orange line from the source volume indicates a SnapMirror relationship error.



5. Click each of the volumes in the SnapMirror cascade.

   As you select each volume, the protection information in the Summary, Topology, History, Events, Related Devices, and Related Alerts areas changes to display details relevant to the selected volume.

6. You look at the **Summary** area and position your cursor over the information icon in the **Update Schedule** field for each volume.

   In this scenario, you note that the SnapMirror policy is DPDefault, and the SnapMirror schedule updates hourly at five minutes after the hour. You realize that all of the volumes in the relationship are attempting to complete a SnapMirror transfer at the same time.

7. To resolve the lag issue, you modify the schedules for two of the cascaded volumes so that each destination begins a SnapMirror transfer after its source has completed a transfer.

Managing and monitoring protection relationships

Active IQ Unified Manager enables you to create protection relationships, to monitor and troubleshoot SnapMirror and SnapVault relationships on managed clusters, and to restore data when it is overwritten or lost.

For SnapMirror operations there are two replication types:

- Asynchronous

  Replication from the primary to the secondary volume is determined by a schedule.

- Synchronous

  Replication is performed simultaneously on the primary and secondary volume.

You can perform up to 10 protection jobs simultaneously with no performance impact. You might experience some performance impact when you run between 11 and 30 jobs simultaneously. Running more than 30 jobs simultaneously is not recommended.

Viewing volume protection status

The Data Protection page presents a holistic view of the data protection details for all the protected volumes in a single cluster, or all clusters in a data center.

You can view these details when you click the right-arrow at the top of the Data Protection panel on the dashboard. There are two sections on this screen. When you select all clusters on the dashboard, the **All Clusters** section displays the protection status of all the clusters at a data center level protected by SnapMirror relationships and Snapshot copy. You can select a specific cluster in the **Individual Cluster** section to view the status of the protected volumes in that cluster.

If you select a single cluster on the dashboard, this page displays the details of the protected volumes on that cluster.

You can hover your mouse over each of the bar charts to view the respective counts. Clicking the bar charts takes you to the Volumes screen with the respective volumes selected. Clicking the link from each of these events takes you to the Event details page. You can click the **View All** link to view all active protection events in the Event Management inventory page.

Steps

1. In the left navigation pane, click **Dashboard**.
2. Depending on whether you want to view data protection status for all monitored clusters or for a single cluster, select **All Clusters** or select a single cluster from the drop-down menu.
3. Click the right-arrow in the Data Protection panel.

Data Protection page

The Data Protection page displays the following panels for protected volumes for all clusters.

For the volume count of the Snapshot copies, both source and destination volumes are considered. For SnapMirror relationships, the source volumes, which are enabled for reading and writing, are counted. Destination and root volumes are not considered. The SnapMirror count includes the number of volumes with sources and destinations on the same or different clusters.

- **Snapshot Overview**: An overview of the volumes protected by Snapshot copies, such as:
  - The total number of volumes protected and not protected by Snapshot copies.

    For considering a volume as protected, the schedule for the Snapshot copy of the volume should be enabled.

  - The total number of volumes that are using or exceeding the reserve space for the Snapshot copies. This value is important for viewing the amount of disk space utilized or calculating the space that can be reclaimed if one or more Snapshot copies are deleted.
- **SnapMirror Overview**: An overview of the volumes protected by SnapMirror policies, such as:
  - The number of volumes protected by the respective SnapMirror policies, such as, volume SnapMirror relationships, storage VM disaster recovery (SVM-DR), and their combinations.
  - The total number of volumes experiencing lag in SnapMirror relationships. If a volume has multiple SnapMirror relationships, the worst lag is selected.

The individual cluster list displays the status of the SnapMirror relationships and Snapshot protection for a specific cluster.

- **Snapshot Copies Analysis** details the following information:
  - Individual events for Snapshot copies, including the events raised in the last 24 hours.
  - Detailed chart for volumes protected and not protected by Snapshot copies.
  - Volumes using, not using, and breaching the reserved Snapshot copy capacity. You can use this information to calculate the space that is utilized or can be reclaimed if one or more Snapshot copies are deleted.
  - Break-up of the volume counts in terms of the number of their Snapshot copies. The number of Snapshot copies returned is for only the volumes that are online and available.
- **SnapMirror Analysis** details the following information:
  - Individual events raised for SnapMirror relationships, including the events raised in the last 24 hours
  - The number of volumes protected by each of the SnapMirror policies, such as, volume SnapMirror relationships, storage VM disaster recovery (SVM-DR), and their combinations.
  - The number of volumes protected by the SnapMirror relationship types, such as Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StrictSync, SnapMirror Business Continuity (SMBC) consistency group, and Sync.
  - The number of volumes with healthy or unhealthy relationship status. A volume is considered healthy only if all its SnapMirror relationships are healthy.
  - Break-up of the volume counts by the rate of their recovery point objective (RPO) lag duration.

Viewing volume protection relationships

From the Relationship: All Relationships view, and from the Volume Relationships page,

you can view the status of existing volume SnapMirror and SnapVault relationships. You can also examine details about protection relationships, including transfer and lag status, source and destination details, schedule and policy information, and so on.

What you'll need

You must have the Application Administrator or Storage Administrator role.

You can also initiate relationship commands from this page.

Steps

1. In the left navigation pane, click **Storage** > **Volumes**.
2. From the View menu, select **Relationship** > **All Relationships**.

   The Relationship: All Relationships view is displayed.

3. Choose one of the following ways to view the volume protection details:
   - To view current information about all the volume relationships, remain on the default **All Relationships** page.
   - To view detailed information about the volume transfer trends over a period of time, in the View menu, select Relationship: Last 1 month Transfer Status view.
   - To view detailed information about the volume transfer activity on a day to day basis, in the View menu, select Relationship: Last 1 month Transfer Rate view.

   The volume transfer views display information for volumes in asynchronous relationships only - volumes in synchronous relationships are not shown.

Monitoring LUNs in a Consistency Group relationship

If your ONTAP environment supports SnapMirror Business Continuity (SM-BC) to protect applications with LUNs, you can view and monitor those LUNs on Active IQ Unified Manager.

SM-BC ensures zero recovery time objective (RTO) during failover in SAN environments. In a typical deployment supporting SM-BC, the LUNs on volumes are protected by Consistency Group relationships.

These primary and secondary LUNs are composite LUNs, or a replica LUN pair with the same UUID and serial number. The I/O operations (both read and write) are multiplexed across the source and destination sites on these composite LUNs, ensuring transparency.

For viewing composite LUNs, both the primary and secondary clusters with the LUNs that are a part of the Consistency Group relationship should be added and discovered on Unified Manager. Only iSCSI and FCP LUNs are supported.

For information about SM-BC, see ONTAP 9 Documentation for SM-BC.

To view composite LUNs in your environment follow these steps:

Steps

1. In the left navigation pane, click **Storage** > **LUNs**.

2. From the View menu, select **Relationship** > **All LUNs**.

   The Relationship: All LUNs view is displayed.

You can view the LUN details, such as the LUN name, volume, storage VM hosting the LUN, cluster, Consistency Group, and the partner LUN. You can click each of these components to drill down to a detailed view. Clicking the Consistency Group takes you to the Relationships page.

Clicking the partner LUN enables you to view its configuration details on the SAN tab of the Storage VM Details page for the storage VM on which the partner LUN is hosted. Information such as the initiators and initiator groups and other aspects of the partner LUN is displayed.

You can perform the standard grid-level functions of sorting, filtering, generating and uploading reports for the protected LUNs in your environment.

Creating a SnapVault protection relationship from the Health: All Volumes view

You can use the Health: All Volumes view to create SnapVault relationships for one or more volumes on the same Storage VM to enable data backups for protection purposes.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.

The **Protect** menu does not display in the following instances:

- If RBAC settings do not allow this action: for example, if you have only operator privileges
- When the volume ID is unknown: for example, when you have an intercluster relationship and the destination cluster has not yet been discovered

Steps

1. In the left navigation pane, click **Storage** > **Volumes**.
2. In the **Health: All Volumes** view, select a volume you want to protect and click **Protect**.

   Alternatively, to create multiple protection relationships on the same storage virtual machine (SVM), select one or more volumes in the Health: All Volumes view, and click **Protect** on the toolbar.

3. Select **SnapVault** from the menu.

   The Configure Protection dialog box is launched.

4. Click **SnapVault** to view the **SnapVault** tab and to configure the secondary volume information.
5. Click **Advanced** to set deduplication, compression, autogrow, and space guarantee as needed, and then click **Apply**.
6. Complete the **Destination Information** area and the **Relationship Settings** area in the **SnapVault** tab.
7. Click **Apply**.

   You are returned to the Health: All Volumes view.

8. Click the protection configuration job link at the top of the **Health: All Volumes** view.

If you are creating only one protection relationship, the Job details page is displayed; however, if you are creating more than one protection relationship, a filtered list of all the jobs associated with the protection operation is displayed.

9. Do one of the following:
   - If you have only one job, click **Refresh** to update the tasks list and task details associated with the protection configuration job and to determine when the job is complete.
   - If you have more than one job:
     i. Click a job in the jobs list.
     ii. Click **Refresh** to update the tasks list and task details associated with the protection configuration job and to determine when the job is complete.
     iii. Use the **Back** button to return to the filtered list and view another job.

Creating a SnapVault protection relationship from the Volume / Health details page

You can create a SnapVault relationship using the Volume / Health details page so that data backups are enabled for protection purposes on volumes.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation to perform this task.

The **Protect** menu does not display in the following instances:

- If RBAC settings do not allow this action: for example, if you have only operator privileges
- When the volume ID is unknown: for example, when you have an intercluster relationship and the destination cluster has not yet been discovered

Steps

1. In the **Protection** tab of the **Volume / Health** details page, right-click a volume in the topology view that you want to protect.
2. Select **Protect** > **SnapVault** from the menu.

   The Configure Protection dialog box is launched.

3. Click **SnapVault** to view the **SnapVault** tab and to configure the secondary resource information.
4. Click **Advanced** to set deduplication, compression, autogrow, and space guarantee as needed, and then click **Apply**.
5. Complete the **Destination Information** area and the **Relationship Settings** area in the **Configure Protection** dialog box.
6. Click **Apply**.

   You are returned to the Volume / Health details page.

7. Click the protection configuration job link at the top of the **Volume / Health** details page.

   The Job details page is displayed.

8. Click **Refresh** to update the tasks list and task details associated with the protection configuration job and to determine when the job is complete.

   When the job tasks are complete, the new relationships are displayed in the Volume / Health details page topology view.

Creating a SnapMirror protection relationship from the Health: All Volumes view

Using the Health: All Volumes view enables you to create several SnapMirror protection relationships at one time by selecting more than one volume on the same storage VM.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.

The **Protect** menu does not display in the following instances:

- If RBAC settings do not allow this action: for example, if you have only operator privileges
- When the volume ID is unknown: for example, when you have an intercluster relationship and the destination cluster has not yet been discovered

Steps

1. In the **Health: All Volumes** view, select a volume that you want to protect.

   Alternatively, to create multiple protection relationships on the same SVM, select one or more volumes in the Health: All Volumes view, and click **Protect** > **SnapMirror** on the toolbar.

   The Configure Protection dialog box is displayed.

2. Click **SnapMirror** to view the **SnapMirror** tab and to configure the destination information.
3. Click **Advanced** to set the space guarantee, as needed, and then click **Apply**.
4. Complete the **Destination Information** area and the **Relationship Settings** area in the **SnapMirror** tab.
5. Click **Apply**.

   You are returned to the Health: All Volumes view.

6. Click the protection configuration job link at the top of the **Health: All Volumes view**.

   If you are creating only one protection relationship, the Job details page is displayed; however, if you are creating more than one protection relationship, a list of all the jobs associated with the protection operation is displayed.

7. Do one of the following:
   - If you have only one job, click **Refresh** to update the tasks list and task details associated with the protection configuration job and to determine when the job is complete.
   - If you have more than one job:
     i. Click a job in the jobs list.
     ii. Click **Refresh** to update the tasks list and task details associated with the protection configuration job and to determine when the job is complete.

iii. Use the **Back** button to return to the filtered list and view another job.

Depending on the destination SVM you specified during configuration or on the options you enabled in your Advanced settings, the resulting SnapMirror relationship might be one of several possible variations:

- If you specified a destination SVM that runs under the same or a newer version of ONTAP compared to that of the source volume, a block-replication-based SnapMirror relationship is the default result.
- If you specified a destination SVM that runs under the same or a newer version of ONTAP compared to that of the source volume, but you enabled version-flexible replication in the Advanced settings, a SnapMirror relationship with version-flexible replication is the result.
- If you specified a destination SVM that runs under an earlier version of ONTAP than that of the source volume, and the earlier version supports version-flexible replication, a SnapMirror relationship with version-flexible replication is the automatic result.

Creating a SnapMirror protection relationship from the Volume / Health details page

You can use the Volume / Health details page to create a SnapMirror relationship so that data replication is enabled for protection purposes. SnapMirror replication enables you to restore data from the destination volume in the event of data loss on the source.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.

The **Protect** menu does not display in the following instances:

- If RBAC settings do not allow this action: for example, if you have only operator privileges
- When the volume ID is unknown: for example, when you have an intercluster relationship and the destination cluster has not yet been discovered

You can perform up to 10 protection jobs simultaneously with no performance impact. You might experience some performance impact when you run between 11 and 30 jobs simultaneously. Running more than 30 jobs simultaneously is not recommended.

Steps

1. In the **Protection tab** of the **Volume / Health** details page, right-click in the topology view the name of a volume that you want to protect.
2. Select **Protect** > **SnapMirror** from the menu.

   The Configure Protection dialog box is displayed.
3. Click **SnapMirror** to view the **SnapMirror** tab and to configure the destination information.
4. Click **Advanced** to set the space guarantee, as needed, and then click **Apply**.
5. Complete the **Destination Information** area and the **Relationship Settings** area in the **Configure Protection** dialog box.
6. Click **Apply**.

   You are returned to the Volume / Health details page.

7. Click the protection configuration job link at the top of the **Volume / Health** details page.

   The job's tasks and details are displayed in the Job details page.

8. In the **Job** details page, click **Refresh** to update the tasks list and task details associated with the protection configuration job and to determine when the job is complete.
9. When the job tasks are complete, click **Back** on your browser to return to the **Volume / Health** details page.

   The new relationship is displayed in the Volume / Health details page topology view.

Depending on the destination SVM you specified during configuration or on the options you enabled in your Advanced settings, the resulting SnapMirror relationship might be one of several possible variations:

- If you specified a destination SVM that runs under the same or a newer version of ONTAP compared to that of the source volume, a block-replication-based SnapMirror relationship is the default result.
- If you specified a destination SVM that runs under the same or a newer version of ONTAP compared to that of the source volume, but you enabled version-flexible replication in the Advanced settings, a SnapMirror relationship with version-flexible replication is the result.
- If you specified a destination SVM that runs under an earlier version of ONTAP, or a version that is higher than that of the source volume and the earlier version supports version-flexible replication, a SnapMirror relationship with version-flexible replication is the automatic result.

Creating a SnapMirror relationship with version-flexible replication

You can create a SnapMirror relationship with version-flexible replication. Version-flexible replication enables you to implement SnapMirror protection even if source and destination volumes run under different versions of ONTAP.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.
- The source and destination SVMs must each have a SnapMirror license enabled.
- The source and destination SVMs must each run under a version of ONTAP software that supports version-flexible replication.

SnapMirror with version-flexible replication enables you to implement SnapMirror protection even in heterogeneous storage environments in which not all storage is running under one version of ONTAP; however, mirror operations performed under SnapMirror with version-flexible replication do not execute as quickly as they would under traditional block replication SnapMirror.

Steps

1. Display the **Configure Protection** dialog box for the volume that you want to protect.
   - If you are viewing the Protection tab of the Volume / Health details page, right-click in the topology view that has the name of a volume that you want to protect and select **Protect** > **SnapMirror** from the menu.
   - If you are viewing the Health: All Volumes view, locate a volume that you want to protect and right-click it; then select **Protect** > **SnapMirror** from the menu. The Configure Protection dialog box is displayed.

2. Click **SnapMirror** to view the **SnapMirror** tab.
3. Complete the **Destination Information** area and the **Relationship Settings** area in the **Configure Protection** dialog box.

   If you specify a destination SVM that runs under an earlier version of ONTAP than the source volume you are protecting, and if that earlier version supports version-flexible replication, this task automatically configures SnapMirror with version-flexible replication.

4. If you specify a destination SVM that runs under the same version of ONTAP as that of the source volume, but you still want to configure SnapMirror with version-flexible replication, click **Advanced** to enable version-flexible replication and then click **Apply**.
5. Click **Apply**.

   You are returned to the Volume / Health details page.

6. Click the protection configuration job link at the top of the **Volume / Health** details page.

   The jobs tasks and details are displayed in the Job details page.

7. In the **Job** details page, click **Refresh** to update the tasks list and task details associated with the protection configuration job and to determine when the job is complete.
8. When the job tasks are complete, click **Back** on your browser to return to the **Volume / Health** details page.

   The new relationship is displayed in the Volume / Health details page topology view.

Creating SnapMirror relationships with version-flexible replication with backup option

You can create a SnapMirror relationship with version-flexible replication and backup option capability. Backup option capability enables you to implement SnapMirror protection and also retain multiple versions of backup copies at the destination location.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.
- The source and destination SVMs must each have a SnapMirror license enabled.
- The source and destination SVMs must each have a SnapVault license enabled.
- The source and destination SVMs must each run under a version of ONTAP software that supports version-flexible replication.

Configuring SnapMirror with backup option capability enables you to protect your data with SnapMirror disaster recovery capabilities, such as volume failover ability, and at the same time provide SnapVault capabilities, such as multiple backup copy protection.

Steps

1. Display the **Configure Protection** dialog box for the volume that you want to protect.
   - If you are viewing the Protection tab of the Volume / Health details page, right-click in the topology view the name of a volume that you want to protect and select **Protect** > **SnapMirror** from the menu.

- If you are viewing the Health: All Volumes view, locate a volume you want to protect and right-click it; then select **Protect** > **SnapMirror** from the menu. The Configure Protection dialog box is displayed.

2. Click **SnapMirror** to view the **SnapMirror** tab.
3. Complete the **Destination Information** area and the **Relationship Settings** area in the **Configure Protection** dialog box.
4. Click **Advanced** to display the **Advanced Destination Settings** dialog box.
5. If the **Version-Flexible Replication** check box is not already selected, select it now.
6. Select the **With backup option** check box to enable backup option capability; then click **Apply**.
7. Click **Apply**.

   You are returned to the Volume / Health details page.

8. Click the protection configuration job link at the top of the **Volume / Health** details page.

   The jobs tasks and details are displayed in the Job details page.

9. In the **Job** details page, click **Refresh** to update the task list and task details associated with the protection configuration job and to determine when the job is complete.
10. When the job tasks are complete, click **Back** on your browser to return to the **Volume / Health** details page.

    The new relationship is displayed in the Volume / Health details page topology view.

Configuring destination efficiency settings

You can configure destination efficiency settings such as deduplication, compression, autogrow, and space guarantee on a protection destination using the Advanced Destination Settings dialog box. You use these settings when you want to maximize space utilization on a destination or secondary volume.

What you'll need

You must have the Application Administrator or Storage Administrator role.

By default, efficiency settings match those of the source volume, except for compression settings in a SnapVault relationship, which are disabled by default.

Steps

1. Click either the **SnapMirror** tab or the **SnapVault** tab in the **Configure Protection** dialog box, depending on the type of relationship you are configuring.
2. Click **Advanced** in the **Destination Information** area.

   The Advanced Destination Settings dialog box is opened.

3. Enable or disable the efficiency settings for deduplication, compression, autogrow, and space guarantee, as required.
4. Click **Apply** to save your selections and return to the **Configure Protection** dialog box.

Creating SnapMirror and SnapVault schedules

You can create basic or advanced SnapMirror and SnapVault schedules to enable automatic data protection transfers on a source or primary volume so that transfers take place more frequently or less frequently, depending on how often the data changes on your volumes.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have already completed the Destination Information area in the Configure Protection dialog box.
- You must have set up Workflow Automation to perform this task.

Steps

1. From the **SnapMirror** tab or **SnapVault** tab of the **Configure Protection** dialog box, click the **Create Schedule** link in the **Relationship Settings** area.

   The Create Schedule dialog box is displayed.

2. In the **Schedule Name** field, type the name you want to give to the schedule.
3. Select one of the following:
   - **Basic**

     Select if you want to create a basic interval-style schedule.

   - **Advanced**

     Select if you want to create a cron-style schedule.

4. Click **Create**.

   The new schedule is displayed in the SnapMirror Schedule or SnapVault Schedule drop-down list.

Creating cascade or fanout relationships to extend protection from an existing protection relationship

You can extend protection from an existing relationship by creating either a fanout from the source volume or a cascade from the destination volume of an existing relationship. You might do this when you need to copy data from one site to many sites or to provide additional protection by creating more backups.

You can extend protection to volumes using consistency group, which is a container that holds several volumes so that you can manage all of the volumes as one entity. You can view the SnapMirror Business Continuity (SM-BC) Consistency Group and the synchronous consistency group relationship in the Relationships page of Unified Manager.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.

Steps

1. Click **Protection** > **Relationships**. Alternatively, you view the relationships from the Volume details page.
2. From the **Volume Relationships** page, select the SnapMirror relationship from which you want to extend protection.
3. On the action bar, click **Extend Protection**.
4. In the menu, select either **From Source** or **From Destination**, depending on whether you are creating a fanout relationship from the source or a cascade relationship from the destination.
5. Select either **With SnapMirror** or **With SnapVault** depending on the type of protection relationship you are creating.

   The **Configure Protection** dialog box is displayed.

   This can be achieved from the unified relationship / Volume Relationship and Volume / Health details page.

6. Complete the information as indicated in the **Configure Protection** dialog box.

Editing protection relationships from the Volume Relationships page

You can edit existing protection relationships to change the maximum transfer rate, the protection policy, or the protection schedule. You might edit a relationship to decrease the bandwidth used for transfers, or to increase the frequency of scheduled transfers because data is changing often.

What you'll need

You must have the Application Administrator or Storage Administrator role.

The selected volumes must be protection relationship destinations. You cannot edit relationships when source volumes, load-sharing volumes, or volumes that are not the destination of a SnapMirror or SnapVault relationship are selected.

Steps

1. From the **Volume Relationships** page, select in the volumes list one or more volumes in the same SVM for which you want to edit relationship settings, and then select **Edit** from the toolbar.

   The Edit Relationship dialog box is displayed.

2. In the **Edit Relationship** dialog box, edit the maximum transfer rate, protection policy, or protection schedule, as needed.
3. Click **Apply**.

   The changes are applied to the selected relationships.

Editing protection relationships from the Volume / Health details page

You can edit existing protection relationships to change the current maximum transfer rate, protection policy, or protection schedule. You might edit a relationship to decrease the bandwidth used for transfers, or to increase the frequency of scheduled transfers

because data is changing often.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have installed and configured Workflow Automation.

The selected volumes must be protection relationship destinations. You cannot edit relationships when source volumes, load-sharing volumes, or volumes that are not the destination of a SnapMirror or SnapVault relationship are selected.

Steps

1. From the **Protection** tab of the **Volume / Health** details page, locate in the topology the protection relationship you want to edit and right-click it.
2. Select **Edit** from the menu.

   Alternatively, from the **Actions** menu, select **Relationship** > **Edit** to edit the relationship for which you are currently viewing the details.

   The **Edit Relationship** dialog box is displayed.
3. In the Edit Relationship dialog box, edit the maximum transfer rate, protection policy, or protection schedule, as needed.
4. Click **Apply**.

   The changes are applied to the selected relationships.

Creating a SnapMirror policy to maximize transfer efficiency

You can create a SnapMirror policy to specify the SnapMirror transfer priority for protection relationships. SnapMirror policies enable you to maximize transfer efficiency from the source to the destination by assigning priorities so that lower-priority transfers are scheduled to run after normal-priority transfers.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.
- This task assumes that you have already completed the Destination Information area in the Configure Protection dialog box.

Steps

1. From the **SnapMirror** tab of the **Configure Protection** dialog box, click the **Create Policy** link in the **Relationship Settings** area.

   The Create SnapMirror Policy dialog box is displayed.
2. In the **Policy Name** field, type a name you want to give the policy.
3. In the **Transfer Priority** field, select the transfer priority you want to assign to the policy.
4. In the **Comment** field, enter an optional comment for the policy.

5. Click **Create**.

   The new policy is displayed in the SnapMirror Policy drop-down list.

Creating a SnapVault policy to maximize transfer efficiency

You can create a new SnapVault policy to set the priority for a SnapVault transfer. You use policies to maximize the efficiency of transfers from the primary to the secondary in a protection relationship.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.
- You must have already completed Destination Information area in the Configure Protection dialog box.

Steps

1. From the **SnapVault** tab of the **Configure Protection** dialog box, click the **Create Policy** link in the **Relationship Settings** area.

   The SnapVault tab is displayed.

2. In the **Policy Name** field, type the name that you want to give the policy.
3. In the **Transfer Priority** field, select the transfer priority that you want to assign to the policy.
4. **Optional:** In the **Comment** field, enter a comment for the policy.
5. In the **Replication Label** area, add or edit a replication label, as necessary.
6. Click **Create**.

   The new policy is displayed in the Create Policy drop-down list.

Aborting an active data protection transfer from the Volume Relationships page

You can abort an active data protection transfer when you want to stop a SnapMirror replication that is in progress. You can also clear the restart checkpoint for transfers subsequent to the baseline transfer. You might abort a transfer when it conflicts with another operation, such as a volume move.

NOTE: You cannot abort volumes relationships that are protected by the Consistency Group.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.

The abort action does not display in the following instances:

- If RBAC settings do not allow this action: for example, if you have only operator privileges
- When the volume ID is unknown: for example, when you have an intercluster relationship and the

destination cluster has not yet been discovered

You cannot clear the restart checkpoint for a baseline transfer.

Steps

1. To abort transfers for one or more protection relationships, from the **Volume Relationships** page, select one or more volumes and, on the toolbar, click **Abort**.

   The Abort Transfer dialog box is displayed.

2. If you want to clear the restart checkpoint for a transfer that is not a baseline transfer, select **Clear Checkpoints**.
3. Click **Continue**.

   The Abort Transfer dialog box is closed, and the status of the abort job displays at the top of the Volume Relationships page, along with a link to the job details.

4. **Optional:** Click the **View details** link to go to the **Job** details page for additional details and to view job progress.

Aborting an active data protection transfer from the Volume / Health details page

You can abort an active data protection transfer when you want to stop a SnapMirror replication that is in progress. You can also clear the restart checkpoint for a transfer if it is not a baseline transfer. You might abort a transfer when it conflicts with another operation, such as a volume move.

You cannot abort volumes relationships that are protected by the Consistency Group.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.

The abort action does not display in the following instances:

- If RBAC settings do not allow this action: for example, if you have only operator privileges
- When the volume ID is unknown: for example, when you have an intercluster relationship and the destination cluster has not yet been discovered

You cannot clear the restart checkpoint for a baseline transfer.

Steps

1. In the **Protection** tab of the **Volume / Health** details page, right-click the relationship in the topology view for the data transfer you want to abort and select **Abort**.

   The Abort Transfer dialog box is displayed.

2. If you want to clear the restart checkpoint for a transfer that is not a baseline transfer, select **Clear Checkpoints**.
3. Click **Continue**.

The Abort Transfer dialog box is closed, and the status of the abort operation displays at the top of the Volume / Health details page along with a link to the job details.

4. **Optional:** Click the **View details** link to go to the **Job** details page for additional details and to view job progress.
5. Click each job task to view its details.
6. Click the Back arrow on your browser to return to the **Volume / Health** details page.

   The abort operation is finished when all job tasks successfully complete.

Quiescing a protection relationship from the Volume Relationships page

From the Volume Relationships page, you can quiesce a protection relationship to temporarily prevent data transfers from occurring. You might quiesce a relationship when you want to create a Snapshot copy of a SnapMirror destination volume that contains a database, and you want to ensure that its contents are stable during the Snapshot copy operation.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.

The quiesce action does not display in the following instances:

- If RBAC settings do not allow this action; for example, if you have only operator privileges
- When the volume ID is unknown; for example, when you have an intercluster relationship and the destination cluster has not yet been discovered
- When you have not paired Workflow Automation and Unified Manager

Steps

1. To quiesce transfers for one or more protection relationships, from the **Volume Relationships** page, select one or more volumes and, on the toolbar, click **Quiesce**.

   The Quiesce dialog box is displayed.

2. Click **Continue**.

   The status of the quiesce job is displayed at the top of the Volume / Health details page, along with a link to the job details.

3. Click the **View details** link to go to the **Job** details page for additional details and job progress.
4. **Optional:** Click the **Back** arrow on your browser to return to the **Volume Relationships** page.

   The quiesce job is finished when all job tasks are successfully completed.

Quiescing a protection relationship from the Volume / Health details page

You can quiesce a protection relationship to temporarily prevent data transfers from

occurring. You might quiesce a relationship when you want to create a Snapshot copy of a SnapMirror destination volume that contains a database, and you want to ensure that its contents are stable during the Snapshot copy.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.

The quiesce action does not display in the following instances:

- If RBAC settings do not allow this action, for example, if you have only operator privileges
- When the volume ID is unknown, for example, when you have an intercluster relationship and the destination cluster has not yet been discovered
- When you have not paired Workflow Automation and Unified Manager

Steps

1. In the **Protection** tab of the **Volume / Health** details page, right-click the relationship in the topology view for the protection relationship that you want to quiesce.
2. Select **Quiesce** from the menu.
3. Click **Yes** to continue.

   The status of the quiesce job is displayed at the top of the Volume / Health details page, along with a link to the job details.
4. Click the **View details** link to go to the **Job** details page for additional details and job progress.
5. **Optional:** Click the Back arrow on your browser to return to the **Volume / Health** details page.

   The quiesce job is finished when all job tasks are successfully completed.

Breaking a SnapMirror relationship from the Volume Relationships page

You can break a protection relationship to stop data transfers between a source volume and a destination volume in a SnapMirror relationship. You might break a relationship when you want to migrate data, for disaster recovery, or for application testing. The destination volume is changed to a read/write volume. You cannot break a SnapVault relationship.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.

Steps

1. From the **Volume Relationships** page, select one or more volumes with protection relationships for which you want to stop data transfers and, on the toolbar, click **Break**.

   The Break Relationship dialog box is displayed.

2. Click **Continue** to break the relationship.
3. In the **Volume Relationships** page, verify in the **Relationship State** column that the relationship is broken.

   The Relationship State column is hidden by default, so you might need to select it in the show/hide column list  .

Removing a protection relationship from the Volume Relationships page

From the Volume Relationships page, you can remove a protection relationship to permanently delete an existing relationship between the selected source and destination: for example, when you want to create a relationship using a different destination. This operation removes all metadata and cannot be undone.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.

Steps

1. From the **Volume Relationships** page, select one or more volumes with protection relationships you want to remove and, on the toolbar, click **Remove**.

   The Remove Relationship dialog box is displayed.

2. Click **Continue** to remove the relationship.

   The relationship is removed from the Volume Relationships page.

Resuming scheduled transfers on a quiesced relationship from the Volume Relationships page

After you have quiesced a relationship to stop scheduled transfers from occurring, you can use **Resume** to re-enable scheduled transfers so that data on the source or primary volume is protected. Transfers resume from a checkpoint, if one exists, at the next scheduled transfer interval.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.

You can select no more than 10 quiesced relationships on which to resume transfers.

Steps

1. From the Volume **Relationships** page, select one or more volumes with quiesced relationships, and, on the toolbar, click **Resume**.
2. In the **Resume** dialog box, click **Continue**.

You are returned to the Volume Relationships page.

3. To view the related job tasks and to track their progress, click the job link that is displayed at the top of the **Volume Relationships** page.
4. Do one of the following:
   - If only one job is displayed, in the Job details page click **Refresh** to update the tasks list and task details associated with the protection configuration job and to determine when the job is complete.
   - If more than one job is displayed,
     i. In the Jobs page, click the job for which you want to view the details.
     ii. In the Job details page, click **Refresh** to update the tasks list and task details associated with the protection configuration job and to determine when the job is complete. After the jobs finish, data transfers are resumed at the next scheduled transfer interval.

Resuming scheduled transfers on a quiesced relationship from the Volume / Health details page

After you have quiesced a relationship to stop scheduled transfers from occurring, you can use **Resume** on the Volume / Health details page to reenable scheduled transfers so that data on the source or primary volume is protected. Transfers resume from a checkpoint, if one exists, at the next scheduled transfer interval.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.

Steps

1. In the **Protection** tab of the **Volume / Health** details page, right-click in the topology view a quiesced relationship that you want to resume.

   Alternatively, select **Resume** from the **Actions** > **Relationship** menu.

2. In the **Resume** dialog box, click **Continue**.

   You are returned to the Volume / Health details page.

3. To view the related job tasks and to track their progress, click the job link that is displayed at the top of the **Volume / Health** details page.
4. In the **Job** details page, click **Refresh** to update the tasks list and task details associated with the protection configuration job and to determine when the job is complete.

   After the jobs are complete, data transfers are resumed at the next scheduled transfer interval.

Initializing or updating protection relationships from the Volume Relationships page

From the Volume Relationships page, you can perform a first-time baseline transfer on a new protection relationship, or update a relationship if it is already initialized and you want to perform a manual, unscheduled incremental update to transfer immediately.

You cannot initialize or update volumes protected by Consistency Groups.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up OnCommand Workflow Automation.

Steps

1. From the **Volume Relationships** page, right-click a volume and select one or more volumes with relationships that you want to update or initialize, and then, on the toolbar, click **Initialize/Update**.

   The **Initialize/Update** dialog box is displayed.

2. In the **Transfer Options** tab, select a transfer priority and the maximum transfer rate.
3. Click **Source Snapshot Copies**; then, in the **Snapshot Copy** column, click **Default**.

   The Select Source Snapshot Copy dialog box is displayed.

4. If you want to specify an existing Snapshot copy rather than transferring the default Snapshot copy, click **Existing Snapshot Copy** and select a Snapshot copy from the list.
5. Click **Submit**.

   You are returned to the **Initialize/Update** dialog box.

6. If you selected more than one source to initialize or update, click **Default** for the next source for which you want to specify an existing Snapshot copy.
7. Click **Submit** to begin the initialization or update job.

   The initialization or update job is started, you are returned to the Volume Relationships page, and a jobs link is displayed at the top of the page.

8. **Optional:** Click **View Jobs** on the **Health: All Volumes** view to track the status of each initialization or update job.

   A filtered list of jobs is displayed.

9. **Optional:** Click each job to see its details.
10. **Optional:** Click the **Back** arrow on your browser to return to the **Volume Relationships** page.

    The initialization or update operation is finished when all tasks successfully finish.

Initializing or updating protection relationships from the Volume / Health details page

You can perform a first-time baseline transfer on a new protection relationship, or update a relationship if it is already initialized and you want to perform a manual, unscheduled incremental update to transfer data immediately.

NOTE: You cannot initialize or update volumes protected by Consistency Groups.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up OnCommand Workflow Automation.

Steps

1. From the **Protection** tab of the **Volume / Health** details page, locate in the topology the protection relationship that you want to initialize or update, and then right-click it.
2. Select **Initialize/Update** from the menu.

   Alternatively, from the **Actions** menu, select **Relationship** > **Initialize/Update** to initialize or update the relationship for which you are currently viewing the details.

   The Initialize/Update dialog box is displayed.
3. In the **Transfer Options** tab, select a transfer priority and the maximum transfer rate.
4. Click **Source Snapshot Copies**; then, in the **Snapshot Copy** column, click **Default**.

   The Select Source Snapshot Copy dialog box is displayed.
5. If you want to specify an existing Snapshot copy rather than transferring the default Snapshot copy, click **Existing Snapshot Copy** and select a Snapshot copy from the list.
6. Click **Submit**.

   You are returned to the Initialize/Update dialog box.
7. If you selected more than one source to initialize or update, click **Default** for the next read/write source for which you want to specify an existing Snapshot copy.

   You cannot select a different Snapshot copy for data protection volumes.
8. Click **Submit** to begin the initialization or update job.

   The initialization or update job is started, you are returned to the Volume / Health details page, and a jobs link is displayed at the top of the page.
9. **Optional:** Click **View Jobs** on the **Volume / Health** details page to track the status of each initialization or update job.

   A filtered list of jobs is displayed.
10. **Optional:** Click each job to see its details.
11. **Optional:** Click the Back arrow on your browser to return to the **Volume / Health** details page.

    The initialization or update operation is finished when all job tasks successfully complete.

Resynchronizing protection relationships from the Volume Relationships page

From the Volume Relationships page, you can resynchronize a relationship either to recover from an event that disabled your source volume or when you want to change the current source to a different volume.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.

Steps

1. From the **Volume Relationships** page, select one or more volumes with quiesced relationships and, from the toolbar, click **Resynchronize**.

   The Resynchronize dialog box is displayed.

2. In the **Resynchronization Options** tab, select a transfer priority and the maximum transfer rate.
3. Click **Source Snapshot Copies**; then, in the **Snapshot Copy** column, click **Default**.

   The Select Source Snapshot Copy dialog box is displayed.

4. If you want to specify an existing Snapshot copy rather than transferring the default Snapshot copy, click **Existing Snapshot Copy** and select a Snapshot copy from the list.
5. Click **Submit**.

   You are returned to the Resynchronize dialog box.

6. If you selected more than one source to resynchronize, click **Default** for the next source for which you want to specify an existing Snapshot copy.
7. Click **Submit** to begin the resynchronization job.

   The resynchronization job is started, you are returned to the Volume Relationships page, and a jobs link is displayed at the top of the page.

8. **Optional:** Click **View Jobs** on the **Volume Relationships** page to track the status of each resynchronization job.

   A filtered list of jobs is displayed.

9. **Optional:** Click the **Back** arrow on your browser to return to the **Volume Relationships** page.

   The resynchronization operation is finished when all job tasks successfully finish.

Reversing protection relationships from the Volume Relationships page

When a disaster disables the source volume in your protection relationship, you can use the destination volume to serve data by converting it to a read/write volume while you repair or replace the source. When the source is again available to receive data, you can use the reverse resynchronization operation to establish the relationship in the reverse direction, synchronizing the data on the source with the data on the read/write destination.

What you'll need

- You must have the Application Administrator or Storage Administrator role.
- You must have set up Workflow Automation.
- The relationship must not be a SnapVault relationship.

- A protection relationship must already exist.
- The protection relationship must be broken.
- Both the source and destination must be online.
- The source must not be the destination of another data protection volume.
- When you perform this task, data on the source that is newer than the data on the common Snapshot copy is deleted.
- Policies and schedules created on reverse resynchronization relationships are the same as those on the original protection relationship.

  If policies and schedules do not exist, they are created.

Steps

1. From the **Volume Relationships** page, select one or more volumes with relationships that you want to reverse, and, on the toolbar, click **Reverse Resync**.

   The Reverse Resync dialog box is displayed.

2. Verify that the relationships displayed in the **Reverse Resync** dialog box are the ones for which you want to perform the reverse resynchronization operation, and then click **Submit**.

   The reverse resynchronization operation is started, you are returned to the Volume Relationships page, and a jobs link is displayed at the top of the page.

3. **Optional:** Click **View Jobs** on the **Volume Relationships** page to track the status of each reverse resynchronization job.

   A filtered list of jobs related to this operation is displayed.

4. **Optional:** Click the **Back** arrow on your browser to return to the **Volume Relationships** page.

   The reverse resynchronization operation is finished when all job tasks successfully complete.

Restoring data using the Health: All Volumes view

You can restore overwritten or deleted files, directories, or an entire volume from a Snapshot copy by using the restore feature on the Health: All Volumes view.

What you'll need

You must have the Application Administrator or Storage Administrator role.

You cannot restore NTFS file streams.

The restore option is not available when:

- The volume ID is unknown: for example, when you have an intercluster relationship and the destination cluster has not yet been discovered.
- The volume is configured for SnapMirror Synchronous replication.

Steps

1. In the **Health: All Volumes** view, select a volume from which you want to restore data.
2. From the toolbar, click **Restore**.

   The Restore dialog box is displayed. The dialog box is modified to have a two column layout to view and select multiple files. But you can only select 10 records at a time.

3. Select the volume and Snapshot copy from which you want to restore data, if different from the default.
4. Select the items you want to restore.

   You can restore the entire volume, or you can specify folders and files you want to restore.

5. Select the location to which you want the selected items restored; either **Original Location** or **Alternate Location**.
6. Click **Restore**.

   The restore process begins.

Restoring data using the Volume / Health details page

You can restore overwritten or deleted files, directories, or an entire volume from a Snapshot copy by using the restore feature on the Volume / Health details page.

What you'll need

You must have the Application Administrator or Storage Administrator role.

You cannot restore NTFS file streams.

The restore option is not available when:

- The volume ID is unknown: for example, when you have an intercluster relationship and the destination cluster has not yet been discovered.
- The volume is configured for SnapMirror Synchronous replication.

Steps

1. In the **Protection tab** of the **Volume / Health** details page, right-click in the topology view the name of the volume that you want to restore.
2. Select **Restore** from the menu.

   Alternatively, select **Restore** from the **Actions** menu to protect the current volume for which you are viewing the details.

   The Restore dialog box is displayed.

3. Select the volume and Snapshot copy from which you want to restore data, if different from the default.
4. Select the items you want to restore.

   You can restore the entire volume, or you can specify folders and files you want to restore.

5. Select the location to which you want the selected items restored: either **Original Location** or **Alternate Existing Location**.

6. If you select an alternate existing location, do one of the following:
    - In the Restore Path text field, type the path of the location to which you want to restore the data and then click **Select Directory**.
    - Click **Browse** to launch the Browse Directories dialog box and complete the following steps:
        i. Select the cluster, SVM, and volume to which you want to restore.
        ii. In the Name table, select a directory name.
        iii. Click **Select Directory**.
7. Click **Restore**.

   The restore process begins.

> If a restore operation fails between Cloud Volumes ONTAP HA clusters with an NDMP error, you may need to add an explicit AWS route in the destination cluster so that the destination can communicate with the source system's cluster management LIF. You perform this configuration step using BlueXP.

What resource pools are

Resource pools are groups of aggregates that are created by a storage administrator using Unified Manager to provide provisioning to partner applications for backup management.

You might pool your resources based on attributes such as performance, cost, physical location, or availability. By grouping related resources into a pool, you can treat the pool as a single unit for monitoring and provisioning. This simplifies the management of these resources and allows for a more flexible and efficient use of the storage.

During secondary storage provisioning, Unified Manager determines the most suitable aggregate in the resource pool for protection using the following criteria:

- The aggregate is a data aggregate (not a root aggregate) and it is ONLINE.
- The aggregate is on a destination cluster node whose ONTAP version is the same or greater than the source cluster major version.
- The aggregate has the largest available space of all the aggregates in the resource pool.
- After provisioning the destination volume, the aggregate space is within the nearly-full and nearly overcommitted threshold defined for the aggregate (global or local threshold, whichever is applicable).
- The number of FlexVol volumes on the destination node must not exceed the platform limit.

Creating resource pools

You can use the Create Resource Pool dialog box to group aggregates for provisioning purposes.

What you'll need

You must have the Application Administrator or Storage Administrator role.

Steps

Resource pools can contain aggregates from different clusters, but the same aggregate cannot belong to different resource pools.

1. In the left navigation pane, click **Protection** > **Resource Pools**.
2. In the **Resource Pools page**, click **Create**.
3. Follow the instructions in the **Create Resource Pool** dialog box to provide a name and description and to add aggregates as members to the resource pool you want to create.

Editing resource pools

You can edit an existing resource pool when you want to change the resource pool name and the description.

What you'll need

You must have the Application Administrator or Storage Administrator role.

The **Edit** button is enabled only when one resource pool is selected. If more than one resource pool is selected, the **Edit** button is disabled.

Steps

1. In the left navigation pane, click **Protection** > **Resource Pools**.
2. Select one resource pool from the list.
3. Click **Edit**.

   The Edit Resource Pool window is displayed.

4. Edit the resource pool name and description as needed.
5. Click **Save**.

   The new name and description are displayed in the resource pool list.

Viewing resource pools inventory

You can use the Resource Pools page to view the resource pool inventory and to monitor the remaining capacity for each resource pool.

What you'll need

You must have the Application Administrator or Storage Administrator role.

Step

1. In the left navigation pane, click **Protection** > **Resource Pools**.

   The resource pool inventory is displayed.

Adding resource pool members

A resource pool consists of a number of member aggregates. You can add aggregates to

existing resource pools to increase the amount of space available for secondary volume provisioning.

What you'll need

You must have the Application Administrator or Storage Administrator role.

You can add no more than 200 aggregates to a resource pool at one time. Aggregates shown in the Aggregates dialog box do not belong to any other resource pool.

Steps

1. In the left navigation pane, click **Protection** > **Resource Pools**.
2. Select a resource pool from the **Resource Pools** list.

   The resource pool members are displayed in the area below the resource pool list.

3. In the resource pool member area, click **Add**.

   The Aggregates dialog box is displayed.

4. Select one or more aggregates.
5. Click **Add**.

   The dialog box is closed and the aggregates are displayed in the member list for the selected resource pool.

Removing aggregates from resource pools

You can remove aggregates from an existing resource pool: for example, when you want to use an aggregate for some other purpose.

What you'll need

You must have the Application Administrator or Storage Administrator role.

Resource pool members are displayed only when a resource pool is selected.

Steps

1. In the left navigation pane, click **Protection** > **Resource Pools**.
2. Select the resource pool from which you want to remove member aggregates.

   The list of member aggregates is displayed in the Members pane.

3. Select one or more aggregates.

   The **Remove** button is enabled.

4. Click **Remove.**

   A warning dialog box is displayed.

5. Click **Yes** to continue.

The selected aggregates are removed from the Members pane.

Deleting resource pools

You can delete resource pools when they are no longer needed. For example, you might want to redistribute the member aggregates from one resource pool to several other resource pools, making the original resource pool obsolete.

What you'll need

You must have the Application Administrator or Storage Administrator role.

The **Delete** button is enabled only when at least one resource pool is selected.

Steps

1. In the left navigation pane, click **Protection** > **Resource Pools**.
2. Select the resource pool you want to delete.
3. Click **Delete**.

   The resource pool is removed from the resource pool list and its aggregates are removed from the members list.

Monitoring Storage VM Disaster Recovery protection relationships

Active IQ Unified Manager supports monitoring of storage VM disaster recovery relationships which provides disaster recovery at the granularity of a storage VM level. The storage VM disaster recovery enables the recovery of data present in the constituent volumes of the storage VM and the recovery of storage VM configuration.

A storage VM DR relationship is created from the source storage VM to the destination storage VM to provide asynchronous disaster recovery. You can select either to replicate all or subset of the storage VM configuration (excluding network and protocol configuration) along with the data volumes based on the cluster setup.

After the storage VM disaster recovery relationship is configured, when the source storage VM becomes unavailable due to either hardware failure or environmental disaster, the destination storage VM is started, that provides access to data with least disruption. Similarly, when the source storage VM becomes available, it is resynchronized with the destination storage VM and then, the source restarts to provide data. You can use SnapMirror commands to configure and manage storage VM disaster recovery relationship.

Monitoring Storage VMs using Relationships page

You can monitor your storage VM disaster recovery relationships from the Relationships page in the PROTECTION section of the INVENTORY. By default, the Relationships page lists only the top level relationships as the constituent relationships filter is applied.

What you'll need

You must have the Application Administrator or Storage Administrator role.

You use filters to view the storage VM disaster recovery relationships.

Steps

1. In the left navigation pane, click **PROTECTION** > **Relationships**.

   The page displays all type of relationships: volume, consistency group, and storage VM relationships.

2. Click **Filter**, and then select **Relationship Object Type** and **Storage VM** to view only storage VM disaster recovery relationships.
3. Click **Apply Filter**.

   You should clear the constituent relationships filter to view all the protection relationships.

   The page displays only storage VM disaster recovery relationships.

Viewing protection relationships from Storage VMs page

Using the Storage VMs page, you can view the status of existing storage VMs' disaster recovery relationships.

What you'll need

You must have the Application Administrator or Storage Administrator role.

You can also examine details of the protection relationships, including transfer and lag status, source, and destination detail. You can schedule reports or download existing reports in the format that you require. The **Show/Hide** button enables you to add the required columns to the reports as they are not displayed by default.

Steps

1. In the left navigation pane, click **STORAGE** > **Storage VMs**.
2. From the **VIEW** menu, select **Relationship** > **All Relationships**.

   The Relationship: All Relationships view is displayed with all the configured storage VMs.

Viewing Storage VMs based on protection status

You can use the Storage VMs page of the Inventory to view all the storage VMs in Active IQ Unified Manager and filter the storage VMs based on their protection status.

What you'll need

You must have the Application Administrator or Storage Administrator role.

A new column Protection Role is added to the storage VMs view that provides information on whether the storage VM is protected or unprotected.

If a source cluster is not added to Active IQ Unified Manager, then all the information related to that cluster is unavailable in the grids.

Steps

1. In the left navigation pane, click **STORAGE** > **Storage VMs**.
2. From the **VIEW** menu, select **Health** > **All Storage VMs**.

The Health: All Storage VMs is displayed.

3. Click **Filter** to view one of the following storage VMs.

To view	Filter value
Protected storage VMs	**Protection Role** is **Protected**
Unprotected storage VMs	**Protection Role** is **Unprotected**

> You cannot view both the protected and unprotected storage VMs at the same time. You will need to clear the existing filter to reapply a new filter option.

4. Click **Apply Filter**.

   The Unsaved view displays all the storage VMs that are either protected or unprotected by storage VM disaster recovery based on your filter selections.

Understanding Storage VM Peers

Storage VM peers are mappings from a source storage VM to a destination storage VM that are used by partner applications for resource selection and secondary volume provisioning.

Peers are always created between a source storage VM and a destination storage VM, regardless of whether the destination storage VM is a secondary destination or a tertiary destination. You cannot use a secondary destination storage VM as a source to create a peer with a tertiary destination storage VM.

You can peer a storage VM in three ways:

- Peer any storage VM

  You can create a peer between any primary source storage VM and one or more destination storage VM. This means that all existing storage VM that currently require protection, as well as any storage VMs that are created in the future, are peered with the specified destination storage VM. For example, you might want applications from several different sources at different locations to be backed up to one or more destination storage VM in one location.

- Peer a particular storage VM

  You can create a peer between a specific source storage VM and one or more specific destination storage VM. For example, if you are providing storage services to many clients whose data must be separate from one another, you can choose this option to associate a specific source storage VM to a specific destination storage VM that is assigned to only that client.

- Peer with an external storage VM

  You can create a peer between a source storage VM and an external flexible volume of a destination storage VM.

SVM and resource pool requirements to support storage services

You can better ensure conformance in partner applications if you observe some SVM association and resource pool requirements that are specific to storage services: for example, when you associate SVM and create resource pools in Unified Manager to support a protection topology in a storage service provided by a partner application.

Some applications partner with the Unified Manager server to provide services that automatically configure and execute SnapMirror or SnapVault backup protection between source volumes and protection volumes in secondary or tertiary locations. To support these protection storage services, you must use Unified Manager to configure the necessary SVM associations and resource pools.

To support storage service single-hop or cascaded protection, including replication from a SnapMirror source or SnapVault primary volume to either destination SnapMirror or to SnapVault backup volumes that reside in secondary or tertiary locations, observe the following requirements:

- SVM associations must be configured between the SVM containing the SnapMirror source or SnapVault primary volume and any SVM on which either a secondary volume or a tertiary volume resides.
  - For example, to support a protection topology in which source volume Vol_A resides on SVM_1, and SnapMirror secondary destination volume Vol_B resides on SVM_2, and tertiary SnapVault backup volume Vol_ C resides on SVM_3, you must use the Unified Manager web UI to configure a SnapMirror association between SVM_1 and SVM_2 and a SnapVault backup association between SVM_1 and SVM_3.

    In this example, any SnapMirror association or SnapVault backup association between SVM_2 and SVM_3 is not necessary and is not used.

  - To support a protection topology in which both source volume Vol_A and SnapMirror destination volume Vol_B reside on SVM_1, you must configure a SnapMirror association between SVM_1 and SVM_1.
- The resource pools must include cluster aggregate resources available to the associated SVMs.

  You configure resource pools through the Unified Manager web UI and then assign through the partner application the storage service secondary target and tertiary target nodes.

Creating Storage VM Peers

The Create Storage Virtual Machine Peers wizard enables partner protection applications to associate a source storage VM with a destination storage VM for use with SnapMirror and SnapVault relationships. Partner applications use these associations at the time of initial provisioning of destination volumes to determine which resources to select.

What you'll need

- The storage VM you are associating must already exist.
- You must have the Application Administrator or Storage Administrator role.

For any source storage VM and relationship type, you can choose only one destination storage VM on each destination cluster.

Changing associations using the delete and create functions affects only future provisioning operations. It does

not move existing destination volumes.

Steps

1. In the left navigation pane, click **Protection** > **Storage VM Peers**.
2. In the **SVM Peers** page, click **Create**.

   The Create Storage Virtual Machine Peers wizard is launched.

3. Select one of the following sources:
   - **Any**

     Choose this option when you want to create an association between any primary storage VM source to one or more destination storage VM. This means that all existing storage VM that currently require protection, as well as any storage VM that are created in the future, are associated with the specified destination storage VM. For example, you might want applications from several different sources at different locations backed up to one or more destination storage VM in one location.

   - **Single**

     Choose this option when you want to select a specific source storage VM associated with one or more destination storage VM. For example, if you are providing storage services to many clients whose data must be separate from one another, choose this option to associate a specific storage VM source to a specific storage VM destination that is assigned only to that client.

   - **None (External)**

     Choose this option when you want to create an association between a source storage VM and an external flexible volume of a destination storage VM.

4. Select one or both of the protection relationship types you want to create:
   - **SnapMirror**
   - **SnapVault**
5. Click **Next**.
6. Select one or more storage VM protection destination.
7. Click **Finish**.

Viewing Storage VM Peers

You can use the Storage VM Peers page to view existing storage VM peers and their properties and to determine if additional storage VMs are required.

What you'll need

You must have the Application Administrator or Storage Administrator role.

Step

1. In the left navigation pane, click **Protection** > **Storage VM Peers**.

   The list of storage VM Peers and their properties is displayed.

Deleting Storage VM Peers

You can delete storage VM peers for partner applications to remove the secondary provisioning relationship between source and destination storage VM; for example, you might do this when the destination storage VM is full and you want to create a new storage VM protection peer.

What you'll need

You must have the Application Administrator or Storage Administrator role.

The **Delete** button is disabled until at least one storage VM peer is selected. Changing associations using the delete and create functions affects only future provisioning operations; it does not move existing destination volumes.

Steps

1. In the left navigation pane, click **Protection** > **Storage VM Peers**.
2. Select at least one storage VM peer.

   The **Delete** button is enabled.

3. Click **Delete.**

   A warning dialog box is displayed.

4. Click **Yes** to continue.

   The selected storage VM peer is removed from the list.

What jobs are

A job is a series of tasks that you can monitor using Unified Manager. Viewing jobs and their associated tasks enables you to determine if they have completed successfully.

Jobs are initiated when you create SnapMirror and SnapVault relationships, when you perform any relationship operation (break, edit, quiesce, remove, resume, resynchronize, and reverse resync), when you perform data restoration tasks, when you log in to a cluster, and so on.

When you initiate a job, you can use the Jobs page and the Job details page to monitor the job and the progress of the associated job tasks.

Monitoring jobs

You can use the Jobs page to monitor job status and to view job properties such as storage service type, state, submitted time, and completed time to determine whether or not a job has successfully completed.

What you'll need

You must have the Application Administrator or Storage Administrator role.

Steps

1. In the left navigation pane, click **Protection** > **Jobs**.

   The Jobs page is displayed.

2. View the **State** column to determine the status of those jobs currently running.
3. Click on a job name to view details about that particular job.

   The Job details page is displayed.

Viewing job details

After you start a job, you can track its progress from the Job details page and monitor the associated tasks for possible errors.

What you'll need

You must have the Application Administrator or Storage Administrator role.

Steps

1. In the left navigation pane, click **Protection** > **Jobs**.
2. In the Jobs page, click a job name in the **Name** column to display the list of tasks associated with the job.
3. Click on a task to display additional information in the **Task Details** pane and the **Task Messages** pane to the right of the task list.

Aborting jobs

You can use the Jobs page to abort a job if it is taking too long to finish, is encountering too many errors, or is no longer needed. You can abort a job only if its status and type allow it. You can abort any running job.

What you'll need

You must have the Application Administrator or Storage Administrator role.

Steps

1. In the left navigation pane, click **Protection** > **Jobs**.
2. From the list of jobs, select one job, and then click **Abort**.
3. At the confirmation prompt, click **Yes** to abort the selected job.

Retrying a failed protection job

After you have taken measures to fix a failed protection job, you can use **Retry** to run the job again. Retrying a job creates a new job using the original job ID.

What you'll need

You must have the Application Administrator or Storage Administrator role.

You can retry only one failed job at a time. Selecting more than one job disables the **Retry** button. Only jobs of the type Protection Configuration and Protection Relationship Operation can be retried.

Steps

1. In the left navigation pane, click **Protection** > **Jobs**.
2. From the list of jobs, select a single failed Protection Configuration or Protection Relationship Operation type job.

   The **Retry** button is enabled.

3. Click **Retry**.

   The job is restarted.

Description of Protection relationships windows and dialog boxes

You can view and manage protection-related details such as resource pools, SVM associations, and protection jobs. You can use the appropriate Health Thresholds page to configure global health threshold values for aggregates, volumes, and relationships.

Resource Pools page

The Resource Pools page displays existing resource pools and their members, and enables you to create, monitor, and manage resource pools for provisioning purposes.

Command buttons

The command buttons enable you to perform the following tasks:

- **Create**

  Launches the Create Resource Pool dialog box, which you can use to create resource pools.

- **Edit**

  Enables you to edit the name and description of the resource pools that you create.

- **Delete**

  Enables you to delete one or more resource pools.

Resource Pools list

The Resource Pools list displays (in tabular format) the properties of existing resource pools.

- **Resource Pool**

  Displays the name of the resource pool.

- **Description**

  Describes the resource pool.

- **SnapLock Type**

  Displays the SnapLock type that is being used by the aggregates in the resource pool. Valid values for

SnapLock type are Compliance, Enterprise, and Non-SnapLock. A resource pool can contain aggregates of only one SnapLock type.

- **Total Capacity**

  Displays the total capacity (in MB, GB, and so on) of the resource pool.

- **Used Capacity**

  Displays the amount of space (in MB, GB, and so on) that is used in the resource pool.

- **Available Capacity**

  Displays the amount of space (in MB, GB, and so on) that is available in the resource pool.

- **Used %**

  Displays the percentage of space that is used in the resource pool.

Members list command buttons

The Members list command buttons enable you to perform the following tasks:

- **Add**

  Enables you to add members to the resource pool.

- **Delete**

  Enables you to delete one or more members from the resource pool.

Members list

The Members list displays (in tabular format) the resource pool members and their properties when a resource pool is selected.

- **Status**

  Displays the current status of the member aggregate. The status can be Critical (), Error (), Warning (), or Normal ().

- **Aggregate Name**

  Displays the name of the member aggregate.

- **State**

  Displays the current state of the aggregate, which can be one of the following:

  - Offline

    Read or write access is not allowed.

  - Online

Read and write access to the volumes that are hosted on this aggregate is allowed.

- Restricted

  Limited operations (such as parity reconstruction) are allowed, but data access is not allowed.

- Creating

  The aggregate is being created.

- Destroying

  The aggregate is being destroyed.

- Failed

  The aggregate cannot be brought online.

- Frozen

  The aggregate is (temporarily) not serving requests.

- Inconsistent

  The aggregate has been marked corrupted; you should contact technical support.

- Iron Restricted

  Diagnostic tools cannot be run on the aggregate.

- Mounting

  The aggregate is in the process of mounting.

- Partial

  At least one disk was found for the aggregate, but two or more disks are missing.

- Quiescing

  The aggregate is being quiesced.

- Quiesced

  The aggregate is quiesced.

- Reverted

  The revert of an aggregate is completed.

- Unmounted

  The aggregate has been unmounted.

- Unmounting

  The aggregate is being taken offline.

- Unknown

  The aggregate is discovered, but the aggregate information is not yet retrieved by the Unified Manager server.

By default, this column is hidden.

- **Cluster**

  Displays the name of the cluster to which the aggregate belongs.

- **Node**

  Displays the name of the node on which the aggregate resides.

- **Total Capacity**

  Displays the total capacity (in MB, GB, and so on) of the aggregate.

- **Used Capacity**

  Displays the amount of space (in MB, GB, and so on) that is used in the aggregate.

- **Available Capacity**

  Displays the amount of space (in MB, GB, and so on) that is available in the aggregate.

- **Used %**

  Displays the percentage of space that is used in the aggregate.

- **Disk Type**

  Displays the RAID configuration type, which can be one of the following:

  - RAID0: All the RAID groups are of type RAID0.
  - RAID4: All the RAID groups are of type RAID4.
  - RAID-DP: All the RAID groups are of type RAID-DP.
  - RAID-TEC: All the RAID groups are of type RAID-TEC.
  - Mixed RAID: The aggregate contains RAID groups of different RAID types (RAID0, RAID4, RAID-DP, and RAID-TEC). By default, this column is hidden.

Create Resource Pool dialog box

You can use the Create Resource Pool dialog box to name and describe a new resource pool and to add aggregates to and delete aggregates from that resource pool.

Resource Pool Name

The text boxes enable you to add the following information to create a resource pool:

Enables you to specify a resource pool name.

Description

Enables you to describe a resource pool.

Members

Displays the members of the resource pool. You can also add and delete members.

Command buttons

The command buttons enable you to perform the following tasks:

- **Add**

  Opens the Aggregates dialog box so that you can add aggregates from a specific cluster to the resource pool. You can add aggregates from different clusters, but the same aggregates cannot be added to more than one resource pool.

- **Remove**

  Enables you to remove selected aggregates from the resource pool.

- **Create**

  Creates the resource pool. This button is not enabled until information has been entered in the Resource Pool Name or Description fields.

- **Cancel**

  Discards the changes and closes the Create Resource Pool dialog box.

Edit Resource Pool dialog box

You can use the Edit Resource Pool dialog box to change the name and description of an existing resource pool. For example, if the original name and description is inaccurate or incorrect, you can change them so they are more precise.

Text boxes

The text boxes enable you to change the following information for the selected resource pool:

- **Resource Pool Name**

  Enables you to enter a new name.

- **Description**

  Enables you to enter a new description.

Command buttons

The command buttons enable you to perform the following tasks:

- **Save**

Saves the changes to the resource pool name and description.

- **Cancel**

  Discards the changes and closes the Edit Resource Pool dialog box.

Aggregates dialog box

You can use the Aggregates dialog box to select the aggregates that you want to add to your resource pool.

Command buttons

The command buttons enable you to perform the following tasks:

- **Add**

  Adds the selected aggregates to the resource pool. The Add button is not enabled until at least one aggregate is selected.

- **Cancel**

  Discards the changes, and closes the Aggregates dialog box.

Aggregates list

The Aggregates list displays (in tabular format) the names and properties of monitored aggregates.

- **Status**

  Displays the current status of a volume. The status can be Critical (), Error (), Warning (), or Normal ().

  You can move the pointer over the status to view more information about the event or events generated for the volume.

- **Aggregate Name**

  Displays the name of the aggregate.

- **State**

  Displays the current state of the aggregate, which can be one of the following:

  - Offline

    Read or write access is not allowed.

  - Restricted

    Limited operations (such as parity reconstruction) are allowed, but data access is not allowed.

  - Online

Read and write access to the volumes that are hosted on this aggregate is allowed.

- Creating

  The aggregate is being created.

- Destroying

  The aggregate is being destroyed.

- Failed

  The aggregate cannot be brought online.

- Frozen

  The aggregate is (temporarily) not serving requests.

- Inconsistent

  The aggregate has been marked corrupted; you should contact technical support.

- Iron Restricted

  Diagnostic tools cannot be run on the aggregate.

- Mounting

  The aggregate is in the process of mounting.

- Partial

  At least one disk was found for the aggregate, but two or more disks are missing.

- Quiescing

  The aggregate is being quiesced.

- Quiesced

  The aggregate is quiesced.

- Reverted

  The revert of an aggregate is completed.

- Unmounted

  The aggregate is offline.

- Unmounting

  The aggregate is being taken offline.

- Unknown

  The aggregate is discovered, but the aggregate information is not yet retrieved by the Unified Manager

server.

- **Cluster**

  Displays the name of the cluster on which the aggregate resides.

- **Node**

  Displays the name of the storage controller that contains the aggregate.

- **Total Capacity**

  Displays the total data size (in MB, GB, and so on) of the aggregate. By default, this column is hidden.

- **Committed Capacity**

  Displays the total space (in MB, GB, and so on) that is committed for all the volumes in the aggregate. By default, this column is hidden.

- **Used Capacity**

  Displays the amount of space (in MB, GB, and so on) that is used in the aggregate.

- **Available Capacity**

  Displays the amount of space (in MB, GB, and so on) that is available for data in the aggregate. By default, this column is hidden.

- **Available %**

  Displays the percentage of space that is available for data in the aggregate. By default, this column is hidden.

- **Used %**

  Displays the percentage of space that is used by data in the aggregate.

- **RAID Type**

  Displays the RAID type of the selected volume. The RAID type can be RAID0, RAID4, RAID-DP, RAID-TEC, or Mixed RAID.

SVM Peers page

The SVM Peers page enables you to view existing storage VM peers between source and destination storage VM and to create new storage VM for use by partner applications to create SnapMirror and SnapVault relationships.

Command buttons

The command buttons enable you to perform the following tasks:

- **Create**

  Opens the Create Storage Virtual Machine Peers page.

- **Delete**

  Enables you to delete the selected storage VM peers.

Storage VM Peers list

The SVM Peers list displays in a table the source and destination storage VM associations that have been created and the type of protection relationship allowed for each association.

- **Source Storage Virtual Machine**

  Displays the name of the source SVM.

- **Source Cluster**

  Displays the name of the source cluster.

- **Destination Storage Virtual Machine**

  Displays the name of the destination SVM.

- **Destination Cluster**

  Displays the name of the destination cluster.

- **Type**

  Displays the type of protection relationship. Relationship types are either SnapMirror or SnapVault.

Create Storage Virtual Machine Peers wizard

The Create Storage Virtual Machine Peers wizard enables you to peer source and destination storage VM for use in SnapMirror and SnapVault protection relationships.

Select Source

The Select Source panel enables you to select the source, or primary, storage VM in the storage VM peer.

- **Any**

  Enables you to create a peer between any storage VM source to one or more destination, or secondary, storage VM. This means that all existing storage VMs that currently require protection, as well as any storage VMs that are created in the future, are peered with the specified destination storage VM. For example, you might want applications from several different sources at different locations backed up to one or more destination storage VM in one location.

- **Single**

  Enables you to peer a specific source storage VM with one or more destination storage VM. For example, if you are providing storage services to many clients whose data must be separate from one another, choose this option to associate a specific storage VM source to a specific storage VM destination that is assigned only to that client.

- **None (External)**

Enables you to create an association between a source storage VM and an external flexible volume of a destination storage VM.

  - Storage Virtual Machine

    Lists the names of the available source storage VM

  - Cluster

    Lists the clusters on which each storage VM resides

- **Allow these kinds of relationships**

  Enables you to select the relationship type for the association:

  - SnapMirror

    Specifies a SnapMirror relationship as the peer type. Selecting this option enables data replication from the selected sources to the selected destinations.

  - SnapVault

    Specifies a SnapVault relationship as the peer type. Selecting this option enables backups from the selected primary locations to the selected secondary locations.

Select Protection Destinations

The Select Protection Destinations panel of the Create Storage Virtual Machine Peers wizard enables you to select where to copy or replicate the data. You can create a peer on only one destination storage VM per cluster.

Command buttons

The command buttons enable you to perform the following tasks:

- **Next**

  Advances you to the next page in the wizard.

- **Back**

  Returns you to the previous page in the wizard.

- **Finish**

  Applies your selections and creates the association.

- **Cancel**

  Discards the selections and closes the Create Storage Virtual Machine Peers wizard.

Jobs page

The Jobs page enables you to view the current status and other information about all

partner application protection jobs that are currently running, as well as jobs that have completed. You can use this information to see which jobs are still running and whether a job has succeeded or failed.

Command buttons

The command buttons enable you to perform the following tasks:

- **Abort**

  Aborts the selected job. This option is available only if the selected job is running.

- **Retry**

  Restarts a failed job of type Protection Configuration or Protection Relationship Operation. You can retry only one failed job at a time. If more than one failed job is selected, the **Retry** button is disabled. You cannot retry failed storage service jobs.

- **Refresh**

  Refreshes the list of jobs and the information associated with them.

Jobs list

The Jobs list displays, in tabular format, a list of the jobs that are in progress. By default, the list displays only the jobs generated within the past week. You can use column sorting and filtering to customize which jobs are displayed.

- **Status**

  Displays the current status of a job. The status can be Error (⚠️) or Normal (✅).

- **Job Id**

  Displays the identification number of the job. By default, this column is hidden.

  The job identification number is unique and is assigned by the server when it starts the job. You can search for a particular job by entering the job identification number in the text box provided by the column filter.

- **Name**

  Displays the name of the job.

- **Type**

  Displays the job type. The job types are as follows:

  - **Cluster Acquisition**

    A Workflow Automation job is rediscovering a cluster.

  - **Protection Configuration**

    A protection job is initiating Workflow Automation workflows, such as cron schedules, SnapMirror policy creation, and so on.

- **Protection Relationship Operation**

  A protection job is running SnapMirror operations.

- **Protection Workflow Chain**

  A Workflow Automation job is executing multiple workflows.

- **Restore**

  A restore job is running.

- **Cleanup**

  The job is cleaning up storage service member artifacts that are no longer needed for restore purposes.

- **Conform**

  The job is checking the configuration of storage service members to ensure that they conform.

- **Destroy**

  The job is destroying a storage service.

- **Import**

  The job is importing unmanaged storage objects into an existing storage service.

- **Modify**

  The job is modifying attributes of an existing storage service.

- **Subscribe**

  The job is subscribing members to a storage service.

- **Unsubscribe**

  The job is unsubscribing members from a storage service.

- **Update**

  A protection update job is running.

- **WFA Configuration**

  A Workflow Automation job is pushing cluster credentials and synchronizing database caches.

- **State**

Displays the running state of the job. State options are as follows:

- **Aborted**

  The job has been aborted.

- **Aborting**

  The job is in the process of aborting.

- **Completed**

  The job has finished.

- **Running**

  The job is running.

- **Submitted Time**

  Displays the time the job was submitted.

- **Duration**

  Displays the amount of time the job took to complete. This column is displayed by default.

- **Completed Time**

  Displays the time the job finished. By default, this column is hidden.

Job details page

The Job details page enables you to view status and other information about specific protection job tasks that are running, that are queued, or that have completed. You can use this information to monitor protection job progress and to troubleshoot job failures.

Job summary

The job summary displays the following information:

- Job ID
- Type
- State
- Submitted Time
- Completed Time
- Duration

Command buttons

The command buttons enable you to perform the following tasks:

- **Refresh**

  Refreshes the task list and the properties associated with each task.

- **View Jobs**

  Returns you to the Jobs page.

Job tasks list

The Job tasks list displays in a table all the tasks associated with a specific job and the properties related to each task.

- **Started Time**

  Displays the day and time the task started. By default, the most recent tasks are displayed at the top of the column and older tasks are displayed at the bottom.

- **Type**

  Displays the type of task.

- **State**

  The state of a particular task:

  - **Completed**

    The task has finished.

  - **Queued**

    The task is about to run.

  - **Running**

    The task is running.

  - **Waiting**

    A job has been submitted and some associated tasks are waiting to be queued and executed.

- **Status**

  Displays the task status:

  - **Error (❗)**

    The task failed.

  - **Normal (✅)**

    The task succeeded.

  - **Skipped (↪)**

    A task failed, resulting in subsequent tasks being skipped.

- **Duration**

  Displays the elapsed time since the task began.

- **Completed Time**

  Displays the time the task completed. By default, this column is hidden.

- **Task ID**

  Displays the GUID that identifies an individual task for a job. The column can be sorted and filtered. By default, this column is hidden.

- **Dependency order**

  Displays an integer representing the sequence of tasks in a graph, with zero being assigned to the first task. By default, this column is hidden.

- **Task Details pane**

  Displays additional information about each job task, including the task name, task description, and, if the task failed, a reason for the failure.

- **Task Messages pane**

  Displays messages specific to the selected task. Messages might include a reason for the error and suggestions for resolving it. Not all tasks display task messages.

Advanced Secondary Settings dialog box

You can use the Advanced Secondary Settings dialog box to enable version-flexible replication, multiple copy backup, and space-related settings on a secondary volume. You might use the Advanced Secondary Settings dialog box when you want to change enable or disable the current settings.

Space-related settings maximize the amount of data being stored, including the following: deduplication, data compression, autogrow, and space guarantee.

The dialog box includes the following fields:

- **Enable Version-Flexible Replication**

  Enables SnapMirror with version-flexible replication. Version-flexible replication enables SnapMirror protection of a source volume even if the destination volume is running under an earlier version of ONTAP than that of the source volume.

  - Enable Backup

    If version-flexible replication is enabled, also enables multiple Snapshot copies of the SnapMirror source data to be transferred to and retained at the SnapMirror destination.

- **Enable Deduplication**

  Enables deduplication on the secondary volume in a SnapVault relationship so that duplicate data blocks are eliminated to achieve space savings. You might use deduplication when space savings are at least 10 percent and when data overwrite rate is not rapid. Deduplication is often used for virtualized environments, file shares, and backup data. This setting is disabled by default. When enabled, this operation is initiated after each transfer.

  - Enable Compression

    Enables transparent data compression. You might use compression when space savings are at least

10 percent, when the potential overhead is acceptable, and when there are sufficient system resources for compression to complete during nonpeak hours. In a SnapVault relationship, this setting is disabled by default. Compression is available only when deduplication is selected.

- Compress Inline

  Enables immediate space savings by compressing data before writing data to disk. You might use inline compression when your system has no more than 50 percent utilization during peak hours, and when the system can accommodate new writes and additional CPU during peak hours. This setting is available only when “Enable Compression” is selected.

- **Enable Autogrow**

  Enables you to automatically grow the destination volume when the free space percentage is below the specified threshold, as long as space is available on the associated aggregate.

- **Maximum Size**

  Sets the maximum percentage to which a volume can grow. The default is 20 percent greater than the source volume size. A volume does not grow automatically if the current size is greater than or equal to the maximum autogrow percentage. This field is enabled only when the autogrow setting is enabled.

- **Increment Size**

  Specifies the percentage increment by which the volume automatically grows before reaching the maximum percentage of the source volume.

- **Space Guarantee**

  Ensures that enough space is allocated on the secondary volume so that data transfers always succeed. The space guarantee setting can be one of the following:

  - File
  - Volume
  - None
    For example, you might have a 200 GB volume that contains files totaling 50 GB; however, those files hold only 10 GB of data. Volume guarantee allocates 200 GB to the destination volume, regardless of contents on the source. File guarantee allocates 50 GB to ensure that enough space is reserved for files on the source; selecting None in this scenario means that only 10 GB is allocated on the destination for the actual space used by file data on the source.

  The space guarantee is set to Volume by default.

Command buttons

The command buttons enable you to perform the following tasks:

- **Apply**

  Saves the selected efficiency settings and applies them when you click **Apply** in the Configure Protection dialog box.

- **Cancel**

  Discards your selections and closes the Advanced Destination Settings dialog box.

Advanced Destination Settings dialog box

You can use the Advanced Destination Settings dialog box to enable space guarantee settings on a destination volume. You might select advanced settings when space guarantee is disabled on the source, but you want it enabled on the destination. The settings for deduplication, compression, and autogrow in a SnapMirror relationship are inherited from the source volume and cannot be changed.

Space Guarantee

Ensures that enough space is allocated on the destination volume so that data transfers always succeed. The space guarantee setting can be one of the following:

- File
- Volume
- None

For example, you might have a 200-GB volume that contains files totaling 50 GB; however, those files hold only 10 GB of data. Volume guarantee allocates 200 GB to the destination volume, regardless of contents on the source. File guarantee allocates 50 GB to ensure that enough space is reserved for source files on the destination; selecting **None** in this scenario means that only 10 GB is allocated on the destination for the actual space used by file data on the source.

The space guarantee is set to Volume by default.

Restore dialog box

You can use the Restore dialog box to restore data to a volume from a specific Snapshot copy.

Restore from

The Restore from area enables you to specify from where you want to restore data.

- **Volume**

  Specifies the volume from which you want to restore data. By default, the volume on which you initiated the restore action is selected. You can select a different volume from the drop-down list that contains all the volumes with protection relationships to the volume on which you initiated the restore action.

- **Snapshot copy**

  Specifies which Snapshot copy you want to use to restore data. By default, the most recent Snapshot copy is selected. You can also select a different Snapshot copy from the drop-down list. The Snapshot copy list changes according to which volume is selected.

- **List maximum of 995 files and directories**

  By default a maximum of 995 objects are shown in the list. You can deselect this checkbox if you want to view all objects within the selected volume. This operation may take some time if the number of items is very large.

Select items to restore

The Select items to restore area enables you to select either the entire volume or specific files and folders you want to restore. You can select a maximum of 10 files, folders, or a combination of both. When the maximum number of items is selected, the item selection check boxes are disabled.

- **Path field**

  Displays the path to the data you want to restore. You can either navigate to the folder and files you want to restore, or you can type the path. This field is empty until you select or type a path. Clicking  after you have chosen a path moves you up one level in the directory structure.

- **Folders and files list**

  Displays the contents of the path you entered. By default, the root folder is initially displayed. Clicking a folder name displays the contents of the folder.

You can select items to restore as follows:

- When you enter the path with a particular file name specified in the path field, the specified file is displayed in the Folders and Files.
- When you enter a path without specifying a particular file, the contents of the folder are displayed in the Folders and Files list, and you can select up to 10 files, folders, or a combination of both to restore.

  If a folder contains more than 995 items, a message displays to indicate there are too many items to display, and if you proceed with the operation all items in the specified folder are restored. You can deselect the “List maximum of 995 files and directories” checkbox if you want to view all objects within the selected volume.

You cannot restore NTFS file streams.

Restore to

The Restore to area enables you to specify where you want to restore the data.

- **Original Location in Volume_Name**

  Restores the selected data to the directory on the source from which the data was originally backed up.

- **Alternate Location**

  Restores the selected data to a new location:

  - Restore Path

    Specifies an alternate path for restoring the selected data. The path must already exist. You can use the **Browse** button to navigate to the location where you want the data restored, or you can enter the path manually using the format cluster://svm/volume/path.

  - Preserve directory hierarchy

    When checked, preserves the structure of the original file or directory. For example, if the source is /A/B/C/myFile.txt and the destination is /X/Y/Z, Unified Manager restores the data using the following

directory structure on the destination: /X/Y/Z/A/B/C/myFile.txt.

Command buttons

The command buttons enable you to perform the following tasks:

- **Cancel**

  Discards your selections and closes the Restore dialog box.

- **Restore**

  Applies your selections and begins the restore process.

Browse Directories dialog box

You can use the Browse Directories dialog box when you want to restore data to a directory on a cluster and SVM that is different from the original source. The original source cluster and volume are selected by default.

The Browse Directories dialog box enables you to select the cluster, SVM, volume, and directory path to which you want data restored.

- **Cluster**

  Lists the available cluster destinations to which you can restore. By default, the cluster of the original source volume is selected.

- **SVM drop-down list**

  Lists the available SVM available for the selected cluster. By default, the SVM of the original source volume is selected.

- **Volume**

  Lists all of the read/write volumes in a selected SVM. You can filter the volumes by name and by space available. The volume with the most space is listed first, and so on, in descending order. By default, the original source volume is selected.

- **File path text box**

  Enables you to type the file path to which you want data restored. The path you enter must already exist.

- **Name**

  Displays the names of the available folders for the selected volume. Clicking a folder in the Name list displays the subfolders, if any exist. Files contained in the folders are not displayed. Clicking  after you have selected a folder moves you up one level in the directory structure.

Command buttons

The command buttons enable you to perform the following tasks:

- **Select Directory**

  Applies your selections and closes the Browse Directories dialog box. If no directory is selected, this button is disabled.

- **Cancel**

  Discards your selections and closes the Browse Directories dialog box.

Configure Protection dialog box

You can use the Configure Protection dialog box to create SnapMirror and SnapVault relationships for all read, write, and data protection volumes on clusters to ensure that the data on a source volume or primary volume is replicated.

Source tab

- **Topology view**

  Displays a visual representation of the relationship that you are creating. The source in the topology is highlighted by default.

- **Source Information**

  Displays details about the selected source volumes, including the following information:

  - Source cluster name
  - Source SVM name
  - Cumulative volume total size

    Displays the total size of all the source volumes that are selected.

  - Cumulative volume used size

    Displays the cumulative volume used size for all the selected source volumes.

  - Source volume

    Displays the following information in a table:

    - Source Volume

      Displays the names of the selected source volumes.

    - Type

      Displays the volume type.

    - SnapLock Type

      Displays the SnapLock type of the volume. The options are Compliance, Enterprise, and Non-SnapLock.

- Snapshot Copy

  Displays the Snapshot copy that is used for the baseline transfer. If the source volume is read/write, the value of Default in the Snapshot copy column indicates that a new Snapshot copy is created by default, and is used for the baseline transfer. If the source volume is a data protection volume, the value of Default in the Snapshot copy column indicates that no new Snapshot copy is created, and all existing Snapshot copies are transferred to the destination. Clicking the Snapshot copy value displays a list of Snapshot copies from which you can select an existing Snapshot copy to use for the baseline transfer. You cannot select a different default Snapshot copy if the source type is data protection.

SnapMirror tab

Enables you to specify a destination cluster, storage virtual machine (SVM), and aggregate for a protection relationship, as well as a naming convention for destinations while creating a SnapMirror relationship. You can also specify a SnapMirror policy and schedule.

- **Topology view**

  Displays a visual representation of the relationship that you are creating. The SnapMirror destination resource in the topology is highlighted by default.

- **Destination Information**

  Enables you to select the destination resources for a protection relationship:

  - Advanced link

    Launches the Advanced Destination Settings dialog box when you are creating a SnapMirror relationship.

  - Cluster

    Lists the clusters that are available as protection destination hosts. This field is required.

  - storage virtual machine (SVM)

    Lists the SVMs that are available on the selected cluster. A cluster must be selected before the SVM list is populated. This field is required.

  - Aggregate

    Lists the aggregates that are available on the selected SVM. A cluster must be selected before the Aggregate list is populated. This field is required. The Aggregate list displays the following information:

    - Rank

      When multiple aggregates satisfy all the requirements for a destination, the rank indicates the priority in which the aggregate is listed, according to the following conditions:

      A. An aggregate that is located on a different node than the source volume node is preferred to enable fault domain separation.
      B. An aggregate on a node with fewer volumes is preferred to enable load balancing across nodes in a cluster.

C. An aggregate that has more free space than other aggregates is preferred to enable capacity balancing. A rank of 1 means that the aggregate is the most preferred according to the three criteria.

- Aggregate Name

  Name of the aggregate

- Available Capacity
- Amount of space that is available on the aggregate for data
- Resource Pool

  Name of the resource pool to which the aggregate belongs

◦ Naming Convention

Specifies the default naming convention that is applied to the destination volume. You can accept the naming convention that is provided, or you can create a custom one. The naming convention can have the following attributes: %C, %M, %V, and %N, where %C is the cluster name, %M is the SVM name, %V is the source volume, and %N is the topology destination node name.

The naming convention field is highlighted in red if your entry is invalid. Clicking the “Preview Name” link displays a preview of the naming convention that you entered, and the preview text updates dynamically as you type a naming convention in the text field. A suffix between 001 and 999 is appended to the destination name when the relationship is created, replacing the nnn that displays in the preview text, with 001 being assigned first, 002 assigned second, and so on.

- **Relationship Settings**

Enables you to specify the maximum transfer rate, SnapMirror policy, and schedule that the protection relationship uses:

◦ Max Transfer Rate

Specifies the maximum rate at which data is transferred between clusters over the network. If you choose not to use a maximum transfer rate, the baseline transfer between relationships is unlimited.

◦ SnapMirror Policy

Specifies the ONTAP SnapMirror policy for the relationship. The default is DPDefault.

◦ Create Policy

Launches the Create SnapMirror Policy dialog box, which enables you to create and use a new SnapMirror policy.

◦ SnapMirror Schedule

Specifies the ONTAP SnapMirror policy for the relationship. Available schedules include None, 5min, 8hour, daily, hourly, and weekly. The default is None, indicating that no schedule is associated with the relationship. Relationships without schedules have no lag status values unless they belong to a storage service.

◦ Create Schedule

Launches the Create Schedule dialog box, which enables you to create a new SnapMirror schedule.

SnapVault tab

Enables you to specify a secondary cluster, SVM, and aggregate for a protection relationship, as well as a naming convention for secondary volumes while creating a SnapVault relationship. You can also specify a SnapVault policy and schedule.

- **Topology view**

  Displays a visual representation of the relationship that you are creating. The SnapVault secondary resource in the topology is highlighted by default.

- **Secondary Information**

  Enables you to select the secondary resources for a protection relationship:

  - Advanced link

    Launches the Advanced Secondary Settings dialog box.

  - Cluster

    Lists the clusters that are available as secondary protection hosts. This field is required.

  - storage virtual machine (SVM)

    Lists the SVMs that are available on the selected cluster. A cluster must be selected before the SVM list is populated. This field is required.

  - Aggregate

    Lists the aggregates that are available on the selected SVM. A cluster must be selected before the Aggregate list is populated. This field is required. The Aggregate list displays the following information:

    - Rank

      When multiple aggregates satisfy all the requirements for a destination, the rank indicates the priority in which the aggregate is listed, according to the following conditions:

      A. An aggregate that is located on a different node than the primary volume node is preferred to enable fault domain separation.
      B. An aggregate on a node with fewer volumes is preferred to enable load balancing across nodes in a cluster.
      C. An aggregate that has more free space than other aggregates is preferred to enable capacity balancing. A rank of 1 means that the aggregate is the most preferred according to the three criteria.

    - Aggregate Name

      Name of the aggregate

    - Available Capacity
    - Amount of space that is available on the aggregate for data

        - Resource Pool

          Name of the resource pool to which the aggregate belongs

    - Naming Convention

      Specifies the default naming convention that is applied to the secondary volume. You can accept the naming convention that is provided, or you can create a custom one. The naming convention can have the following attributes: %C, %M, %V, and %N, where %C is the cluster name, %M is the SVM name, %V is the source volume, and %N is the topology secondary node name.

      The naming convention field is highlighted in red if your entry is invalid. Clicking the “Preview Name” link displays a preview of the naming convention that you entered, and the preview text updates dynamically as you type a naming convention in the text field. If you type an invalid value, the invalid information displays as red question marks in the preview area. A suffix between 001 and 999 is appended to the secondary name when the relationship is created, replacing the nnn that displays in the preview text, with 001 being assigned first, 002 assigned second, and so on.

- **Relationship Settings**

  Enables you to specify the maximum transfer rate, SnapVault policy, and SnapVault schedule that the protection relationship uses:

    - Max Transfer Rate

      Specifies the maximum rate at which data is transferred between clusters over the network. If you choose not to use a maximum transfer rate, the baseline transfer between relationships is unlimited.

    - SnapVault Policy

      Specifies the ONTAP SnapVault policy for the relationship. The default is XDPDefault.

    - Create Policy

      Launches the Create SnapVault Policy dialog box, which enables you to create and use a new SnapVault policy.

    - SnapVault Schedule

      Specifies the ONTAP SnapVault schedule for the relationship. Available schedules include None, 5min, 8hour, daily, hourly, and weekly. The default is None, indicating that no schedule is associated with the relationship. Relationships without schedules have no lag status values unless they belong to a storage service.

    - Create Schedule

      Launches the Create Schedule dialog box, which enables you to create a SnapVault schedule.

Command buttons

The command buttons enable you to perform the following tasks:

- **Cancel**

  Discards your selections, and closes the Configure Protection dialog box.

- **Apply**

  Applies your selections, and begins the protection process.

Create Schedule dialog box

The Create Schedule dialog box enables you to create a basic or advanced protection schedule for SnapMirror and SnapVault relationship transfers. You might create a new schedule to increase the frequency of data transfers due to frequent data updates, or you might create a less frequent schedule when data changes infrequently.

Schedules cannot be configured for SnapMirror Synchronous relationships.

- **Destination Cluster**

  The name of the cluster you selected in the SnapVault tab or SnapMirror tab of the Configure Protection dialog box.

- **Schedule Name**

  The name you provide for the schedule. Schedule names can consist of the characters A through Z, a through z, 0 through 9, as well as any of the following special characters: ! @ # $ % ^ & * ( ) _ -. Schedule names may not include the following characters: < >.

- **Basic or Advanced**

  The schedule mode you want to use.

  Basic mode includes the following elements:

  - Repeat

    How often a scheduled transfer occurs. Choices include hourly, daily, and weekly.

  - Day

    When a repeat of weekly is selected, the day of the week a transfer occurs.

  - Time

    When Daily or Weekly is selected, the time of day a transfer occurs.

  Advanced mode includes the following elements:

  - Months

    A comma-separated numerical list representing the months of the year. Valid values are 0 through 11, with zero representing January, and so on. This element is optional. Leaving the field blank implies that transfers occur every month.

  - Days

    A comma-separated numerical list representing the day of the month. Valid values are 1 through 31. This element is optional. Leaving the field blank implies that a transfer occurs every day of the month.

- Weekdays

  A comma-separated numerical list representing the days of the week. Valid values are 0 through 6, with 0 representing Sunday, and so on. This element is optional. Leaving the field blank implies that a transfer occurs every day of the week. If a day of the week is specified but a day of the month is not specified, a transfer occurs only on the specified day of the week and not every day.

- Hours

  A comma-separated numerical list representing the number of hours in a day. Valid values are 0 through 23, with 0 representing midnight. This element is optional.

- Minutes

  A comma-separated numerical list representing the minutes in an hour. Valid values are 0 through 59. This element is required.

Create SnapMirror Policy dialog box

The Create SnapMirror Policy dialog box enables you to create a policy to set the priority for SnapMirror transfers. You use policies to maximize the efficiency of transfers from the source to the destination.

- **Destination Cluster**

  The name of the cluster you selected in the SnapMirror tab of the Configure Protection dialog box.

- **Destination SVM**

  The name of the SVM you selected in the SnapMirror tab of the Configure Protection dialog box.

- **Policy Name**

  The name you provide for the new policy. Policy names can consist of the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underscore (_).

- **Transfer Priority**

  The priority at which a transfer runs for asynchronous operations. You can select either Normal or Low. Transfer relationships with policies that specify a normal transfer priority run before those with policies that specify a low transfer priority.

- **Comment**

  An optional field in which you can add comments about the policy.

- **Transfer Restart**

  Indicates what restart action to take when a transfer is interrupted by an abort operation or any type of failure, such as a network outage. You can select one of the following:

  - Always

    Specifies that a new Snapshot copy is created before restarting a transfer, then, if one exists, the transfer is restarted from a checkpoint, followed by an incremental transfer from the newly created

Snapshot copy.

- Never

  Specifies that interrupted transfers are never restarted.

Command buttons

The command buttons enable you to perform the following tasks:

- **Cancel**

  Discards the selections and closes the Configure Protection dialog box.

- **Apply**

  Applies your selections and begins the protection process.

Create SnapVault Policy dialog box

The Create SnapVault Policy dialog box enables you to create a policy to set the priority for SnapVault transfers. You use policies to maximize the efficiency of transfers from the primary to the secondary volume.

- **Destination Cluster**

  The name of the cluster that you selected in the SnapVault tab of the Configure Protection dialog box.

- **Destination SVM**

  The name of the SVM that you selected in the SnapVault tab of the Configure Protection dialog box.

- **Policy Name**

  The name you provide for the new policy. Policy names can consist of the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underscore (_).

- **Transfer Priority**

  The priority at which the transfer is run. You can select either Normal or Low. Transfer relationships with policies that specify a normal transfer priority run before those with policies that specify a low transfer priority. The default setting is Normal.

- **Comment**

  An optional field in which you can a add comment of up to 255 characters about the SnapVault policy.

- **Ignore Access Time**

  Specifies whether incremental transfers are ignored for files that have only their access time changed.

- **Replication Label**

  Lists in a table the rules associated with Snapshot copies selected by ONTAP that have a specific

replication label in a policy. The following information and actions are also available:

- Command buttons

  The command buttons enable you to perform the following actions:

  - Add

    Enables you to create a Snapshot copy label and retention count.

  - Edit Retention Count

    Enables you to change the retention count for an existing Snapshot copy label. The retention count must be a number between 1 and 251. The sum of all retention counts for all rules cannot exceed 251.

  - Delete

    Enables you to delete an existing Snapshot copy label.

- Snapshot Copy Label

  Displays the Snapshot copy label. If you select one or more volumes with the same local Snapshot copy policy, an entry for each label in the policy is displayed. If you select multiple volumes that have two or more local Snapshot copy policies, the table displays all labels from all policies

- Schedule

  Displays the schedule associated with each Snapshot copy label. If a label has more than one schedule associated with it, the schedules for that label are displayed in a comma-separated list. If you select multiple volumes with the same label but with different schedules, the schedule displays “Various” to indicate that more than one schedule is associated with the selected volumes.

- Destination Retention Count

  Displays the number of Snapshot copies with the specified label that are retained on the SnapVault secondary. Retention counts for labels with multiple schedules displays the sum of retention counts of each label and schedule pair. If you select multiple volumes with two or more local Snapshot copy policies, the retention count is empty.

Edit Relationship dialog box

You can edit an existing protection relationship to change the maximum transfer rate, the protection policy, or the protection schedule.

Destination Information

- **Destination Cluster**

  The name of the selected destination cluster.

- **Destination SVM**

  The name of the selected SVM

- **Relationship Settings**

  Enables you to specify the maximum transfer rate, SnapMirror policy, and schedule that the protection relationship uses:

  - Max Transfer Rate

    Specifies the maximum rate at which baseline data is transferred between clusters over the network. When selected, network bandwidth is limited to the value you specify. You can enter a numerical value and then select either kilobytes per second (KBps), megabytes per second (MBps), gigabytes per second (GBps), or terabytes per second (TBps). The maximum transfer rate that you specify must be greater than 1 KBps and less than 4 TBps. If you choose not to use a maximum transfer rate, the baseline transfer between relationships is unlimited. If the primary cluster and the secondary cluster are the same, this setting is disabled.

  - SnapMirror Policy

    Specifies the ONTAP SnapMirror policy for the relationship. The default is DPDefault.

  - Create Policy

    Launches the Create SnapMirror Policy dialog box, which enables you to create and use a new SnapMirror policy.

  - SnapMirror Schedule

    Specifies the ONTAP SnapMirror policy for the relationship. Available schedules include None, 5min, 8hour, daily, hourly, and weekly. The default is None, indicating that no schedule is associated with the relationship. Relationships without schedules have no lag status values unless they belong to a storage service.

  - Create Schedule

    Launches the Create Schedule dialog box, which enables you to create a new SnapMirror schedule.

Command buttons

The command buttons enable you to perform the following tasks:

- **Cancel**

  Discards the selections and closes the Configure Protection dialog box.

- **Submit**

  Applies your selections and closes the Edit Relationship dialog box.

Initialize/Update dialog box

The Initialize/Update dialog box enables you to perform a first-time baseline transfer on a new protection relationship, or to update a relationship if it is already initialized and you want to perform a manual, unscheduled, incremental update.

Transfer Options tab

The Transfer Options tab enables you to change the initialization priority of a transfer and to change the bandwidth used during transfers.

- **Transfer Priority**

  The priority at which the transfer is run. You can select either Normal or Low. Relationships with policies that specify a normal transfer priority run before those that specify a low transfer priority. Normal is selected by default.

- **Max Transfer Rate**

  Specifies the maximum rate at which data is transferred between clusters over the network. If you choose not to use a maximum transfer rate, the baseline transfer between relationships is unlimited. If you select more than one relationship with different maximum transfer rates, you can specify one of the following maximum transfer rate settings:

  - Use values specified during individual relationship setup or edit

    When selected, initialization and update operations use the maximum transfer rate specified at the time of each relationship's creation or edit. This field is available only when multiple relationships with different transfer rates are being initialized or updated.

  - Unlimited

    Indicates that there is no bandwidth limitation on transfers between relationships. This field is available only when multiple relationships with different transfer rates are being initialized or updated.

  - Limit bandwidth to

    When selected, network bandwidth is limited to the value you specify. You can enter a numerical value and then select either kilobytes per second (KBps), Megabytes per second (MBps), Gigabytes per second (GBps), or Terabytes per second (TBps). The maximum transfer rate that you specify must be greater than 1 KBps and less than 4 TBps.

Source Snapshot Copies tab

The Source Snapshot Copies tab displays the following information about the source Snapshot copy that is used for the baseline transfer:

- **Source Volume**

  Displays the names of the corresponding source volumes.

- **Destination Volume**

  Displays the names of the selected destination volumes.

- **Source Type**

  Displays the volume type. The type can be either Read/write or Data Protection.

- **Snapshot Copy**

  Displays the Snapshot copy that is used for the data transfer. Clicking the Snapshot copy value displays

the Select Source Snapshot Copy dialog box, in which you can select a specific Snapshot copy for your transfer, depending on the type of protection relationship that you have and the operation that you are performing. The option to specify a different Snapshot copy is not available for data protection type sources.

Command buttons

The command buttons enable you to perform the following tasks:

- **Cancel**

  Discards your selections and closes the Initialize/Update dialog box.

- **Submit**

  Saves your selections and starts the initialize or update job.

Resynchronize dialog box

The Resynchronize dialog box enables you to resynchronize data on a SnapMirror or SnapVault relationship that was previously broken and then the destination was made a read/write volume. You might also resynchronize when a required common Snapshot copy on the source volume is deleted causing SnapMirror or SnapVault updates to fail.

Resynchronization Options tab

The Resynchronization Options tab enables you to set the transfer priority and the maximum transfer rate for the protection relationship that you are resynchronizing.

- **Transfer Priority**

  The priority at which the transfer is run. You can select either Normal or Low. Relationships with policies that specify a normal transfer priority run before those with policies that specify a low transfer priority.

- **Max Transfer Rate**

  Specifies the maximum rate at which data is transferred between clusters over the network. When selected, network bandwidth is limited to the value that you specify. You can enter a numerical value and then select either kilobytes per second (KBps), megabytes per second (MBps), gigabytes per second (GBps), or TBps. If you choose not to use a maximum transfer rate, the baseline transfer between relationships is unlimited.

Source Snapshot Copies tab

The Source Snapshot Copies tab displays the following information about the source Snapshot copy that is used for the baseline transfer:

- **Source Volume**

  Displays the names of the corresponding source volumes.

- **Destination Volume**

Displays the names of the selected destination volumes.

- **Source Type**

  Displays the volume type: either Read/write or Data Protection.

- **Snapshot Copy**

  Displays the Snapshot copy that is used for the data transfer. Clicking the Snapshot copy value displays the Select Source Snapshot Copy dialog box, in which can select a specific Snapshot copy for your transfer, depending on the type of protection relationship you have and the operation you are performing.

Command buttons

- **Submit**

  Begins the resynchronization process and closes the Resynchronize dialog box.

- **Cancel**

  Cancels your selections and closes the Resynchronize dialog box.

Select Source Snapshot Copy dialog box

You use the Select Source Snapshot Copy dialog box to select a specific Snapshot copy to transfer data between protection relationships, or you select the default behavior, which varies depending on whether you are initializing, updating, or resynchronizing a relationship, and whether the relationship is a SnapMirror or SnapVault.

Default

Enables you to select the default behavior for determining which Snapshot copy is used for initialize, update, and resynchronize transfers for SnapVault and SnapMirror relationships.

If you are performing a SnapVault transfer, the default behavior for each operation is as follows:

Operation	Default SnapVault behavior when source is read/write	Default SnapVault behavior when source is Data Protection (DP)
Initialize	Creates a new Snapshot copy and transfers it.	Transfers the last exported Snapshot copy.
Update	Transfers only labeled Snapshot copies, as specified in the policy.	Transfers the last exported Snapshot copy.
Resynchronize	Transfers all labeled Snapshot copies created after the newest common Snapshot copy.	Transfers the newest labeled Snapshot copy.

If you are performing a SnapMirror transfer, the default behavior for each operation is as follows:

Operation	Default SnapMirror behavior	Default SnapMirror behavior when relationship is second hop in a SnapMirror to SnapMirror cascade
Initialize	Creates a new Snapshot copy and transfers it and all Snapshot copies created prior to the new Snapshot copy.	Transfers all Snapshot copies from the source.
Update	Creates a new Snapshot copy and transfers it and all Snapshot copies created prior to the new Snapshot copy.	Transfers all Snapshot copies.
Resynchronize	Creates a new Snapshot copy and then transfers all Snapshot copies from the source.	Transfers all Snapshot copies from the secondary volume to the tertiary volume, and deletes any data added after creation of the newest common Snapshot copy.

Existing Snapshot Copy

Enables you to select an existing Snapshot copy from the list if Snapshot copy selection is allowed for that operation.

- **Snapshot Copy**

  Displays the existing Snapshot copies from which you can select for a transfer.

- **Date Created**

  Displays the date and time the Snapshot copy was created. Snapshot copies are listed from most recent to least recent, with the most recent at the top of the list.

If you are performing a SnapVault transfer and you want to select an existing Snapshot copy to transfer from a source to a destination, the behavior for each operation is as follows:

Operation	SnapVault behavior when specifying a Snapshot copy	SnapVault behavior when specifying a Snapshot copy in a cascade
Initialize	Transfers the specified Snapshot copy.	Source Snapshot copy selection is not supported for data protection volumes.
Update	Transfers the specified Snapshot copy.	Source Snapshot copy selection is not supported for data protection volumes.

Operation	SnapVault behavior when specifying a Snapshot copy	SnapVault behavior when specifying a Snapshot copy in a cascade
Resynchronize	Transfers the selected Snapshot copy.	Source Snapshot copy selection is not supported for data protection volumes.

If you are performing a SnapMirror transfer and you want to select an existing Snapshot copy to transfer from a source to a destination, the behavior for each operation is as follows:

Operation	SnapMirror behavior when specifying a Snapshot copy	SnapMirror behavior when specifying a Snapshot copy in a cascade
Initialize	Transfers all Snapshot copies on the source, up to the specified Snapshot copy.	Source Snapshot copy selection is not supported for data protection volumes.
Update	Transfers all Snapshot copies on the source, up to the specified Snapshot copy.	Source Snapshot copy selection is not supported for data protection volumes.
Resynchronize	Transfers all Snapshot copies from the source, up to the selected Snapshot copy, and then deletes any data added after creation of the newest common Snapshot copy.	Source Snapshot copy selection is not supported for data protection volumes.

Command buttons

The command buttons enable you to perform the following tasks:

- **Submit**

  Submits your selections and closes the Select Source Snapshot Copy dialog box.

- **Cancel**

  Discards your selections and closes the Select Source Snapshot Copy dialog box.

Reverse Resync dialog box

When you have a protection relationship that is broken because the source volume is disabled and the destination is made a read/write volume, reverse resynchronization enables you to reverse the direction of the relationship so that the destination becomes the new source and the source becomes the new destination.

When a disaster disables the source volume in your protection relationship, you can use the destination volume to serve data by converting it to read/write, while you repair or replace the source, update the source, and reestablish the relationship. When you perform a reverse resync operation, data on the source that is

newer than the data on the common Snapshot copy is deleted.

Before reverse resync

Displays the source and destination of a relationship before a reverse resync operation.

- **Source Volume**

  The name and location of the source volume before a reverse resync operation.

- **Destination Volume**

  The name and location of the destination volume before a reverse resync operation.

After reverse resync

Displays what the source and destination of a relationship is after a reserve resync operation.

- **Source Volume**

  The name and location of the source volume after a reverse resync operation.

- **Destination Volume**

  The name and location of the destination volume after a reverse resync operation.

Command buttons

The command buttons enable you to perform the following actions:

- **Submit**

  Begins the reverse resynchronization process.

- **Cancel**

  Closes the Reverse Resync dialog box without initiating a reverse resync operation.

Relationship: All Relationships view

The Relationship: All Relationships view displays information about protection relationships on the storage system.

By default, when you access the Relationships page, the report that is displayed includes the top level protection relationships for both volumes and storage VMs. The controls along the top of the page enable you to select a particular view, perform searches to locate specific objects, create and apply filters to narrow the list of displayed data, add/remove/reorder columns on the page, and export the data on the page to a .csv, .pdf, or .xlsx file. After you have customized the page, you can save the results as a custom view and then schedule a report of this data to be generated and emailed on a regular basis. By default, when you select the **Relationships** menu, the report displayed includes protection relationships for both volumes and storage VMs in your datacenter. You can use the **Filter** option to view only selected storage systems like only volumes or only storage VMs. The same report is displayed in the Storage page and only for the selected storage entity. If you want to view either volume or storage VM relationships, you can access either the **Storage** > **Volumes** > **Relationship: All Relationships** page or access **Protection** > **Relationships** > **Relationship: All**

Relationships, and use the **Relationship Object Type** option in the **Filter** to filter out only volumes or storage VMs data.

The Relationships page that lists all the protection relationships has the link **View in System Manager** for the Destination cluster that allows you to view the same objects in ONTAP System Manager.

- **Status**

  Displays the current status of the protection relationship.

  The status can be one of Error (), Warning (), or OK ().

- **Source Storage VM**

  Displays the name of the source SVM. You can view more details about the source SVM by clicking the SVM name.

  When a SVM exists on the cluster but has not yet been added to the Unified Manager inventory, or that the SVM was created after the cluster's last refresh, this field will be empty. You must ensure that the SVM exists, or perform a rediscovery on the cluster to refresh the list of resources.

- **Source**

  Displays either the source volume or source storage VM being protected based on your selection. You can view more details about the source volume or storage VM by clicking the volume or storage VM name.

  If the message `Resource-key not discovered` is displayed, this might indicate that the volume exists on the cluster but has not yet been added to the Unified Manager inventory, or that the volume was created after the cluster's last refresh. You must ensure that the volume exists, or perform a rediscovery on the cluster to refresh the list of resources.

- **Destination Storage VM**

  Displays the name of the destination SVM. You can view more details about the destination SVM by clicking the SVM name.

- **Destination**

  Displays the name of the destination volume or storage VM based on your selection. You can view more details about the destination volume or storage VM by clicking the respective object name.

- **Relationship Object Type**

  Displays the type of object used in the relationship, such as storage VM, volume, and Consistency Group. For objects in a Consistency Relationship, the relationship source and destinations display the Consistency Group, and clicking them takes you to the LUNs page to view the relationship.

- **Policy**

  Displays the name of the protection policy for SnapMirror relationship. You can click the policy name to view details associated with that policy, including the following information:

  - Transfer Priority

    Specifies the priority at which a transfer runs for asynchronous operations. The transfer priority is Normal or Low. Normal priority transfers are scheduled before low priority transfers. The default is

Normal.

- Ignore Access Time

  Applies only to SnapVault relationships. This specifies whether incremental transfers ignore files which have only their access time changed. The values are either True or False. The default is False.

- When Relationship is Out of Sync

  Specifies the action ONTAP performs when a synchronous relationship is not able to be synchronized. StrictSync relationships will restrict access to the primary volume if there is a failure to synchronize with the secondary volume. Sync relationships do not restrict access to the primary if there is a failure to synchronize with the secondary.

- Tries Limit

  Specifies the maximum number of times to attempt each manual or scheduled transfer for a SnapMirror relationship. The default is 8.

- Comments

  Provides a text field for comments for specific to the selected policy.

- SnapMirror Label

  Specifies the SnapMirror label for the first schedule associated with the Snapshot copy policy. The SnapMirror label is used by the SnapVault subsystem when you back up Snapshot copies to a SnapVault destination.

- Retention Setting

  Specifies how long backups are kept, based on the time or the number of backups.

- Actual Snapshot Copies

  Specifies the number of Snapshot copies on this volume that match the specified label.

- Preserve Snapshot Copies

  Specifies the number of SnapVault Snapshot copies that are not deleted automatically even if the maximum limit for the policy is reached. The values are either True or False. The default is False.

- Retention Warning Threshold

  Specifies the Snapshot copy limit at which a warning is sent to indicate that the maximum retention limit is nearly reached.

- **Lag Duration**

  Displays the amount of time that the data on the mirror lags behind the source.

  The lag duration should be close to, or equal to, 0 seconds for StrictSync relationships.

- **Lag Status**

  Displays the lag status for managed relationships, and for unmanaged relationships that have a schedule

associated with that relationship. Lag status can be:

  - Error

    The lag duration is greater than or equal to the lag error threshold.

  - Warning

    The lag duration is greater than or equal to the lag warning threshold.

  - OK

    The lag duration is within normal limits.

  - Not Applicable

    The lag status is not applicable for synchronous relationships because a schedule cannot be configured.

- **Last Successful Update**

  Displays the time of the last successful SnapMirror or SnapVault operation.

  The last successful update is not applicable for synchronous relationships.

- **Constituent Relationships**

  Displays whether there are any volumes in the selected object.

- **Relationship Type**

  Displays the relationship type used to replicate a volume. Relationship types include:

  - Asynchronous Mirror
  - Asynchronous Vault
  - Asynchronous MirrorVault
  - StrictSync
  - Sync

- **Transfer Status**

  Displays the transfer status for the protection relationship. The transfer status can be one of the following:

  - Aborting

    SnapMirror transfers are enabled; however, a transfer abort operation that might include removal of the checkpoint is in progress.

  - Checking

    The destination volume is undergoing a diagnostic check and no transfer is in progress.

  - Finalizing

    SnapMirror transfers are enabled. The volume is currently in the post-transfer phase for incremental

SnapVault transfers.

- Idle

  Transfers are enabled and no transfer is in progress.

- In-Sync

  The data in the two volumes in the synchronous relationship are synchronized.

- Out-of-Sync

  The data in the destination volume is not synchronized with the source volume.

- Preparing

  SnapMirror transfers are enabled. The volume is currently in the pre-transfer phase for incremental SnapVault transfers.

- Queued

  SnapMirror transfers are enabled. No transfers are in progress.

- Quiesced

  SnapMirror transfers are disabled. No transfer is in progress.

- Quiescing

  A SnapMirror transfer is in progress. Additional transfers are disabled.

- Transferring

  SnapMirror transfers are enabled and a transfer is in progress.

- Transitioning

  The asynchronous transfer of data from the source to the destination volume is complete, and the transition to synchronous operation has started.

- Waiting

  A SnapMirror transfer has been initiated, but some associated tasks are waiting to be queued.

- **Last Transfer Duration**

  Displays the time taken for the last data transfer to complete.

  The transfer duration is not applicable for StrictSync relationships because the transfer should be simultaneous.

- **Last Transfer Size**

  Displays the size, in bytes, of the last data transfer.

  The transfer size is not applicable for StrictSync relationships.

- **State**

  Displays the state of the SnapMirror or SnapVault relationship. The state can be Uninitialized, SnapMirrored, or Broken-Off. If a source volume is selected, the relationship state is not applicable and is not displayed.

- **Relationship Health**

  Displays the relationship heath of the cluster.

- **Unhealthy Reason**

  The reason the relationship is in an unhealthy state.

- **Transfer Priority**

  Displays the priority at which a transfer runs. The transfer priority is Normal or Low. Normal priority transfers are scheduled before low priority transfers.

  The transfer priority is not applicable for synchronous relationships because all transfers are treated with the same priority.

- **Schedule**

  Displays the name of the protection schedule assigned to the relationship.

  The schedule is not applicable for synchronous relationships.

- **Version Flexible Replication**

  Displays either Yes, Yes with backup option, or None.

- **Source Cluster**

  Displays the FQDN, short name, or IP address of the source cluster for the SnapMirror relationship.

- **Source Cluster FQDN**

  Displays the name of the source cluster for the SnapMirror relationship.

- **Source Node**

  Displays the name of the source node name link for the SnapMirror relationship of a volume and displays the SnapMirror relationship node count link when the object is a Storage VM or Consistency Group.

In the custom view, when you click the node name link, you can view and extend protection for storage objects on which the volumes of those Consistency Groups that belong to SM-BC relationship.

When you click the node count link, it takes you to the node page with respective nodes associated with that relationship. When the node count is 0, there is no value displayed as there are no nodes associated with the relationship.

- **Destination Node**

  Displays the name of the destination node name link for the SnapMirror relationship of a volume and displays the SnapMirror relationship node count link when the object is a Storage VM or Consistency

Group.

When you click the node count link, it takes you to the node page with respective nodes associated with that relationship. When the node count is 0, there is no value displayed as there are no nodes associated with the relationship.

- **Destination Cluster**

  Displays the name of the destination cluster for the SnapMirror relationship.

- **Destination Cluster FQDN**

  Displays the FQDN, short name, or IP address of the destination cluster for the SnapMirror relationship.

- **Protected By**

  Displays the different relationships. In this column, you can view volume and consistency group relationships for clusters and storage virtual machines order, including:

  - SnapMirror
  - Storage VM DR
  - SnapMirror, Storage VM DR
  - Consistency Group
  - SnapMirror, Consistency Group.

Relationship: Last 1 month Transfer Status view

The Relationship: Last 1 month Transfer Status view enables you to analyze the transfer trends over a period of time for volumes and Storage VMs in asynchronous relationships. This page also displays whether the transfer was a success or a failure.

The controls along the top of the page enable you to perform searches to locate specific objects, create, and apply filters to narrow the list of displayed data, add/remove/reorder columns on the page, and export the data on the page to a `.csv`, `.pdf`, or `.xlsx` file. After you have customized the page, you can save the results as a custom view and then schedule a report of this data to be generated and emailed on a regular basis. You can use the **Filter** option to view only selected storage systems like only volumes or only Storage VMs. The same report is displayed in the Storage page and only for the selected storage entity. For example, if you want to view volume relationships you can access either the Relationship: Last 1 Month Transfer Status report for the Storage VMs either from the **Storage** > **Storage VMs** > **Relationship: Last 1 Month Transfer Status** menu or from **Protection** > **Relationships** > **Relationship: Last 1 Month Transfer Status** menu, and use the **Filter** to only view data for volumes.

- **Source Volume**

  Displays the source volume name.

- **Destination Volume**

  Displays the destination volume name.

- **Operation Type**

  Displays the type of volume transfer.

- **Operation Result**

  Displays whether volume transfer was successful.

- **Transfer Start Time**

  Displays the volume transfer start time.

- **Transfer End Time**

  Displays the volume transfer end time.

- **Transfer Duration**

  Displays the time taken (in hours) to complete the volume transfer.

- **Transfer Size**

  Displays the size (in MB) of the transferred volume.

- **Source SVM**

  Displays the storage virtual machine (SVM) name.

- **Source Cluster**

  Displays the source cluster name.

- **Destination SVM**

  Displays the destination SVM name.

- **Destination Cluster**

  Displays the destination cluster name.

Relationship: Last 1 month Transfer Rate view

The Relationship: Last 1 month Transfer Rate view enables you to analyze the amount of data volume that is transferred on a day-to-day basis for volumes in asynchronous relationships. This page also provides details about daily transfers and the time required to complete the transfer operation for volumes and Storage VMs.

The controls along the top of the page enable you to perform searches to locate specific objects, create and apply filters to narrow the list of displayed data, add/remove/reorder columns on the page, and export the data on the page to a .csv, .pdf, or .xlsx file. After you have customized the page, you can save the results as a custom view and then schedule a report of this data to be generated and emailed on a regular basis. For example, if you want to view volume relationships, you can access either the **Storage** > **Volumes** > **Relationship: Last 1 Month Transfer Rate** menu or access **Protection** > **Relationships** > **Relationships:Last 1 Month Transfer Rate** menu, and use the **Filter** to only view data for volumes.

- **Total Transfer Size**

  Displays the total size of the volume transfer in gigabytes.

- **Day**

  Displays the day on which the volume transfer was initiated.

- **End Time**

  Displays the volume transfer end time with date.

Copyright information

Trademark information