Migrating data and configuration from 7-Mode volumes

ONTAP 7-Mode Transition

NetApp
May 31, 2021

Table of Contents

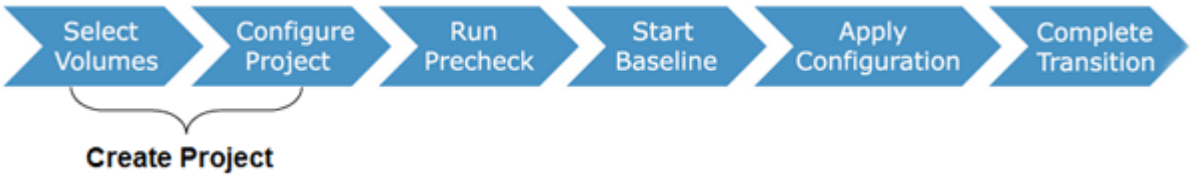
Migrating data and configuration from 7-Mode volumes

To migrate volumes or a volume SnapMirror relationship by using the 7-Mode Transition Tool, you must first configure projects, start a baseline copy, and complete the projects.

- The 7-Mode controllers and clusters that you want to include in the transition must be reachable from the Windows host where the tool is installed.
- You must have all administrator-level privileges for the controllers and clusters that you want to include in the transition project.
- The 7-Mode Transition Tool service must be running on the machine on which it is installed.

  The service is set to automatic by default, and should start when you restart the machine.
- You should not perform assessment and migration operations on a controller simultaneously.
- You should not modify the objects (volumes, IP addresses, system information, and so on) on the 7-Mode controllers and clusters after fixing errors and warnings that are reported by precheck.
- You should avoid using multiple web interface sessions that are writing to the same SVM simultaneously to prevent undesired results.
- You should avoid modifying the controller and cluster passwords during the transition process.
- You should avoid using the **Back**and **Forward** browser buttons, as the tool does not support web browser navigation and might cause undesired results.
- You should avoid browser refresh while transition is in progress, because it might cause undesired results.

The following image illustrates the migration process:



Related information

How you transition a stand-alone volume

How you transition volumes in a SnapMirror relationship

Transition preparation checklist

Before you start transition, you should verify that you have met all of the prerequisites for transition.

ONTAP version requirements

Item	Yes
Supported 7-Mode version NetApp Interoperability Matrix Tool	
Your cluster must be running one of the following Data ONTAP versions: • Data ONTAP 8.2.x • Data ONTAP 8.3.x	
You must transition to one of the following ONTAP releases: • Using 7-Mode Transition Tool 3.3.3: ◦ ONTAP 9.8 or earlier supported releases • Using 7-Mode Transition Tool 3.3.2: ◦ ONTAP 9.7P2 or later 9.7 P release (earlier 9.7 releases are not supported) ◦ ONTAP 9.6P7 or later 9.6 P release (earlier 9.6 releases are not supported) ◦ ONTAP 9.5 or earlier ONTAP 9 release ◦ Clustered Data ONTAP 8.1.4P4 or later 8.x release • Using 7-Mode Transition Tool 3.3.1: ◦ ONTAP 9.5 or earlier ONTAP 9 release ◦ Clustered Data ONTAP 8.1.4P4 or later 8.x release	

Licensing requirements

Item	Yes
SnapMirror license is enabled on the 7-Mode system	
SnapMirror licenses are enabled on the primary and secondary clusters for transitioning a volume SnapMirror relationship	
CIFS license is enabled on the cluster, if it is enabled on the 7-Mode system	
NFS license is enabled on the cluster, if it is enabled on the 7-Mode system	

Item	Yes
iSCSI license is enabled on the cluster, if it is enabled on the 7-Mode system	
FC license is enabled on the cluster, if it is enabled on the 7-Mode system	
Other feature licenses, if available on the 7-Mode system, are added to the cluster	

SnapMirror requirements on the 7-Mode system

Item	Yes
SnapMirror license	
`options snapmirror.enable on`	
`options interface.snapmirror.blocked ""`	
Verify if one of the following is true: • The `snapmirror.access` option is set to all • The `snapmirror.access` option is set to the IP addresses of all the intercluster LIFs on the cluster • If the `snapmirror.access` option is set to `legacy` and the `snapmirror.checkip.enable` option is `off`, the SVM name is added to the `/etc/snapmirror.allow` file • If the `snapmirror.access` option is set to legacy and the `snapmirror.checkip.enable` option is `on`, the IP addresses of the intercluster LIFs are added to the `/etc/snapmirror.allow` file	

Volume settings on the 7-Mode system

Item	Yes
Volume is online	
Volume is not restricted	

Item	Yes
The following volume options are disabled: • `no_i2p` • `read_realloc` • `nvfail`	

Managing access to the cluster

Item	Yes
SSL is enabled `system services web show`	
HTTPS is allowed on the cluster-management LIF `system services firewall policy show`	

Managing access to the 7-Mode system

Item	Yes
HTTPS is enabled `options httpd.admin.ssl.enable on`	

SSL is enabled
`secureadmin setup ssl`
`options ssl.enable on`	

SSLv2 and SSLv3 are disabled
`options ssl.v2.enable off`
`options ssl.v3.enable off`	

Networking requirements

Item	Yes
Cluster is reachable using the cluster-management LIF	

Item	Yes
One or more intercluster LIFs are set up on each node of the cluster For multipathing, two intercluster LIFs are required on each node	
Static routes are created for the intercluster LIFs	
7-Mode system and cluster are reachable from the Windows system on which 7-Mode Transition Tool is installed	
NTP server is configured and the 7-Mode system time is synchronized with the cluster time	

Port requirements

Item	Yes
7-Mode system • 10565/TCP • 10566/TCP • 10567/TCP • 10568/TCP • 10569/TCP • 10670/TCP • 80/TCP • 443/TCP	
Cluster • 10565/TCP • 10566/TCP • 10567/TCP • 10568/TCP • 10569/TCP • 10670/TCP • 11105/TCP • 80/TCP • 443/TCP	

NFS requirements

Item	Yes
NFS license is added to the cluster	
DNS entry must be configured for AD domain on the SVM	
NFS is added to the list of allowed protocols for the SVM	
Clock skews between KDC and the cluster is less than or equal to 5 minutes	

CIFS requirements

Item	Yes
CIFS license is added to the cluster	
If MultiStore license is enabled, CIFS must be added to the list of allowed protocols for the vFiler unit that owns the transitioning volumes	
CIFS is set up and running on the 7-Mode system	
Authentication type in 7-Mode for CIFS is Active Directory (AD) or Workgroup	
CIFS is added to the list of allowed protocols for the SVM	
DNS is configured for the SVM	
CIFS server is configured for the SVM	
CIFS is running on the SVM	

Related information

Preparing for copy-based transition

Adding controllers and clusters

Before you start the transition, you must add the 7-Mode controllers and clusters that are required for the transition. The 7-Mode controllers that are included for assessment are

automatically added for migration.

- The 7-Mode controller and cluster information that you provide is not persistent.

  If the 7-Mode Transition Tool service is restarted, the tool prompts you for information about controllers and clusters that are part of active projects. You must provide the same host name that you provided for your system when you created the project.

- If a 7-Mode controller is part of an HA pair, the tool does not request for credentials of the HA partner of the 7-Mode controller (unless the HA partner is part of another active project.)
  1. From the top pane, click **Storage Systems**.
  2. In the **Hostname** field, enter the FQDN or IP address of the 7-Mode controller or the ONTAP system.

     For a cluster, you can specify the IP address or FQDN of the cluster-management interface. For a 7-Mode controller, you must specify the IP address of the default vFiler unit, because the IP addresses of individual vFiler units are not accepted.

Steps

1. Enter the administrator credentials for the specified host, and then click **Add**.

   The 7-Mode controllers are added to the "7-Mode Controllers" table and clusters are added to the "Clustered Data ONTAP Systems" table.

2. Repeat Steps 2 and 3 to add all of the controllers and clusters that you require for the transition.
3. If the Status column indicates that the credentials of the system are missing or the credentials have changed from what was initially entered in the tool, click the  icon, and then enter the credentials again.

Creating a transition project

Creating a transition project includes selecting and mapping 7-Mode volumes to the storage virtual machine (SVM), mapping interfaces, and creating data copy schedules for SnapMirror relationships.

You must have created the required SVM on the cluster.

All of the volumes within a project are migrated to the same SVM. If you want to migrate the volumes to different SVMs, you must create multiple projects.

If the target cluster is running Data ONTAP 8.3.1 or earlier and you want to run the precutover operation in read/write mode for NAS volumes, then you must create separate projects for the NAS volumes and SAN volumes. This action is required because the precutover read/write mode is not supported if you have SAN volumes in your project.

If the project contains SnapLock Compliance volumes and you want to run the precutover operation in read/write mode for non-SnapLock Compliance volumes, then you must create separate projects for SnapLock Compliance volumes and non-SnapLock Compliance volumes. This action is required because the precutover read/write mode is not supported if you have SnapLock Compliance volumes in your project.

Steps

1. Select the **Copy-Based Transition** migration method from the homepage, and then click **Start Planning**.

If the controller and cluster that are required by the new project have not been added, you can enter the details in the Enter Device Credentials pane.

2. Verify that all of the required Data ONTAP operating in 7-Mode systems and ONTAP systems are added to the tool, and then click **Next**.

   The Select Source Volume page appears.

3. Select the 7-Mode volumes that you want to transition.
   a. From the 7-Mode Controller pane, select the 7-Mode controller or the vFiler unit from which you want to add volumes.
   b. Add the volumes that you want to include in the project group:

If you want to transition…	Then…
Stand-alone volumes	Select **Transition as stand-alone** for the volumes that you want to transition. A stand-alone project is created if you select the first volume from this column.
Volume SnapMirror relationship	i. Select **Transition with SnapMirror Relationship** for all of the primary volumes. Two projects are created: a primary project for the primary volumes and a secondary project. ii. **Optional:** If the secondary controller is not included in the project, enter the details for the controller in the Need additional storage system credentials dialog box.

   If you have at least one LUN in your volume, the volume type is shown as SAN.

   The hyperlink that is provided on the volume name opens a dialog box that lists the qtrees and LUNs in the volume and their attributes.

   It is a best practice to have all of the volumes within a single project to be of the same definition (stand-alone, primary, or secondary). For example, a project should contain all stand-alone volumes rather than a mix of stand-alone and SnapMirror relationships.

   c. After you have selected all of the volumes that you want to include in the project, click **Create Project and Continue**, enter the project name and project group details from the dialog box that appears, and then click **Save** to create the project.

4. Select the 7-Mode IP address and multipath IP address to be used for SnapMirror data copy.
   a. Enter the 7-Mode data copy IP address.

      By default, this field is prepopulated with the management IP address of the 7-Mode system. If required, you can change this IP address to any valid IPv4 address with data copy permission.

b. If you want to use multiple paths for load balancing the data transfers, enter an IP address in the IP Configuration pane, and then click **Next**.

5. From the Select SVM page, select the target cluster and SVM and follow these steps:

   a. Select the target cluster by clicking on the cluster name in the Select a Clustered Data ONTAP System drop-down list.

      The SVMs are loaded in the Select SVM pane.

   b. Select the target SVM to transition the volumes from the Select SVM pane.

   c. Click **Next**.

   For transitioning 7-Mode volumes to a MetroCluster configuration in ONTAP, the SVM subtype must be `sync-source`.

   + If you select an SVM that belongs to clustered Data ONTAP 8.2, a dialog box is displayed to confirm whether local users and groups or CIFS shares or files are configured on the 7-Mode storage system. The 7-Mode Transition Tool does not support the transition of local users and groups to clustered Data ONTAP 8.2. If you have local users and groups, you can select an SVM that belongs to ONTAP 8.2.1 and later supported releases.

6. In the SVM audit logs destination path dialog box, enter a path on the destination SVM to enable transition of the audit configuration from the 7-Mode storage system.

   This path is used to save the audit logs in the ONTAP system.

7. From the Map Volumes page, select the target volumes for transition to map each source volume to the required aggregate.

   a. From the Map Origin Volumes to Aggregates on Target Cluster pane, select the aggregates to which the 7-Mode volumes must be copied.

   b. To change the name of the target volume on the cluster, enter a different name in the **Target Volume** field.

   c. Click **Next**.

   If all of the volumes and qtrees that are included in the project are configured to serve only NFS requests, then you do not have to provide the audit path because the audit configuration is not transitioned (even if you provide the audit path, this input is ignored) .

8. From the Network Configuration pane, provide information about the LIFs that must be created on the SVM.

   FC and iSCSI LIFs cannot be transitioned. You must manually create them on the SVM.

If you want to…	Then…
Transition an existing 7-Mode IP address	a. Click **Select 7-Mode LIF**. b. Select the required 7-Mode IP addresses, and provide target node and target port details. c. Click **Save**.

If you want to…	Then…
Create a new LIF	a. Click **Add New LIF**. b. In the dialog box that appears, enter the details for the new LIF. c. Click **Save**.

To provide network connectivity after a successful transition, you must transition the 7-Mode IP addresses to a similar network topology in ONTAP. For example, if the 7-Mode IP addresses are configured on physical ports, the IP addresses should be transitioned to appropriate physical ports in ONTAP. Similarly, IP addresses configured on VLAN ports or interface groups should be transitioned to appropriate VLAN ports or interface groups in ONTAP.

9. After you add all the required IP addresses, click **Next**.
10. In the Configure Schedule page, configure the data copy schedules for baseline and incremental transfers, the number of concurrent volume SnapMirror transfers, and the throttle limit for the SnapMirror transfers for transition.

    You can provide data copy schedules and a throttle limit to effectively manage your DR and transition data copy operations. You can create multiple schedules, with a maximum of seven schedules for each project. For example, you can create customized schedules for weekdays and weekends.

    The schedules are effective based on the source 7-Mode controller time zone.

    a. In the Configure Schedule pane, click **Create Schedule**.
    b. In the Create Data Copy Schedule dialog box, enter a name for the new schedule.
    c. In the Recurring Days pane, select **Daily** or **Select Days** to specify the days on which the data copy operations should run.
    d. In the Time Interval pane, specify the **Start Time** and **Duration** for the data transfers.
    e. In the Time Interval pane, either specify the **Update Frequency** for the incremental transfers or select **Continuous Update**.

       If you enable continuous updates, the updates start with a minimum delay of 5 minutes, depending on the availability of concurrent SnapMirror transfers.

    f. In the Parameters for Transition Data Copy Operations (based on Volume SnapMirror) pane, specify the maximum number of concurrent volume SnapMirror transfers (as a percentage of available SnapMirror transfers at run time and as a number) and the throttle limit (maximum bandwidth for all of the volumes in the project).

       The default values that are provided in the fields are the recommended values. When changing the default values, you must analyze the 7-Mode SnapMirror schedules and ensure that the values that you provide do not affect these schedules.

    g. Click **Create**.

       The new schedule is added to the Transition Schedule pane.

    h. After you add all of the required data copy schedules, click **Next**.

11. If you have SnapLock volumes to transition, plan the volumes that require Chain of Custody verification after transition.
    a. Select the source SnapLock volumes that require Chain of Custody verification.

       The Chain of Custody verification process is supported only for read/write 7-Mode SnapLock volumes and is not supported for read-only volumes. Only SnapLock volumes that have file names with ASCII characters are supported for Chain of Custody verification.

    b. Provide details about the ONTAP volume that will be used to store the fingerprint data generated during the Chain of Custody verification operation.

       The ONTAP volume must already exist on the specified SVM.

    c. Click **Next**.

Related information

Considerations for creating a data copy schedule

Creating a data copy schedule for SnapMirror transfers

Managing SnapMirror transfers and schedule

Customizing the transition of 7-Mode configurations by using the CLI

Managing logical interfaces

Removing volumes from a project

Customizing the transition of 7-Mode configurations

When planning the transition of configurations from 7-Mode to ONTAP, you can customize the configuration transition in two ways. You can ignore or skip the transition of one or more configurations. You can consolidate the 7-Mode NFS export rules, and then reuse an existing NFS export policy and Snapshot policy on the target SVM.

You must perform this task before you apply the configuration (precutover) phase. This is because after this phase, the Plan Configuration pane is disabled for any modification. You use the command-line interface (CLI) of the 7-Mode Transition Tool for excluding the configurations that are applied during the cutover phase.

The 7-Mode Transition Tool does not perform prechecks for the configuration that is excluded.

By default, all 7-Mode configurations are selected for transition.

It is a best practice to run the prechecks with all configurations first, and then exclude one or more configurations in the subsequent run of the prechecks. This helps you to understand which configurations are excluded from transition and which prechecks are skipped subsequently.

Steps

1. From the Plan Configuration page, select the following options from the **SVM Configuration** pane:
   - For excluding the transition of configurations, clear the check box for those configurations.
   - For consolidating similar 7-Mode NFS export rules to a single export policy in ONTAP, which can then

be applied to the transitioned volume or qtree, select the **Consolidate NFS Export Policies on 7-Mode** check box.

- For reusing an existing NFS export policy on the SVM that matches the export policy that will be created by the tool, which can then be applied to the transitioned volumes or qtrees, select the **Reuse Export Policies of SVM** check box.
- For consolidating similar 7-Mode Snapshot schedules to a single Snapshot policy in ONTAP, which can then be applied to the transitioned volume, select the **Consolidate 7-Mode Snapshot Policies** check box.
- For reusing an existing Snapshot policy on the SVM that matches the Snapshot policy that will be created by the tool, which can then be applied to the transitioned volumes, select the **Reuse Snapshot Policies of SVM** check box.

2. Click **Save and go to Dashboard**.

Related information

Supported and unsupported CIFS configurations for transition to ONTAP

NFS transition: supported and unsupported configurations, and required manual steps

Name services transition: supported and unsupported configurations, and required manual steps

SAN transition: supported and unsupported configurations, and required manual steps

Examples of consolidating NFS export rules and Snapshot schedules for transition

Configurations that can be excluded from transition

Running prechecks

You can run prechecks to identify any issues before you start a transition. Prechecks verify that the 7-Mode sources, ONTAP targets, and configurations are valid for your transition. You can run prechecks any number of times.

The prechecks run more than 200 different checks. For example, the tool checks for items such as if volumes are online and network access exists between the systems.

Steps

1. From Dashboard, select the project for which you want to run the prechecks.
2. Click **Run Prechecks**.

   After the prechecks are complete, the result summary is displayed in the dialog box.

   The prechecks usually take only a few minutes to run, but the duration of the precheck phase depends on the number and type of errors or warnings that you resolve.

3. Choose an option under **Apply Type Filter** to filter the results:
   - To view all messages related to security, select **Error**, **Warning**, **Informational**, and **Security Only**.
   - To view all error messages related to security, select **Error** and **Security Only**.
   - To view all warning messages related to security, select **Warning**and **Security Only**.

    - To view all informational messages related to security, select **Informational** and **Security Only**.
4. To save the raw results in comma-separated values (CSV) format and export the results, click **Save As CSV**.

   You can view the transition operations that have been performed during the transition along with the operation type, status, start time, end time, and results in the Operation History tab on the Dashboard pane.

You must resolve all the errors detected by the prechecks before you start data copy. It is also a best practice to resolve all warnings prior to proceeding with the migration process. Resolution can be resolving the source issue of the warning message, implementing a workaround, or accepting the result of the issue.

Severity levels for precheck messages

You can verify whether the 7-Mode volumes can be transitioned by running the transition precheck operation. Transition precheck reports all the transition issues. Transition issues are assigned different severity levels, depending on the impact of the issue on the transition process.

The issues detected by the prechecks are classified into the following categories:

- **Error**

  Configurations that cannot be transitioned.

  You cannot continue the transition if there is even one error. The following are a few example configurations on the 7-Mode system that cause an error:

    - Traditional volumes
    - SnapLock volumes
    - Offline volumes
- **Warning**

  Configurations that can cause minor problems after transition.

  Features that are supported in ONTAP, but are not transitioned by the 7-Mode Transition Tool, also generate a warning message. You can continue the transition with these warnings. However, after the transition you might lose some of these configurations or might have to complete some manual tasks for enabling these configurations in ONTAP.

  The following are a few example configurations on the 7-Mode system that generate a warning:

    - IPv6
    - NFSv2
    - NDMP configurations
    - Interface groups and VLANs
    - Routing Information Protocol (RIP)
- **Information**

Configurations that have been successfully transitioned.

Starting baseline data copy

After you create a project and complete the precheck operation, you must initiate data copy from the 7-Mode volumes to ONTAP. You can start baseline data copy operation for individual projects. You should stop unnecessary system processes and network activity during the data copy.

You must have created at least one data copy schedule.

You can estimate the time to complete baseline transfers and evaluate the performance achieved by volume SnapMirror transfers in your environment by performing a test migration. The following are some of the factors that can affect performance:

- Transition data copy schedule options selected

  This schedule controls both the maximum number of SnapMirror concurrent transfers and the maximum bandwidth to be used for the transfers.

- Maximum number of concurrent volume SnapMirror transfers supported by the 7-Mode source controllers
- Network bandwidth between the 7-Mode source and ONTAP destination controllers

  Network traffic that is unrelated to the migration activity must be minimized so that the throughput is maximized and response time is minimized between the source and destination systems.

- Performance capabilities of both the source and destination controllers

  The source and destination systems should have optimum CPU utilization and memory available.

- Number of 7-Mode volume SnapMirror transfers occurring during the data copy

Steps

1. From Dashboard, select the project for which you want to start the baseline data copy.
2. Click **Start Baseline**.

   The precheck is run once again in the background, and if no errors are detected, the baseline transfer is started based on the data copy schedule. The Operation Progress dialog box displays the information about the status of the precheck operations run during the baseline data copy.

3. Click the **Volumes** tab to view the status and progress of the baseline transfer.

   To view the detailed SnapMirror details of each volume, you can click **View Transition Details**. The number of concurrent SnapMirror transfers is based on the input provided in the schedule that is currently active. You can track the active schedule from the Data Copy Schedule tab on Dashboard.

   After the baseline data copy operation is completed, the incremental SnapMirror updates start based on the schedule provided while creating the project.

Related information

Creating a data copy schedule for SnapMirror transfers

Applying 7-Mode configurations

After the baseline data copy is completed, you can copy and apply all configurations from the 7-Mode system (including protocols and services configuration) to the ONTAP volumes. If the target cluster is running any version from ONTAP 8.3.2 and later supported releases, SAN configuration is transitioned in this phase.

If you are transitioning SAN volumes, you must have created at least one data LIF of the appropriate protocol (iSCSI or FC) for every node in the cluster.

- The configurations are applied in the apply configuration (precutover) phase, which has two modes: precutover read-only mode and precutover read/write mode.

The precutover read/write mode is not supported when the project contains:

- SAN volumes and the target cluster is running Data ONTAP 8.3.1 or earlier. In this situation, the following configurations are not applied in the precutover phase, instead they are applied during the cutover phase:
  - SAN configurations
  - Snapshot Schedule configurations
- SnapLock Compliance volumes.

  If the project contains SnapLock Compliance volumes, then the Snapshot Schedule configurations are not applied in the precutover phase, instead these configurations are applied during the cutover phase.

  See Considerations for transitioning of SnapLock Compliance volumes.

Steps

1. From the Dashboard, select the project.
2. Apply the configurations:

If you want to apply all configurations in…	Then…
Read-only mode	Click **Apply Configuration**.
Read/write mode	a. Select the **Test Mode** check box. b. Click **Apply Configuration**. The ONTAP volumes are made read/write and you can test the configurations and data access operations. c. Select **Apply configuration in test mode** in the Apply Configuration (Precutover) dialog box.

3. Select the **Customize the number of concurrent SnapMirror transfers and Throttle limit for this operation** check box to specify the number of SnapMirror data copy operations and throttle limit:
   a. Enter the maximum number of concurrent SnapMirror transfers to run during transition.
   b. Enter the percentage of available streams that can be used for SnapMirror transfers.

By default, the tool uses 50% of the available volume SnapMirror transfers.

c. Either enter a throttle limit or select **Maximum** to use the maximum bandwidth.

By default, the tool uses maximum throttle for configuration transition.

4. Select the **Transition Kerberos Configuration** check box to provide UNIX-based or Microsoft AD based Kerberos server configuration details for transition.

This option is enabled only when Kerberos is configured on the source 7-Mode storage system.

a. Enter the Kerberos server details such as the host name, IP address, user name, and password.

To transition the Kerberos configuration, at least one LIF has to be transitioned as part of the project and the LIF must be resolvable to a host name.

5. Click **Continue**.

The Operation Progress dialog box is displayed, and the copy configuration operation is started.

6. If the configuration transition is performed in read/write mode, click **Finish Testing** after the testing and verification of the configurations is complete.

This mode should be used only for testing purposes. All data written to the cluster on the volumes being migrated during test mode is lost.

The tool reestablishes the SnapMirror relationship and resynchronizes (based on the active schedule for that project at that time) the ONTAP volumes. Any data written to the 7-Mode is resynchronized with the ONTAP volumes.

For a successful resynchronization, a common Snapshot copy must exist between the 7-Mode and clustered Data ONTAP volumes. You should not manually delete the common Snapshot copy; otherwise, resynchronization fails.

The 7-Mode IP addresses remain operational. The LIFs are configured on the storage virtual machine (SVM) in the following ways:

- Existing 7-Mode IP addresses are created in the administrative down state.

  During the storage cutover, these IP addresses are removed from the 7-Mode system and the corresponding storage virtual machine (SVM) LIFs are brought to the administrative up state. If you select the precutover read/write mode, you must use a different LIF to gain access to the volumes being migrated to the cluster.

- New IP addresses are created in the administrative up state.

  If you select the precutover read/write mode, these LIFs can be used for testing access to the volumes being migrated in the cluster.

Related information

Managing logical interfaces

Considerations for quotas

7MTT v2.0/Transitioned Data ONTAP features

Configuring zones by using the FC zone plan

Before transitioning a SAN FC environment, you must configure zones by using the FC zone planner to group the initiator hosts and targets.

- The cluster and initiator hosts must be connected to the switch.
- The FC zone script file must be accessible.

Steps

1. If there are any changes to the igroup configurations on the 7-Mode systems, modify and regenerate the FC zone plan.

   Generating an assessment report by adding systems to the 7-Mode Transition Tool

2. Log in to the CLI of the switch.
3. Copy and execute the required zone commands one at a time.

   The following example runs the zone commands on the switch:

```
switch1:admin>config terminal
# Enable NPIV feature
feature npiv
zone name auto_transition_igroup_d31_194bf3 vsan 10
member pwwn 21:00:00:c0:dd:19:4b:f3
member pwwn 20:07:00:a0:98:32:99:07
member pwwn 20:09:00:a0:98:32:99:07
.......
.......
.......
copy running-config startup-config
```

4. Verify the data access from the cluster by using the test initiator hosts.
5. After the verification is complete, perform the following steps:
   a. Disconnect the test initiator hosts.
   b. Remove the zone configuration.

Performing on-demand SnapMirror updates

You can perform SnapMirror incremental updates for all the volumes before the cutover operation to reduce the cutover time.

- You cannot perform on-demand SnapMirror updates when incremental data transfers are scheduled after

baseline data copy and after precutover operation.

- This is an optional task.
  1. Click **Update Now** to perform a manual SnapMirror update.

     The Transition Update dialog box is displayed, where you can choose to customize the number of SnapMirror transfers and throttle limit for this operation.

  2. Select the **Customize the number of concurrent SnapMirror transfers and Throttle limit for this operation** check box to specify the number of SnapMirror data copy operations and throttle limit.
     a. Enter the maximum number of concurrent SnapMirror transfers to run during transition.
     b. Enter the percentage of available streams that the tool can use for SnapMirror transfers.

        By default, the tool uses 50% of the available volume SnapMirror transfers.

     c. Enter the throttle limit to use the maximum bandwidth.

        By default, the tool uses maximum throttle for configuration transition.

  3. Click **Continue**.

Related information

Starting baseline data copy

Creating a data copy schedule for SnapMirror transfers

Completing a transition project

You can complete a transition by completing the individual projects. Because this operation is disruptive, you should evaluate when to run it. When transitioning volumes in a SnapMirror relationship, the secondary project must be completed before completing the transition of the primary project.

The storage cutover is completed in a few minutes. The time required for the clients to remount the data varies. The timing of the storage cutover or outage window depends on the following factors:

- Final update

  The final update of the data depends on the amount of change in the source data since the last update. Incremental transfers minimize the amount of data that has to be transferred during cutover.

- Reconnecting clients

  If updates are required for each client to connect to the cluster, the number of clients that have to be updated determines the cutover time.

Outages apply only to the volumes that are being migrated. You do not need to shut down the entire source 7-Mode storage system. Volumes on the source system that are not being migrated can remain online and accessible.

1. From the Migration Dashboard, select the project that you want to complete.

2. Disconnect client access manually.
3. Click **Complete Transition**.

    a. If you want to keep the 7-Mode source volumes online after the transition, clear the **Take source volumes offline after transition** checkbox.

    By default, this option is selected, and the source volumes are taken offline.

    b. If you have selected SnapLock volumes for Chain of Custody verification, select the **I understand that I must not take 7-Mode SnapLock volumes offline during Chain of Custody verification** checkbox to keep the SnapLock volumes online after transition.

    c. If you have selected the transition of a SnapMirror relationship between clusters that are running ONTAP 9.3 or later supported releases, select the **I understand that I must manually convert SnapMirror relationship type from data_protection to extended_data_protection** checkbox.

    d. Select the **Customize the number of concurrent SnapMirror transfers and Throttle limit for this operation** checkbox to specify the number of SnapMirror data copy operations and the throttle limit.

    e. Click **Continue**.

    The results of the cutover operation are displayed.

The 7-Mode IP addresses selected for the transition are unconfigured from the 7-Mode storage system, and the associated LIFs created before the cutover are brought to the administrative up state. The 7-Mode volumes are offline.

From the cluster, run the vserver check lif-multitenancy run command to verify that the name servers are reachable by using the transitioned LIFs.

If you have created a new LIF, the users and applications of the transitioned volumes must be remapped to the drives by using the new IP addresses and ports after all of the projects have been completed.

If you have completed the transition of a SnapMirror relationship between clusters that are running ONTAP 9.3 or later supported releases, you must convert the SnapMirror relationship from type DP to type XDP.

Data protection

Related information

Guidelines for deciding when to perform cutover

Completing the Chain of Custody verification

If one or more SnapLock volumes are selected for Chain of Custody verification, then you must perform the Chain of Custody operation to generate a Chain of Custody report.

You must have completed the transition of the project.

SnapLock Chain of Custody operation is supported for volumes with files that have file names with only ASCII characters.

1. From the Migration Dashboard, click **Start Chain of Custody**.

If you want to keep the 7-Mode SnapLock volumes online after the Chain of Custody verification, you should clear the **Take 7-Mode SnapLock volumes selected for Chain of Custody verification offline after Chain of Custody verification operation is completed** check box.

2. Click **Continue**.

   The Chain of Custody verification operation is initiated. This operation can take a significant amount of time based on the number of files on the SnapLock volumes. You can click **Run in Background** to perform the operation in the background.

   You can track the progress of the Chain of Custody verification operation by clicking the SnapLock Chain of Custody tab in the Migration Dashboard window. This tab displays per volume progress of the Chain of Custody operation.

3. After the Chain of Custody operation is complete, click **Download Report** in the SnapLock Chain of Custody tab to download the Chain of Custody verification report.

   The Chain of Custody verification report contains details about whether the SnapLock Chain of Custody verification succeeded. The report shows the total file count and the number of non-WORM files in each of the 7-Mode SnapLock volumes that are selected for the Chain of Custody operation. You can also verify the number of files for which the fingerprints matched and unmatched. The report also shows the number of WORM files for which the Chain of Custody verification failed and reason for the failure.