Revert ONTAP

ONTAP 9

NetApp
November 01, 2023

Table of Contents

Revert ONTAP

Revert ONTAP overview

To transition a cluster to an earlier ONTAP release, you must perform a reversion.

The information in this section will guide you through the steps you should take before and after you revert, including the resources you should read and the necessary pre- and post-revert checks you should perform.

If you need to transition a cluster from ONTAP 9.1 to ONTAP 9.0, you need to use the downgrade procedure documented here.

Do I need technical support to revert?

You can revert without assistance on new or test clusters. You should call technical support to revert production clusters. You should also call technical support if you experience any of the following:

- You are in a production environment and revert fails or you encounter any problems before or after the revert such as:
  - The revert process fails and cannot finish.
  - The revert process finishes, but the cluster is unusable in a production environment.
  - The revert process finishes and the cluster goes into production, but you are not satisfied with its behavior.
- You created volumes in ONTAP 9.5 or later and you need to revert to an earlier version. Volumes using adaptive compression must be uncompressed before reverting.

Revert paths

The version of ONTAP that you can revert to varies based on the version of ONTAP currently running on your nodes. You can use the `system image show` command to determine the version of ONTAP running on each node.

These guidelines refer only to on-premises ONTAP releases. For information about reverting ONTAP in the cloud, see Reverting or downgrading Cloud Volumes ONTAP.

You can revert from…	To…
ONTAP 9.13.1	ONTAP 9.12.1
ONTAP 9.12.1	ONTAP 9.11.1
ONTAP 9.11.1	ONTAP 9.10.1
ONTAP 9.10.1	ONTAP 9.9.1

You can revert from…	To…
ONTAP 9.9.1	ONTAP 9.8
ONTAP 9.8	ONTAP 9.7
ONTAP 9.7	ONTAP 9.6
ONTAP 9.6	ONTAP 9.5
ONTAP 9.5	ONTAP 9.4
ONTAP 9.4	ONTAP 9.3
ONTAP 9.3	ONTAP 9.2
ONTAP 9.2	ONTAP 9.1
ONTAP 9.1 or ONTAP 9	Data ONTAP 8.3.x

If you need to change from ONTAP 9.1 to 9.0, you should follow the downgrade process documented here.

What should I read before I revert?

Resources to review before you revert

Before you revert ONTAP, you should confirm hardware support and review resources to understand issues you might encounter or need to resolve.

1. Review the ONTAP 9 Release Notes for the target release.

   The “Important cautions” section describes potential issues that you should be aware of before downgrading or reverting.

2. Confirm that your hardware platform is supported in the target release.

   NetApp Hardware Universe

3. Confirm that your cluster and management switches are supported in the target release.

   You must verify that the NX-OS (cluster network switches), IOS (management network switches), and reference configuration file (RCF) software versions are compatible with the version of ONTAP to which you are reverting.

   NetApp Downloads: Cisco Ethernet Switch

4. If your cluster is configured for SAN, confirm that the SAN configuration is fully supported.

All SAN components—including target ONTAP software version, host OS and patches, required Host Utilities software, and adapter drivers and firmware—should be supported.

NetApp Interoperability Matrix Tool

Revert considerations

You need to consider the revert issues and limitations before beginning an ONTAP reversion.

- Reversion is disruptive.

  No client access can occur during the reversion. If you are reverting a production cluster, be sure to include this disruption in your planning.

- Reversion affects all nodes in the cluster.

  The reversion affects all nodes in the cluster; however, the reversion must be performed and completed on each HA pair before other HA pairs are reverted.

- The reversion is complete when all nodes are running the new target release.

  When the cluster is in a mixed-version state, you should not enter any commands that alter the cluster operation or configuration except as necessary to satisfy reversion requirements; monitoring operations are permitted.

  > If you have reverted some, but not all of the nodes, do not attempt to upgrade the cluster back to the source release.

- When you revert a node, it clears the cached data in a Flash Cache module.

  Because there is no cached data in the Flash Cache module, the node serves initial read requests from disk, which results in decreased read performance during this period. The node repopulates the cache as it serves read requests.

- A LUN that is backed up to tape running on ONTAP 9.x can be restored only to 9.x and later releases and not to an earlier release.
- If your current version of ONTAP supports In-Band ACP (IBACP) functionality, and you revert to a version of ONTAP that does not support IBACP, the alternate path to your disk shelf is disabled.
- If LDAP is used by any of your storage virtual machines (SVMs), LDAP referral must be disabled before reversion.
- In MetroCluster IP systems using switches which are MetroCluster compliant but not MetroCluster validated, the reversion from ONTAP 9.7 to 9.6 is disruptive as there is no support for systems using ONTAP 9.6 and earlier.

Things to verify before you revert

Before revert, you should verify your cluster health, storage health, and system time. You should also delete any cluster jobs that are running and gracefully terminate any SMB sessions that are not continuously available.

Verify cluster health

Before you revert cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum.

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster: `cluster show`

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
```

   If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. Set the privilege level to advanced:
   `set -privilege advanced`

   Enter `y` to continue.

3. Verify the configuration details for each RDB process.
   - The relational database epoch and database epochs should match for each node.
   - The per-ring quorum master should be the same for all nodes.

     Note that each ring might have a different quorum master.

To display this RDB process…	Enter this command…
Management application	`cluster ring show -unitname mgmt`
Volume location database	`cluster ring show -unitname vldb`
Virtual-Interface manager	`cluster ring show -unitname vifmgr`
SAN management daemon	`cluster ring show -unitname bcomd`

     This example shows the volume location database process:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. Return to the admin privilege level:
   `set -privilege admin`
5. If you are operating in a SAN environment, verify that each node is in a SAN quorum: `event log show -severity informational -message-name scsiblade.*`

   The most recent scsiblade event message for each node should indicate that the scsi-blade is in quorum.

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time              Node        Severity       Event
---------------  ---------- -------------- ---------------------------
MM/DD/YYYY TIME  node0       INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1       INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

Related information

System administration

Verify storage health

Before you revert a cluster, you should verify the status of your disks, aggregates, and volumes.

1. Verify disk status:

To check for…	Do this…
Broken disks	a. Display any broken disks: `storage disk show -state broken` b. Remove or replace any broken disks.

To check for…	Do this…
Disks undergoing maintenance or reconstruction	a. Display any disks in maintenance, pending, or reconstructing states: `storage disk show -state maintenance|pending|reconstructing` b. Wait for the maintenance or reconstruction operation to finish before proceeding.

2. Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates: `storage aggregate show -state !online`

   This command displays the aggregates that are *not* online. All aggregates must be online before and after performing a major upgrade or reversion.

   ```
   cluster1::> storage aggregate show -state !online
   There are no entries matching your query.
   ```

3. Verify that all volumes are online by displaying any volumes that are *not* online: `volume show -state !online`

   All volumes must be online before and after performing a major upgrade or reversion.

   ```
   cluster1::> volume show -state !online
   There are no entries matching your query.
   ```

4. Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

   See the Knowledge Base article Volume Showing WAFL Inconsistent on how to address the inconsistent volumes.

Related information

Disk and aggregate management

Verifying the system time

Before you revert, you should verify that NTP is configured, and that the time is synchronized across the cluster.

1. Verify that the cluster is associated with an NTP server: `cluster time-service ntp server show`
2. Verify that each node has the same date and time: `cluster date show`

```
cluster1::> cluster date show
Node      Date                Timezone
--------- ------------------- -------------------------
node0     4/6/2013 20:54:38   GMT
node1     4/6/2013 20:54:38   GMT
node2     4/6/2013 20:54:38   GMT
node3     4/6/2013 20:54:38   GMT
4 entries were displayed.
```

Verify that no jobs are running

Before you revert the ONTAP software, you must verify the status of cluster jobs. If any aggregate, volume, NDMP (dump or restore), or Snapshot jobs (such as create, delete, move, modify, replicate, and mount jobs) are running or queued, you must allow the jobs to finish successfully or stop the queued entries.

1. Review the list of any running or queued aggregate, volume, or Snapshot jobs: `job show`

```
cluster1::> job show
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
8629   Vol Reaper           cluster1   -              Queued
       Description: Vol Reaper Job
8630   Certificate Expiry Check
                            cluster1   -              Queued
       Description: Certificate Expiry Check
.
.
.
```

2. Delete any running or queued aggregate, volume, or Snapshot copy jobs: `job delete -id job_id`

```
cluster1::> job delete -id 8629
```

3. Verify that no aggregate, volume, or Snapshot jobs are running or queued: `job show`

   In this example, all running and queued jobs have been deleted:

```
cluster1::> job show
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
9944   SnapMirrorDaemon_7_2147484678
                            cluster1   node1          Dormant
       Description: Snapmirror Daemon for 7_2147484678
18377  SnapMirror Service Job
                            cluster1   node0          Dormant
       Description: SnapMirror Service Job
2 entries were displayed
```

SMB sessions that should be terminated

Before you revert, you should identify and gracefully terminate any SMB sessions that are not continuously available.

Continuously available SMB shares, which are accessed by Hyper-V or Microsoft SQL Server clients using the SMB 3.0 protocol, do not need to be terminated before upgrading or downgrading.

1. Identify any established SMB sessions that are not continuously available: `vserver cifs session show -continuously-available No -instance`

   This command displays detailed information about any SMB sessions that have no continuous availability. You should terminate them before proceeding with the ONTAP downgrade.

```
cluster1::> vserver cifs session show -continuously-available No
-instance

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
      Workstation IP address: 203.0.113.20
    Authentication Mechanism: NTLMv2
                Windows User: CIFSLAB\user1
                   UNIX User: nobody
                 Open Shares: 1
                  Open Files: 2
                  Open Other: 0
              Connected Time: 8m 39s
                   Idle Time: 7m 45s
           Protocol Version: SMB2_1
      Continuously Available: No
1 entry was displayed.
```

2. If necessary, identify the files that are open for each SMB session that you identified: `vserver cifs session file show -session-id session_ID`

```
cluster1::> vserver cifs session file show -session-id 1

Node:       node1
Vserver:    vs1
Connection: 4160072788
Session:    1
File    File      Open Hosting
Continuously
ID      Type      Mode Volume          Share                 Available
------- --------- ---- --------------- ---------------------
------------
1       Regular   rw   vol10           homedirshare          No
Path: \TestDocument.docx
2       Regular   rw   vol10           homedirshare          No
Path: \file1.txt
2 entries were displayed.
```

NVMe/TCP secure authentication

If you are running the NVMe/TCP protocol and you have established secure authentication using DH-HMAC-CHAP, you must remove any host using DH-HMAC-CHAP from the NVMe subsystem before you revert. If the hosts are not removed, revert will fail.

What else should I check before I revert?

Pre-revert checks

Depending on your environment, you need to consider certain factors before revert. Get started by reviewing the table below to see what special considerations you need to consider.

Ask yourself…	If your answer is yes, then do this…
Is my cluster running SnapMirror?	• Review considerations for reverting systems with SnapMirror Synchronous relationships • Review reversion requirements for SnapMirror and SnapVault relationships
Is my cluster running SnapLock?	Set autocommit periods
Do I have Split FlexClone volumes?	Reverse physical block sharing
Do I have FlexGroup volumes?	Disable qtree functionality
Do I have CIFS servers in workgroup mode?	Move or delete CIFS servers in workgroup mode
Do I have deduplicated volumes?	Verify volume contains enough free space
Do I have Snapshot copies?	Prepare Snapshop copies
Am I reverting to ONTAP 8.3.x?	Identify user accounts that use SHA-2 hash function
Is anti-ransomware protection configured for ONTAP 9.11.1 or later?	Check anti-ransomware licensing
Is S3 multiprotocol access configured for 9.12.1 or later?	Remove S3 NAS bucket configuration

MetroCluster pre-revert checks

Depending on your MetroCluster configuration, you need to consider certain factors before revert. Get started by reviewing the table below to see what special considerations you need to consider.

Ask yourself…	If your answer is yes, then do this…
Do I have a two- or four-node MetroCluster configuration?	Disable automatic unplanned switchover
Do I have a four- or eight-node MetroCluster IP or fabric-attached configuration running ONTAP 9.12.1 or later?	Disable IPsec

SnapMirror

Considerations for reverting systems with SnapMirror Synchronous relationships

You must be aware of the considerations for SnapMirror Synchronous relationships before reverting from ONTAP 9.6 to ONTAP 9.5.

Before reverting, you must take the following steps if you have SnapMirror Synchronous relationships:

- You must delete any SnapMirror Synchronous relationship in which the source volume is serving data using NFSv4 or SMB.

  ONTAP 9.5 does not support NFSv4 and SMB.

- You must delete any SnapMirror Synchronous relationships in a mirror-mirror cascade deployment.

  A mirror-mirror cascade deployment is not supported for SnapMirror Synchronous relationships in ONTAP 9.5.

- If the common Snapshot copies in ONTAP 9.5 are not available during revert, you must initialize the SnapMirror Synchronous relationship after reverting.

  After two hours of upgrade to ONTAP 9.6, the common Snapshot copies from ONTAP 9.5 are automatically replaced by the common Snapshot copies in ONTAP 9.6. Therefore, you cannot resynchronize the SnapMirror Synchronous relationship after reverting if the common Snapshot copies from ONTAP 9.5 are not available.

Reversion requirements for SnapMirror and SnapVault relationships

The system node revert-to command notifies you of any SnapMirror and SnapVault relationships that need to be deleted or reconfigured for the reversion process to be completed. However, you should be aware of these requirements before you begin the reversion.

- All SnapVault and data protection mirror relationships must be quiesced and then broken.

  After the reversion is completed, you can resynchronize and resume these relationships if a common Snapshot copy exists.

- SnapVault relationships must not contain the following SnapMirror policy types:
  - async-mirror

    You must delete any relationship that uses this policy type.

  - MirrorAndVault

    If any of these relationships exist, you should change the SnapMirror policy to mirror-vault.

- All load-sharing mirror relationships and destination volumes must be deleted.
- SnapMirror relationships with FlexClone destination volumes must be deleted.
- Network compression must be disabled for each SnapMirror policy.

- The all_source_snapshot rule must be removed from any async-mirror type SnapMirror policies.

  > The Single File Snapshot Restore (SFSR) and Partial File Snapshot Restore (PFSR) operations are deprecated on the root volume.

- Any currently running single file and Snapshot restore operations must be completed before the reversion can proceed.

  You can either wait for the restore operation to finish, or you can abort it.

- Any incomplete single file and Snapshot restore operations must be removed by using the snapmirror restore command.

Set autocommit periods for SnapLock volumes before reverting

To revert from ONTAP 9, the value of the autocommit period for SnapLock volumes must be set in hours, not days. Before attempting to revert, you must check the autocommit value for your SnapLock volumes and modify it from days to hours, if necessary.

1. Verify that there are SnapLock volumes in the cluster that have unsupported autocommit periods:`volume snaplock show -autocommit-period *days`
2. Modify the unsupported autocommit periods to hours: `volume snaplock modify -vserver vserver_name -volume volume_name -autocommit-period value hours`

Reverse physical block sharing in split FlexClone volumes

If you have split a FlexClone volume from its parent volume, you must undo the sharing of any physical block between the clone and its parent volume before reverting from ONTAP 9.4 or later to an earlier version of ONTAP.

This task is applicable only for AFF systems when split has been run on any of the FlexClone volumes.

1. Log in to the advanced privilege level: `set -privilege advanced`
2. Identify the split FlexClone volumes with shared physical blocks: `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
Node            Vserver   Volume        Aggregate
--------------- --------- ------------- -------------
node1           vs1       vol_clone1    aggr1
node2           vs2       vol_clone2    aggr2
2 entries were displayed.
```

3. Undo the physical block sharing in all of the split FlexClone volumes across the cluster: `volume clone sharing-by-split undo start-all`
4. Verify that there are no split FlexClone volumes with shared physical blocks: `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
This table is currently empty.
```

Disable qtree functionality in FlexGroup volumes before reverting

Qtrees for FlexGroup volumes are not supported prior to ONTAP 9.3. You must disable the qtree functionality on FlexGroup volumes before reverting from ONTAP 9.3 to an earlier version of ONTAP.

The qtree functionality is enabled either when you create a qtree or if you modify the security-style and oplock-mode attributes of the default qtree.

1. Identify and delete all of the non-default qtrees in each FlexGroup volume that are enabled with the qtree functionality:
   a. Log in to the advanced privilege level: `set -privilege advanced`
   b. Verify if any FlexGroup volume is enabled with the qtree functionality.

      For ONTAP 9.6 or later, use: `volume show -is-qtree-caching-enabled true`

      For ONTAP 9.5 or earlier, use: `volume show -is-flexgroup-qtree-enabled true`

      ```
      cluster1::*> volume show -is-flexgroup-qtree-enabled true
      Vserver   Volume       Aggregate    State      Type       Size
      Available Used%
      --------- ------------ ------------ ---------- ---- ----------
      ---------- -----
      vs0       fg           -            online     RW        320MB
      220.4MB   31%
      ```

   c. Delete all of the non-default qtrees in each FlexGroup volume that are enabled with the qtree functionality: `volume qtree delete -vserver svm_name -volume volume_name -qtree qtree_name`

      If the qtree functionality is enabled because you modified the attributes of the default qtree and if you do not have any qtrees, you can skip this step.

      ```
      cluster1::*> volume qtree delete -vserver vs0 -volume fg -qtree
      qtree4
      WARNING: Are you sure you want to delete qtree qtree4 in volume fg
      vserver vs0?  {y|n}: y
      [Job 38] Job is queued: Delete qtree qtree4 in volume fg vserver vs0.
      ```

2. Disable the qtree functionality on each FlexGroup volume: `volume flexgroup qtree-disable -vserver svm_name -volume volume_name`

```
cluster1::*> volume flexgroup qtree-disable -vserver vs0 -volume fg
```

3. Identify and delete any Snapshot copies that are enabled with the qtree functionality.
   a. Verify if any Snapshot copies are enabled with the qtree functionality: `volume snapshot show -vserver vserver_name -volume volume_name -fields is-flexgroup-qtree-enabled`

```
cluster1::*> volume snapshot show -vserver vs0 -volume fg -fields is-
flexgroup-qtree-enabled
vserver volume snapshot is-flexgroup-qtree-enabled
------- ------ -------- --------------------------
vs0     fg     fg_snap1 true
vs0     fg     daily.2017-09-27_0010 true
vs0     fg     daily.2017-09-28_0010 true
vs0     fg     snapmirror.0241f354-a865-11e7-a1c0-
00a098a71764_2147867740.2017-10-04_124524 true
```

   b. Delete all of the Snapshot copies that are enabled with the qtree functionality: `volume snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot_name -force true -ignore-owners true`

      The Snapshot copies that must be deleted include regular Snapshot copies and the Snapshot copies taken for SnapMirror relationships. If you have created any SnapMirror relationship for the FlexGroup volumes with a destination cluster that is running ONTAP 9.2 or earlier, you must delete all of the Snapshot copies that were taken when the source FlexGroup volume was enabled for the qtree functionality.

```
cluster1::> volume snapshot delete -vserver vs0 -volume fg -snapshot
daily.2017-09-27_0010 -force true -ignore-owners true
```

Related information

FlexGroup volumes management

Identify and move SMB servers in workgroup mode

Before performing a revert, you must delete any SMB servers in workgroup mode or move them in to a domain. Workgroup mode is not supported on ONTAP versions prior to ONTAP 9.

1. Identify any SMB servers with a Authentication Style of workgroup: `vserver cifs show`
2. Move or delete the servers you identified:

If you are going to…	Then use this command….
Move the SMB server from the workgroup to an Active Directory domain:	`vserver cifs modify -vserver vserver_name -domain domain_name`
Delete the SMB server	`vserver cifs delete -vserver vserver_name`

3. If you deleted the SMB server, enter the username of the domain, then enter the user password.

Related information

SMB management

Verify deduplicated volumes have enough free space before reverting

Before reverting from any version of ONTAP 9, you must ensure that the volumes contain sufficient free space for the revert operation.

The volume must have enough space to accommodate the savings that were achieved through the inline detection of blocks of zeros. See the Knowledge Base article How to see space savings from deduplication, compression, and compaction in ONTAP 9.

If you have enabled both deduplication and data compression on a volume that you want to revert, then you must revert data compression before reverting deduplication.

1. Use the volume efficiency show command with the -fields option to view the progress of the efficiency operations that are running on the volumes.

   The following command displays the progress of efficiency operations: `volume efficiency show -fields vserver,volume,progress`

2. Use the volume efficiency stop command with the -all option to stop all active and queued deduplication operations.

   The following command stops all active and queued deduplication operations on volume VolA: `volume efficiency stop -vserver vs1 -volume VolA -all`

3. Use the set -privilege advanced command to log in at the advanced privilege level.
4. Use the volume efficiency revert-to command with the -version option to downgrade the efficiency metadata of a volume to a specific version of ONTAP.

   The following command reverts the efficiency metadata on volume VolA to ONTAP 9.x: `volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x`

   > The volume efficiency revert-to command reverts volumes that are present on the node on which this command is executed. This command does not revert volumes across nodes.

5. Use the volume efficiency show command with the -op-status option to monitor the progress of the downgrade.

   The following command monitors and displays the status of the downgrade: `volume efficiency show`

`-vserver vs1 -op-status Downgrading`

6. If the revert does not succeed, use the volume efficiency show command with the -instance option to see why the revert failed.

   The following command displays detailed information about all fields: `volume efficiency show -vserver vs1 -volume vol1 - instance`

7. After the revert operation is complete, return to the admin privilege level: `set -privilege admin`

   Logical storage management

Prepare Snapshot copies before reverting

Before reverting to an earlier ONTAP release, you must disable all Snapshot copy policies and delete any Snapshot copies that were created after upgrading to the current release.

If you are reverting in a SnapMirror environment, you must first have deleted the following mirror relationships:

- All load-sharing mirror relationships
- Any data protection mirror relationships that were created in ONTAP 8.3.x
- All data protection mirror relationships if the cluster was re-created in ONTAP 8.3.x

1. Disable Snapshot copy policies for all data SVMs: `volume snapshot policy modify -vserver * -enabled false`
2. Disable Snapshot copy policies for each node's aggregates:
   a. Identify the node's aggregates by using the run-nodenodenameaggr status command.
   b. Disable the Snapshot copy policy for each aggregate: `run -node nodename aggr options aggr_name nosnap on`
   c. Repeat this step for each remaining node.
3. Disable Snapshot copy policies for each node's root volume:
   a. Identify the node's root volume by using the run-nodenodenamevol status command.

      You identify the root volume by the word root in the Options column of the vol status command output.

      ```
      vs1::> run -node node1 vol status

               Volume State           Status            Options
                 vol0 online          raid_dp, flex     root, nvfail=on
                                      64-bit
      ```

   b. Disable the Snapshot copy policy on the root volume: `run -node nodename vol options root_volume_name nosnap on`
   c. Repeat this step for each remaining node.

4. Delete all Snapshot copies that were created after upgrading to the current release:
   a. Set the privilege level to advanced: `set -privilege advanced`
   b. Disable the snapshots:`snapshot policy modify -vserver * -enabled false`
   c. Delete the node's newer-version Snapshot copies: `volume snapshot prepare-for-revert -node nodename`

      This command deletes the newer-version Snapshot copies on each data volume, root aggregate, and root volume.

      If any Snapshot copies cannot be deleted, the command fails and notifies you of any required actions you must take before the Snapshot copies can be deleted. You must complete the required actions and then rerun the volume snapshot prepare-for-revert command before proceeding to the next step.

      ```
      cluster1::*> volume snapshot prepare-for-revert -node node1

      Warning: This command will delete all Snapshot copies that have
      the format used by the current version of ONTAP. It will fail if
      any Snapshot copy polices are enabled, or
               if any Snapshot copies have an owner. Continue? {y|n}: y
      ```

   d. Verify that the Snapshot copies have been deleted: `volume snapshot show -node nodename`

      If any newer-version Snapshot copies remain, force them to be deleted: `volume snapshot delete {-fs-version 9.0 -node nodename -is-constituent true} -ignore -owners -force`

   e. Repeat this step c for each remaining node.
   f. Return to the admin privilege level: `set -privilege admin`

You must perform these steps on both the clusters in MetroCluster configuration.

Identify user accounts that use SHA-2 hash function

If you are reverting from ONTAP 9.1 or ONTAP 9.0 to ONTAP 8.3.x, SHA-2 account users can no longer be authenticated with their passwords. Before you revert, you should identify the user accounts that use the SHA-2 hash function, so that after reverting, you can have them reset their passwords to use the encryption type (MD5) that is supported by the release you revert to.

1. Change to the privilege setting to advanced: `set -privilege advanced`
2. Identify the user accounts that use the SHA-2 has function: `security login show -vserver * -username * -application * -authentication-method password -hash-function !md5`
3. Retain the command output for use after the revert.

During the revert, you will be prompted to run the advanced command `security login password-prepare-to-downgrade` to reset your own password to use the MD5 hash function. If your password is not encrypted with MD5, the command prompts you for a new password and encrypts it with MD5, enabling your credential to be authenticated after the revert.

Check Autonomous Ransomware Protection licensing before reverting from ONTAP 9.11.1 or later

If you have configured Autonomous Ransomware Protection (ARP) and you revert from ONTAP 9.11.1 or later to ONTAP 9.10.1 or earlier, you might experience warning messages and limited ARP functionality.

In ONTAP 9.11.1, the Anti-ransomware license replaced the Multi-Tenant Key Management (MTKM) license. If your system has the Anti_ransomware license but no MT_EK_MGMT license, you will see a warning during revert that ARP cannot be enabled on new volumes upon revert.

The volumes with existing protection will continue to work normally after revert, and ARP status can be displayed using the ONTAP CLI. However, System Manager cannot show ARP status without the MTKM license.

Therefore, if you want ARP to continue after reverting to ONTAP 9.10.1, be sure the MTKM license is installed before reverting. Learn about ARP licensing.

Remove S3 NAS bucket configuration before reverting from ONTAP 9.12.1 or later

If you have configured S3 client access for NAS data and you revert from ONTAP 9.12.1 or later to ONTAP 9.11.1 or earlier, you must remove the NAS bucket configuration, and you must remove any name mappings (S3 users to Windows or Unix users) before reverting.

About this task

The following tasks are completed in the background during the revert process.

- Remove all partially completed singleton object creations (that is, all entries in hidden directories).
- Remove all hidden directories; there might be one on for each volume that is accessible from the root of the export mapped from the S3 NAS bucket.
- Remove the upload table.
- Delete any default-unix-user and default-windows-user values for all configured S3 servers.

System Manager

1. Remove a S3 NAS bucket configuration.
   Click **Storage > Buckets**, click ⋮ for each configured S3 NAS bucket, then click **Delete**.
2. Remove local name mappings for UNIX or Windows clients (or both).
   a. Click **Storage > Buckets**, then select the S3/NAS-enabled storage VM.
   b. Select **Settings**, then click → in **Name Mapping** (under **Host Users and Groups**).
   c. In the **S3 to Windows** or **S3 to UNIX tiles** (or both), click ⋮ for each configured mapping, then click **Delete**.

CLI

1. Remove S3 NAS bucket configuration.
   `vserver object-store-server bucket delete -vserver` *`svm_name`* `-bucket` *`s3_nas_bucket_name`*
2. Remove name mappings.
   `vserver name-mapping delete -vserver` *`svm_name`* `-direction s3-unix`
   `vserver name-mapping delete -vserver` *`svm_name`* `-direction s3-win`

Disable automatic unplanned switchover before reverting two-node and four-node MetroCluster configurations

Before reverting a two-node or four-node MetroCluster configuration, you must disable automatic unplanned switchover (AUSO).

1. On both the clusters in MetroCluster, disable automatic unplanned switchover: `metrocluster modify -auto-switchover-failure-domain auso-disabled`

Related information

MetroCluster management and disaster recovery

Disable IPsec before reverting MetroCluster configurations

Before reverting a MetroCluster configuration, you must disable IPsec.

You cannot revert ONTAP in a MetroCluster configuration running ONTAP 9.12.1 with IPsec enabled. A check is performed before revert to ensure there are no IPsec configurations within the MetroCluster configuration. You must remove any IPsec configurations present and disable IPsec before continuing with the revert. Reverting ONTAP is blocked if IPsec is enabled, even when you have not configured any user policies.

Download and install the ONTAP software image

Related information

You must first download the ONTAP software from the NetApp Support site; then you can install it.

Download the software image

To downgrade or revert from ONTAP 9.4 and later, you can copy the ONTAP software image from the NetApp Support Site to a local folder. For a downgrade or revert to ONTAP 9.3 or earlier, you must copy the ONTAP software image to an HTTP server or FTP server on your network.

You should note the following important information:

- Software images are specific to platform models.

  You must obtain the correct image for your cluster. Software images, firmware version information, and the latest firmware for your platform model are available on the NetApp Support Site.

- Software images include the latest version of system firmware that was available when a given version of ONTAP was released.
- If you are downgrading a system with NetApp Volume Encryption from ONTAP 9.5 or later, you must download the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption.

  If you use the ONTAP software image for restricted countries to downgrade or revert a system with NetApp Volume Encryption, the system panics and you lose access to your volumes.

  1. Locate the target ONTAP software in the Software Downloads area of the NetApp Support Site.
  2. Copy the software image.
     - For ONTAP 9.3 or earlier, copy the software image (for example, 93_q_image.tgz) from the NetApp Support Site to the directory on the HTTP server or FTP server from which the image will be served.
     - For ONTAP 9.4 or later, copy the software image (for example, 97_q_image.tgz) from the NetApp Support Site to the directory on the HTTP server or FTP server from which the image will be served or to a local folder.

Install the software image

You must install the target software image on the cluster's nodes.

- If you are downgrading or reverting a system with NetApp Volume Encryption from ONTAP 9.5 or later, you must have downloaded the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption.

  If you use the ONTAP software image for restricted countries to downgrade or revert a system with NetApp Volume Encryption, the system panics and you lose access to your volumes.

  1. Set the privilege level to advanced, entering **y** when prompted to continue: `set -privilege advanced`

     The advanced prompt (`*>`) appears.

  2. Install the software image on the nodes.

     This command downloads and installs the software image on all of the nodes simultaneously. To download and install the image on each node one at a time, do not specify the -background parameter.

     - If you are downgrading or reverting a non-MetroCluster configuration or a two-node MetroCluster

configuration:`system node image update -node * -package location -replace -package true -setdefault true -background true`

This command uses an extended query to change the target software image, which is installed as the alternate image, to be the default image for the node.

- If you are dowgrading or reverting a four or eight-node MetroCluster configuration, you must issue the following command on both clusters: `system node image update -node * -package location -replace-package true true -background true -setdefault false`

  This command uses an extended query to change the target software image, which is installed as the alternate image on each node.

3. Enter `y` to continue when prompted.
4. Verify that the software image is downloaded and installed on each node: `system node image show-update-progress -node *`

   This command displays the current status of the software image download and installation. You should continue to run this command until all nodes report a Run Status of Exited, and an Exit Status of Success.

   The system node image update command can fail and display error or warning messages. After resolving any errors or warnings, you can run the command again.

   This example shows a two-node cluster in which the software image is downloaded and installed successfully on both nodes:

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

Revert an ONTAP cluster

To take the cluster offline to revert to an earlier ONTAP release, you must disable storage failover and the data LIFs, address reversion preconditions, revert the cluster and file

system configurations on a node, and then repeat the process for each additional node in the cluster.

You must have completed the revert verifications and pre-checks.

Reverting a cluster requires you to take the cluster offline for the duration of the reversion.

1. Set the privilege level to advanced: `set -privilege advanced`

   Enter **y** when prompted to continue.

2. Verify that the target ONTAP software is installed: `system image show`

   The following example shows that version 9.1 is installed as the alternate image on both nodes:

```
cluster1::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   true    true    9.2         MM/DD/YYYY TIME
         image2   false   false   9.1         MM/DD/YYYY TIME
node1
         image1   true    true    9.2         MM/DD/YYYY TIME
         image2   false   false   9.1         MM/DD/YYYY TIME
4 entries were displayed.
```

3. Disable all of the data LIFs in the cluster: `network interface modify {-role data} -status -admin down`
4. Determine if you have inter-cluster flexcache relationships: `flexcache origin show-caches -relationship-type inter-cluster`
5. If inter-cluster flexcaches are present, disable the data lifs on the cache cluster: `network interface modify -vserver vserver_name -lif lif_name -status-admin down`
6. If the cluster consists of only two nodes, disable cluster HA: `cluster ha modify -configured false`
7. Disable storage failover for the nodes in the HA pair from either node: `storage failover modify -node nodename -enabled false`

   You only need to disable storage failover once for the HA pair. When you disable storage failover for a node, storage failover is also disabled on the node's partner.

8. Log in to the node that you want to revert.

   To revert a node, you must be logged in to the cluster through the node's node management LIF.

9. Set the node's target ONTAP software image to be the default image: `system image modify -node nodename -image target_image -isdefault true`

10. Verify that the target ONTAP software image is set as the default image for the node that you are reverting: `system image show`

    The following example shows that version 9.1 is set as the default image on node0:

```
cluster1::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   false   true    9.2         MM/DD/YYYY TIME
         image2   true    false   9.1         MM/DD/YYYY TIME
node1
         image1   true    true    9.2         MM/DD/YYYY TIME
         image2   false   false   9.1         MM/DD/YYYY TIME
4 entries were displayed.
```

11. If the cluster consists of only two nodes, verify that the node does not hold epsilon:
    a. Check whether the node currently holds epsilon: `cluster show -node nodename`

       The following example shows that the node holds epsilon:

```
cluster1::*> cluster show -node node1

          Node: node1
          UUID: 026efc12-ac1a-11e0-80ed-0f7eba8fc313
       Epsilon: true
   Eligibility: true
        Health: true
```

    b. If the node holds epsilon, mark epsilon as false on the node so that epsilon can be transferred to the node's partner: `cluster modify -node nodenameA -epsilon false`
    c. Transfer epsilon to the node's partner by marking epsilon true on the partner node: `cluster modify -node nodenameB -epsilon true`
12. Verify that the node is ready for reversion: `system node revert-to -node nodename -check -only true -version 9.x`

    The check-only parameter identifies any preconditions that must be addressed before reverting, such as the following examples:

    - Disabling storage failover
    - Disabling the Snapshot policy
    - Deleting Snapshot copies that were created after upgrading to the later version of ONTAP
13. Verify that all of the preconditions have been addressed: `system node revert-to -node nodename -check-only true -version 9.x`

14. Revert the cluster configuration of the node: `system node revert-to -node nodename -version 9.x`

    The -version option refers to the target release. For example, if the software you installed and verified is ONTAP 9.1, the correct value of the -version option is 9.1.

    The cluster configuration is reverted, and then you are logged out of the clustershell.

15. Log back in to the clustershell, and then switch to the nodeshell: `run -node nodename`

    After logging on the clustershell again, it might take a few minutes before it is ready to accept the nodeshell command. So, if the command fails, wait a few minutes and try it again.

16. Revert the file system configuration of the node: `revert_to 9.x`

    This command verifies that the node's file system configuration is ready to be reverted, and then reverts it. If any preconditions are identified, you must address them and then rerun the revert_to command.

    

    Using a system console to monitor the revert process displays greater details than seen in nodeshell.

    If AUTOBOOT is true, when the command finishes, the node will reboot to ONTAP.

    If AUTOBOOT is false, when the command finishes the LOADER prompt is displayed. Enter `yes` to revert; then use `boot_ontap` to manually reboot the node.

17. After the node has rebooted, confirm that the new software is running: `system node image show`

    In the following example, image1 is the new ONTAP version and is set as the current version on node0:

```
cluster1::*> system node image show
                  Is      Is                    Install
Node     Image    Default Current Version       Date
-------- -------  ------- ------- --------      -------------------
node0
         image1   true    true    X.X.X          MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y         MM/DD/YYYY TIME
node1
         image1   true    false   X.X.X         MM/DD/YYYY TIME
         image2   false   true    Y.Y.Y         MM/DD/YYYY TIME
4 entries were displayed.
```

18. Verify that the revert status is complete for each node: `system node upgrade-revert show -node nodename`

    The status should be listed as complete.

19. Repeat [step-6] through [step-16] on the other node in the HA pair.
20. If the cluster consists of only two nodes, reenable cluster HA: `cluster ha modify -configured`

`true`

21. Reenable storage failover on both nodes if it was previously disabled: `storage failover modify -node nodename -enabled true`
22. Repeat [step-5] through [step-19] for each additional HA pair and both the clusters in MetroCluster Configuration.

What should I do after reverting my cluster?

Verify cluster and storage health after downgrade or revert

After you downgrade or revert a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum. You should also verify the status of your disks, aggregates, and volumes.

Verify cluster health

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster: `cluster show`

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
```

   If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. Set the privilege level to advanced:
   `set -privilege advanced`

   Enter `y` to continue.

3. Verify the configuration details for each RDB process.
   - The relational database epoch and database epochs should match for each node.
   - The per-ring quorum master should be the same for all nodes.

     Note that each ring might have a different quorum master.

To display this RDB process…	Enter this command…
Management application	`cluster ring show -unitname mgmt`
Volume location database	`cluster ring show -unitname vldb`
Virtual-Interface manager	`cluster ring show -unitname vifmgr`

To display this RDB process…	Enter this command…
SAN management daemon	`cluster ring show -unitname bcomd`

This example shows the volume location database process:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. Return to the admin privilege level: `set -privilege admin`
5. If you are operating in a SAN environment, verify that each node is in a SAN quorum: `event log show -severity informational -message-name scsiblade.*`

   The most recent scsiblade event message for each node should indicate that the scsi-blade is in quorum.

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time              Node       Severity       Event
---------------  ---------- -------------- ---------------------------
MM/DD/YYYY TIME  node0      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

Related information

System administration

Verify storage health

After you revert or downgrade a cluster, you should verify the status of your disks, aggregates, and volumes.

1. Verify disk status:

To check for…	Do this…
Broken disks	a. Display any broken disks: `storage disk show -state broken` b. Remove or replace any broken disks.

To check for…	Do this…
Disks undergoing maintenance or reconstruction	a. Display any disks in maintenance, pending, or reconstructing states: `storage disk show -state maintenance|pending|reconstructing` b. Wait for the maintenance or reconstruction operation to finish before proceeding.

2. Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates: `storage aggregate show -state !online`

   This command displays the aggregates that are *not* online. All aggregates must be online before and after performing a major upgrade or reversion.

   ```
   cluster1::> storage aggregate show -state !online
   There are no entries matching your query.
   ```

3. Verify that all volumes are online by displaying any volumes that are *not* online: `volume show -state !online`

   All volumes must be online before and after performing a major upgrade or reversion.

   ```
   cluster1::> volume show -state !online
   There are no entries matching your query.
   ```

4. Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

   See the Knowledge Base article Volume Showing WAFL Inconsistent on how to address the inconsistent volumes.

Related information

Disk and aggregate management

Enable automatic switchover for MetroCluster configurations

This topic provides information regarding the additional tasks that you must perform after the reversion of MetroCluster configurations.

1. Enable automatic unplanned switchover: `metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster`
2. Validate the MetroCluster configuration: `metrocluster check run`

Enable and revert LIFs to home ports after a revert

During a reboot, some LIFs might have been migrated to their assigned failover ports.

After you revert a cluster, you must enable and revert any LIFs that are not on their home ports.

The network interface revert command reverts a LIF that is not currently on its home port back to its home port, provided that the home port is operational. A LIF's home port is specified when the LIF is created; you can determine the home port for a LIF by using the network interface show command.

1. Display the status of all LIFs: `network interface show`

   This example displays the status of all LIFs for a storage virtual machine (SVM).

```
cluster1::> network interface show -vserver vs0
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001    down/down  192.0.2.120/24     node0         e0e
true
            data002    down/down  192.0.2.121/24     node0         e0f
true
            data003    down/down  192.0.2.122/24     node0         e2a
true
            data004    down/down  192.0.2.123/24     node0         e2b
true
            data005    down/down  192.0.2.124/24     node0         e0e
false
            data006    down/down  192.0.2.125/24     node0         e0f
false
            data007    down/down  192.0.2.126/24     node0         e2a
false
            data008    down/down  192.0.2.127/24     node0         e2b
false
8 entries were displayed.
```

   If any LIFs appear with a Status Admin status of down or with an Is home status of false, continue with the next step.

2. Enable the data LIFs: `network interface modify {-role data} -status-admin up`

```
cluster1::> network interface modify {-role data} -status-admin up
8 entries were modified.
```

3. Revert LIFs to their home ports: `network interface revert *`

This command reverts all LIFs back to their home ports.

```
cluster1::> network interface revert *
8 entries were acted on.
```

4. Verify that all LIFs are in their home ports: `network interface show`

   This example shows that all LIFs for SVM vs0 are on their home ports.

```
cluster1::> network interface show -vserver vs0
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node0         e0e
true
            data002      up/up    192.0.2.121/24     node0         e0f
true
            data003      up/up    192.0.2.122/24     node0         e2a
true
            data004      up/up    192.0.2.123/24     node0         e2b
true
            data005      up/up    192.0.2.124/24     node1         e0e
true
            data006      up/up    192.0.2.125/24     node1         e0f
true
            data007      up/up    192.0.2.126/24     node1         e2a
true
            data008      up/up    192.0.2.127/24     node1         e2b
true
8 entries were displayed.
```

Enable Snapshot copy policies after reverting

After reverting to an earlier version of ONTAP, you must enable Snapshot copy policies to start creating Snapshot copies again.

You are reenabling the Snapshot schedules that you disabled before you reverted to an earlier version of ONTAP.

1. Enable Snapshot copy policies for all data SVMs:

```
volume snapshot policy modify -vserver * -enabled true

snapshot policy modify pg-rpo-hourly -enable true
```

2. For each node, enable the Snapshot copy policy of the root volume by using the run-nodenodenamevol optionsroot_vol_namenosnap off command.

```
cluster1::> run -node node1 vol options vol0 nosnap off
```

Verify client access (SMB and NFS)

For the configured protocols, test access from SMB and NFS clients to verify that the cluster is accessible.

Verify IPv6 firewall entries

A reversion from any version of ONTAP 9 might result in missing default IPv6 firewall entries for some services in firewall policies. You need to verify that the required firewall entries have been restored to your system.

1. Verify that all firewall policies are correct by comparing them to the default policies: `system services firewall policy show`

   The following example shows the default policies:

```
cluster1::*> system services firewall policy show
Policy           Service    Action IP-List
---------------- ---------- ------ --------------------
cluster
                 dns        allow  0.0.0.0/0
                 http       allow  0.0.0.0/0
                 https      allow  0.0.0.0/0
                 ndmp       allow  0.0.0.0/0
                 ntp        allow  0.0.0.0/0
                 rsh        allow  0.0.0.0/0
                 snmp       allow  0.0.0.0/0
                 ssh        allow  0.0.0.0/0
                 telnet     allow  0.0.0.0/0
data
                 dns        allow  0.0.0.0/0, ::/0
                 http       deny   0.0.0.0/0, ::/0
                 https      deny   0.0.0.0/0, ::/0
                 ndmp       allow  0.0.0.0/0, ::/0
                 ntp        deny   0.0.0.0/0, ::/0
                 rsh        deny   0.0.0.0/0, ::/0
.
.
.
```

2. Manually add any missing default IPv6 firewall entries by creating a new firewall policy: `system services firewall policy create`

```
cluster1::*> system services firewall policy create -policy newIPv6
-service ssh -action allow -ip-list ::/0
```

3. Apply the new policy to the LIF to allow access to a network service: `network interface modify`

```
cluster1::*> network interface modify -vserver VS1 -lif LIF1
-firewall-policy newIPv6
```

Revert password hash function to the supported encryption type

If you reverted from ONTAP 9.1 or ONTAP 9.0 to ONTAP 8.3.x, SHA-2 account users can no longer be authenticated with their passwords. Passwords must be reset to use the MDS encryption type.

1. Set a temporary password for each SHA-2 user account that you identified prior to reverting: `security login password -username user_name -vserver vserver_name`

2. Communicate the temporary password to the affected users and have them log in through a console or SSH session to change their passwords as prompted by the system.

Considerations for whether to manually update the SP firmware

If the SP automatic update functionality is enabled (the default), downgrading or reverting to ONTAP 8.3.x does not require a manual SP firmware update. The SP firmware is automatically updated to the newest compatible version that is supported by the ONTAP version you reverted or downgraded to.

If the SP automatic update functionality is disabled (not recommended), after the ONTAP revert or downgrade process is complete, you must manually update the SP firmware to a version that is supported for the ONTAP version you reverted or downgraded to.

NetApp BIOS/ONTAP Support Matrix

NetApp Downloads: System Firmware and Diagnostics

Change in user accounts that can access the Service Processor

If you created user accounts on ONTAP 9.8 or earlier, upgraded to ONTAP 9.9.1 or later (when the `-role` parameter is changed to `admin`), and then reverted back to ONTAP 9.8 or earlier, the `-role` parameter is restored to its original value. You should nonetheless verify that the modified values are acceptable.

During revert, if the role for an SP user has been deleted, the "rbac.spuser.role.notfound" EMS message will be logged.

For more information, see Accounts that can access the SP.

Copyright information

Trademark information