



# **Back up and restore cluster configurations (cluster administrators only)**

**ONTAP 9**

NetApp  
July 22, 2022

# Table of Contents

- Back up and restore cluster configurations (cluster administrators only) . . . . . 1
  - What configuration backup files are . . . . . 1
  - Manage configuration backups . . . . . 1
  - Recovering a node configuration . . . . . 3
  - Recover a cluster configuration . . . . . 5
  - Synchronize a node with the cluster . . . . . 8

# Back up and restore cluster configurations (cluster administrators only)

## What configuration backup files are

Configuration backup files are archive files (.7z) that contain information for all configurable options that are necessary for the cluster, and the nodes within it, to operate properly.

These files store the local configuration of each node, plus the cluster-wide replicated configuration. You use configuration backup files to back up and restore the configuration of your cluster.

There are two types of configuration backup files:

- **Node configuration backup file**

Each healthy node in the cluster includes a node configuration backup file, which contains all of the configuration information and metadata necessary for the node to operate healthy in the cluster.

- **Cluster configuration backup file**

These files include an archive of all of the node configuration backup files in the cluster, plus the replicated cluster configuration information (the replicated database, or RDB file). Cluster configuration backup files enable you to restore the configuration of the entire cluster, or of any node in the cluster. The cluster configuration backup schedules create these files automatically and store them on several nodes in the cluster.



Configuration backup files contain configuration information only. They do not include any user data. For information about restoring user data, see [Data Protection](#).

## Manage configuration backups

### How the node and cluster configurations are backed up automatically

Three separate schedules automatically create cluster and node configuration backup files and replicate them among the nodes in the cluster.

The configuration backup files are automatically created according to the following schedules:

- Every 8 hours
- Daily
- Weekly

At each of these times, a node configuration backup file is created on each healthy node in the cluster. All of these node configuration backup files are then collected in a single cluster configuration backup file along with the replicated cluster configuration and saved on one or more nodes in the cluster.

For single-node clusters (including Data ONTAP Edge systems), you can specify the configuration backup destination during software setup. After setup, those settings can be modified using ONTAP commands.

## Commands for managing configuration backup schedules

You can use the `system configuration backup settings` commands to manage configuration backup schedules.

These commands are available at the advanced privilege level.

| If you want to...   | Use this command...   |
|---|---|
| <p>Change the settings for a configuration backup schedule:</p> <ul style="list-style-type: none"><li>• Specify a remote URL (HTTP, HTTPS, FTP, FTPS, or TFTP ) where the configuration backup files will be uploaded in addition to the default locations in the cluster</li><li>• Specify a user name to be used to log in to the remote URL</li><li>• Set the number of backups to keep for each configuration backup schedule</li></ul> | <p><code>system configuration backup settings modify</code></p> <p>When you use HTTPS in the remote URL, use the <code>-validate-certification</code> option to enable or disable digital certificate validation. Certificate validation is disabled by default.</p> <div><p>The web server to which you are uploading the configuration backup file must have PUT operations enabled for HTTP and POST operations enabled for HTTPS. For more information, see your web server's documentation.</p></div> |
| <p>Set the password to be used to log in to the remote URL</p>  | <p><code>system configuration backup settings set-password</code></p>   |
| <p>View the settings for the configuration backup schedule</p>  | <p><code>system configuration backup settings show</code></p> <div><p>You set the <code>-instance</code> parameter to view the user name and the number of backups to keep for each schedule.</p></div>  |

## Commands for managing configuration backup files

You use the `system configuration backup` commands to manage cluster and node configuration backup files.

These commands are available at the advanced privilege level.

| If you want to...  | Use this command...                                    |
|--|--|
| <p>Create a new node or cluster configuration backup file</p>                      | <p><code>system configuration backup create</code></p> |
| <p>Copy a configuration backup file from a node to another node in the cluster</p> | <p><code>system configuration backup copy</code></p>   |

| If you want to...  | Use this command...   |
|--|---|
| Upload a configuration backup file from a node in the cluster to a remote URL (FTP, HTTP, HTTPS, TFTP, or FTPS)                      | <p><code>system configuration backup upload</code></p> <p>When you use HTTPS in the remote URL, use the <code>-validate-certification</code> option to enable or disable digital certificate validation. Certificate validation is disabled by default.</p> <div>  <p>The web server to which you are uploading the configuration backup file must have PUT operations enabled for HTTP and POST operations enabled for HTTPS. Some web servers might require the installation of an additional module. For more information, see your web server's documentation. Supported URL formats vary by ONTAP release. See the command line help for your ONTAP version.</p> </div> |
| Download a configuration backup file from a remote URL to a node in the cluster, and, if specified, validate the digital certificate | <p><code>system configuration backup download</code></p> <p>When you use HTTPS in the remote URL, use the <code>-validate-certification</code> option to enable or disable digital certificate validation. Certificate validation is disabled by default.</p>   |
| Rename a configuration backup file on a node in the cluster  | <p><code>system configuration backup rename</code></p>  |
| View the node and cluster configuration backup files for one or more nodes in the cluster  | <p><code>system configuration backup show</code></p>  |
| Delete a configuration backup file on a node   | <p><code>system configuration backup delete</code></p> <div>  <p>This command deletes the configuration backup file on the specified node only. If the configuration backup file also exists on other nodes in the cluster, it remains on those nodes.</p> </div>  |

## Recovering a node configuration

### Find a configuration backup file to use for recovering a node

You use a configuration backup file located at a remote URL or on a node in the cluster to recover a node configuration.

### About this task

You can use either a cluster or node configuration backup file to restore a node configuration.

### Step

1. Make the configuration backup file available to the node for which you need to restore the configuration.

| If the configuration backup file is located... | Then...   |
|--|---|
| At a remote URL                                | Use the <code>system configuration backup download</code> command at the advanced privilege level to download it to the recovering node.  |
| On a node in the cluster                       | <ol style="list-style-type: none"><li>a. Use the <code>system configuration backup show</code> command at the advanced privilege level to view the list of configuration backup files available in the cluster that contains the recovering node's configuration.</li><li>b. If the configuration backup file you identify does not exist on the recovering node, then use the <code>system configuration backup copy</code> command to copy it to the recovering node.</li></ol> |

If you previously re-created the cluster, you should choose a configuration backup file that was created after the cluster recreation. If you must use a configuration backup file that was created prior to the cluster recreation, then after recovering the node, you must re-create the cluster again.

## Restore the node configuration using a configuration backup file

You restore the node configuration using the configuration backup file that you identified and made available to the recovering node.

### About this task

You should only perform this task to recover from a disaster that resulted in the loss of the node's local configuration files.

### Steps

1. Change to the advanced privilege level:  
`set -privilege advanced`
2. If the node is healthy, then at the advanced privilege level of a different node, use the `cluster modify` command with the `-node` and `-eligibility` parameters to mark it ineligible and isolate it from the cluster.  
If the node is not healthy, then you should skip this step.  
This example modifies node2 to be ineligible to participate in the cluster so that its configuration can be restored:

```
cluster1::*> cluster modify -node node2 -eligibility false
```

1. Use the `system configuration recovery node restore` command at the advanced privilege level

to restore the node's configuration from a configuration backup file.

If the node lost its identity, including its name, then you should use the `-nodename-in-backup` parameter to specify the node name in the configuration backup file.

This example restores the node's configuration using one of the configuration backup files stored on the node:

```
cluster1::*> system configuration recovery node restore -backup
cluster1.8hour.2011-02-22.18_15_00.7z
```

```
Warning: This command overwrites local configuration files with
         files contained in the specified backup file. Use this
         command only to recover from a disaster that resulted
         in the loss of the local configuration files.
         The node will reboot after restoring the local configuration.
Do you want to continue? {y|n}: y
```

The configuration is restored, and the node reboots.

1. If you marked the node ineligible, then use the `system configuration recovery cluster sync` command to mark the node as eligible and synchronize it with the cluster.
2. If you are operating in a SAN environment, use the `system node reboot` command to reboot the node and reestablish SAN quorum.

### After you finish

If you previously re-created the cluster, and if you are restoring the node configuration by using a configuration backup file that was created prior to that cluster re-creation, then you must re-create the cluster again.

## Recover a cluster configuration

### Find a configuration to use for recovering a cluster

You use the configuration from either a node in the cluster or a cluster configuration backup file to recover a cluster.

#### Steps

1. Choose a type of configuration to recover the cluster.
  - A node in the cluster

If the cluster consists of more than one node, and one of the nodes has a cluster configuration from when the cluster was in the desired configuration, then you can recover the cluster using the configuration stored on that node.

In most cases, the node containing the replication ring with the most recent transaction ID is the best node to use for restoring the cluster configuration. The `cluster ring show` command at the advanced privilege level enables you to view a list of the replicated rings available on each node in the cluster.

- A cluster configuration backup file

If you cannot identify a node with the correct cluster configuration, or if the cluster consists of a single node, then you can use a cluster configuration backup file to recover the cluster.

Recovering a cluster from a configuration backup file might require the use of diagnostic tools to resolve discrepancies between the backup and the cluster configuration present on the recovering node. Therefore, if you use a configuration backup file, you should plan to contact technical support.

2. If you chose to use a cluster configuration backup file, then make the file available to the node you plan to use to recover the cluster.

| If the configuration backup file is located... | Then...   |
|--|---|
| At a remote URL                                | Use the <code>system configuration backup download</code> command at the advanced privilege level to download it to the recovering node.  |
| On a node in the cluster                       | <ol style="list-style-type: none"><li>a. Use the <code>system configuration backup show</code> command at the advanced privilege level to find a cluster configuration backup file that was created when the cluster was in the desired configuration.</li><li>b. If the cluster configuration backup file is not located on the node you plan to use to recover the cluster, then use the <code>system configuration backup copy</code> command to copy it to the recovering node.</li></ol> |

## Restore a cluster configuration from an existing configuration

To restore a cluster configuration from an existing configuration after a cluster failure, you re-create the cluster using the cluster configuration that you chose and made available to the recovering node, and then rejoin each additional node to the new cluster.

### About this task

You should only perform this task to recover from a disaster that resulted in the loss of the cluster's configuration.



If you are re-creating the cluster from a configuration backup file, you must contact technical support to resolve any discrepancies between the configuration backup file and the configuration present in the cluster.

### Steps

1. Disable storage failover for each HA pair:

```
storage failover modify -node node_name -enabled false
```

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

2. Halt each node except for the recovering node:



```
system node halt -node node_name -reason "text"
```

```
cluster1::*> system node halt -node node0 -reason "recovering cluster"

Warning: Are you sure you want to halt the node? {y|n}: y
```

3. Set the privilege level to advanced:

```
set -privilege advanced
```

4. On the recovering node, use the **system configuration recovery cluster recreate** command to re-create the cluster.

This example re-creates the cluster using the configuration information stored on the recovering node:

```
cluster1::*> configuration recovery cluster recreate -from node

Warning: This command will destroy your existing cluster. It will
        rebuild a new single-node cluster consisting of this node
        and its current configuration. This feature should only be
        used to recover from a disaster. Do not perform any other
        recovery operations while this operation is in progress.
Do you want to continue? {y|n}: y
```

A new cluster is created on the recovering node.

5. If you are re-creating the cluster from a configuration backup file, verify that the cluster recovery is still in progress:

```
system configuration recovery cluster show
```

You do not need to verify the cluster recovery state if you are re-creating the cluster from a healthy node.

```
cluster1::*> system configuration recovery cluster show
Recovery Status: in-progress
Is Recovery Status Persisted: false
```

6. Boot each node that needs to be rejoined to the re-created cluster.

You must reboot the nodes one at a time.

7. For each node that needs to be joined to the re-created cluster, do the following:

- a. From a healthy node on the re-created cluster, rejoin the target node:

```
system configuration recovery cluster rejoin -node node_name
```

This example rejoins the “node2” target node to the re-created cluster:

```
cluster1::*> system configuration recovery cluster rejoin -node node2

Warning: This command will rejoin node "node2" into the local
cluster, potentially overwriting critical cluster
configuration files. This command should only be used
to recover from a disaster. Do not perform any other
recovery operations while this operation is in progress.
This command will cause node "node2" to reboot.
Do you want to continue? {y|n}: y
```

The target node reboots and then joins the cluster.

- b. Verify that the target node is healthy and has formed quorum with the rest of the nodes in the cluster:

```
cluster show -eligibility true
```

The target node must rejoin the re-created cluster before you can rejoin another node.

```
cluster1::*> cluster show -eligibility true
Node           Health  Eligibility  Epsilon
-----
node0           true    true         false
node1           true    true         false
2 entries were displayed.
```

8. If you re-created the cluster from a configuration backup file, set the recovery status to be complete:

```
system configuration recovery cluster modify -recovery-status complete
```

9. Return to the admin privilege level:

```
set -privilege admin
```

10. If the cluster consists of only two nodes, use the **cluster ha modify** command to reenoble cluster HA.

11. Use the **storage failover modify** command to reenoble storage failover for each HA pair.

#### After you finish

If the cluster has SnapMirror peer relationships, then you also need to re-create those relationships. For more information, see [Data Protection](#).

## Synchronize a node with the cluster

If cluster-wide quorum exists, but one or more nodes are out of sync with the cluster, then you must synchronize the node to restore the replicated database (RDB) on the node and bring it into quorum.

## Step

1. From a healthy node, use the `system configuration recovery cluster sync` command at the advanced privilege level to synchronize the node that is out of sync with the cluster configuration.

This example synchronizes a node (*node2*) with the rest of the cluster:

```
cluster1::*> system configuration recovery cluster sync -node node2
```

Warning: This command will synchronize node "node2" with the cluster configuration, potentially overwriting critical cluster configuration files on the node. This feature should only be used to recover from a disaster. Do not perform any other recovery operations while this operation is in progress. This command will cause all the cluster applications on node "node2" to restart, interrupting administrative CLI and Web interface on that node.

Do you want to continue? {y|n}: y

All cluster applications on node "node2" will be restarted. Verify that the cluster applications go online.

## Result

The RDB is replicated to the node, and the node becomes eligible to participate in the cluster.

## Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

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

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

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

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

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

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.