# Commit files to WORM

ONTAP 9

NetApp
November 22, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/snaplock/commit-files-worm-state-manual-task.html on November 22, 2022. Always check docs.netapp.com for the latest.

# Table of Contents

Commit files to WORM . . . 1
Commit files to WORM manually . . . 1
Autocommit files to WORM . . . 1
Use a command or program to create a WORM appendable file . . . 2
Use volume append mode to create WORM appendable files . . . 3

# Commit files to WORM

## Commit files to WORM manually

You commit a file to WORM manually by making the file read-only. You can use any suitable command or program over NFS or CIFS to change the read-write attribute of a file to read-only.

**What you'll need**

- The file you want to commit must reside on a SnapLock volume.
- The file must be writable.

**About this task**

The volume ComplianceClock time is written to the `ctime` field of the file when the command or program is executed. The ComplianceClock time determines when the retention time for the file has been reached.

**Steps**

1. Use a suitable command or program to change the read-write attribute of a file to read-only.

   In a UNIX shell, use the following command to make a file named `document.txt` read-only:

   ```
   chmod -w document.txt
   ```

   In a Windows shell, use the following command to make a file named `document.txt` read-only:

   ```
   attrib +r document.txt
   ```

## Autocommit files to WORM

The SnapLock autocommit feature enables you to commit files to WORM automatically.

**What you'll need**

- The files you want to autocommit must reside on a SnapLock volume.
- The SnapLock volume must be online.
- The SnapLock volume must be a read-write volume.

> The SnapLock autocommit feature scans through all of the files in the volume and commits a file if it meets the autocommit requirement. There might be a time interval between when the file is ready for autocommit and when it is actually committed by the SnapLock autocommit scanner. However, the file is still protected from modifications and deletion by the file system as soon as it is eligible for autocommit.

**About this task**

The *autocommit period* specifies the amount of time that files must remain unchanged before they are

autocommitted. Changing a file before the autocommit period has elapsed restarts the autocommit period for the file.

The following table shows the possible values for the autocommit period:

| Value | Unit | Notes |
|---|---|---|
| none | - | The default. |
| 5 - 5256000 | minutes | - |
| 1 - 87600 | hours | - |
| 1 - 3650 | days | - |
| 1 - 120 | months | - |
| 1 - 10 | years | - |

The minimum value is 5 minutes and the maximum value is 10 years.

**Steps**

1. Autocommit files on a SnapLock volume to WORM:

   **`volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-autocommit -period` *`autocommit_period`***

   For a complete list of options, see the man page for the command.

   The following command autocommits the files on volume `vol1` of SVM vs1, as long as the files remain unchanged for 5 hours:

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
   -period 5hours
   ```

# Use a command or program to create a WORM appendable file

You can use any suitable command or program over NFS or CIFS to create a WORM appendable file. A WORM appendable file retains data written incrementally, like log entries. Data is appended to the file in 256 KB chunks. As each chunk is written, the previous chunk becomes WORM-protected. You cannot delete the file until the retention period has elapsed.

**What you'll need**

The WORM appendable file must reside on a SnapLock volume.

**About this task**

Data does not have to be written sequentially to the active 256 KB chunk. When data is written to byte n×256KB+1 of the file, the previous 256 KB segment becomes WORM-protected.

**Steps**

1. Use a suitable command or program to create a zero-length file with the desired retention time.

   In a UNIX shell, use the following command to set a retention time of 21 November 2020 6:00 a.m. on a zero-length file named `document.txt`:

   ```
   touch -a -t 202011210600 document.txt
   ```

2. Use a suitable command or program to change the read-write attribute of the file to read-only.

   In a UNIX shell, use the following command to make a file named `document.txt` read-only:

   ```
   chmod 444 document.txt
   ```

3. Use a suitable command or program to change the read-write attribute of the file back to writable.

   This step is not deemed a compliance risk because there is no data in the file.

   In a UNIX shell, use the following command to make a file named `document.txt` writable:

   ```
   chmod 777 document.txt
   ```

4. Use a suitable command or program to start writing data to the file.

   In a UNIX shell, use the following command to write data to `document.txt`:

   ```
   echo test data >> document.txt
   ```

   Change the file permissions back to read-only when you no longer need to append data to the file.

# Use volume append mode to create WORM appendable files

Beginning with ONTAP 9.3, you can use the SnapLock *volume append mode* (VAM) feature to create WORM appendable files by default. A WORM appendable file retains data written incrementally, like log entries. Data is appended to the file in 256 KB chunks. As each chunk is written, the previous chunk becomes WORM-protected. You cannot delete the file until the retention period has elapsed.

**What you'll need**

- The WORM appendable file must reside on a SnapLock volume.
- The SnapLock volume must be unmounted and empty of Snapshot copies and user-created files.

**About this task**

Data does not have to be written sequentially to the active 256 KB chunk. When data is written to byte n×256KB+1 of the file, the previous 256 KB segment becomes WORM-protected.

If you specify an autocommit period for the volume, WORM appendable files that are not modified for a period greater than the autocommit period are committed to WORM.

VAM is not supported on SnapLock audit log volumes.

**Steps**

1. Enable VAM:

   **`volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-is-volume-append -mode-enabled true|false`**

   For a complete list of options, see the man page for the command.

   The following command enables VAM on volume `vol1` of SVM`vs1`:

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
   -append-mode-enabled true
   ```

2. Use a suitable command or program to create files with write permissions.

   The files are WORM-appendable by default.

## 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## 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.