



Audit S3 events

ONTAP 9

NetApp
November 04, 2021

Table of Contents

Audit S3 events	1
Audit S3 events	1

Audit S3 events

Audit S3 events

Beginning with ONTAP 9.10.1, you can audit data and management events in ONTAP S3 environments. S3 audit functionality is similar to existing NAS auditing capabilities, and S3 and NAS auditing can coexist in a cluster.

When you create and enable an S3 auditing configuration on an SVM, S3 events are recorded in a log file. The you can specify the following events to be logged:

- Object access (data) events
GetObject, PutObject, and DeleteObject
- Management events
PutBucket and DeleteBucket

The combined limit for S3 and NFS auditing configurations is 50 SVMs per cluster.

The following license bundle is required: * Core Bundle, for ONTAP S3 protocol and storage

For more information, see [How the ONTAP auditing process works](#).

Guaranteed auditing

By default, S3 and NAS auditing is guaranteed. ONTAP guarantees that all auditable bucket access events are recorded, even if a node is unavailable. A requested bucket operation cannot be completed until the audit record for that operation is saved to the staging volume on persistent storage. If audit records cannot be committed in the staging files, either because of insufficient space or because of other issues, client operations are denied.

Space requirements for auditing

In the ONTAP auditing system, audit records are initially stored in binary staging files on individual nodes. Periodically, they are consolidated and converted to user-readable event logs, which are stored in the audit event log directory for the SVM.

The staging files are stored in a dedicated staging volume, which is created by ONTAP when the auditing configuration is created. There is one staging volume per aggregate.

You must plan for sufficient available space in the auditing configuration:

- For the staging volumes in aggregates that contain audited buckets.
- For the volume containing the directory where converted event logs are stored.

You can control the number of event logs, and hence the available space in the volume, using one of two methods when creating the S3 auditing configuration:

- A numerical limit; the `-rotate-limit` parameter controls the minimum number of audit files that must be preserved.

- A time limit; the `-retention-duration` parameter controls the maximum period that files can be preserved.

In both parameters, once that configured is exceeded, older audit files can be deleted to make room for newer ones. For both parameters, the value is 0, indicating that all files must be maintained. In order to ensure sufficient space, it is therefore a best practice to set one of the parameters to a non-zero value.

Because of guaranteed auditing, if the space available for audit data runs out before the rotation limit, newer audit data cannot be created, resulting in failure to clients accessing data. Therefore, the choice of this value and of the space allocated to auditing must be chosen carefully, and you must respond to warnings about available space from the auditing system.

For more information, see [Basic auditing concepts](#).

Copyright Information

Copyright © 2021 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.