arw events

ONTAP 9.11.1 EMS reference

NetApp
August 29, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap-ems-9111/arw-analytics-events.html on August 29, 2024. Always check docs.netapp.com for the latest.

Table of Contents

arw events 1
arw.analytics events 1
arw.volume events 3
arw.vserver events 3

arw events

arw.analytics events

arw.analytics.ext.report

Severity

NOTICE

Description

This message occurs when anti-ransomware analytics generates or updates the "suspicious file extensions" report for a volume.

Corrective Action

(None).

Syslog Message

Anti-ransomware file extension analytics has found %s across high entropy data on the volume "%s" in Vserver "%s". Report location: %s.

Parameters

fileExtension (STRING): Previously unseen file extension or suspicious file extension
volumeName (STRING): Name of the volume.
vserverName (STRING): Name of the Vserver.
fileExtensionReport (STRING): Link to report run after file extension analysis.

arw.analytics.high.entropy

Severity

ERROR

Description

This message occurs when the number of high entropy data log messages (pertaining to ransomware detection and analysis) that were generated for a volume cross the predefined threshold.

Corrective Action

To correct this issue: 1) Restore data from the last Snapshot copy that were saved before high entropy data was detected. 2) Refer to the anti-ransomware documentation to learn how to implement ransomware protection and mitigation strategies.

Syslog Message

A large amount of high entropy data was found on volume "%s" in Vserver "%s".

Parameters

volumeName (STRING): Name of the volume.
vserverName (STRING): Name of the Vserver.

arw.analytics.probability

Severity

ERROR

Description

This message occurs when an anti-ransomware attack probability has changed from "low" to "high" on a volume.

Corrective Action

To correct this issue: 1) Restore to the last safe Snapshot copy before attack probabilty became high. 2) Refer to the anti-ransomware documentation to diagnose further and take remedial measures.

Syslog Message

Anti-ransomware attack probability changed from low to high on volume "%s" in Vserver "%s".

Parameters

volumeName (STRING): Name of the volume.
vserverName (STRING): Name of the Vserver.

arw.analytics.report

Severity

NOTICE

Description

This message occurs when an anti-ransomware analytics report is generated or updated for a volume.

Corrective Action

(None).

Syslog Message

Anti-ransomware analytics report has been generated for volume %s of Vserver %s. The report is available at %s.

Parameters

volumeName (STRING): Name of the volume.
vserverName (STRING): Name of the Vserver.
report_path (STRING): Path to anti-ransomware report.

arw.analytics.suspects

Severity

ERROR

Description

This message occurs when a list of suspects generated by anti-ransomware analytics grows to a point where further investigation is needed.

Corrective Action

(None).

Syslog Message

Anti-ransomware analytics on volume "%s" in Vserver "%s" has outstanding suspect files.

Parameters

volumeName (STRING): Name of the volume.
vserverName (STRING): Name of the Vserver.

arw.volume events

arw.volume.state

Severity

NOTICE

Description

This message occurs when the anti-ransomware state of a volume is changed.

Corrective Action

(None).

Syslog Message

Anti-ransomware state was changed to "%s" on volume "%s" (UUID: "%s") in Vserver "%s" (UUID: "%s").

Parameters

op (STRING): Monitoring state (enabled, disabled, dry-run).
volumeName (STRING): Name of the volume.
volumeUuid (STRING): UUID of the volume.
vserverName (STRING): Name of the Vserver.
vserverUuid (STRING): UUID of the Vserver.

arw.vserver events

arw.vserver.state

Severity

NOTICE

Description

This message occurs when the anti-ransomware state of a Vserver is changed.

Corrective Action

(None).

Syslog Message

Anti-ransomware was changed to "%s" on Vserver "%s" (UUID: "%s").

Parameters

op (STRING): Anti-ransomware state (enabled, disabled,or dry-run).
vserverName (STRING): Name of the Vserver.
vserverUuid (STRING): UUID of the Vserver.

Copyright information

Copyright © 2024 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.