



ekmip events

ONTAP 9.11.1 EMS reference

NetApp
December 15, 2022

Table of Contents

- ekmip events 1
- ekmip.akv events 1
- ekmip.gckms events 3

ekmip events

ekmip.akv events

ekmip.akv.available

Severity

NOTICE

Description

This message occurs when a configured Azure Key Vault (AKV) that was previously reported unavailable for key operations is now available.

Corrective Action

(None).

Syslog Message

The Azure Key Vault "%s" configured for Vserver "%s" is now available.

Parameters

name (STRING): URI of the AKV.

vserver (STRING): Name of the Vserver where the AKV is configured.

ekmip.akv.keyExpired

Severity

ERROR

Description

This message occurs when the current key version associated with the key identifier of the configured Azure Key Vault (AKV) has expired. The key version might be out of compliance. It is recommended that you update the key version to an active, non-expired key. ONTAP will still be able to unwrap the top-level internal key protection key with the expired key version and there will be no interruption to data availability.

Corrective Action

Update the key-id to an active, non-expired key at the AKV portal.

Syslog Message

The key-id "%s", owned by the Azure Key Vault "%s" and configured for Vserver "%s", has expired.

Parameters

name (STRING): URI of the AKV.

vserver (STRING): Name of the Vserver where the AKV is configured.

keyId (STRING): Key ID.

ekmip.akv.keyVersionChanged

Severity

NOTICE

Description

This message occurs when the current key version associated with the key identifier of the configured Azure Key Vault (AKV), the AKV key-id, changes. The key version might have been auto-rotated or manually changed at the AKV. Additionally, the top-level internal key protection key has been successfully re-wrapped with the current key version of the AKV key-id.

Corrective Action

(None).

Syslog Message

The key version of the key-id owned by the Azure Key Vault "%s" configured for Vserver "%s" has been changed from "%s" to "%s".

Parameters

name (STRING): URI of the AKV.

vserver (STRING): Name of the Vserver where the AKV is configured.

oldKeyVersion (STRING): Previous key version.

newKeyVersion (STRING): Current key version.

ekmip.akv.notAvailable

Severity

ALERT

Description

This message occurs when a check for the availability of the configured Azure Key Vault (AKV) for key operations fails. The AKV might be down or there might be a network-related problem preventing communication. Without access to the AKV, the node might not be able to restore authentication keys needed to unlock NSE or SED drives or encryption keys needed to mount encrypted volumes. If the AKV is not available, the next time this node boots, then the failure to restore the keys might prevent the node from booting successfully or prevent the encrypted volumes hosted on this node from coming online.

Corrective Action

Ensure that the AKV configuration is correct by using the "security key-manager external azure show -vserver <vserver>" command and verifying that the cluster state is available. If it is not available, run the "security key-manager external azure restore" command to bring the cluster state to available. If the issue still persists, contact technical support.

Syslog Message

The Azure Key Vault "%s" configured for Vserver "%s" is not available.

Parameters

name (STRING): URI of the AKV.

vserver (STRING): Name of the Vserver where the AKV is configured.

ekmip.akv.volOffline

Severity

ALERT

Description

This message occurs when all the encrypted volumes belonging to the Vserver have been taken offline due to errors received when attempting to access the key owned by the Azure Key Vault (AKV). Reasons for AKV key access errors include a disabled key, a key not being found and a key missing encryption and decryption privileges. ONTAP polls the AKV every 15 minutes to verify key accessibility. If, for 60 minutes, ONTAP does not receive a successful response to a poll, all encrypted volumes are taken offline and remain offline until the key access issues are resolved at the AKV. When ONTAP does receive a successful response, the volumes are brought back online automatically.

Corrective Action

Resolve the key access issues at the AKV portal. Ensure that the key is active and has the required encryption and decryption privileges.

Syslog Message

Encrypted volumes belonging to Vserver "%s" have been taken offline due to key access errors associated with the key-id "%s" owned by Azure Key Vault "%s".

Parameters

name (STRING): URI of the AKV.

vserver (STRING): Name of the Vserver where the AKV is configured.

keyId (STRING): Key ID.

ekmip.gckms events

ekmip.gckms.available

Severity

NOTICE

Description

This message occurs when a configured Google Cloud Key Management Service (GCKMS) that was previously reported as unavailable for key operations is now available.

Corrective Action

(None).

Syslog Message

The GCKMS with project ID: %s, key ring location: %s, key ring: %s and key name: %s configured for Vserver "%s" is now available.

Parameters

projectId (STRING): Project ID.

keyringLocation (STRING): Location of the key ring.

keyringName (STRING): Name of the key ring.

keyName (STRING): Name of the key.

vserver (STRING): Name of the Vserver where the GCKMS is configured.

ekmip.gckms.keyVersionChg

Severity

NOTICE

Description

This message occurs when a change is made to the current key version associated with the key name of the configured Google Cloud KMS (GCKMS). The key version might have been auto-rotated or manually changed at the GCKMS. Additionally, the top-level internal key-protection key has been successfully re-wrapped with the current key version of the GCKMS key name.

Corrective Action

(None).

Syslog Message

The version of the key "%s" owned by Google Cloud KMS Project "%s", with key ring "%s" at "%s", configured for Vserver "%s", has been changed from "%s" to "%s".

Parameters

keyName (STRING): Name of the key.
projectId (STRING): Project ID of the GCKMS.
keyringName (STRING): Name of the key ring.
keyringLocation (STRING): Location of the key ring.
vserver (STRING): Name of the Vserver where the GCKMS is configured.
oldKeyVersion (STRING): Prior key version.
newKeyVersion (STRING): New key version.

ekmip.gckms.notAvailable

Severity

ALERT

Description

This message occurs when a check for the availability of the configured Google Cloud Key Management Service (GCKMS) fails. The GCKMS might be down or there might be a network-related problem preventing communication. Without access to the GCKMS, the node might not be able to restore authentication keys needed to unlock NSE drives or encryption keys needed to mount encrypted volumes. If the GCKMS is not available, then the next time this node boots, the failure to restore the keys might prevent the node from booting successfully or the encrypted volumes hosted on this node from coming online.

Corrective Action

Verify that the GCKMS configuration is correct by using the "security key-manager external gcp show -vserver <vserver_name>" command, and verify that the cluster state is available. If the cluster state is not available, run the "security key-manager external gcp restore" command to bring the cluster state to available. If the issue still persists, contact technical support.

Syslog Message

The GCKMS with project ID: %s, key ring location: %s, key ring: %s and key name: %s configured for Vserver "%s" is not available.

Parameters

projectId (STRING): Project ID.
keyringLocation (STRING): Location of the key ring.
keyringName (STRING): Name of the key ring.

keyName (STRING): Name of the key.

vserver (STRING): Name of the Vserver where the GCKMS is configured.

ekmip.gckms.volOffline

Severity

ALERT

Description

This message occurs when the volumes belonging to the Vserver have been taken offline due to errors received when trying to access the key owned by the Google Cloud KMS (GCKMS). Reasons for GCKMS key access errors include a disabled key, a destroyed key, key not found, or a user not having sufficient privileges to access the key. ONTAP polls the GCKMS every 15 minutes to verify key accessibility. If, after 60 minutes, ONTAP has not received a successful response to a poll, volumes are taken offline and remain offline until the key access issues are resolved at the GCKMS. Subsequently, if ONTAP does receive a successful response, the volumes will be brought back online automatically.

Corrective Action

Resolve the key access issues at the GCKMS portal. Ensure that the key is active and the user has the required privileges to access the key.

Syslog Message

Encrypted volumes belonging to Vserver "%s" have been taken offline due to key access errors associated with key "%s" owned by Google Cloud KMS Project "%s" with key ring location "%s" and key ring "%s".

Parameters

vserver (STRING): Name of the Vserver where the GCKMS is configured.

keyName (STRING): Name of the key.

projectId (STRING): ID of the GCKMS project.

keyringLocation (STRING): Location of the key ring.

keyringName (STRING): Name of the key ring.

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.