



km events

ONTAP 9.11.1 EMS reference

NetApp
December 15, 2022

Table of Contents

- km events 1
- km.cluster events 1
- km.extkeysvr events 1
- km.keyretrieve events 2
- km.keyserver events 2
- km.mcc events 3
- km.onboard events 4
- km.restore events 4
- km.run events 5

km events

km.cluster events

km.cluster.okm.hierarchy.bad

Severity

ALERT

Description

This message occurs in a MetroCluster(tm) configuration, when one or both clusters have been configured with the Onboard Key Manager, but one or both of the Onboard Key Manager key hierarchies are corrupted. Specifically, the 'hashed_pass' object does not match the 'hashed_pass_!' object in at least one cluster.

Corrective Action

Reboot each of the nodes in the MetroCluster configuration.

Syslog Message

This cluster is part of a MetroCluster configuration. The Onboard Key Manager key hierarchy on one or both of the clusters is corrupted. Specifically, the 'hashed_pass' object does not match the 'hashed_pass_!' object, part of the 'cluster_kdb' table, in either cluster.

Parameters

(None).

km.extkeysvr events

km.extkeysvr.details

Severity

NOTICE

Description

This message occurs when a key is retrieved or restored from an external KMIP server. This is an informational message that describes the external KMIP server where the key is stored.

Corrective Action

(None).

Syslog Message

Key ID "%s" restored/retrieved from external key server "%s".

Parameters

keyId (STRING): Key ID of the key being restored or retrieved.

hostPort (STRING): Host port details of the external KMIP server.

km.keyretrieve events

km.keyretrieve.failed

Severity

ALERT

Description

This message occurs when a node fails to retrieve a complete set of encryption keys from the configured key servers by the time the management process comes online. Should this node take ownership of an encrypted volume associated with a missing key before the key becomes available, the encrypted volume cannot come online.

Corrective Action

Use the "security key-manager external restore -node <node> -vserver <vserver>" command to manually restore the keys.

Syslog Message

Key auto-retrieve failed on node %s for Vserver %s (ID %u, UUID %s).

Parameters

node (STRING): Name of the node whose management process goes online.

vserver (STRING): Name of the Vserver that could not retrieve all of the keys.

vserverId (INT): Vserver ID of the Vserver.

vserverUuid (STRING): UUID of the related Vserver.

km.keyserver events

km.keyserver.available

Severity

NOTICE

Description

This message occurs when a check by the key manager for connectivity with a configured key management server indicates that the key management server that was previously unavailable is now available.

Corrective Action

(None).

Syslog Message

The external key management server "%s" is now available for Vserver "%s".

Parameters

vserver (STRING): Name of the Vserver where the key management server is configured.

address (STRING): IP address of the key management server.

km.keyserver.notavailable

Severity

ALERT

Description

This message occurs when a check by the key manager for connectivity with a configured key management server indicates that the key management server is not available. The key management server might be down, there might be a network-related problem preventing communication with the key server, or the security certificates used to authenticate with the key management server might have expired. Without access to the key management server, 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 key management server 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 key management server is online using the server's management interface. If the server is online, use the "network ping -lif <lif> -vserver <vserver> -destination <address>" command to verify that the node can communicate with the server. If this command indicates that the server is available, use the "security key-manager external show -vserver <vserver>" command to get the certificate names, and then check whether they are expired with the "security certificate show-user-installed -vserver <vserver> -cert -name <cert>" command. If so, install the updated certificates with the "security certificate install" and "security key-manager external modify" commands.

Syslog Message

The external key management server "%s" is not available for Vserver "%s", status: "%s".

Parameters

vserver (STRING): Name of the Vserver where the key management server is configured.

address (STRING): IP address of the key management server.

keyserver_status (STRING): Status of the key management server.

km.mcc events

km.mcc.okm.hierarchy.bad

Severity

ALERT

Description

This message occurs in a MetroCluster(tm) configuration, when one or both clusters have been configured with the Onboard Key Manager, but one or both of the Onboard Key Manager key hierarchies are corrupted. Specifically, the 'hashed_pass' object does not contain the same value in each Onboard Key Manager key hierarchy.

Corrective Action

Reboot each of the nodes in the MetroCluster configuration.

Syslog Message

This cluster is part of a MetroCluster configuration. The Onboard Key Manager key hierarchy on one or both of the clusters is corrupted. The replication subsystem has failed to update the 'hashed_pass' field in the 'cluster_kdb' table.

Parameters

(None).

km.mcc.okmkey.mismatch

Severity

ALERT

Description

This message occurs in a NetApp MetroCluster configuration, where both peer clusters are configured with Onboard Key Manager (OKM) and the lists of OKM hierarchy keys on the peer clusters are not consistent. A mismatch in the OKM hierarchy keys can lead to a failure during a reboot or future switchover/switchback event.

Corrective Action

Contact NetApp technical support.

Syslog Message

This cluster is part of a MetroCluster configuration. The list of OKM hierarchy keys on one or both of the clusters is potentially corrupted.

Parameters

(None).

km.onboard events

km.onboard.ccmode.wrongpass

Severity

NOTICE

Description

This message occurs when a cluster administrator supplies the wrong Onboard Key Manager cluster-wide passphrase more than three times in a row while attempting to enable Common Criteria (CC) mode.

Corrective Action

(None).

Syslog Message

The Onboard Key Manager cluster-wide passphrase has been entered incorrectly %s times by user "%s" while attempting to enable Common Criteria mode.

Parameters

username (STRING): Name of the user who issued the command to enable CC mode.

failure_count (STRING): Number of sequential times that the cluster-wide passphrase has been entered incorrectly.

km.restore events

km.restore.invalid.key

Severity

ALERT

Description

This message occurs when the key manager attempts to restore a key which has an invalid length.

Corrective Action

Run the "security key-manager restore" command to restore keys from external key servers.

Syslog Message

ONTAP has attempted to restore an %s key which has an invalid key length. Vserver: %s, Key ID: %s, Key server: %s.

Parameters

keyType (STRING): Key type (NSE, AES, XTS) that has invalid length.

vserverName (STRING): Vserver name.

keyId (STRING): Key ID of the key being restored.

keyServer (STRING): Key server from which the key is being restored.

km.run events

km.run.external.setup

Severity

ERROR

Description

This message occurs when a node successfully performs a join operation to join a cluster, but the other nodes in the cluster have the External Key Manager configured and the new node does not. The new node cannot perform External Key Manager-related tasks, such as creating encrypted volumes, until it has the External Key Manager configured.

Corrective Action

Set up the External Key Manager on the new node by using the "security key-manager setup" command.

Syslog Message

External Key Manager setup required after the cluster "%s" operation for node "%s", serial "%s".

Parameters

operation_type (STRING): Type of cluster operation.

node (STRING): Name of the node that successfully joined the cluster.

serial (STRING): System serial number of the node that successfully joined the cluster.

km.run.extrnl.enable.needed

Severity

ALERT

Description

This message occurs when a cluster in a MetroCluster(tm) configuration has configured external key management via the "security key-manager external enable -key-servers <ip_address:port> -client-cert <client_cert_name> -server-ca-certs <server_ca_cert_name>" command. This is an alert that the external key management configuration on the two clusters is not consistent, and that the "security key-manager external enable -key-servers <ip_address:port> -client-cert <client_cert_name> -server-ca-certs <server_ca_cert_name>" command should be run on the local cluster or peer cluster, specifying the same set of key servers. Otherwise, encrypted volumes and NSE drives will not come online after a future switchover or switchback event. This message will be generated on both the local cluster and the peer cluster.

Corrective Action

Run the "security key-manager external enable" command on the local cluster or the peer cluster (identified in the "cluster" parameter), specifying the same set of configured key servers, to make the external key management consistent.

Syslog Message

The external key management configuration is not consistent between the local cluster and the peer cluster of the MetroCluster configuration. This can lead to a failure during a future switchover or switchback event. Synchronize the configuration on the %s cluster.

Parameters

cluster (STRING): Local cluster or peer cluster on which to run the command.

km.run.extrnl.setup.needed

Severity

ALERT

Description

This message occurs when a cluster in a MetroCluster(tm) configuration has configured external key management via the "security key-manager setup" command. This is an alert that the external key management configuration on the two clusters is not consistent, and that the "security key-manager setup" command should be run on the local cluster or peer cluster. Otherwise, encrypted volumes and NSE drives will not come online after a future switchover or switchback event. This message will be generated on both the local cluster and the peer cluster.

Corrective Action

Run the "security key-manager setup" command on the local cluster or the peer cluster (identified in the "cluster" parameter) to make the external key management configurations consistent.

Syslog Message

The external key management configuration is not consistent between the local cluster and the peer cluster of the MetroCluster configuration. This can lead to a failure during a future switchover or switchback event. Synchronize the configuration on the %s cluster.

Parameters

cluster (STRING): Local cluster or peer cluster on which to run the command.

km.run.onboard.setup

Severity

ERROR

Description

This message occurs when a node successfully performs a join operation to join a cluster, but the other nodes in the cluster have the Onboard Key Manager configured and the new node does not. The new node cannot perform the Onboard Key Manager-related tasks, such as creating encrypted volumes, until it has the Onboard Key Manager configured.

Corrective Action

Set up the Onboard Key Manager on the new node by using the "security key-manager setup" command.

Syslog Message

The Onboard Key Manager setup required after the cluster "%s" operation for node "%s", serial "%s".

Parameters

operation_type (STRING): Type of cluster operation.

node (STRING): Name of the node that successfully joined the cluster.

serial (STRING): System serial number of the node that successfully joined the cluster.

km.run.onboard.setup.needed**Severity**

ALERT

Description

This message occurs when a cluster in a MetroCluster(tm) configuration has either configured the Onboard Key Manager via the "security key-manager setup" command or has reconfigured the cluster passphrase via the "security key-manager update-passphrase" command. This is an alert that the onboard key hierarchies on the two clusters are not consistent, and that the "security key-manager setup -sync -metrocluster-config yes" command should be run on the local cluster or peer cluster. Otherwise, a future switchover or switchback event could fail. This message will be generated on both the local cluster and the peer cluster.

Corrective Action

Run the "security key-manager setup -sync-metrocluster-config yes" command on the local cluster or the peer cluster (identified in the "cluster" parameter) to make the two onboard key hierarchies consistent.

Syslog Message

The Onboard Key Manager configuration is not consistent between the local cluster and the peer cluster of the MetroCluster configuration. This can lead to a failure during a future switchover or switchback event. Synchronize the configuration on the %s cluster.

Parameters

cluster (STRING): Local cluster or peer cluster on which to run the command.

km.run.onboard.sync.needed**Severity**

ALERT

Description

This message occurs when a cluster in a MetroCluster(tm) configuration has either configured the Onboard Key Manager via the "security key-manager onboard enable" command or has reconfigured the cluster passphrase via the "security key-manager onboard update-passphrase" command. This is an alert that the onboard key hierarchies on the two clusters are not consistent, and that the "security key-manager onboard sync" command should be run on the local cluster or peer cluster. Otherwise, a future switchover or switchback event could fail. This message will be generated on both the local cluster and the peer cluster.

Corrective Action

Run the "security key-manager onboard sync" command on the local cluster or the peer cluster (identified in the "cluster" parameter) to make the two onboard key hierarchies consistent.

Syslog Message

The Onboard Key Manager configuration is not consistent between the local cluster and the peer cluster of the MetroCluster configuration. This can lead to a failure during a future switchover or switchback event. Synchronize the configuration on the %s cluster.

Parameters

cluster (STRING): Local cluster or peer cluster on which to run the command.

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.