km events

ONTAP 9.15.1 EMS reference

NetApp
June 10, 2024

Table of Contents

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_l' 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_l' object, part of the 'cluster_kdb' table, in either cluster.

Parameters

(None).

km.cmek events

km.cmek.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 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.

km.cmek.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 Key Management Service (GCKMS). The key version might have been auto-rotated or manually changed at the GCKMS. Additionally, the top-level internal key protection key is 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 GCKMS project ID "%s", with key ring "%s" at "%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.
oldKeyVersion (STRING): Prior key version.
newKeyVersion (STRING): New key version.

km.cmek.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 system might not be able to restore encryption keys needed to mount encrypted volumes. If the GCKMS is not available, then the next time this system boots, the failure to restore the keys might prevent the system from booting successfully or the encrypted volumes hosted on this system from coming online.

Corrective Action

Verify that the GCKMS configuration is correct and verify the permissions and connectivity are correct. 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" 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.

km.cmek.init.failed

Severity

ALERT

Description

This message occurs when the system fails to initialize the key hierarchy required for volume encryption and that is protected by the Customer Managed Encryption Key (CMEK). Reasons for failure include failure to create the key hierarchy, incorrect CMEK configuration, identity, networking or permission issues in communicating with the CMEK hosted service and failure to store the CMEK wrapped key hierarchy in an external store like etcd.

Corrective Action

Ensure that the configuration, identity, networking and permissions required to communicate with the CMEK hosted service are configured correctly. If the issue persists, contact technical support.

Syslog Message

Initialization of the CMEK protected key hierarchy fails. Reason: "%s".

Parameters

reason (STRING): Reason for failure.

km.cmek.init.success

Severity

NOTICE

Description

This message occurs when the system successfully initializes and protects the key hierarchy with a Customer Managed Encryption Key (CMEK). The system is ready to support encrypted volumes.

Corrective Action

(None).

Syslog Message

CMEK protected key hierarchy initialization successfully completed.

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.mcc.svmkek.missing.local

Severity

ALERT

Description

This message occurs in a NetApp MetroCluster configuration, where both peer clusters are configured with Onboard Key Manager (OKM) and an SVM key encryption key is created on the remote peer, but due to various conditions, is not replicated to the local cluster. Creation of a new SVM key encryption key (KEK) on the local cluster is prevented to avoid failure during a reboot or future switchover/switchback event.

Corrective Action

Contact Contact NetApp technical support. for assistance.

Syslog Message

This cluster is part of a MetroCluster configuration. An SVM key encryption key created on the remote cluster has not been replicated to the local cluster.

Parameters

(None).

km.okmdb events

km.okmdb.read.failed

Severity

ALERT

Description

This message occurs when a read of the Onboard Key Manager’s database file fails. This may occur when the Onboard Key Manager has been configured to use a USB based mount-point and the USB device has not been mounted on the node.

Corrective Action

Check that the USB device is attached to the node.

Syslog Message

The system is not able to read from the Onboard Key Manager’s database file.

Parameters

(None).

km.okmdb.write.failed

Severity

ALERT

Description

This message occurs when a write to the Onboard Key Manager’s database file fails. This may occur when the Onboard Key Manager has been configured to use a USB based mount-point and the USB device has either not been mounted on the node or the USB device is write-protected.

Corrective Action

Check that the USB device is attached to the node and that it is not write-protected.

Syslog Message

The system is not able to write to the Onboard Key Manager’s database file.

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.

km.volume events

km.volume.mount.fail

Severity

ALERT

Description

This message occurs during the recovery of the key manager when a volume is placed online, but fails to mount. Volumes need to be mounted manually.

Corrective Action

The volume needs to be mounted manually with the provided junction using the "volume mount" command.

Syslog Message

Vserver "%s" failed to mount volume: "%s" to junction path: "%s" during key manager recovery.

Parameters

vserver (STRING): Name of the Vserver that owns the volumes being placed online.
volume (STRING): Name of the the volume being placed online.
junction (STRING): Name of the junction path to mount.

km.volume.mount.mismatch

Severity

ALERT

Description

This message occurs during recovery of the key manager when a junction path cannot identify the volume to mount. Pair the supplied junction with its volume and mount manually.

Corrective Action

The volumes are online but need to be mounted manually using the "volume mount" command.

Syslog Message

During health monitor recovery of the key manager on Vserver "%s", the junction path "%s" cannot be associated with the volume to mount.

Parameters

vserver (STRING): Name of the Vserver that owns the volume that could not be mounted.
junction (STRING): Name of the junction path to mount.

Copyright information

Trademark information