



km events

ONTAP EMS reference

NetApp
November 18, 2025

This PDF was generated from <https://docs.netapp.com/us-en/ontap-ems/km-cluster-events.html> on November 18, 2025. Always check docs.netapp.com for the latest.

Table of Contents

km events	1
km.cluster events	1
km.cluster.okm.hierarchy.bad	1
km.cmek events	1
km.cmek.akvkms.active	1
km.cmek.akvkms.available	2
km.cmek.akvkms.blocked	2
km.cmek.akvkms.keyExpired	3
km.cmek.akvkms.keyVersionChg	3
km.cmek.akvkms.notAvailable	4
km.cmek.akvkms.volOffline	4
km.cmek.akvkms.volOnline	5
km.cmek.gckms.active	5
km.cmek.gckms.available	6
km.cmek.gckms.blocked	6
km.cmek.gckms.keyVersionChg	7
km.cmek.gckms.notAvailable	7
km.cmek.gckms.volOffline	8
km.cmek.gckms.volOnline	8
km.cmek.init.failed	8
km.cmek.init.success	9
km.extkeysvr events	9
km.extkeysvr.details	9
km.keyretrieve events	10
km.keyretrieve.failed	10
km.keyserver events	10
km.keyserver.available	10
km.keyserver.notavailable	11
km.kmip events	11
km.kmip.key.mismatch	11
km.kmip.key.missing	12
km.mcc events	12
km.mcc.okm.hierarchy.bad	12
km.mcc.okmkey.mismatch	13
km.mcc.svmkek.missing.local	13
km.okm events	13
km.okm.count.invalid	13
km.okm.digest.missing	14
km.okm.key.mismatch	14
km.okm.key.missing	15
km.okmdb events	15
km.okmdb.read.failed	15
km.okmdb.write.failed	16

km.onboard events	16
km.onboard.ccmode.wrongpass	16
km.restore events	17
km.restore.invalid.key	17
km.run events	17
km.run.external.setup	17
km.run.extrnl.enable.needed	17
km.run.extrnl.setup.needed	18
km.run.onboard.setup	19
km.run.onboard.setup.needed	19
km.run.onboard.sync.needed	19
km.volume events	20
km.volume.mount.fail	20
km.volume.mount.mismatch	20

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.akvkms.active

Severity

NOTICE

Description

This message occurs when the configured Azure Key Vault Key Management Service (AKV-KMS) transitions to the active state after previously being in the blocked state. In this state, new volume creation is allowed and all existing volumes will be brought online.

Corrective Action

(None).

Syslog Message

The Azure Key Vault (AKV) configuration for the storage pool has been moved to the active state. New volumes can now be created and the existing volumes which were previously taken offline, will be brought back online. AKV configuration details are key ID: "%s", client ID: "%s", tenant ID: "%s", vault host: "%s", and key vault: "%s".

Parameters

keyId (STRING): Key ID.

clientId (STRING): Client ID.

tenantId (STRING): Tenant ID.
vaultHost (STRING): Vault Host.
keyVault (STRING): Key Vault.

km.cmek.akvkms.available

Severity

NOTICE

Description

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

Corrective Action

(None).

Syslog Message

The AKV-KMS configuration with client ID: "%s", tenant ID: "%s", vault host: "%s", key vault: "%s", and key ID: "%s" is now available.

Parameters

clientId (STRING): Client ID.
tenantId (STRING): Tenant ID.
vaultHost (STRING): Vault Host.
keyVault (STRING): Key Vault.
keyId (STRING): Key ID.

km.cmek.akvkms.blocked

Severity

ALERT

Description

This message occurs when the configured Azure Key Vault Key Management Service (AKV-KMS) transitions to the blocked state. In this state, no new volumes can be created and the existing volumes will be taken offline. This state occurs when fatal errors are received for an extended period while polling the AKV-KMS configuration. Fatal errors include a disabled key, a key not being found, and a key missing encryption and decryption privileges.

Corrective Action

Resolve the key access issues at the Azure Key Vault (AKV) portal. Ensure that the key is enabled and has the required encryption and decryption privileges.

Syslog Message

The Azure Key Vault (AKV) configuration for the storage pool has been moved to the blocked state. No new volumes can be created and all existing volumes will be taken offline. AKV configuration details are key ID: "%s", client ID: "%s", tenant ID: "%s", vault host: "%s", and key vault: "%s".

Parameters

keyId (STRING): Key ID.
clientId (STRING): Client ID.
tenantId (STRING): Tenant ID.

vaultHost (STRING): Vault Host.

keyVault (STRING): Key Vault.

km.cmek.akvkms.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. The top-level internal key protection key can still be unwrapped with the expired key version and there is no interruption to data availability.

Corrective Action

Renew the existing key version or create a new one at the Azure Key Vault (AKV) portal.

Syslog Message

The AKV key version has expired. AKV configuration details are key ID with expired version: "%s", client ID: "%s", tenant ID: "%s", vault host: "%s", and key vault: "%s".

Parameters

keyId (STRING): Key ID.

clientId (STRING): Client ID.

tenantId (STRING): Tenant ID.

vaultHost (STRING): Vault Host.

keyVault (STRING): Key Vault.

km.cmek.akvkms.keyVersionChg

Severity

NOTICE

Description

This message occurs when a change is made to the current key version associated with the key ID of the configured Azure Key Vault Key Management Service (AKV-KMS). The key version might have been auto-rotated or manually changed at the AKV-KMS. Additionally, the top-level internal key protection key is successfully re-wrapped with the current key version of the AKV-KMS key name.

Corrective Action

(None).

Syslog Message

The version of the key "%s" owned by AKV-KMS configuration with client ID: "%s", tenant ID: "%s", vault host: "%s", and key vault: "%s", has been changed from "%s" to "%s".

Parameters

keyId (STRING): Key ID.

clientId (STRING): Client ID.

tenantId (STRING): Tenant ID.

vaultHost (STRING): Vault Host.

keyVault (STRING): Key Vault.

oldKeyVersion (STRING): Prior key version.
newKeyVersion (STRING): New key version.

km.cmek.akvkms.notAvailable

Severity

ALERT

Description

This message occurs when a check for the availability of the configured Azure Key Vault Key Management Service (AKV-KMS) fails. The AKV-KMS might be down or there might be a network-related problem preventing communication. Without access to the AKV-KMS, the system might not be able to restore encryption keys needed to mount encrypted volumes. If the AKV-KMS 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 AKV-KMS configuration and permissions are correct. Verify connectivity.

Syslog Message

The AKV-KMS configuration with client ID: "%s", tenant ID: "%s", vault host: "%s", key vault: "%s", and key ID: "%s" is not available.

Parameters

clientId (STRING): Client ID.
tenantId (STRING): Tenant ID.
vaultHost (STRING): Vault Host.
keyVault (STRING): Key Vault.
keyId (STRING): Key ID.

km.cmek.akvkms.volOffline

Severity

ERROR

Description

This message occurs when the volumes belonging to a storage pool have been taken offline due to fatal errors received when attempting to access the key owned by the Azure Key Vault (AKV). Fatal errors include a disabled key, a key not being found, and a key missing encryption and decryption privileges. All volumes will remain offline until the key access issues are resolved at the AKV. When a successful poll is received, the volumes are brought back online automatically.

Corrective Action

Resolve the key access issues at the Azure Key Vault (AKV) portal. Ensure that the key is active and has the required encryption and decryption privileges.

Syslog Message

All volumes belonging to the storage pool have been taken offline due to key access errors. AKV configuration details are key ID : "%s", client ID: "%s", tenant ID: "%s", vault host: "%s", and key vault: "%s".

Parameters

keyId (STRING): Key ID.
clientId (STRING): Client ID.
tenantId (STRING): Tenant ID.
vaultHost (STRING): Vault Host.
keyVault (STRING): Key Vault.

km.cmek.akvkms.volOnline

Severity

NOTICE

Description

This message occurs when the volumes belonging to the storage pool have been brought back online due to successfully polling the Azure Key Vault (AKV) configuration.

Corrective Action

(None).

Syslog Message

All volumes belonging to the storage pool that were previously taken offline, are now back online. AKV configuration details are key ID: "%s", client ID: "%s", tenant ID: "%s", vault host: "%s", and key vault: "%s".

Parameters

keyId (STRING): Key ID.
clientId (STRING): Client ID.
tenantId (STRING): Tenant ID.
vaultHost (STRING): Vault Host.
keyVault (STRING): Key Vault.

km.cmek.gckms.active

Severity

NOTICE

Description

This message occurs when the configured Google Cloud Management Service (GCKMS) transitions to the active state after previously being in the blocked state. In this state, new volume creation is allowed and all existing volumes will be brought online.

Corrective Action

(None).

Syslog Message

The Google Cloud Key Management Service (GCKMS) configuration for the storage pool has been moved to the active state. New volumes can now be created and the existing volumes which were previously taken offline, will be brought back online. The GCKMS configuration details are key name: "%s", project ID: "%s", key ring: "%s", key ring location: "%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.

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.blocked

Severity

ALERT

Description

This message occurs when the configured Google Cloud Key Management Service (GCKMS) transitions to the blocked state. In this state, no new volumes can be created and the existing volumes will be taken offline. This state occurs when fatal errors are received for an extended period while polling the GCKMS configuration. Fatal errors include a disabled key, a key not being found, and a key missing encryption and decryption privileges.

Corrective Action

Resolve the key access issues at the Google Cloud Key Management Service (GCKMS) portal. Ensure that the key is enabled and has the required encryption and decryption privileges.

Syslog Message

The Google Cloud Key Management Service (GCKMS) configuration for the storage pool has been moved to the blocked state. No new volumes can be created and all existing volumes will be taken offline. The GCKMS configuration details are key name: "%s", project ID: "%s", key ring: "%s", key ring location: "%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.

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.gckms.volOffline

Severity

ALERT

Description

This message occurs when the volumes belonging to a storage pool are taken offline due to fatal errors received when attempting to access the key owned by the Google Cloud Key Management Service (GCKMS). Fatal errors include a disabled key, a key not being found, and a key missing encryption and decryption privileges. All volumes will remain offline until the key access issues are resolved at the GCKMS. When the GCKMS is successfully polled, the volumes are brought back online automatically.

Corrective Action

Resolve the key access issues at the Google Cloud Key Management Service (GCKMS) portal. Ensure that the key is enabled and has the required encryption and decryption privileges.

Syslog Message

All volumes belonging to the storage pool have been taken offline due to key access errors. The GCKMS configuration details are key name: "%s", project ID: "%s", key ring: "%s", key ring location: "%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.

km.cmek.gckms.volOnline

Severity

NOTICE

Description

This message occurs when the volumes belonging to the storage pool that were previously offline have been brought back online due to successfully polling the Google Cloud Key Management Service (GCKMS) configuration.

Corrective Action

(None).

Syslog Message

All volumes belonging to the storage pool that were previously taken offline are now back online. The GCKMS configuration details are key name: "%s", project ID: "%s", key ring: "%s", key ring location: "%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.

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

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

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

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

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

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

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

km.kmip events

km.kmip.key.mismatch

Severity

ALERT

Description

This message occurs in a NetApp MetroCluster configuration where both peer clusters are configured with the external key manager on the admin Vserver, but the NSE-AK keys do not match between the local and remote clusters. A mismatch in the NSE-AK keys can cause a failure during a reboot or future switchover/switchback event.

Corrective Action

Contact Contact NetApp technical support. for assistance.

Syslog Message

In a MetroCluster configuration with the external key manager enabled on the admin Vserver, the NSE-AK key digests do not match between the local and remote clusters.

Parameters

(None).

km.kmip.key.missing

Severity

ALERT

Description

This message occurs in a NetApp MetroCluster configuration where both peer clusters are configured with the external key manager on the admin Vserver, but one or more NSE-AK keys are missing on either the local or remote cluster. A missing key can cause a failure during a reboot or future switchover/switchback event.

Corrective Action

Contact Contact NetApp technical support. for assistance.

Syslog Message

In a MetroCluster configuration with the external key manager enabled on the admin Vserver, an NSE-AK key is missing on cluster %s.

Parameters

clusterID (STRING): Cluster ID where the NSE-AK key is missing.

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 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.okm events

km.okm.count.invalid

Severity

ALERT

Description

This message occurs in a NetApp MetroCluster configuration where both peer clusters are configured with the Onboard Key Manager (OKM), but the number of keys of the specified type is invalid. An incorrect number of OKM hierarchy keys can cause a failure during a reboot or future switchover/switchback event.

Corrective Action

Contact NetApp technical support. for assistance.

Syslog Message

In a MetroCluster configuration with the Onboard Key Manager enabled, the number of %s keys is incorrect on cluster %s. Expected Count: %s, Actual Count: %s.

Parameters

keyType (STRING): Type of the key with the invalid count.

clusterID (STRING): Cluster ID where the invalid count occurred.

expectedCount (STRING): Expected number of keys of the specified type.

actualCount (STRING): Actual number of keys of the specified type.

km.okm.digest.missing**Severity**

ALERT

Description

This message occurs in a NetApp MetroCluster configuration where both peer clusters are configured with the Onboard Key Manager (OKM), but an SVM-KEK key is missing a digest on either the local or remote cluster. A missing key digest in the OKM hierarchy can cause a failure during a reboot or future switchover/switchback event.

Corrective Action

Contact NetApp technical support. for assistance.

Syslog Message

In a MetroCluster configuration with the Onboard Key Manager enabled, the following SVM-KEK key (%s) is missing a digest on cluster %s.

Parameters

keyID (STRING): Key ID of the SVM-KEK key that is missing a digest.

clusterID (STRING): Cluster ID where the SVM-KEK key digest is missing.

km.okm.key.mismatch**Severity**

ALERT

Description

This message occurs in a NetApp MetroCluster configuration where both peer clusters are configured with the Onboard Key Manager (OKM), but the keys of the specified type do not match between the peer clusters. A mismatch in the OKM hierarchy keys can cause a failure during a reboot or future

switchover/switchback event.

Corrective Action

Contact NetApp technical support. for assistance.

Syslog Message

In a MetroCluster configuration with the Onboard Key Manager enabled, the %s keys do not match between the local and remote clusters.

Parameters

keyType (STRING): Type of the key with the mismatch.

km.okm.key.missing

Severity

ALERT

Description

This message occurs in a NetApp MetroCluster configuration where both peer clusters are configured with the Onboard Key Manager (OKM), but one or more keys of the specified type are missing on either the local or peer cluster. A missing key in the OKM hierarchy can cause a failure during a reboot or future switchover/switchback event.

Corrective Action

Contact NetApp technical support. for assistance.

Syslog Message

In a MetroCluster configuration with the Onboard Key Manager enabled, %s keys are missing from cluster %s.

Parameters

keyType (STRING): Type of the missing key.

clusterID (STRING): Cluster ID where the key is missing.

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

Copyright © 2025 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—with 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.