ekmip events

ONTAP 9.12.1 EMS reference

NetApp
December 14, 2022

Table of Contents

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 the Vserver has been blocked and any 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

The Vserver has been blocked and any 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.awskms events

ekmip.awskms.available

Severity

NOTICE

Description

This message occurs when a configured Amazon Web Services (AWS) Key Management Service (KMS) that was unavailable for key operations is now available.

Corrective Action

(None).

Syslog Message

The AWS KMS with region: "%s" and key ID: "%s" configured for Vserver "%s" is now available.

Parameters

region (STRING): AWS KMS region.
keyId (STRING): Key ID.
vserver (STRING): Name of the Vserver where the AWS KMS is configured.

ekmip.awskms.keyChg

Severity

NOTICE

Description

This message occurs when the key material associated with the key ID of the configured Amazon Web Services (AWS) Key Management Service (KMS) changes. The key material might have been auto-rotated or manually changed at the AWS KMS. Additionally, as a result of updated key material, the top-level internal key-protection key is successfully rewrapped with the current key material of the AWS KMS key ID.

Corrective Action

(None).

Syslog Message

The key material for key "%s" owned by AWS KMS region "%s" and configured for Vserver "%s" has changed.

Parameters

keyId (STRING): Key ID.
region (STRING): AWS KMS region.
vserver (STRING): Name of the Vserver where the AWS KMS is configured.

ekmip.awskms.keyVersionChg

Severity

NOTICE

Description

This message occurs when the key version associated with the key ID of the configured Amazon Web Services (AWS) Key Management Service (KMS) changes. The key version might have been auto-rotated or manually changed at the AWS KMS. Additionally, as a result of updated key version, the top-level internal key-protection key is successfully rewrapped with the current key version of the AWS KMS key ID.

Corrective Action

(None).

Syslog Message

The version of the key "%s" owned by AWS KMS region "%s", configured for Vserver "%s", is changed from "%s" to "%s".

Parameters

keyId (STRING): Key ID.
region (STRING): AWS KMS region.
vserver (STRING): Name of the Vserver where the AWS KMS is configured.
oldKeyVersion (STRING): Prior key version.
newKeyVersion (STRING): New key version.

ekmip.awskms.notAvailable

Severity

ALERT

Description

This message occurs when a check for the availability of the configured Amazon Web Services (AWS) Key Management Service (KMS) fails. The AWS KMS might be down or there might be a network-related problem preventing communication. Without access to the AWS KMS, the node might be unable to restore

authentication keys needed to unlock NetApp Storage Encryption (NSE) drives or encryption keys needed to mount encrypted volumes. If the AWS KMS is unavailable, 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 AWS KMS configuration is correct by using the "security key-manager external aws show -vserver <vserver_name>" command, and verify that the AWS KMS cluster state is available. If the cluster state is unavailable, run the "security key-manager external aws restore" command to bring the cluster state to available. If the issue still persists, contact NetApp technical support.

Syslog Message

The AWS KMS with region: %s and key ID: %s configured for Vserver "%s" is not available.

Parameters

region (STRING): AWS KMS region.
keyId (STRING): Key ID.
vserver (STRING): Name of the Vserver where the AWS KMS is configured.

ekmip.awskms.volOffline

Severity

ALERT

Description

This message occurs when the Vserver has been blocked and any encrypted volumes belonging to the Vserver have been taken offline due to errors received when trying to access the key owned by the Amazon Web Services (AWS) Key Management Service (KMS). Reasons for AWS KMS 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 AWS KMS 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 AWS KMS. 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 AWS KMS portal. Ensure that the key is active and the user has the required privileges to access the key.

Syslog Message

The Vserver has been blocked and any encrypted volumes belonging to Vserver "%s" have been taken offline due to key access errors associated with key "%s" owned by AWS KMS region "%s".

Parameters

vserver (STRING): Name of the Vserver where the AWS KMS is configured.
keyId (STRING): Key ID.
region (STRING): AWS KMS region.

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 Vserver has been blocked and any encrypted 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

The Vserver has been blocked and any 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.

ekmip.ikpkms events

ekmip.ikpkms.200.missingField

Severity

ALERT

Description

This message occurs when trying to access the key owned by the IBM Key Protect (IKP) Key Management Service (KMS) and an "OK" response (code 200) is received but one field of the response is not populated. Reasons for IKP KMS 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 IKP KMS to verify key accessibility. The missing field is integral in determining the status of the key.

Corrective Action

The IKP KMS provided a response with a status of 200 (OK) that did not contain all of the expected fields. Contact technical support to resolve this issue.

Syslog Message

A 200 OK response was received from IKP KMS but the field "%s" was missing for Vserver "%s" with Keymanager Name "%s" associated with key "%s" owned by IKP KMS region "%s" with instance ID "%s".

Parameters

missingField (STRING): Name of the field that is not populated.
vserver (STRING): Name of the Vserver where the IKP KMS is configured.
kmName (STRING): The name of the IKP KMS.
keyId (STRING): The Key ID associated with this IKP KMS instance.
region (STRING): The region associated with this IKP KMS instance.
instanceId (STRING): IKP KMS Instance ID.

ekmip.ikpkms.available

Severity

NOTICE

Description

This message occurs when a configured IBM Key Protect (IKP) Key Management Service (KMS) that was unavailable for key operations is now available.

Corrective Action

(None).

Syslog Message

The IKP KMS with region: "%s", instance ID: "%s", and key ID: "%s" configured for Vserver "%s" with Keymanager Name "%s" is now available.

Parameters

region (STRING): The region associated with this IKP KMS instance.
instanceId (STRING): IKP KMS Instance ID.
keyId (STRING): The Key ID associated with this IKP KMS instance.
vserver (STRING): Name of the Vserver where the IKP KMS is configured.
kmName (STRING): The name of the IKP KMS.

ekmip.ikpkms.keyVersionChg

Severity

NOTICE

Description

This message occurs when the key version associated with the key ID of the configured IBM Key Protect (IKP) Key Management Service (KMS) changes. The key version might have been auto-rotated or manually changed at the IKP KMS. Additionally, as a result of updated key version, the top-level internal key-protection key has been successfully rewrapped with the current key version of the IKP KMS key ID.

Corrective Action

(None).

Syslog Message

The version of the key "%s" owned by IKP KMS region "%s" and instance ID "%s", configured for Vserver "%s" with Keymanager Name "%s", has been changed from "%s" to "%s".

Parameters

keyId (STRING): The Key ID associated with this IKP KMS instance.
region (STRING): The region associated with this IKP KMS instance.
instanceId (STRING): IKP KMS Instance ID.
vserver (STRING): Name of the Vserver where the IKP KMS is configured.
kmName (STRING): The name of the IKP KMS.
oldKeyVersion (STRING): Prior key version.
newKeyVersion (STRING): New key version.

ekmip.ikpkms.notAvailable

Severity

ALERT

Description

This message occurs when a check for the availability of the configured IBM Key Protect (IKP) Key Management Service (KMS) fails. The IKP KMS might be down or there might be a network-related problem preventing communication. Without access to the IKP KMS, the node might be unable to restore authentication keys needed to unlock NetApp Storage Encryption (NSE) drives or encryption keys needed to mount encrypted volumes. If the IKP KMS is unavailable, 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 IKP KMS configuration is correct by using the "security key-manager external ikp show -vserver <vserver_name>" command, and verify that the IKP KMS cluster state is available. If the cluster state is unavailable, run the "security key-manager external ikp restore" command to bring the cluster state to available. If the issue still persists, contact NetApp technical support.

Syslog Message

The IKP KMS with region: "%s", instance ID: "%s", and key ID: "%s" configured for Vserver "%s" with Keymanager Name "%s" is not available.

Parameters

region (STRING): The region associated with this IKP KMS instance.
instanceId (STRING): IKP KMS Instance ID.
keyId (STRING): The Key ID associated with this IKP KMS instance.
vserver (STRING): Name of the Vserver where the IKP KMS is configured.
kmName (STRING): The name of the IKP KMS.

ekmip.ikpkms.volOffline

Severity

ALERT

Description

This message occurs when the volumes belonging to the Vserver are taken offline due to errors received when trying to access the key owned by the IBM Key Protect (IKP) Key Management Service (KMS). Reasons for IKP KMS 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 IKP KMS 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 IKP KMS. 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 IKP KMS 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" with Keymanager Name "%s" were taken offline due to key access errors associated with key "%s" owned by IKP KMS region "%s" and instance ID "%s".

Parameters

vserver (STRING): Name of the Vserver where the IKP KMS is configured.
kmName (STRING): The name of the IKP KMS.
keyId (STRING): The Key ID associated with this IKP KMS instance.
region (STRING): The region associated with this IKP KMS instance.
instanceId (STRING): IKP KMS Instance ID.

Copyright information

Trademark information