security key-manager commands

ONTAP commands

NetApp
February 03, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-cli-9161/security-key-manager-delete-key-database.html on February 03, 2026. Always check docs.netapp.com for the latest.

Table of Contents

security key-manager commands

security key-manager delete-key-database

(DEPRECATED)-Deletes the key hierarchy for the Onboard Key Manager

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

This command is deprecated and might be removed in a future release. Use security key-manager onboard disable instead.

The `security key-manager delete-key-database` command permanently deletes the Onboard Key Manager configuration from all nodes of the cluster.

Examples

The following example deletes the Onboard Key Manager configuration from all nodes of the cluster:

```
cluster-1::*> security key-manager delete-key-database

Warning: This command will permanently delete all keys from the Onboard
Key Manager.
Do you want to continue? {y|n}: y
```

Related Links

- security key-manager onboard disable

security key-manager delete-kmip-config

(DEPRECATED)-Deletes the KMIP configuration

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

This command is deprecated and may be removed in a future release. Use security key-manager external disable instead.

The `security key-manager delete-kmip-config` command permanently deletes the Key Management Interoperability Protocol (KMIP) server configuration from all nodes of the cluster.

The keys stored by the external KMIP servers cannot be deleted by ONTAP, and must be deleted by using external tools.

Examples

The following example deletes the KMIP-server configuration from all nodes of the cluster:

```
cluster-1::*> security key-manager delete-kmip-config

Warning: This command will permanently delete the KMIP-server
configuration
         from all nodes of the cluster.
Do you want to continue? {y|n}: y
The KMIP-server configuration has been deleted from all nodes of the
cluster.
The keys stored by the external KMIP servers cannot be deleted by ONTAP,
and must be deleted by using external tools.
```

Related Links

- security key-manager external disable

security key-manager prepare-to-downgrade

Prepares all configured Key managers for downgrade

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

This command is deprecated and might be removed in a future release.

The `security key-manager prepare-to-downgrade` command disables the Onboard Key Manager features that are not supported in releases prior to ONTAP 9.1.0. The features that are disabled are Onboard Key Manager support for MetroCluster configurations and Volume Encryption (VE).

Examples

The following example disables the Onboard Key Manager support for MetroCluster configurations and Volume Encryption (VE):

```
cluster1::*> security key-manager prepare-to-downgrade
```

security key-manager setup

(DEPRECATED)-Configure key manager connectivity

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

> This command is deprecated and might be removed in a future release. To set up external key manager, use security key-manager external enable , and to set up the Onboard Key Manager use security key-manager onboard enable instead.

The `security key-manager setup` command enables you to configure key management. ONTAP supports two mutually exclusive key management methods: external via one or more key management interoperability protocol (KMIP) servers, or internal via an Onboard Key Manager. This command is used to configure an external or internal key manager. When configuring an external key management server, this command records networking information on all node that is used during the boot process to retrieve keys needed for booting from the KMIP servers. For the Onboard Key Manager, this command prompts you to configure a passphrase to protect internal keys in encrypted form.

This command can also be used to refresh missing onboard keys. For example, if you add a node to a cluster that has the Onboard Key Manager configured, you will run this command to refresh the missing keys.

For the Onboard Key Manager in a MetroCluster configuration, if the security key-manager update-passphrase command is used to update the passphrase on one site, then run the `security key-manager setup` command with the new passphrase on the partner site before proceeding with any key-manager operations.

Parameters

`[-node <nodename>]` - Node Name

This parameter is used only with the Onboard Key Manager when a refresh operation is required (see command description). This parameter is ignored when configuring external key management and during the initial setup of the Onboard Key Manager.

`[-cc-mode-enabled {yes|no}]` - Enable Common Criteria Mode?

When configuring the Onboard Key Manager, this parameter is used to specify that Common Criteria (CC) mode should be enabled. When CC mode is enabled, you will be required to provide a cluster passphrase that is between 64 and 256 ASCII character long, and you will be required to enter that passphrase each time a node reboots.

`[-sync-metrocluster-config {yes|no}]` - Sync MetroCluster Configuration from Peer

When configuring the Onboard Key Manager in a MetroCluster configuration, this parameter is used to indicate that the `security key-manager setup` command has been performed on the peer cluster, and that the `security key-manager setup` command on this cluster should import the peer's configuration.

`[-are-unencrypted-metadata-volumes-allowed-in-cc-mode {yes|no}]` - Are Unencrypted Metadata Volumes Allowed in CC-Mode

If Common Criteria (CC) mode is enabled this parameter allows unencrypted metadata volumes to exist. These metadata volumes are created internally during normal operation. Examples are volumes created during SnapMirror and Vserver migrate operations. The default value is *no* .

Examples

The following example creates a configuration for external key management:

```
cluster-1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default or omit a question, do not enter a value.

Would you like to configure the Onboard Key Manager? {yes, no} [yes]: no
Would you like to configure the KMIP server environment? {yes, no} [yes]:
yes
```

The following example creates a configuration for the Onboard Key Manager:

```
cluster-1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default or omit a question, do not enter a value.

Would you like to configure the Onboard Key Manager? {yes, no} [yes]: yes
Enter the cluster-wide passphrase for the Onboard Key Manager. To continue
the
configuration, enter the passphrase, otherwise type "exit":
Re-enter the cluster-wide passphrase:
After configuring the Onboard Key Manager, save the encrypted
configuration data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the "security key-manager backup show"
command.
```

The following example creates a configuration for the Onboard Key Manager with Common Criteria mode enabled:

```
cluster-1::> security key-manager setup -cc-mode-enabled yes
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default or omit a question, do not enter a value.

Would you like to configure the Onboard Key Manager? {yes, no} [yes]: yes
Enter the cluster-wide passphrase for the Onboard Key Manager. To continue
the
configuration, enter the passphrase, otherwise type "exit":
Re-enter the cluster-wide passphrase:
After configuring the Onboard Key Manager, save the encrypted
configuration data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the "security key-manager backup show"
command.
```

Related Links

- security key-manager external enable
- security key-manager onboard enable
- security key-manager update-passphrase

security key-manager show-key-store

(DEPRECATED)-Displays the configured key manager key stores.

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command is deprecated. Use the "security key-manager keystore show" command to display all keystore configurations instead.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, then the command will list the key manager configured for the given Vserver.

[-key-store <Key Store>] - Key Store

If you specify this parameter, then the command displays only the vservers that have the given key-store configured.

[-state <Key Store state>] - Key Store State

If you specify this parameter, then the command displays only the vservers that have the given state configured.

[-keystore-type <Key Store Type>] - Key Store Type (Azure/AWS etc)

If you specify this parameter, then the command displays only the vservers that have the given keystore-type configured. This parameter is used to specify a particular type of external key manager. If this parameter is specified and 'key-store' is provided as 'onboard', the "security key-manager show-key-store" command will not return any entries.

[-policy <text>] - Key Manager Policy Name

If you specify this parameter, then the command displays only the vservers that have the given policy.

Examples

The following example shows all configured key managers in the cluster. In the example, the admin vserver has the Onboard Key Manager configured and the data vserver "datavs1" has external key management configured:

```
cluster-1::> security key-manager show-key-store

Vserver                 Key Store Key Store Type
----------------------- --------- --------------
cluster-1               onboard   -
datavs1                 external  AKV
```

security key-manager update-passphrase

(DEPRECATED)-Update cluster-wide passphrase

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

This command is deprecated and might be removed in a future release. Use security key-manager onboard update-passphrase instead.

The `security key-manager update-passphrase` command provides a way to update the cluster-wide passphrase, created initially by running the security key-manager setup command, that is used for the Onboard Key Manager. This command prompts for the existing passphrase, and if that passphrase is correct then the command prompts for a new passphrase.

When the `security key-manager update-passphrase` command is executed in a MetroCluster configuration, then run the security key-manager setup command with the new passphrase on the partner site before proceeding with any key-manager operations. This allows the updated passphrase to be replicated to the partner site.

Parameters

Examples

The following example updates the cluster-wide passphrase used for the Onboard Key Manager:

```
cluster-1::*> security key-manager update-passphrase

Warning: This command will reconfigure the cluster passphrase for the
Onboard
         Key Manager.
Do you want to continue? {y|n}: y

Enter current passphrase:

Enter new passphrase:

Reenter the new passphrase:
Update passphrase has completed. Save the new encrypted configuration data
in
a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the "security key-manager backup show"
command.
```

Related Links

- security key-manager onboard update-passphrase
- security key-manager setup

security key-manager config modify

Modify key management configuration options

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

This command modifies the key management configuration options.

Parameters

`[-cc-mode-enabled {true|false}]` - Enable Common Criteria Mode (privilege: advanced)

This parameter modifies the configuration state of the Onboard Key Manager (OKM) Common Criteria (CC) mode. CC mode enforces some of the policies required by the Common Criteria "Collaborative Protection Profile for Full Drive Encryption-Authorization Acquisition" (FDE-AA cPP) and "Collaborative Protection Profile for Full Drive Encryption-Encryption Engine" documents.

`[-health-monitor-polling-interval <integer>]` - Health Monitor Polling Period (in minutes) (privilege: advanced)

This parameter modifies the the polling interval of the keyserver health monitor at the cluster level.

`[-cloud-kms-retry-count <integer>]` - Cloud KMS connection retry count (privilege: advanced)

This parameter modifies the the cloud keymanager connection retry count at the cluster level.

`[-are-unencrypted-metadata-volumes-allowed-in-cc-mode {true|false}]` - Are Unencrypted Metadata Volumes Allowed in Common Criteria Mode (privilege: advanced)

If Common Criteria (CC) mode is enabled this parameter allows unencrypted metadata volumes to exist. These metadata volumes are created internally during normal operation. Examples are volumes created during SnapMirror and Vserver migrate operations. The default value is *`false`* .

Examples

The following command enables Common Criteria mode in the cluster:

```
cluster-1::*> security key-manager config modify -cc-mode-enabled true
```

The following command modifies the keyserver health monitor polling interval to be 30 minutes:

```
cluster-1::*> security key-manager config modify -health-monitor-polling
-interval 30
```

The following command modifies the cloud keymanager connection retry count to 3:

```
cluster-1::*> security key-manager config modify -cloud-kms-retry-count 3
```

security key-manager config show

Display key management configuration options

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

This command displays the key management configuration options.

The "cc-mode-enabled" option reflects the current configuration state for Common-Criteria (CC) mode for the Onboard Key Manager. CC mode is an operational mode that enforces some of the policies required by the Common Criteria "Collaborative Protection Profile for Full Drive Encryption-Authorization Acquisition" (FDE-AA cPP) and "Collaborative Protection Profile for Full Drive Encryption-Encryption Engine" documents. The feature can be enabled when the Onboard Key Manager is configured using the security key-manager setup command or after the Onboard Key Manager is configured using the security key-manager config modify command.

Examples

The following example displays the state of all key-manager configuration options:

```
cluster-1::*> security key-manager config show
CC-Mode  health-monitor-polling-interval  cloud-kms-retry-count
Enabled  (in minutes)
-------  ------------                    ---------------------
true     30                              0
```

Related Links

- security key-manager setup
- security key-manager config modify

security key-manager external add-servers

Add external key management servers

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command adds the key management servers of the given hosts and ports to the given Vserver's external key manager's list of four possible key management servers. When adding key management servers to the external key manager associated with the admin Vserver, you must run the same command specifying the same set of key servers on the peer cluster. When adding key management servers to a data Vserver, you can run the `security key-manager external add-servers` command on the active cluster only, as the command is replicated to the peer cluster. However, you need to ensure that the key management servers specified are reachable from both clusters. This command is not supported if external key management is not enabled for the Vserver. Use this command to add primary key servers. To modify the list of secondary key servers associated with a primary key server, use the security key-manager external modify-server command.

Parameters

`-vserver <vserver name>` - Vserver Name

Use this parameter to specify the Vserver on which to add the key management servers.

`-key-servers <Hostname and Port>,…` - External Key Management Servers

Use this parameter to specify the list of additional key management servers that the external key manager uses to store keys.

Examples

The following example adds two key management servers to the list of servers used by the external key manager for Vserver cluster-1. The first key management server's hostname is keyserver1.local and is listening on the default port 5696, and the second key management server's IP is 10.0.0.20 and is listening on port 15696:

```
cluster-1::> security key-manager external add-servers -vserver cluster-1
-key-servers keyserver1.local, 10.0.0.20:15696
```

Related Links

- security key-manager external modify-server

security key-manager external create-config

Create an inactive external key manager

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command enables an ONTAP administrator to create an inactive external key manager configuration for the admin Vserver. This facilitates the switching between the Onboard Key Manager (OKM) and an external key manager (EKM) without migrating the keys to a data SVM

Parameters

`-vserver <vserver name>` - Vserver Name

Use this parameter to specify the Vserver on which the external key manager configuration is to be created.

`-key-servers <Hostname and Port>,…` - List of External Key Management Servers

Use this parameter to specify a list of up to four key management servers that the external key manager will use to store keys.

`-client-cert <text>` - Name of the Client Certificate

Use this parameter to specify the unique name of the client certificate that the key management servers will use to verify the identity of the ONTAP client.

-server-ca-certs <text>,… - Names of the Server CA Certificates

Use this parameter to specify the unique names of server-ca certificates that ONTAP will use to verify the identity of the key management servers.

Examples

The following example creates an inactive external key manager configuration for Vserver cluster-1 with the configuration name "default". The command includes three key management servers. The first key server's hostname is ks1.local and is listening on port 5696. The second key server's IP address is 10.0.0.10 and is listening on the default port 5696. The third key server's IPv6 address is fd20:8b1e:b255:814e:32bd:f35c:832c:5a09, and is listening on port 5696.

```
cluster-1::> security key-manager external create-config -vserver cluster-
1 -key-servers
ks1.local:5696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:5696
-client-cert AdminVserverClientCert -server-ca-certs
ServerCaCert1,ServerCaCert2
```

security key-manager external disable

Disable external key management

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command disables the external key manager associated with the given Vserver. If the key manager is in use by ONTAP, you cannot disable it. When disabling the external key manager associated with the admin Vserver, you must run the same command on the peer cluster. When disabling the external key manager for a data Vserver, you can run the `security key-manager external disable` command on the active cluster only, as the command is replicated on the peer cluster. This command is not supported when the Onboard Key Manager is enabled for the given Vserver.

Parameters

-vserver <vserver name> - Vserver Name (privilege: advanced)

Use this parameter to specify the Vserver on which the external key manager is to be disabled.

Examples

The following example removes the external key manager for Vserver cluster-1:

```
cluster-1::*> security key-manager external disable -vserver cluster-1
Warning: This command will permanently delete the external key management
 configuration for Vserver "cluster-1".
 Do you want to continue? {y|n}: y
```

security key-manager external enable

Enable external key management

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command enables the external key manager associated with the given Vserver. This command is not supported when a key manager for the given Vserver is already enabled. When enabling the external key manager associated with the admin Vserver, you must run the same command specifying the same set of key servers on the peer cluster. When enabling the external key manager for a data Vserver, you can run the `security key-manager external enable` command on the active cluster only, as the configuration will be replicated on the peer cluster. However, you must ensure that the key management servers specified in the `security key-manager external enable` command are reachable from both clusters. Only primary key servers can be added using this command.

Parameters

`-vserver <vserver name>` - Vserver Name

Use this parameter to specify the Vserver on which the external key manager is to be enabled.

`-key-servers <Hostname and Port>,…` - List of External Key Management Servers

Use this parameter to specify the list of up to four key management servers that the external key manager uses to store keys.

`-client-cert <text>` - Name of the Client Certificate

Use this parameter to specify the unique name of the client certificate that the key management servers use to ensure the identity of ONTAP.

`-server-ca-certs <text>,…` - Names of the Server CA Certificates

Use this parameter to specify the unique names of server-ca certificates that ONTAP uses to ensure the identify of the key management servers.

`[-policy <text>]` - Key Manager Policy

Use this parameter to specify a specific key manager security policy to be used by this key manager.

Examples

The following example enables the external key manager for Vserver cluster-1. The command includes three key management servers. The first key server's hostname is ks1.local and is listening on port 15696. The second key server's IP address is 10.0.0.10 and is listening on the default port 5696. The third key server's IPv6 address is fd20:8b1e:b255:814e:32bd:f35c:832c:5a09, and is listening on port 1234.

```
cluster-1::> security key-manager external enable -vserver cluster-1 -key
-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
ServerCaCert1,ServerCaCert2
```

security key-manager external modify-server

Modify key server properties

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command modifies configuration information for configured key management servers. When modifying a key management server from the external key manager associated with the admin Vserver, you must run the same command specifying the same set of parameters on the peer cluster. When modifying a key management server from a data Vserver, you can run the `security key-manager external modify-server` command on the active cluster only as the command is replicated on the peer cluster. However, if the password associated with a key management server is modified, then you must run the `security key-manager external modify-server` command specifying the same password on the peer cluster as the password is not replicated between clusters. This command is supported only when external key manager has been enabled for the given Vserver.

Parameters

`-vserver <vserver name>` - Vserver Name

Use this parameter to specify the Vserver on which to modify the key management server configuration.

`-key-server <Hostname and Port>` - External Key Server

Use this parameter to specify the primary key management server for which the command modifies the configuration.

`[-secondary-key-servers <Remote InetAddress>,…]` - Secondary Key Servers

Use this parameter to specify the secondary key management servers that will be members of the set of clustered key servers. When specifying a secondary key server, a port number cannot be associated with the secondary key server.

`[-timeout <integer>]` - Key Server I/O Timeout (privilege: advanced)

Use this parameter to specify the I/O timeout, in seconds, for the selected key management server.

`[-username <text>]` - Authentication User Name (privilege: advanced)

Use this parameter to specify the username with which ONTAP authenticates with the key management server.

`[-create-remove-timeout <integer>]` - Key Server Timeout for Create and Remove

Use this parameter to specify a shorter I/O timeout, in seconds, to be used for create and delete operations for the selected key management server.

Examples

The following example modifies the I/O timeout to 45 seconds for Vserver cluster-1, key server keyserver1.local:

```
cluster-1::> security key-manager external modify-server -vserver cluster-
1 -key-server keyserver1.local -timeout 45
```

The following example modifies the username and passphrase used to authenticate with key server keyserver1.local:

```
cluster-1::> security key-manager external modify-server -vserver cluster-
1 -key-server keyserver1.local -username ksuser
Enter the password:
Reenter the password:
```

The following example modifies the secondary key management servers secondarykeyserver1.local and secondarykeyserver2.local to be in a cluster configuration with the primary key management server keyserver1.local

```
cluster-1::> security key-manager external modify-server -vserver cluster-
1 -key-server keyserver1.local -secondary-key-servers
secondarykeyserver1.local,secondarykeyserver2.local
```

security key-manager external modify

Modify external key management

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command modifies the external key manager configuration associated with the given Vserver. When modifying the external key manager configuration associated with the admin Vserver, you must run the same command specifying the same parameters on the peer cluster. When modifying the external key manager configuration associated with a data Vserver, you can run the `security key-manager external modify` command on the active cluster only as the configuration modifications are replicated on the peer cluster. This command is not supported when external key management is not enabled for the given Vserver.

Parameters

`-vserver <vserver name>` - Vserver Name

Use this parameter to specify the Vserver on which the key manager to be modified is located.

`[-client-cert <text>]` - Name of the Client Certificate

Use this parameter to modify the name of the client certificate that the key management servers use to ensure the identity of ONTAP. If the keys of the new certificate do not match the keys of the existing certificate, or if the TLS connectivity with key-management servers fails with the new certificate, the operation fails. Running this command in the diagnostic privilege mode ignores failures and allows the command to complete.

[-server-ca-certs <text>,…] - Names of the Server CA Certificates

Use this parameter to modify the names of server-ca certificates that ONTAP uses to ensure the identity of the key management servers. Note that the list provided completely replaces the existing list of certificates. If the TLS connectivity with key-management servers fails with the new list of server-ca certificates, the operation fails. Running this command in the diagnostic privilege mode ignores failures and allows the command to complete.

Examples

The following example updates the client certificate used with the key management servers:

```
cluster-1::> security key-manager external modify -vserver cluster-1
-client-cert NewClientCert
```

security key-manager external remove-servers

Remove external key management servers

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command removes the key management servers at the given hosts and ports from the given Vserver's external key manager's list of key management servers. If any of the specified key management servers is the sole storage location for any key that is in use by ONTAP, then you are unable to remove the key server. When removing key management servers from the external key manager associated with the admin Vserver, you must run the same command specifying the same set of key servers on the peer cluster. When removing key management servers from a data Vserver, you can run the `security key-manager external remove-servers` command on the active cluster only as the the command is replicated on the peer cluster. This command is not supported when external key management is not enabled for the given Vserver. Use this command is remove primary key servers. To modify the list of secondary key servers associated with a primary key server, use the security key-manager external modify-server command.

Parameters

-vserver <vserver name> - Vserver Name

Use this parameter to specify the Vserver on which the external key manager is to be removed.

-key-servers <Hostname and Port>,… - External Key Management Servers

Use this parameter to specify the list of key management servers that you want to remove from the external key manager.

[-force {true|false}] - Bypass OOQ Check?

Set this parameter to true to bypass checks for out of quorum nodes.

Examples

The following example removes the key management server keyserver1.local, listening on the default port of 5696 and the key management server at IP 10.0.0.20, listening on port of 15696.

```
cluster-1::*> security key-manager external remove-servers -vserver
cluster-1
 -key-servers keyserver1.local,10.0.0.20:15696
```

Related Links

- security key-manager external modify-server

security key-manager external restore

Restore the key ID pairs from the key management servers.

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command retrieves and restores any current unrestored keys associated with the storage controller from the specified key management servers. When restoring keys from the external key manager associated with the admin Vserver, you must run the same command on the peer cluster. When restoring keys from a data Vserver, you can run the `security key-manager external restore` command on the active cluster only as the command is replicated on the peer cluster. This command is not supported when external key management has not been enabled for the Vserver. This command only restores keys from primary key servers.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node

This parameter specifies the name of the node that will load unrestored key IDs into its internal key table. If not specified, all nodes retrieve unrestored keys into their internal key table.

[-vserver <vserver name>] - Vserver Name

This parameter specifies the Vserver for which to list the keys. If not specified, this command restores key for all Vservers.

[-key-server <Hostname and Port>] - Key Server

If this parameter is specified, this command restores keys from the key management server identified by the host and port. If not specified, this command restores keys from all available key management servers.

[-key-id <Hex String>] - Key ID

If you specify this parameter, then the command restores only the key IDs that match the specified value.

[-key-tag <text>] - Key Tag

If you specify this parameter, then the command restores only the key IDs that match the specified key-tag. The key-tag for Volume Encryption Keys (VEKs) is set to the UUID of the encrypted volume. If not specified, all key ID pairs for any key tags are restored.

Examples

The following command restores keys that are currently on a key server but are not stored within the key tables on the cluster. One key is missing for vserver clus- ter-1 on node1, and another key is missing for vserver datavs on node1 and node2:

```
cluster-1::> security key-manager external restore
Node: node1
            Vserver: cluster-1
         Key Server: 10.0.0.1:5696

Key ID
 ------------------------------------------------------------------------
-------
0000000000000000020000000000100a04fc7303d9abd1e0f00896192fa9c3f0000000000
000000
Node: node1
            Vserver: datavs
         Key Server: tenant.keysever:5696
Key ID
 ------------------------------------------------------------------------
-------
0000000000000000020000000000400a05a7c294a7abc1e0911897132f49c380000000000
000000
Node: node2
            Vserver: datavs
         Key Server: tenant.keysever:5696

Key ID
 ------------------------------------------------------------------------
-------
0000000000000000020000000000400a05a7c294a7abc1e0911897132f49c380000000000
000000
```

security key-manager external show-status

Show the set of configured external key management servers

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays connectivity information between ONTAP nodes and configured external key management servers.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node Name

If you specify this parameter, then the command displays the connectivity information for only the given node.

[-vserver <vserver name>] - Vserver Name

If you specify this parameter, then the command displays the key management servers for only the given Vserver.

[-key-server <Hostname and Port>] - Primary Key Server

If you specify this parameter, then the command displays the connectivity information for only the key management servers with the given primary key server host name or IP address listening on the given port.

[-key-server-status {available|not-responding|unknown}] - Overall Key Server Status

If you specify this parameter, then the command displays the connectivity information for only the key management servers with the given status.

[-status-details <text>] - Overall Key Server Status Details

If you specify this parameter, then the command displays the connectivity information for only the key management servers with the given status details.

[-operational-status {true|false}] - Overall Operational Status

If you specify this parameter, then the command displays the connectivity information for only the key management servers with the given operational status.

[-secondary-key-servers <text>,…] - Secondary Key Servers

If you specify this parameter, then the command displays the connectivity information of only the primary key management servers that have the given secondary key management servers.

[-kmip-version <text>] - KMIP version

If you specify this parameter, then the command displays the connectivity information for only the key management servers with the given KMIP protocol version.

[-port <integer>] - Key Server Port

If you specify this parameter, then the command displays the connectivity information for only the key management servers listening on the given port.

[-key-servers <text>,…] - Individual Key Servers

Use this parameter to show the host name or IP address of the key management server(s).

[-roles <text>,…] - Individual Key Server Roles

Use this parameter to show the role of the key management server(s).

[-key-server-status-list {available|not-responding|unknown}] - Individual Key Server Statuses

Use this parameter to show the status of the key management server(s).

[-status-details-list <text>,…] - Individual Key Server Status Details

Use this parameter to show the status details of the key management server(s).

Examples

The following example lists all configured key management servers for all Vservers:

```
cluster-2::*> security key-manager external show-status
Node: sti219-vsim-sr044e
             Vserver: C1_sti219-vsim-sr044e_1711266079
     Key Server Port: 12014
 KMIP is operational: true

Key Server           Role           Server Status     Reason
-------------------  ------------   ---------------   ------
10.234.2.30          primary        available         -
10.237.80.83         secondary      available         -
10.237.80.223        secondary      available         -
Node: sti219-vsim-sr044f
             Vserver: C1_sti219-vsim-sr044e_1711266079
     Key Server Port: 12014
 KMIP is operational: true

Key Server           Role           Server Status     Reason
-------------------  ------------   ---------------   ------
10.234.2.30          primary        available         -
10.237.80.83         secondary      available         -
10.237.80.223        secondary      available         -
2 entries were displayed.
```

security key-manager external show

Show the set of configured external key management servers.

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays the external key management servers configured on the cluster for a given Vserver. No entries are displayed when external key management is not enabled for the given Vserver. This command displays the primary external key management servers, along with any associated secondary key servers, configured on the cluster for a given Vserver.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver Name

If you specify this parameter, then the command displays only the key management servers for the given Vserver.

[-key-server <text>] - Key Server Name with port

If you specify this parameter, then the command displays only the key management servers with the given primary key server host name or IP address listening on the given port.

[-client-cert <text>] - Name of the Client Certificate

If you specify this parameter, then the command displays only the key management servers using a client certificate with the given name.

[-server-ca-certs <text>,…] - Names of the Server CA Certificates

If you specify this parameter, then the command displays only the key management servers using server-ca certificates with the given names.

[-timeout <integer>] - Server I/O Timeout

If you specify this parameter, then the command displays only the key management servers using the given I/O timeout.

[-username <text>] - Authentication User Name

If you specify this parameter, then the command displays only the key management servers using the given authentication username.

[-policy <text>] - Security Policy

If you specify this parameter, then the command displays only the key management servers using the given key manager policy.

[-secondary-key-servers <text>,…] - Secondary Key Servers

If you specify this parameter, then the command displays only the key management servers with the given secondary key servers.

[-create-remove-timeout <integer>] - Key Server Timeout for Create and Remove

If you specify this parameter, then the command displays only the key management servers using the given

create-remove I/O timeout.

[-enabled {true|false}] - Is Configuration Enabled?

If you specify this parameter, then the command displays only the key management servers that are enabled.

Examples

The following example lists all configured key management servers for all Vservers:

```
cluster-1::> security key-manager external show
Vserver: datavs
       Client Certificate: datavsClientCert
   Server CA Certificates: datavsServerCaCert1, datavsServerCaCert2
          Security Policy: IBM_Key_Lore
                  Enabled: true

Primary Key Server
 ------------------------------------------------------------------------
keyserver.datavs.com:5696
Vserver: cluster-1
       Client Certificate: AdminClientCert
   Server CA Certificates: AdminServerCaCert
          Security Policy:
                  Enabled: true
Primary Key Server
 ------------------------------------------------------------------------
10.0.0.10:1234
    Secondary Servers: ks1.local, ks2.local
fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234
ks1.local:1234
4 entries were displayed.
```

The following example lists all configured key management servers with more detail, including timeouts and usernames:

```
cluster-1::> security key-manager external show -instance
Vserver: datavs
       Client Certificate: datavsClientCert
   Server CA Certificates: datavsServerCaCert1, datavsServerCaCert2
       Primary Key Server: keyserver.datavs.com:5696
                  Timeout: 25
                 Username: datavsuser
            Security Policy: IBM_Key_Lore
                  Enabled: true
    Secondary Key Servers:
Vserver: cluster-1
       Client Certificate: AdminClientCert
   Server CA Certificates: AdminServerCaCert
       Primary Key Server: 10.0.0.10:1234
                  Timeout: 25
                 Username:
            Security Policy:
                  Enabled: true
    Secondary Key Servers: ks1.local, ks2.local
Vserver: cluster-1
       Client Certificate: AdminClientCert
   Server CA Certificates: AdminServerCaCert
       Primary Key Server: fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234
                  Timeout: 25
                 Username:
            Security Policy:
                  Enabled: true
    Secondary Key Servers:
Vserver: cluster-1
       Client Certificate: AdminClientCert
   Server CA Certificates: AdminServerCaCert
       Primary Key Server: ks1.local:1234
                  Timeout: 45
                 Username:
            Security Policy:
                  Enabled: true
    Secondary Key Servers:
4 entries were displayed.
```

security key-manager external aws check

Show detailed status of the AWS KMS configurations

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command displays the Amazon Web Service (AWS) Key Management Service (KMS) status.

Parameters

[-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] (privilege: advanced) }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node (privilege: advanced)

If this parameter is specified then the command displays only the AWS KMS status for the given node.

[-vserver <Vserver Name>] - Vserver Name (privilege: advanced)

If this parameter is specified then the command displays only the AWS KMS status for the given Vserver.

[-category <Categories for Cloud KMS status check>] - Component (privilege: advanced)

If this parameter is specified then the command displays only the AWS KMS status for the given category.

```
            Category                    Description
            --------                    -----------
            service_reachability        Cloud KMS Reachability
            ekmip_server                Embedded KMIP Server Reachability
            kms_wrapped_key_status      Status of KMS Wrapped Keys On
Cluster
```

[-status <Status Check>] - Status (privilege: advanced)

If this parameter is specified then the command displays only the AWS KMS status entries matching the given status.

```
            OK
            FAILED
            UNKNOWN
```

[-detail <text>] - Status Details (privilege: advanced)

This field displays a detailed status message, if available.

Examples

The example below displays the status of all components of all AWS KMS instances configured on node vsim1.

```
cluster-1::> security key-manager external aws check -node vsim1
Vserver: vs1
Node: vsim1

Category: service_reachability
              Status: OK

Category: ekmip_server
              Status: OK

Category: kms_wrapped_key_status
              Status: OK
```

security key-manager external aws disable

Disable AWS KMS

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command disables the Amazon Web Service Key Management Service (AWSKMS) associated with the given Vserver. AWSKMS cannot be disabled if it is in use by ONTAP. This command will fail if AWSKMS has not been enabled for the Vserver.

Parameters

`-vserver <Vserver Name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver on which the AWSKMS is to be disabled.

Examples

The following example disables the AWSKMS for Vserver v1.

```
cluster-1::>security key-manager external aws disable -vserver v1
```

security key-manager external aws enable

Enable AWS KMS

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command enables the Amazon Web Service Key Management Service (AWSKMS) associated with the given Vserver. An AWS project and AWSKMS must be deployed on the AWS portal prior to running this

command. AWSKMS can only be enabled on a data Vserver that doesn't already have a key manager configured. AWSKMS cannot be enabled in a MetroCluster environment.

Parameters

`-vserver <Vserver Name>` - Vserver

Use this parameter to specify the Vserver on which the AWSKMS is to be enabled.

`-region <text>` - AWS KMS Region

Use this parameter to specify the region of the deployed AWS project.

`-key-id <text>` - AWS Key Id

Use this parameter to specify the key ID of the deployed AWS project.

`[-access-key-id <text>]` - AWS Access Key ID

Use this parameter to specify the access key ID of the deployed AWS project.

`[-encryption-context <text>]` - Additional Layer of Authentication and Logging

Use this parameter to specify the encryption context to satisfy AWS grant constraint if it is configured. The parameter should be in JSON format.

Examples

The following example enables the AWSKMS for Vserver v1. The parameters in the example command identify an Amazon Web Service (AWS) project application deployed on the AWS. The AWS project application has a region "test_na_region", a key ID "test_KEYID", an access key ID "test_accessKeyID" and an encryption context of "{"team": "NVEsecurity"}".

```
cluster-1::*> security key-manager external aws enable -vserver v1 -region
test_na_region -key-id test_KEYID -access-key-id test_accessKeyID
-encryption-context {"team": "NVEsecurity"}

Enter the Amazon Web Service Key Management Service secret access key:
Press <Enter> when done
```

security key-manager external aws rekey-external

Rekey an external key of the Vserver

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command replaces the existing AWS KMS key encryption key (KEK) and results in the key hierarchy being protected by the new user specified AWS KMS KEK. Prior to running this command, the user should have already made the necessary changes on the AWS KMS Portal to use the new KEK. Upon successful completion of this command, the internal keys for the given Vserver will be protected by the new AWS KMS KEK.

Parameters

-vserver <Vserver Name> - Vserver

This parameter specifies the Vserver for which ONTAP should rekey the AWS KMS KEK

-key-id <text> - AWS Key ID

This parameter specifies the key ID of the new AWS KMS KEK that should be used by ONTAP for the provided Vserver. In the case of automatic AWS KMS KEK rotation, the key ID will be the identifier of the user's already existing AWS KMS Customer Managed Key (CMK). In the case of manual AWS KMS KEK rotation, the key ID will be the identifier of the user's new AWS KMS CMK.

Examples

The following command rekeys the AWS KMS KEK for data Vserver vs1 using a new key-id key3.

```
cluster-1::> security key-manager external aws rekey-external -vserver vs1
-key-id  key3
```

security key-manager external aws rekey-internal

Rekey an internal key of the Vserver

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command updates the internal Vserver key hierarchy by rekeying the top-level internal key encryption key (KEK). Upon successful completion of the command, all keys in the Vserver key hierarchy will be protected by the new top-level KEK.

Parameters

-vserver <Vserver Name> - Vserver (privilege: advanced)

This parameter specifies the Vserver for which ONTAP should rekey the top-level KEK

Examples

The following command rekeys the top-level KEK for data Vserver vs1.

```
cluster-1::> security key-manager external aws rekey-internal -vserver vs1
```

security key-manager external aws restore

Restore missing keys of AWS KMS

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command retrieves and restores any unrestored keys associated with the given Vserver to each node's internal key tables.

Parameters

-vserver <Vserver Name> - Vserver

This parameter specifies the Vserver to which the missing keys will be restored.

Examples

The following command restores missing keys for the data Vserver v1 (which has AWSKMS enabled) to the internal key tables on each node in the cluster.

```
cluster-1::> security key-manager external aws restore -vserver v1
```

security key-manager external aws show

Display AWS KMS configuration

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays the Amazon Web Service Key Management Service (AWSKMS) configuration for a given Vserver.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver

If you specify this parameter, then the command displays only the AWSKMS configuration for the given Vserver.

[-region <text>] - AWS KMS Region

If you specify this parameter, then the command displays only the AWSKMS configuration with the given region.

[-key-id <text>] - AWS Key ID

If you specify this parameter, then the command displays only the AWSKMS configuration with the given key-id.

[-access-key-id <text>] - AWS Access Key ID

If you specify this parameter, then the command displays only the AWSKMS configuration with the given access key ID.

[-service <text>] - AWS Service Type

If you specify this parameter, then the command displays only the AWSKMS configurations with the given AWS service type.

[-default-domain <text>] - AWS KMS Default Domain

If you specify this parameter, then the command displays only the AWSKMS configurations with the given AWS KMS default domain.

[-state {available|not-responding|unknown}] - AWS KMS Cluster State

If you specify this parameter, then the command displays only the AWSKMS configurations with the given state. The state can be either available or unknown.

[-unavailable-nodes <text>] - Names of Unavailable Nodes

If you specify this parameter, then the command displays only the AWSKMS configurations with the given unavailable-nodes.

[-polling-period <integer>] - Polling period (in minutes)

If you specify this parameter, then the command displays only the AWSKMS configurations with the given polling period.

[-port <integer>] - AWS KMS Port

If you specify this parameter, then the command displays only the AWSKMS configurations with the given AWS KMS port.

[-verify {true|false}] - Verify the AWS KMS Host

If you specify this parameter, then the command displays only the AWSKMS configurations with the given value of the verify flag.

[-verify-host {true|false}] - Verify the AWS KMS Host's Hostname

If you specify this parameter, then the command displays only the AWSKMS configurations with the given value of the verify-host flag.

[-verify-ip {true|false}] - Verify the AWS KMS Host's IP

If you specify this parameter, then the command displays only the AWSKMS configurations with the given value of the verify-ip flag.

[-host <text>] - AWS KMS Host Name

If you specify this parameter, then the command displays only the AWSKMS configurations with the given AWS KMS host name.

[-encryption-context <text>] - Additional Layer of Authentication and Logging

If you specify this parameter, then the command displays only the AWSKMS configurations with the given value of the AWS encryption-context. The parameter should be in JSON format.

Examples

The following example lists all AWSKMS configurations.

```
cluster-1::>security key-manager external aws show
            Vserver: SAMPLE_VSERVER
             Region: SAMPLE_NA_REGION

Access Key Id                                 State
--------------------------------------------  -------
SAMPLE_ACCESS_KEY_ID                          unknown
SAMPLE_ACCESS_KEY_ID_2                        unknown
Unavailable Nodes:                            node1
```

The following example lists the AWSKMS configurations that have the given encryption context of "{"team": "NVEsecurity"}".

```
cluster-1::>security key-manager external aws show -encryption-context
{"team": "NVEsecurity"}
            Vserver: SAMPLE_VSERVER
             Region: SAMPLE_NA_REGION

Access Key Id                                 State
--------------------------------------------  -------
SAMPLE_ACCESS_KEY_ID                          unknown
Unavailable Nodes:                            node1
```

security key-manager external aws update-credentials

Update AWS secret access key and access key ID

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command allows the user to update the secret access key which is used by the Amazon Web Service Key Management Service (AWSKMS) configured for the given Vserver. The secret access key is initially set by running the security key-manager external aws enable command. This command will fail if AWSKMS has not been enabled for the Vserver.

Parameters

`-vserver <Vserver Name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the AWSKMS secret access key will be updated.

-access-key-id <text> - Access Key ID (privilege: advanced)

Use this parameter to specify the new access key id of the updated credentials.

[-skip-verify {true|false}] - Don't verify user credentials (privilege: advanced)

Set this parameter to true to skip verification of the updated credentials.

Examples

The following example updates the AWSKMS secret access key for Vserver v1.

```
cluster-1::> security key-manager external aws update-credentials -vserver
v1

Enter the new secret access key: Press <Enter> when done
```

Related Links

- security key-manager external aws enable

security key-manager external azure check

Show detailed status of the enabled Azure Key Vault configurations

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command displays the Azure Key Vault (AKV) Key Management Service (KMS) status.

Parameters

[-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] (privilege: advanced) }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node (privilege: advanced)

If this parameter is specified then the command displays only the AKV status for the given node.

[-vserver <Vserver Name>] - Vserver Name (privilege: advanced)

If this parameter is specified then the command displays only the AKV status for the given Vserver.

[-category <Categories for Cloud KMS status check>] - Component (privilege: advanced)

If this parameter is specified then the command displays only the AKV status for the given category.

```
            Category                    Description
            --------                    -----------
            service_reachability        Cloud KMS Reachability
            ekmip_server                Embedded KMIP Server Reachability
            kms_wrapped_key_status      Status of KMS Wrapped Keys On
Cluster
```

[-status <Status Check>] - Status (privilege: advanced)

If this parameter is specified then the command displays only the AKV status entries matching the given status.

```
            OK
            FAILED
            UNKNOWN
```

[-detail <text>] - Status Details (privilege: advanced)

This field displays the detailed status message, if available.

Examples

The example below displays the status of all components of all AKV KMS configured on the node.

```
cluster-1::> security key-manager external azure check -node vsim1
Vserver: vs1
Node: vsim1

Category: service_reachability
              Status: OK

Category: ekmip_server
              Status: OK

Category: kms_wrapped_key_status
              Status: OK
```

security key-manager external azure create-config

Create an inactive Azure Key Vault configuration

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command creates an Azure Key Vault (AKV) configuration which can be enabled on a Vserver.

Parameters

-vserver <Vserver Name> - Vserver

The name of the Vserver.

-config-name <text> - Configuration name

The name of the configuration.

-client-id <text> - Application (Client) ID of Deployed Azure Application

The ID of the client.

-tenant-id <text> - Directory (Tenant) ID of Deployed Azure Application

The ID of the tenant.

-name {scheme://(hostname|IPv4 Address|'['IPv6 Address']')…} - Deployed Azure Key Vault DNS Name

The DNS name of the deployed AKV .

-key-id {scheme://(hostname|IPv4 Address|'['IPv6 Address']')…} - Key Identifier of AKV Key Encryption Key

The ID of the key.

[-oauth-host <text>] - Open Authorization Host Name

The hostname of the OAuth server.

[-authentication-method <AKV Authentication Method>] - Authentication Method for Azure Application

Use this parameter to specify the authentication method.

Examples

The example below creates a configuration on a node with the following details: Configuration name: sampleConfig, Client ID: client1, Tenant ID: tenant1, Deployed AKV name: https://samplevault.vault.azure.net, Key ID: https://samplevault.vault.azure.net/keys/key1/keyversion, OAuth Host: https://sampleoauth.net, for Vserver vsTest.

```
cluster-1::> security key-manager external azure create-config -config
-name sampleConfig -client-id client1 -tenant-id tenant1 -name
https://samplevault.vault.azure.net -key-id
https://samplevault.vault.azure.net/keys/key1/keyversion -oauth-host
https://sampleoauth.net -vserver vsTest
```

security key-manager external azure disable

Disable Azure Key Vault

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command disables the Azure Key Vault (AKV) associated with the given Vserver and deletes its configuration. If the AKV is in use by ONTAP, it cannot be disabled. This command is not supported if AKV has not been enabled for the Vserver.

Parameters

`-vserver <Vserver Name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver on which the AKV is to be disabled.

Examples

The following example disables the AKV for Vserver v1.

```
cluster-1::>security key-manager external azure disable -vserver v1
```

security key-manager external azure enable

Enable Azure Key Vault

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command enables the Azure Key Vault (AKV) associated with the given Vserver and creates a configuration with the name "default". An Azure application and an AKV must be deployed on the Azure portal prior to running this command. This command is not supported for the admin Vserver, or if a key manager for the given data Vserver is already enabled. This command is also not supported in a MetroCluster environment.

Parameters

`-vserver <Vserver Name>` - Vserver

Use this parameter to specify the Vserver on which the AKV is to be enabled.

`-client-id <text>` - Application (Client) ID of Deployed Azure Application

Use this parameter to specify the client (application) ID of the deployed Azure application.

`-tenant-id <text>` - Directory (Tenant) ID of Deployed Azure Application

Use this parameter to specify the tenant (directory) ID of the deployed Azure application.

-name {scheme://(hostname|IPv4 Address|'['IPv6 Address']')…} - Deployed Azure Key Vault DNS Name

Use this parameter to specify the DNS name of the deployed AKV.

[-authentication-method <AKV Authentication Method>] - Authentication Method for Azure Application

Use this parameter to specify either client_secret authentication or certificate authentication for the deployed AKV.

-key-id {scheme://(hostname|IPv4 Address|'['IPv6 Address']')…} - Key Identifier of AKV Key Encryption Key

Use this parameter to specify the key identifier of the AKV Key Encryption Key (KEK).

[-oauth-host <text>] - Open Authorization Host Name

Use this parameter to specify the host name of the Open Authorization server.

Examples

The following example enables the AKV for Vserver v1. An Azure application with client-id "4a0f9c98-c5aa-4275-abe3-2780cf2801c3", tenant-id "8e21f23a-10b9-46fb-9d50-720ef604be98", client secret (not echoed to the screen for security purposes), OAuth host at 10.12.34.1 and an AKV with DNS name "https://akv-keyvault.vault.azure.net" is deployed on the Azure portal. An AKV KEK with DNS name "https://akv-keyvault.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74" is created on the Azure portal for the AKV.

```
cluster-1::>security key-manager external azure enable -client-id
4a0f9c98-c5aa-4275-abe3-2780cf2801c3 -tenant-id 8e21f23a-10b9-46fb-9d50-
720ef604be98 -name https://akv-keyvault.vault.azure.net -key-id
https://akv-
keyvault.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74
-authentication-method client_secret -vserver v1 -oauth-host 10.12.34.1

Enter the client secret for Azure Key Vault:

Re-enter the client secret for Azure Key Vault:
```

The following example enables the AKV for Vserver v1. An Azure application with client-id "4a0f9c98-c5aa-4275-abe3-2780cf2801c3", tenant-id "8e21f23a-10b9-46fb-9d50-720ef604be98", a client certificate (not echoed to the screen for security purposes), OAuth host at 10.12.34.1 and an AKV with DNS name "https://akv-keyvault.vault.azure.net" is deployed on the Azure portal. An AKV KEK with DNS name "https://akv-keyvault.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74" is created on the Azure portal for the AKV.

```
cluster-1::>security key-manager external azure enable -client-id
4a0f9c98-c5aa-4275-abe3-2780cf2801c3 -tenant-id 8e21f23a-10b9-46fb-9d50-
720ef604be98 -name https://akv-keyvault.vault.azure.net -key-id
https://akv-
keyvault.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74
-authentication-method certificate -vserver v1 -oauth-host 10.12.34.1

Enter the client certificate for Azure Key Vault:
```

security key-manager external azure rekey-external

Rekey an external key of the Vserver

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command results in the key hierarchy being protected by the user designated AKV key encryption key (KEK). Prior to running this command, the user should have already made the necessary change on the Azure portal to use a new KEK for their key vault. The key-id used in this command is the key ID associated with the user's new AKV KEK. Upon successful completion of this command, the internal keys for the given Vserver will be protected by the new AKV KEK.

Parameters

`-vserver <Vserver Name>` - Vserver (privilege: advanced)

This parameter specifies the Vserver for which ONTAP should rekey the AKV KEK.

`-key-id {scheme://(hostname|IPv4 Address|'['IPv6 Address']')…}` - Key Identifier of a new AKV Key Encryption Key (privilege: advanced)

This parameter specifies the key id of the new AKV KEK that should be used by ONTAP for the provided Vserver.

Examples

The following command rekeys AKV KEK for data Vserver v1 using a new key, key2 with version 123456781234123412341234123456789012.

```
cluster-1::> security key-manager external azure rekey-external -vserver
v1 -key-id  https://kmip-akv-
keyvault.vault.azure.net/keys/key2/123456781234123412341234123456789012
```

security key-manager external azure rekey-internal

Rekey an internal key of the Vserver

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command rekeys the internal Vserver key hierarchy by changing the top-level internal key encryption key (KEK). Upon successful completion of the command, all keys in the Vserver key hierarchy will be protected by the new top-level KEK.

Parameters

`-vserver <Vserver Name>` - Vserver (privilege: advanced)

This parameter specifies the Vserver for which ONTAP should rekey the SVM KEK.

Examples

The following command rekeys the SVM KEK for data Vserver v1.

```
cluster-1::> security key-manager external azure rekey-internal -vserver
v1
```

security key-manager external azure restore

Restore missing keys of Azure Key Vault

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command retrieves and restores any current unrestored keys associated with the given Vserver to the nodes internal key tables. This command is not supported when AKV has not been enabled for the Vserver.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the Vserver to which the missing keys will be restored.

Examples

The following command restores missing keys for the data vserver v1 (which has AKV configuration) to the internal key tables on the cluster.

```
cluster-1::> security key-manager external azure restore -vserver v1
```

security key-manager external azure show

Display Azure Key Vaults configuration

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays the Azure Key Vault (AKV) configuration for a given Vserver.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver

If you specify this parameter, then the command displays only the AKV configuration for the given Vserver.

[-config-name <text>] - Configuration Name

If you specify this parameter, then the command displays only the AKV configurations with the given configuration name.

[-enabled {true|false}] - Is This Azure Key Vault Configuration Enabled?

If you specify this parameter, then the command displays only the AKV configurations with the given enabled value.

[-client-id <text>] - Application (Client) ID of Deployed Azure Application

If you specify this parameter, then the command displays only the AKV configuration with the given client id.

[-tenant-id <text>] - Directory (Tenant) ID of Deployed Azure Application

If you specify this parameter, then the command displays only the AKV configuration with the given tenant id.

[-name {scheme://(hostname|IPv4 Address|'['IPv6 Address']')…}] - Deployed Azure Key Vault DNS Name

If you specify this parameter, then the command displays only the AKV configuration with the given key vault name.

[-state {available|not-responding|unknown}] - Azure Key Vault Cluster State

If you specify this parameter, then the command displays only the AKV configuration with the given state. The state can be either available or unknown.

[-key-id {scheme://(hostname|IPv4 Address|'['IPv6 Address']')…}] - Key Identifier of AKV Key Encryption Key

If you specify this parameter, then the command displays only the AKV configuration with the given key id.

[-unavailable-nodes <text>] - Names of Unavailable Nodes

If you specify this parameter, then the command displays only the AKV configuration with the given unavailable-nodes.

[-authentication-method <AKV Authentication Method>] - AKV Authentication Method

If you specify this parameter, then the command displays only the AKV configurations with the given authentication method.

Examples

The following example lists all Vservers with AKV configuration.

```
cluster-1::>security key-manager external azure show
          Vserver: vs0
      Config Name: default
          Enabled: true
        Client ID: client1
        Tenant ID: tenant1
           Key ID:
https://vault.azure.net/keys/key1/9a2b8c1f7e6d5430e5f4a1b69d87c2e2
   Authentication: client_secret
             Name: https://vault.azure.net
            State: unknown
Unavailable Nodes: node-1,node-2
```

security key-manager external azure update-client-secret

(DEPRECATED)-Update client secret for Azure Key Vault

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command is deprecated and may be removed in a future release. Use security key-manager external azure update-credentials instead.

This command provides a way to update the client secret that is used for the Azure Key Vault (AKV) configured for the given Vserver. The command is initially set by running the security key-manager external azure enable command. This command is not supported if AKV has not been enabled for the Vserver.

Parameters

-vserver <Vserver Name> - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the AKV client secret is to be updated.

Examples

The following example updates the AKV client secret for the data Vserver v1.

```
cluster-1::> security key-manager external azure update-client-secret
-vserver v1

Enter new client secret:

Re-enter new client secret:
```

Related Links

- security key-manager external azure update-credentials
- security key-manager external azure enable

security key-manager external azure update-credentials

Update client credentials for an Azure Key Vault configuration

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command provides a way to update the authentication credentials that are used for an Azure Key Vault (AKV) configuration. The -config-name parameter can optionally be set to specify a specific AKV configuration of the given Vserver. If the -config-name parameter is not set, the credentials of the given Vserver's enabled configuration are updated. The credentials are initially set by running either the security key-manager external azure enable or security key-manager external azure create-config command.

Parameters

`-vserver <Vserver Name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the AKV client credentials are to be updated.

`[-config-name <text>]` - Configuration Name (privilege: advanced)

Use this parameter to specify the configuration name for which the AKV client credentials are to be updated.

`-authentication-method <AKV Authentication Method>` - Authentication Method for the Azure Application (privilege: advanced)

Use this parameter to specify the authentication method.

Examples

The following examples show different ways of updating the AKV client credentials for the data Vserver v1.

```
cluster-1::> security key-manager external azure update-credentials
-vserver v1 -authentication-method client_secret

Enter new client secret:

Re-enter new client secret:

cluster-1:> security key-manager external azure update-credentials
-vserver v1 -authentication-method certificate

Enter the client certificate for Azure Key Vault:

cluster-1:> security key-manager external azure update-credentials
-vserver v1 -config-name config10 -authentication-method certificate

Enter the client certificate for Azure Key Vault:
```

Related Links

- security key-manager external azure enable
- security key-manager external azure create-config

security key-manager external gcp check

Show detailed status of the Google Cloud KMS configurations

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command displays the Google Cloud Key Management Service (KMS) status.

Parameters

[-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] (privilege: advanced) }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node (privilege: advanced)

If this parameter is specified then the command displays only the Google Cloud KMS status for the given node.

[-vserver <Vserver Name>] - Vserver Name (privilege: advanced)

If this parameter is specified then the command displays only the Google Cloud KMS status for the given Vserver.

[-category <Categories for Cloud KMS status check>] - Component (privilege: advanced)

If this parameter is specified then the command displays only the Google Cloud KMS status for the given category.

```
            Category                    Description
            --------                    -----------
            service_reachability        Cloud KMS Reachability
            ekmip_server                Embedded KMIP Server Reachability
            kms_wrapped_key_status      Status of KMS Wrapped Keys On
Cluster
```

[-status <Status Check>] - Status (privilege: advanced)

If this parameter is specified then the command displays only the Google Cloud KMS status entries matching the given status.

```
            OK
            FAILED
            UNKNOWN
```

[-detail <text>] - Status Details (privilege: advanced)

This field displays the detailed status message, if available.

Examples

The example below displays the status of all components of all Google Cloud KMS configured on the node.

```
cluster-1::> security key-manager external gcp check -node vsim1
Vserver: vs1
Node: vsim1

Category: service_reachability
             Status: OK

Category: ekmip_server
             Status: OK

Category: kms_wrapped_key_status
             Status: OK
```

security key-manager external gcp disable

Disable a Google Cloud KMS

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command disables the Google Cloud Key Management Service (GCKMS) associated with the given Vserver. GCKMS cannot be disabled if it is in use by ONTAP. This command will fail if GCKMS has not been enabled for the Vserver.

Parameters

`-vserver <Vserver Name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver on which the GCKMS is to be disabled.

Examples

The following example disables the GCKMS for Vserver v1.

```
cluster-1::>security key-manager external gcp disable -vserver v1
```

security key-manager external gcp enable

Create and enable a Google Cloud KMS configuration

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command enables the Google Cloud Key Management Service (GCKMS) associated with the given Vserver. A GCP project and GCKMS must be deployed on the GCP portal prior to running this command. GCKMS can only be enabled on a data Vserver that doesn't already have a key manager configured. GCKMS cannot be enabled in a MetroCluster environment.

Parameters

`-vserver <Vserver Name>` - Vserver

Use this parameter to specify the Vserver on which the GCKMS is to be enabled.

`-project-id <text>` - Google Cloud KMS Project (Application) ID

Use this parameter to specify the project ID of the deployed GCP project.

`-key-ring-name <text>` - Google Cloud KMS Key Ring Name

Use this parameter to specify the key ring name of the deployed GCP project.

-key-ring-location <text> - Google Cloud KMS Key Ring Location

Use this parameter to specify the location of the key ring.

-key-name <text> - Google Cloud KMS Key Encryption Key Name

Use this parameter to specify the key name of the GCKMS Key Encryption Key (KEK).

[-port <integer>] - Google Cloud KMS Port Number

Use this parameter to specify the port of the deployed Google Cloud KMS.

[-cloudkms-host <text>] - Google Cloud KMS Host's Subdomain

Use this parameter to specify the Google Cloud KMS Host's Subdomain.

[-verify {true|false}] - Verify Identity of Google Cloud KMS?

Use this parameter to specify whether to verify the identity of Google Cloud KMS.

[-verify-host {true|false}] - Verify Identity of Google Cloud KMS's Hostname?

Use this parameter to specify whether to verify the identity of Google Cloud KMS hostname.

[-verify-ip {true|false}] - Verify Identity of Google Cloud KMS's IP Address?

Use this parameter to specify whether to verify the identity of Google Cloud KMS ip address.

[-proxy-type {http|https}] - Proxy Type

Use this parameter to specify the proxy type.

[-proxy-host <text>] - Proxy Host

Use this parameter to specify the proxy hostname.

[-proxy-port <integer>] - Proxy Port

Use this parameter to specify the proxy port.

[-proxy-username <text>] - Proxy Username

Use this parameter to specify the proxy username.

[-proxy-password <text>] - Proxy Password

Use this parameter to specify the proxy password.

[-oauth-host <text>] - Google Cloud KMS Authorization Host

Use this parameter to specify the host name of the Open Authorization server.

[-oauth-url <text>] - Google Cloud KMS Authorization Url

Use this parameter to specify the URL of the Open Authorization access token.

[-timeout <integer>] - Google Cloud Platform Connection Timeout in Seconds

Use this parameter to specify the Google Cloud connection timeout in seconds.

[-privileged-account <text>] - Google Cloud Privileged Service Account

Use this parameter to specify a privileged service account (email address) with both cloudkms.cryptoKeyVersions.useToEncrypt and cloudkms.cryptoKeyVersions.useToDecrypt permissions. If this parameter is specified, any calls made to the GCKMS will first use

iam.serviceAccounts.getAccessToken to impersonate the privileged account.

Examples

The following example enables the GCKMS for Vserver v1. The parameters in the example command identify a Google Cloud Platform (GCP) project application deployed on the GCP. The GCP project application has a Project ID "test_project", a key ring name "key_ring_for_test_project", a key ring location "secure_location_for_key_ring", a key name "testKEK" and OAuth server at 10.12.34.1.

```
cluster-1::*> security key-manager external gcp enable -vserver v1
-project-id test_project -key-ring-name key_ring_for_test_project -key
-ring-location secure_location_for_key_ring -key-name testKEK -oauth-host
10.12.34.1

Enter the contents of the Google Cloud Key Management Service account key
file (json file): Press <Enter> when done
```

security key-manager external gcp rekey-external

Rekey an external key of the Vserver

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command replaces the existing GCP key encryption key (KEK) and results in the key hierarchy being protected by the user specified GCP KEK. The GCP key ring in use by the GCP Portal should be updated to use the new KEK prior to running this command. Upon successful completion of this command, the internal keys for the given Vserver will be protected by the new GCP KEK.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the Vserver for which ONTAP should rekey the GCP KEK.

`-key-name <text>` - Google Cloud KMS Key Encryption Key Name

This parameter specifies the key name of the new GCP KEK that should be used by ONTAP for the provided Vserver.

`[-project-id <text>]` - Google Cloud KMS Project (Application) ID

This parameter specifies the new project ID of the new GCP KEK that should be used by ONTAP for the provided Vserver.

`[-key-ring-name <text>]` - Google Cloud KMS Key Ring Name

This parameter specifies the new key ring name of the new GCP KEK that should be used by ONTAP for the provided Vserver.

[-key-ring-location <text>] - Google Cloud KMS Key Ring Location

This parameter specifies the new key ring location of the new GCP KEK that should be used by ONTAP for the provided Vserver.

Examples

The following command rekeys GCP KEK for data Vserver v1 using a new key-name key1.

```
cluster-1::> security key-manager external gcp rekey-external -vserver v1
-key-name key1
```

security key-manager external gcp rekey-internal

Rekey an internal key of the Vserver

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command rekeys the internal Vserver key hierarchy by changing the SVM key encryption key (KEK). Upon successful completion of the command, all keys in the Vserver key hierarchy will be protected by the new top-level KEK.

Parameters

-vserver <Vserver Name> - Vserver (privilege: advanced)

This parameter specifies the Vserver for which ONTAP should rekey the SVM KEK.

Examples

The following command rekeys the SVM KEK for data Vserver v1.

```
cluster-1::> security key-manager external gcp rekey-internal -vserver v1
```

security key-manager external gcp restore

Restore missing keys of a Google Cloud KMS

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command retrieves and restores any unrestored keys associated with the given Vserver to each node's internal key tables.

Parameters

-vserver <Vserver Name> - Vserver

This parameter specifies the Vserver to which the missing keys will be restored.

Examples

The following command restores missing keys for the data Vserver v1 (which has GCKMS enabled) to the internal key tables on each node in the cluster.

```
cluster-1::> security key-manager external gcp restore -vserver v1
```

security key-manager external gcp show

Display Google Cloud KMS configuration

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays the Google Cloud Key Management Service (GCKMS) configuration.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver

If you specify this parameter, then the command displays only the GCKMS configurations for the given Vserver.

[-project-id <text>] - Google Cloud KMS Project (Application) ID

If you specify this parameter, then the command displays only the GCKMS configurations with the given project id.

[-key-ring-name <text>] - Google Cloud KMS Key Ring Name

If you specify this parameter, then the command displays only the GCKMS configurations with the given key ring name.

[-key-ring-location <text>] - Google Cloud KMS Key Ring Location

If you specify this parameter, then the command displays only the GCKMS configurations with the given key ring location.

[-key-name <text>] - Google Cloud KMS Key Encryption Key Name

If you specify this parameter, then the command displays only the GCKMS configurations with the given key name.

[-state {available|not-responding|unknown}] - Google Cloud KMS Cluster State

If you specify this parameter, then the command displays only the GCKMS configurations with the given state. The state can be either available or unknown.

[-unavailable-nodes <text>] - Names of Unavailable Nodes

If you specify this parameter, then the command displays only the GCKMS configurations with the given unavailable-nodes.

[-privileged-account <text>] - Google Cloud Privileged Service Account

If you specify this parameter, then the command displays only the GCKMS configurations with the given privileged account.

[-caller-account <text>] - Google Cloud Caller Service Account

If you specify this parameter, then the command displays only the GCKMS configurations with the given caller account.

Examples

The following example lists all Vservers with GCKMS configuration.

```
cluster-1::>security key-manager external gcp show
            Vserver: SAMPLE_VSERVER
         Project ID: SAMPLE_PROJECT_ID
  Key Ring Location: SAMPLE_KEY_RING_LOCATION
           Key Name: SAMPLE_KEY_NAME
     Caller Account: SAMPLE@CALLER.COM
 Privileged Account: SAMPLE@PRIVILEGED.COM

Key Ring Name                                 State
--------------------------------------------  -------
SAMPLE_KEY_RING_NAME                          unknown
Unavailable Nodes:                            node1
```

security key-manager external gcp update-credentials

Update Google Cloud Project's Service Account Credentials

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command allows the user to update the application credential which is used by the Google Cloud Key Management Service (GCKMS) configured for the given Vserver. The application credential is initially set by running the security key-manager external gcp enable command. This command will fail if GCKMS has not

been enabled for the Vserver.

Parameters

`-vserver <Vserver Name>` - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the GCKMS application credential will be updated.

Examples

The following example updates the GCKMS application credential for the data Vserver v1.

```
cluster-1::> security key-manager external gcp update-credentials -vserver
v1

Enter the new application credential: Press <Enter> when done
```

Related Links

- security key-manager external gcp enable

security key-manager health policy modify

Modify the health monitor policy of the given keystore-type

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

This command modifies the health monitor policy

Parameters

`-keystore-type <Key Store Type>` - Keystore Type

Use this parameter to specify the keystore-type of the health monitor policy to be updated.

`[-enabled {true|false}]` - Health Monitor Enabled?

Use this parameter to specify if the health monitor is enabled.

`[-manage-volume-offline {true|false}]` - Automatically Manage Volume Offline?

Use this parameter to specify if the health monitor can automatically offline the volumes if the key manager cannot be reached.

Examples

The following example updates the AWS 'keystore-type' health monitor policy "enabled" and "manage-volume-offline" values.

```
cluster-1::> security key-manager health policy modify -keystore-type AWS
-enabled false -manage-volume-offline false
```

security key-manager health policy show

Show the health monitor policy of the given keystore-type

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

This command displays the health monitor policies

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-keystore-type <Key Store Type>] - Keystore Type

If you specify this parameter, then the command displays only the health monitor policies with the given keystore-type value.

[-enabled {true|false}] - Health Monitor Enabled?

If you specify this parameter, then the command displays only the health monitor policies with the given enabled value.

[-manage-volume-offline {true|false}] - Automatically Manage Volume Offline?

If you specify this parameter, then the command displays only the health monitor policies with the given manage-volume-offline value.

Examples

The following example lists all health monitor policies.

```
cluster-1::> security key-manager health policy show
              Health Monitor Automatically Manage
Keystore Type Enabled?       Volume Offline?
------------- -------------- --------------------
OKM           true           false
KMIP          true           false
AKV           true           true
GCP           true           false
AWS           true           false
IKP           true           true
6 entries were displayed.
```

security key-manager key create

Create a new authentication key

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

This command creates a new authentication key (AK) and stores it on the the admin Vserver's key management servers. The command fails if the configured key management servers are already storing more than 256 AKs. If this command fails because there are more than 256 AKs in the cluster, delete unused keys on the Vserver's key management servers and retry the command. This command is not supported when external key management is not enabled for the admin Vserver.

Parameters

[-key-tag <text>] - Key Tag

This parameter specifies the key tag to associate with the new authentication key (AK). The default value is the node name. This parameter can be used to help identify created authentication keys (AKs). For example, the security key-manager key query command's key-tag parameter can be used to query for a specific key-tag value.

[-prompt-for-key {true|false}] - Prompt for Authentication Passphrase

If you specify this parameter as true, then the command prompts you to enter an authentication passphrase manually instead of generating it automatically. For security reasons, the authentication passphrase you entered is not displayed at the command prompt. You must enter the authentication passphrase a second time for verification. To avoid errors, copy and paste authentication passphrases electronically instead of entering them manually. ONTAP saves the resulting authentication key/key ID pair automatically on the configured key management servers.

Examples

The following example creates an authentication key with the node name as the default key-tag value:

```
cluster-1::> security key-manager key create
Key ID:
00000000000000000200000000000100d0f7c2462d626b739fe81b89f29a092f0000000000
000000
```

The following example creates an authentication key with a user-specified authentication passphrase:

```
cluster-1::> security key-manager key create -prompt-for-key true
Enter a new passphrase:
Reenter the passphrase:
Key ID:
00000000000000000200000000000100626833 3f870860128fbe17d393e5083b0000000000
000000
```

Related Links

- security key-manager key query

security key-manager key delete

Delete an existing authentication key

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

This command removes an authentication key from the configured key management servers on the admin Vserver. The command fails if the given key is currently in use by ONTAP. This command is not supported when external key management is not enabled for the admin Vserver.

Parameters

`-key-id <Hex String>` - Authentication Key ID (privilege: advanced)

Use this parameter to specify the key ID of the key that you want to remove.

Examples

The following example deletes an authentication key:

```
cluster-1::*> security key-manager key delete -key-id
00000000000000000200000000000100626833 3f870860128fbe17d393e5083b0000000000
000000
```

security key-manager key migrate

Migrate keys from the admin Vserver's the Onboard Key Manager to a data Vserver's external key manager and vice versa

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

This command provides a mechanism to migrate the existing keys of a data Vserver from the admin Vserver's key manager to their own key manager or vice versa. The keys stay the same and the data is not rekeyed, only the keys are migrated from one Vserver's key manager to another. After a successful migration to the new key manager, the data Vserver keys are deleted from the previous key manager.

Parameters

`-from-vserver <vserver name>` - Vserver Name (privilege: advanced)

Use this parameter to specify the name of the Vserver whose key manager the keys are migrated from.

`-to-vserver <vserver name>` - Vserver Name (privilege: advanced)

Use this parameter to specify the name of the Vserver whose key manager the keys are migrated to.

Examples

The following example migrates the keys of "datavs" data Vserver from "cluster-1" admin Vserver's key manager to "datavs" data Vserver's key manager:

```
cluster-1::> security key-manager key migrate -from-vserver cluster-1 -to
-vserver datavs
```

The following example migrates the keys of "datavs" data Vserver from "datavs" data Vserver's key manager to "cluster-1" admin Vserver's key manager:

```
cluster-1::> security key-manager key migrate -from-vserver datavs -to
-vserver cluster-1
```

security key-manager key query

Display the key IDs.

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays the IDs of the keys that are stored in the configured key managers. This command does not update the key tables on the node. Primary key servers, along with any associated secondary key servers, are displayed in the output.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node

Use this parameter to specify the name of the node that queries the specified key management servers. If this parameter is not specified, then all nodes query the specified key management servers.

[-vserver <vserver name>] - Vserver Name

Use this parameter to specify the Vserver for which to list the keys.

[-key-server <Hostname and Port>] - Key Server

This parameter specifies the host and port of the key management server that you want to query. This parameter is used only with external key managers.

[-key-id <Hex String>] - Key Identifier

If you specify this parameter, then the command displays only the key IDs that match the specified value.

[-key-tag <text>] - Key Tag

If you specify this parameter, then the command displays only the key IDs that match the specified value. The key-tag for Volume Encryption Keys (VEKs) is set to the UUID of the encrypted volume.

[-key-type <Key Usage Type>] - Key Type

If you specify this parameter, then the command displays only the key IDs that match the specified value.

[-restored {true|false}] - Restored

This parameter specifies whether the key corresponding to the displayed key ID is present in the specified node's internal key table. If you specify 'true' for this parameter, then the command displays the key IDs of only those keys that are present in the system's internal key table. If you specify 'false' for this parameter, then the command displays the key IDs of only those keys that are not present in the system's internal key table.

[-key-store <Key Store>] - Key Store

Use this parameter to specify the key manager type from which to list the keys.

[-key-user <vserver name>] - Key User

If you specify this parameter, then the command displays only the key IDs that are used by the specified Vserver.

[-key-manager <text>] - Key Manager

This parameter specifies the identity of the key manager. For external key managers that will be the host and the port of the key server. In other cases that will be the name of a corresponding key manager.

[-key-store-type <Key Store Type>] - Key Store Type

If you specify this parameter, then the command displays only the key IDs that are used by the specified key manager type.

[-crn <text>] - Cloud Resource Name

This parameter specifies the Cloud Resource Name (CRN) of the key. If you specify this parameter, then the command displays only the key IDs that contains such CRN.

[-policy <text>] - Key Store Policy

This optional parameter specifies the policy name of the key manager. If you specify this parameter, then the command displays only the key IDs that are associated with the specified policy.

[-encryption-algorithm <text>] - Encryption algorithm for the key

This optional parameter specifies the encryption algorithm of the key. If you specify this parameter, then the command displays only the keys of the specified algorithm type.

Examples

The following example shows all of the keys on all configured key servers, and whether or not those keys have been restored for all nodes in the cluster:

```
cluster-1::> security key-manager key query
Node: node1
            Vserver: cluster-1
        Key Manager: onboard
   Key Manager Type: OKM

Key Tag                                  Key Type Encryption   Restored
---------------------------------------  -------- ------------ --------
node1                                    NSE-AK   AES-256      true
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000000
000000
node1                                    NSE-AK   AES-256      true
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000000
000000
node1                                    NSE-AK   AES-256      true
    Key ID:
000000000000000002000000000001100e1f6b27094485d2d74408bca673b25eb0000000000
000000
node1                                    NSE-AK   AES-256      true
    Key ID:
000000000000000002000000000001100ea73be83ec42a7a2bd262f369cda83a40000000000
000000
Node: node1
            Vserver: datavs
```

```
        Key Manager: keyserver.datavs.com:5965
   Key Manager Type: KMIP

Key Tag                                  Key Type Encryption   Restored
---------------------------------------  -------- ------------ --------
eb9f8311-e8d8-487e-9663-7642d7788a75  VEK      XTS-AES-256  true
    Key ID:
000000000000000002000000000004001cb18336f7c8223743d3e75c6a7726e0000000000
000000
9d09cbbf-0da9-4696-87a1-8e083d8261bb  VEK      XTS-AES-256  true
    Key ID:
000000000000000002000000000004064f2e1533356a470385274a9c3ffb9770000000000
000000
40c3546e-600c-401c-b312-f01be52258dd  VEK      XTS-AES-256  true
    Key ID:
000000000000000002000000000000401e6f2b09744582d74d084cb6a372be5b0000000000
000000
9b195ecb-35ee-4d11-8f61-15a8de377ad7  VEK      XTS-AES-256  true
    Key ID:
000000000000000002000000000000040ea73be83ec42a7a2bd262f369cda83a40000000000
000000
Node: node2
            Vserver: cluster-1
        Key Manager: onboard
   Key Manager Type: OKM

Key Tag                                  Key Type Encryption   Restored
---------------------------------------  -------- ------------ --------
node1                                    NSE-AK   AES-256      true
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000000
000000
node1                                    NSE-AK   AES-256      true
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000000
000000
node1                                    NSE-AK   AES-256      true
    Key ID:
000000000000000002000000000000100e1f6b27094485d2d74408bca673b25eb0000000000
000000
node1                                    NSE-AK   AES-256      true
    Key ID:
000000000000000002000000000000100ea73be83ec42a7a2bd262f369cda83a40000000000
000000
Node: node2
            Vserver: datavs
```

```
         Key Manager: keyserver.datavs.com:5965
    Key Manager Type: KMIP

Key Tag                                  Key Type Encryption   Restored
---------------------------------------  -------- ------------ --------
eb9f8311-e8d8-487e-9663-7642d7788a75  VEK      XTS-AES-256  true
    Key ID:
00000000000000000200000000000004001cb18336f7c8223743d3e75c6a7726e0000000000
000000
9d09cbbf-0da9-4696-87a1-8e083d8261bb  VEK      XTS-AES-256  true
    Key ID:
00000000000000000200000000000004064f2e1533356a470385274a9c3ffb9770000000000
000000
40c3546e-600c-401c-b312-f01be52258dd  VEK      XTS-AES-256  true
    Key ID:
00000000000000000200000000000401e6f2b09744582d74d084cb6a372be5b0000000000
000000
9b195ecb-35ee-4d11-8f61-15a8de377ad7  VEK      XTS-AES-256  true
    Key ID:
00000000000000000200000000000040ea73be83ec42a7a2bd262f369cda83a40000000000
000000
```

security key-manager key key-table create

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

This command creates an entry in the key manager key table. It does not create a new key.

Parameters

-key-id <Hex String> - Key ID

This parameter specifies the key ID of the new entry in the table.

-key-type <Key Usage Type> - Key Usage Type

This parameter specifies the key type of the new entry. The following key types are supported: NSE-AK, AEK, VEK, NEK and SVM-KEK.

-encryption-algorithm <text> - Encryption Algorithm For The Key

This parameter specifies the encryption algorithm associated with the key.

-creation-time <MM/DD/YYYY HH:MM:SS> - Key Creation Time

This parameter specifies the date and time that the key was created. The date and time format is "MM/DD/YYYY HH:MM:SS".

Examples

The following example creates an entry in the table:

```
cluster-1::> security key-manager key key-table create -key-id
00000000000000000200000000000500e9ccf3f08e7533d9cd0298e1ebe6c1000000000000
000000 -key-type SVM-KEK -encryption-algorithm AES-256 -creation-time
01/01/2022 01:01:59

cluster-1::> security key-manager key key-table show

Key ID
Key Type Encryption   Creation Time
------------------------------------------------------------------------
------- -------- ------------ --------------------
00000000000000000200000000000500e9ccf3f08e7533d9cd0298e1ebe6c1000000000000
000000  SVM-KEK  AES-256      1/1/2022 01:01:59
1 entry was displayed.
```

security key-manager key key-table delete

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

This command removes an entry from the key table.

Parameters

-key-id <Hex String> - Key ID

Use this parameter to specify the key ID of the entry that you want to remove from the key table.

Examples

The following example deletes an entry from the key table:

```
cluster-1::> security key-manager key key-table show

Key ID
Key Type Encryption   Creation Time
------------------------------------------------------------------------
------- -------- ------------ --------------------
00000000000000000200000000000100239c17902e7515ed397892f75f52e38e0000000000
000000  NSE-AK   AES-256      2/8/2022 10:54:46
00000000000000000200000000000a00a7af571b8397e7df297128fdeb83f4ba0000000000
000000  SVM-KEK  AES-256      1/1/2022 01:01:59
2 entries were displayed.

cluster-1::*> security key-manager key key-table delete -key-id
00000000000000000200000000000100239c17902e7515ed397892f75f52e38e0000000000
000000

cluster-1::> security key-manager key key-table show

Key ID
Key Type Encryption   Creation Time
------------------------------------------------------------------------
------- -------- ------------ --------------------
00000000000000000200000000000a00a7af571b8397e7df297128fdeb83f4ba0000000000
000000  SVM-KEK  AES-256      1/1/2022 01:01:59
1 entry was displayed.
```

security key-manager key key-table modify

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

This command modifies an entry in the key table. Changes made using this command do not affect the key; only the table entry is modified, not the key itself.

Parameters

-key-id <Hex String> - **Key ID**

This parameter specifies the key ID of the entry to be modified.

[-key-type <Key Usage Type>] - **Key Usage Type**

If this optional parameter is specified, the key type field is modified accordingly.

[-encryption-algorithm <text>] - Encryption Algorithm For The Key

If this optional parameter is specified, the encryption algorithm field is modified accordingly.

[-creation-time <MM/DD/YYYY HH:MM:SS>] - Key Creation Time

If this optional parameter is specified, the creation time field is modified accordingly.

Examples

The following example shows the key table before and after the modify command:

```
cluster-1::> security key-manager key key-table show

Key ID
Key Type Encryption   Creation Time
------------------------------------------------------------------------------
------- -------- ------------ --------------------
00000000000000000200000000000500e9ccf3f08e7533d9cd0298e1ebe6c1190000000000
000000  VEK      XTS-AES-256  1/1/2022 10:00:00

cluster-1::> security key-manager key key-table modify -key-id
00000000000000000200000000000500e9ccf3f08e7533d9cd0298e1ebe6c1190000000000
000000 -creation-time "12/25/2022 00:00:00"

cluster-1::> security key-manager key key-table show

Key ID
Key Type Encryption   Creation Time
------------------------------------------------------------------------------
------- -------- ------------ --------------------
00000000000000000200000000000500e9ccf3f08e7533d9cd0298e1ebe6c1190000000000
000000  VEK      XTS-AES-256  12/25/2022 00:00:00
```

security key-manager key key-table show

Display details of a specific key ID.

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

This command displays date and time information for all keys.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified

field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-key-id <Hex String>] - Key ID

If this parameter is specified, the command displays the key that has the specified key ID.

[-key-type <Key Usage Type>] - Key Usage Type

If this parameter is specified, the command only displays information about keys with the specified key type.

[-encryption-algorithm <text>] - Encryption Algorithm For The Key

If this parameter is specified, the command only displays information about keys with the specified encryption algorithm.

[-creation-time <MM/DD/YYYY HH:MM:SS>] - Key Creation Time

If this parameter is specified, the command displays only information about keys with the specified creation time.

Examples

The following example shows all date and time information for all keys:

```
cluster-1::> security key-manager key key-table show

Key ID
Key Type Encryption   Creation Time
------------------------------------------------------------------------------
------- -------- ------------ --------------------
00000000000000000200000000000000f3ee496cd5820cfb76dd2ce3fa7661b00000000000
000000  NSE-AK   AES-256      1/30/2022 04:21:40
00000000000000000200000000000100658779529aa57ddfef953f305b16c7b20000000000
000000  NSE-AK   AES-256      1/30/2022 04:21:40
00000000000000000200000000000005004100a4355062ea078fdc2fc16b2018d70000000000
000000  VEK      XTS-AES-256  1/30/2022 04:23:14
00000000000000000200000000000a0059f8f7f92612e85664630eed8fb855170000000000
000000  SVM-KEK  AES-256      1/30/2022 04:23:14
4 entries were displayed.
```

security key-manager keystore delete

Remove a disabled key manager keystore configuration.

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command is used to delete keystore configurations. Only keystore configurations that are not enabled can be deleted. Use the security key-manager keystore show -enable false command to see a list of all the keystore configurations that are not enabled.

Parameters

-vserver <Vserver Name> - Vserver

If you specify this parameter, then the command deletes only the keystore configurations with the given Vserver.

-keystore-type <Key Store Type> - Keystore Type

If you specify this parameter, then the command deletes only the keystore configurations with the given keystore type. This command only deletes keystore configurations with a keystore type of Azure Key Vault (AKV).

-config-name <text> - Configuration Name

If you specify this parameter, then the command deletes only the keystore configurations with the given configuration name.

Examples

The following example deletes all keystore configurations with the name "NewConfig" that are not enabled.

```
Cluster-1::*> security key-manager keystore delete -vserver * -keystore
-type * -config-name NewConfig
1 entry was deleted.

Cluster-1::*>
```

The following example deletes the keystore configuration on Vserver vs0 with a keystore type AKV and "NewConfig" configuration name.

```
Cluster-1::*> security key-manager keystore delete -vserver vs0 -keystore
-type AKV -config-name NewConfig
1 entry was deleted.

Cluster-1::*>
```

The following example attempts and fails to delete an enabled keystore configuration.

```
Cluster-1::*> security key-manager keystore delete -vserver vs0 -keystore
-type AKV -config-name default

Error: command failed: The keystore configuration with name "default" and
       keystore type "AKV" is currently enabled for Vserver "vs0" and
cannot be
       deleted.

Cluster-1::*>
```

Related Links

- security key-manager keystore show

security key-manager keystore enable

Enable or switch to an inactive keystore configuration

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command enables the keystore represented by the supplied Vserver, keystore-type, and config-name combination. If the specified Vserver already has a keystore enabled, then the enabled configuration is switched to the desired keystore configuration and the previous configuration is left in an inactive/disabled state.

Parameters

-vserver <vserver name> - Vserver Name

Use this parameter to specify the Vserver of the desired configuration.

-keystore-type <Key Store Type> - Keystore Type

Use this parameter to specify the keystore type of the desired configuration.

-config-name <text> - Configuration Name

Use this parameter to specify the configuration name of the desired configuration.

Examples

The following example enables a configuration named sampleConfig for the configured AKV on Vserver vsTest.

```
cluster-1::> security key-manager keystore enable -vserver vsTest
-keystore-type AKV -config-name sampleConfig
```

The following example switches the configuration on Vserver vsTest to a new keystore configuration named newConfig.

```
cluster-1::> security key-manager keystore enable -vserver vsTest
-keystore-type AKV -config-name newConfig
```

security key-manager keystore show

Displays the configured key manager keystores.

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays all keystore configurations.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver

If you specify this parameter, then the command displays only the keystore configurations with the given Vserver.

[-keystore-type <Key Store Type>] - Keystore Type

If you specify this parameter, then the command displays only the keystore configurations with the given keystore type.

[-config-name <text>] - Configuration Name

If you specify this parameter, then the command displays only the keystore configurations with the given configuration name.

[-enabled {true|false}] - Configuration Is Enabled?

If you specify this parameter, then the command displays only the keystore configurations with the given enabled value.

[-uuid <UUID>] - Key Store UUID

If you specify this parameter, then the command displays only the keystore configuration with the given universal unique identifier (UUID) value.

[-state <Key Store state>] - Key Store State

If you specify this parameter, then the command displays only the keystores with the given state.

Examples

The following example lists all keystore configurations.

```
Cluster-1::*> security key-manager keystore show

Vserver                 Keystore Type  Config Name        Enabled
----------------------- -------------- ------------------ -------
Cluster-1               OKM            default            true
vs0                     AKV            default            true
vs0                     AKV            AKV-Config-1       false
vs1                     AKV            AWS-Config-1       true
4 entries were displayed.
```

The following example lists only the keystore configurations that are enabled.

```
Cluster-1::*> security key-manager keystore show -enabled true

Vserver                 Keystore Type  Config Name        Enabled
----------------------- -------------- ------------------ -------
Cluster-1               OKM            default            true
vs0                     AKV            default            true
vs1                     AKV            AWS-Config-1       true
3 entries were displayed.
```

security key-manager onboard create-config

Add an inactive Onboard Key Manager

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

This command enables an ONTAP administrator to create an inactive configuration for the named Vserver. This facilitates the switching between the Onboard Key Manager (OKM) and an external key manager (EKM) without migrating the keys to a data SVM.

Parameters

Examples

The following example creates an inactive configuration for the Onboard Key Manager:

```
cluster-1::*> security key-manager onboard create-config
```

security key-manager onboard disable

Disable the Onboard Key Manager

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

This command disables the Onboard Key Manager associated with the admin Vserver and permanently deletes the Onboard Key Manager configuration associated with the admin Vserver. The Onboard Key Manager cannot be disabled if there are any encrypted volumes that use encryption keys created by the Onboard Key Manager. This command fails if the Onboard Key Manager is not enabled.

Examples

The following example disables the Onboard Key Manager for the admin Vserver:

```
cluster-1::*> security key-manager onboard disable

Warning: This command will permanently delete all keys from Onboard Key
         Manager.
Do you want to continue? {y|n}: y
```

security key-manager onboard enable

Enable the Onboard Key Manager

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

This command enables the Onboard Key Manager for the admin Vserver.

Parameters

`[-cc-mode-enabled {yes|no}]` - Enable Common Criteria Mode?

Use this parameter to specify whether the Common Criteria (CC) mode should be enabled or not. When CC mode is enabled, you are required to provide a cluster passphrase that is between 64 and 256 ASCII characters long, and you are required to enter that passphrase each time a node reboots. CC mode cannot be enabled in a MetroCluster configuration.

`[-are-unencrypted-metadata-volumes-allowed-in-cc-mode {yes|no}]` - Are Unencrypted Metadata Volumes Allowed in Common Criteria Mode

If Common Criteria (CC) mode is enabled this parameter allows unencrypted metadata volumes to exist. These metadata volumes are created internally during normal operation. Examples are volumes created during SnapMirror and Vserver migrate operations. the default value is *`no`* .

Examples

The following example enables the Onboard Key Manager for the admin Vserver cluster-1:

```
cluster-1::> security key-manager onboard enable

Enter the cluster-wide passphrase for the Onboard Key Manager:

Re-enter the cluster-wide passphrase:

After configuring the Onboard Key Manager, save the encrypted
configuration data in a safe location so that you can use it if you need
to perform a manual recovery operation. To view the data, use the
"security key-manager onboard show-backup" command.
```

The following example enables the Onboard Key Manager for the admin Vserver cluster-1 with the cluster-wide passphrase "myPassphrase" on an external USB mass storage device:

```
cluster-1::> security key-manager onboard enable -vserver cluster-1 -okm
-on-usb-enabled true -onboard-passphrase myPassphrase

Enter the cluster-wide passphrase for the Onboard Key Manager:

Re-enter the cluster-wide passphrase:
After configuring the Onboard Key Manager, save the encrypted
configuration data in a safe location so that you can use it if you need
to perform a manual recovery operation. To view the data, use the
"security key-manager onboard show-backup" command.
```

security key-manager onboard show-backup

Display the Onboard Key Management backup

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays the backup information for the Onboard Key Manager for the admin Vserver, which can be used to recover the cluster in case of catastrophic situations. The information displayed is for the cluster as a whole (not individual nodes).

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

Examples

The following example displays the Onboard Key Manager backup data for the admin Vserver:

```
cluster-1::> security key-manager onboard show-backup
--------------------------BEGIN BACKUP--------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAAAA
IgAAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAAAAACQAAAAAAAAAAAgAAAAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJs
b2IAAQAAAAMAAAAYAQAAAAAAADA5/
ccAAAAAIgAAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAAAJAGr3t
JA/LRzUQRHwv+1aWvAAAAAAAAAAAAACIAAAAAAAAAAAKAAAAAAAAAAAACI8z/
bAAAAAAAAAAAAAAAAAgAAAAAAAAQAbxMcI4qiaMS4Uts5tTUnUAAAAAAAAAAAAkAAA
AAAAAAIAAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5SmyjLSgoK/
qc8FAmMMcrRXY6uriulnL0WPB/
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBL
ZXkgQmxvYgABAAAAAwAAABgBAAAAAAAAA1cNLLwAAAAAiAAAAAAAAAAACgAAAAAAAAAAA
Q5NxHQAAAAAAAAAAAAAAAAIAAAAAAAAAkAave0kD8tHNRBEfC/
7Vpa8AAAAAAAAAAAAIgAAAAAAAAAAAoAAAAAAAAAAAJ4/
cQsAAAAAAAAAAAAAAAACAAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAACQA
AAAAAAAAgAAAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rr
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA
---------------------------END BACKUP---------------------------
```

security key-manager onboard sync

Sync the Onboard Key Manager keys

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

This command synchronizes missing onboard keys on any node in the cluster. For example, if you add a node to a cluster that has the Onboard Key Manager configured, you should then run this command to synchronize the keys. In a MetroCluster configuration, if the security key-manager onboard enable command is used to enable the Onboard Key Manager on one site, then run the `security key-manager onboard sync` command on the partner site. In a MetroCluster configuration, if the security key-manager onboard update-passphrase command is used to update the passphrase on one site, then run this command with the new passphrase on the partner site before proceeding with any key management operations.

Parameters

Examples

The following example synchronizes the Onboard Key Manager key database across all nodes in the cluster. In a MetroCluster configuration, this command synchronizes nodes in the local site.

```
cluster-1::> security key-manager onboard sync
```

Related Links

- security key-manager onboard enable
- security key-manager onboard update-passphrase

security key-manager onboard update-passphrase

Update the Onboard Key Manager Passphrase

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

This command provides a way to update the cluster-wide passphrase that is used for the Onboard Key Manager and initially created by running the security key-manager onboard enable command. This command prompts for the existing passphrase, and if that passphrase is correct then the command prompts for a new passphrase. When the Onboard Key Manager is enabled for the admin Vserver, run the security key-manager onboard show-backup command after updating the passphrase and save the output for emergency recovery scenarios. When the `security key-manager onboard update-passphrase` command is executed in a MetroCluster configuration, then run the security key-manager onboard sync command with the new passphrase on the partner site before proceeding with any key-manager operations. This allows the updated passphrase to be replicated to the partner site.

Parameters

Examples

The following example updates the cluster-wide passphrase used for the Onboard Key Manager:

```
cluster-1::*> security key-manager onboard update-passphrase

Warning: This command will reconfigure the cluster passphrase for onboard
         key management.
Do you want to continue? {y|n}: y

Enter current passphrase:

Enter new passphrase:

Reenter the new passphrase:
Update passphrase has completed. Save the new encrypted configuration data
in
a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the "security key-manager onboard show-
backup"
command.
```

Related Links

- security key-manager onboard enable
- security key-manager onboard show-backup
- security key-manager onboard sync

security key-manager onboard verify-backup

Verify the onboard key management backup and its passphrase

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command verifies the backup data and the passphrase of the Onboard Key Manager for the admin Vserver.

Examples

The following example displays the verification of the onboard key management backup data for the admin Vserver:

```
cluster-1::> security key-manager onboard verify-backup

Enter the Onboard Key Manager backup data:
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAACgAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAAAACQAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJs
b2IAAQAAAAMAAAAYAQAAAAAAADA5/
ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3t
JA/LRzUQRHwv+1aWvAAAAAAAAAAAACIAAAAAAAAAKAAAAAAAAAACI8z/
bAAAAAAAAAAAAAAAAAgAAAAAAAAQAbxMcI4qiaMS4Uts5tTUnUAAAAAAAAAAAAkAAA
AAAAAAIAAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5SmyjLSgoK/
qc8FAmMMcrRXY6uriulnL0WPB/
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBL
ZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA1cNLLwAAAAAiAAAAAAAAACgAAAAAAAAA
Q5NxHQAAAAAAAAAAAAAAAAIAAAAAAAkAave0kD8tHNRBEfC/
7Vpa8AAAAAAAAAAAIgAAAAAAAAAoAAAAAAAAAJ4/
cQsAAAAAAAAAAAAAAAACAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAACQA
AAAAAAAAgAAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rr
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

Enter the cluster-wide passphrase for the Onboard Key Manager:

The Onboard Key Manager backup data was successfully verified
```

security key-manager policy show

Display key manager policy

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

This command displays the defined key management key policies.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-policy <text>] - Policy name

If you specify this parameter, then the command will list the key manager policy with the given name.

[-check-key-on-online {true|false}] - Pull key from key manager during volume online?

If you specify this parameter, then the command displays only the key manager policies with the given check-key-on-online value.

[-purge-key-on-offline {true|false}] - Purge key from memory during volume offline?

If you specify this parameter, then the command displays only the key manager policies with the given purge-key-on-offline value.

[-support-on-admin-vserver {true|false}] - Support policy on admin Vserver?

If you specify this parameter, then the command displays only the key manager policies with the given support-on-admin-vserver value.

[-key-manager-attribute-required {true|false}] - Key manager attribute required for volume?

If you specify this parameter, then the command displays only the key manager policies with the given key-manager-attribute-required value.

Examples

The following example lists all configured key management policies:

```
cluster-1::*> security key-manager policy show

Policy             Check Key on Online?  Purge Key on Offline?
-----------------  --------------------  ---------------------
IBM_Key_Lore       true                  true
```

Copyright information

Copyright © 2026 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.