security key-manager commands

ONTAP 9.6 commands

NetApp
June 26, 2024

Table of Contents

security key-manager commands . . . 1
- security key-manager add . . . 1
- security key-manager create-key . . . 2
- security key-manager delete-key-database . . . 3
- security key-manager delete-kmip-config . . . 4
- security key-manager delete . . . 5
- security key-manager prepare-to-downgrade . . . 6
- security key-manager query . . . 6
- security key-manager restore . . . 9
- security key-manager setup . . . 12
- security key-manager show-key-store . . . 15
- security key-manager show . . . 16
- security key-manager update-passphrase . . . 17
- security key-manager backup show . . . 18
- security key-manager config modify . . . 20
- security key-manager config show . . . 21
- security key-manager external add-servers . . . 22
- security key-manager external disable . . . 22
- security key-manager external enable . . . 23
- security key-manager external modify-server . . . 24
- security key-manager external modify . . . 25
- security key-manager external remove-servers . . . 25
- security key-manager external restore . . . 26
- security key-manager external show-status . . . 28
- security key-manager external show . . . 30
- security key-manager external boot-interfaces modify . . . 33
- security key-manager external boot-interfaces show . . . 34
- security key-manager key create . . . 37
- security key-manager key delete . . . 38
- security key-manager key migrate . . . 38
- security key-manager key query . . . 39
- security key-manager key show . . . 42
- security key-manager onboard disable . . . 45
- security key-manager onboard enable . . . 46
- security key-manager onboard show-backup . . . 47
- security key-manager onboard sync . . . 48
- security key-manager onboard update-passphrase . . . 49

security key-manager commands

security key-manager add

(DEPRECATED)-Add a key management server

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

Description

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

This command adds a key management server at the indicated IP address to its list of four possible active key management servers. The command fails if there are already four key management servers configured. This command is not supported when onboard key management is enabled.

Parameters

`-address <IP Address>` - IP Address

This parameter specifies the IP address of the key management server you want to use to store keys.

`[-server-port <integer>]` - Server TCP Port

This parameter specifies the TCP port on which the key management server will listen for incoming connections.

Examples

The following example adds the key management server with address 10.233.1.98, listening for incoming connections on the default TCP port 5696, to the list of key management servers used by the external key manager:

```
cluster-1::> security key-manager add -address 10.233.1.198
```

The following example adds the key management server with address 10.233.1.98, listening for incoming connections on TCP port 15696, to the list of key management servers used by the external key manager:

```
cluster-1::> security key-manager add -address 10.233.1.198 -server-port
15696
```

Related Links

- security key-manager external add-servers

security key-manager create-key

(DEPRECATED)-Create a new authentication key

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

Description

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

This command creates a new authentication key (AK) and stores it on the configured key management servers. The command fails if the configured key management servers are already storing more than 128 AKs. If command fails due to more than 128 keys in cluster, delete unused keys on your key management servers and try the command again. This command is not supported when onboard key management is enabled.

Parameters

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

This parameter specifies the key tag that you want 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 key-manager query command 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, 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. Data 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 create-key

Verifying requirements...

Node: node1
Creating authentication key...
Authentication key creation successful.
Key ID: 00000000000000000200000000000100D0F7C2462D626B739FE81B89F29A092F.

Node: node2
Key manager restore operation initialized.
Successfully restored key information.
```

The following example creates an authentication key with key-tag "disk1-key":

```
cluster-1::> security key-manager create-key -key-tag disk1-key

Verifying requirements...

Node: node1
Creating authentication key...
Authentication key creation successful.
Key ID: 00000000000000000200000000000100B8297A6189BC24B9B84C1916ED576857.

Node: node2
Key manager restore operation initialized.
Successfully restored key information.
```

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

```
cluster-1::> security key-manager create-key -prompt-for-key true

Enter a new passphrase::

Reenter the passphrase::

Verifying requirements...

Node: node1
Creating authentication key...
Authentication key creation successful.
Key ID: 00000000000000000200000000000001006268333F870860128FBE17D393E5083B.

Node: node2
Key manager restore operation initialized.
Successfully restored key information.
```

Related Links

- security key-manager key create

security key-manager delete-key-database

(DEPRECATED)-Deletes the key hierarchy for 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-management configuration from all nodes of the cluster.

Examples

The following example deletes the onboard key-management configuration from all nodes of the cluster:

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

Warning: This command will permanently delete all keys from onboard key
management.
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 Data 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 successfully deleted from all nodes
of the
cluster. The keys stored by the external KMIP servers cannot be deleted by
Data ONTAP,
and must be deleted by using external tools.
```

Related Links

- security key-manager external disable

security key-manager delete

(DEPRECATED)-Delete a key management server

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

Description

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

This command removes the key management server at the indicated IP address from the list of active key management servers. If the indicated key management server is the sole storage location for any key that is in use by Data ONTAP, you will be unable to remove the key server. This command is not supported when onboard key management is enabled.

Parameters

`-address <IP Address>` - IP Address

This parameter specifies the IP address of the key management server you want to remove from use.

Examples

The following example removes the key server at IP address 10.233.1.198 from the set of configured key management servers:

```
cluster-1::> security key-manager delete -address 10.233.1.198
```

Related Links

- security key-manager external remove-servers

security key-manager prepare-to-downgrade

(DEPRECATED)-Disables onboard keymanagement features for unsupported versions

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 management features that are not supported in releases prior to ONTAP 9.1.0. The features that are disabled are onboard key management support for Metrocluster configurations and Volume Encryption (VE).

Examples

The following example disables the onboard key management support for Metrocluster configurations and Volume Encryption (VE):

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

security key-manager query

(DEPRECATED)-Displays the key IDs stored in a key management server.

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

Description

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

This command displays the IDs of the keys that are stored on the key management servers. This command does not update the key tables on the node. To refresh the key tables on the nodes with the key management server key tables, run the security key-manager restore command. This command is not supported when onboard key management is enabled.

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 queries the specified key management servers. If this parameter is not specified, then all nodes will query the specified key management servers.

[-address <IP Address>] - IP Address

This parameter specifies the IP address of the key management server that you want to query.

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

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.

[-count <integer>] - (DEPRECATED)-Key Server's Total Key Count

The value *count* is deprecated and may be removed in a future release of Data ONTAP. This parameter specifies the total number of keys stored in the key management servers. If you specify this parameter, then the command displays only the key IDs retrieved from the key management servers whose total key count matches the specified count number.

[-restored {yes|no}] - Key/Key ID Pair Present in Node's Key Table?

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 'yes' 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 'no' 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-manager-server-status {available|not-responding|unknown}] - Command Error Code

This parameter specifies the connectivity status of the key management server. If you specify this parameter, then the command displays only the key IDs retrieved from the key management servers with specified status.

Examples

The following example shows all the keys on all configured key servers, and whether those keys have been restored for all nodes in the cluster:

```
cluster-1::> security key-manager query
Node: node1
   Key Manager: 10.0.0.10
 Server Status: available

Key Tag                                  Key Type  Restored
-------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001001d71f3b2468d7e16a6e6972d3e6645200000000000
000000
301a4e57-9efb-11e7-b2bc-0050569c227f  VEK       yes
    Key ID:
000000000000000002000000000005004d03aca5b72cd20b2f83eae1531c605e0000000000
000000
Node: node2
   Key Manager: 10.0.0.10
 Server Status: available

Key Tag                                  Key Type  Restored
-------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001001d71f3b2468d7e16a6e6972d3e6645200000000000
000000
301a4e57-9efb-11e7-b2bc-0050569c227f  VEK       no
    Key ID:
000000000000000002000000000005004d03aca5b72cd20b2f83eae1531c605e0000000000
000000

If any listed keys have "no" in the "Restored" column, run "security key-
manager
restore" to restore those keys.
```

The following example shows all keys stored on the key server with address "10.0.0.10" from node "node1" with key-tag "node1":

```
cluster-1::> security key-manager query -address 10.0.0.10 -node node1
-key-tag node1
Node: node1
   Key Manager: 10.0.0.10
 Server Status: available

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001001d71f3b2468d7e16a6e6972d3e6645200000000000
000000

If any listed keys have "no" in the "Restored" column, run "security key-
manager
restore" to restore those keys.
```

The following example shows the Volume Encryption Key (VEK) with key-tag (i.e., volume UUID) "301a4e57-9efb-11e7-b2bc-0050569c227f" on nodes where that key has not been restored:

```
cluster-1::*> security key-manager query -key-type VEK -key-tag 301a4e57-
9efb-11e7-b2bc-0050569c227f -restored no
Node: node2
   Key Manager: 10.0.0.10
 Server Status: available

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
301a4e57-9efb-11e7-b2bc-0050569c227f  VEK       no
    Key ID:
000000000000000002000000000005004d03aca5b72cd20b2f83eae1531c605e0000000000
000000

If any listed keys have "no" in the "Restored" column, run "security key-
manager restore" to restore those keys.
```

Related Links

- security key-manager key query
- security key-manager restore

security key-manager restore

(DEPRECATED)-Restore the key ID pairs from the key management servers.

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

Description

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

This command retrieves and restores any current unrestored keys associated with the storage controller from the specified key management servers. This command is not supported when onboard key management is enabled.

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 is to load the key IDs into its internal key table. If not specified, all nodes retrieve keys into their internal key table.

[-address <IP Address>] - IP Address

If this parameter is specified, the command restores only from key management server at the specified IP address. If not specified the command restores from all available key management servers.

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

If this parameter is specified, the command restores only the specified key IDs.

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

This parameter specifies the value associated with the key ID pair at the time of their creation. If specified, restore only key ID pairs associated with the specified key tag. If not specified, all key ID pairs for the cluster are retrieved.

[-count <integer>] - (DEPRECATED)-Key Server's total Key Count

The value *`count`* is deprecated and may be removed in a future release of Data ONTAP. This parameter specifies the total number of keys stored in the key management servers. If this parameter is specified, then the command displays only the key IDs retrieved from the key management servers whose total key count matches the specified count number.

[-key-manager-server-status {available|not-responding|unknown}] - Command Error Code

This parameter specifies the connectivity status of the key management server. If you specify this parameter the command displays only the key IDs retrieved from key management servers with specified status.

Examples

The following command restores keys that are currently on a key server but are not stored within the key tables

on the cluster:

```
cluster-1::> security key-manager restore
Node: node1
   Key Manager: 10.0.0.10
 Server Status: available

Key IDs
---------------------------------------------------------
000000000000000002000000000001001d71f3b2468d7e16a6e6972d3e6645200000000000
000000
000000000000000002000000000005004d03aca5b72cd20b2f83eae1531c605e0000000000
000000
Node: node2
   Key Manager: 10.0.0.10
 Server Status: available

Key IDs
---------------------------------------------------------
000000000000000002000000000001001d71f3b2468d7e16a6e6972d3e6645200000000000
000000
000000000000000002000000000005004d03aca5b72cd20b2f83eae1531c605e0000000000
000000
```

The following loads any keys that exist on the key servers with IP address 10.0.0.10 with key-tag "node1" that are not currently stored in key tables of the nodes in the cluster. In this example, a key with that key-tag was missing from two nodes in the cluster:

```
cluster-1::> security key-manager restore -address 10.0.0.10 -key-tag
node1
Node: node1
   Key Manager: 10.0.0.10
 Server Status: available

Key IDs
---------------------------------------------------------
00000000000000000200000000000001001d71f3b2468d7e16a6e6972d3e6645200000000000
000000
Node: node2
   Key Manager: 10.0.0.10
 Server Status: available

Key IDs
---------------------------------------------------------
00000000000000000200000000000001001d71f3b2468d7e16a6e6972d3e6645200000000000
000000
```

Related Links

- security key-manager external restore

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 onboard key manager use security key-manager onboard enable instead.

The `security key-manager setup` command enables you to configure key management. Data 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 onboard key management, 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 onboard key management configured, you will run this command to refresh the missing keys.

For onboard key management 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 onboard key management when a refresh operation is required (see command description). This parameter is ignored when configuring external key management and during the initial setup of onboard key management.

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

When configuring onboard key management, 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 onboard key management 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.

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 onboard key management? {yes, no} [yes]: no
Would you like to configure the KMIP server environment? {yes, no} [yes]:
yes
```

The following example creates a configuration for onboard 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 onboard key management? {yes, no} [yes]: yes
Enter the cluster-wide passphrase for onboard key management. To continue
the
configuration, enter the passphrase, otherwise type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, 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 onboard key management with Common Critera 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 onboard key management? {yes, no} [yes]: yes
Enter the cluster-wide passphrase for onboard key management. To continue
the
configuration, enter the passphrase, otherwise type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, 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

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 displays the list of configured key managers.

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.

Examples

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

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

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

security key-manager show

(DEPRECATED)-Display key management servers

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

Description

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

This command displays the key management servers configured on the cluster. This command is not supported when onboard key management is enabled.

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.

| [-status]

If you specify this parameter, the command displays the status of each key management server.

| [-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 you want to retrieve key management server status for. If parameter is not specified, all nodes will retrieve the key management servers status.

[-address <IP Address>] - IP Address

Shows only a key management server registered with the input address. It is also possible to show multiple key management servers.

[-server-port <integer>] - Server TCP Port

If you specify this parameter, the command displays only key servers listening on this port.

Examples

The following example lists all configured key management servers:

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

Node                     Registered Key Manager
-----------------------  ---------------------------
node1                    10.225.89.33
node2                    10.225.89.33
```

The following example lists all configured key management servers, the TCP port on which those servers are expected to listen for incoming KMIP connections, and their server status:

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

Node                     Port    Registered Key Manager       Status
-----------------------  ------  ----------------------------
---------------
node1                    5696    10.225.89.33                 available
node2                    5696    10.225.89.33                 available
```

Related Links

- security key-manager external show

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 onboard key management. 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.

Examples

The following example updates the cluster-wide passphrase used for onboard key management:

```
cluster-1::*> security key-manager 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 backup show"
command.
```

Related Links

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

security key-manager backup show

(DEPRECATED)-Show salt and wrapped keys as a hex dump

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. Use security key-manager onboard show-backup instead.

This command displays the backup information for onboard key management, which would be used to recover the cluster in case of catastrophic situations. The information displayed is for the cluster as a whole (not individual nodes). This command is not supported for an external key management configuration.

Examples

The following example displays the onboard key management backup data for the cluster:

```
cluster-1::> security key-manager backup show
--------------------------BEGIN BACKUP--------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJs
b2IAAQAAAAMAAAAYAQAAAAAAADA5/
ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3t
JA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAAKAAAAAAAAACI8z/
bAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnUAAAAAAAAAAAAkAAA
AAAAAAIAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5SmyjLSgoK/
qc8FAmMMcrRXY6uriulnL0WPB/
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBL
ZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA1cNLLwAAAAAiAAAAAAAAACgAAAAAAAAA
Q5NxHQAAAAAAAAAAAAAAAAIAAAAAAAkAave0kD8tHNRBEfC/
7Vpa8AAAAAAAAAAAIgAAAAAAAAAoAAAAAAAAAJ4/
cQsAAAAAAAAAAAAAAAACAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAACQA
AAAAAAAAgAAAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rr
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA
---------------------------END BACKUP---------------------------
```

Related Links

- security key-manager onboard show-backup

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.

Examples

The following command enables Common Criterial mode in the cluster:

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

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 configuraton state for Common-Criteria (CC) mode for onboard key management. 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
Enabled
-------
true
```

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. 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 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
```

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 Data ONTAP, you cannot disable it. This command is not supported when onboard key management 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.

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 Data ONTAP.

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

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

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 *advanced* privilege level.

Description

This command modifies configuration information for configured key management servers. This command is supported only when external key manager has been enabled for the given Vserver.

Parameters

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

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

`-key-server <Hostname and Port>` - External Key Server (privilege: advanced)

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

`[-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 Data ONTAP authenticates with the 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 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 modify-server -vserver cluster-1 -key
-server keyserver1.local -username ksuser
Enter the password:
Reenter the password:
```

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. 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 Data 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 Data 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 Data ONTAP, then you are unable to remove the key server. 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 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.

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
```

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. This command is not supported when external key management has not been enabled for the 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.

`[-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 Data 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>] - Key Server

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

[-key-server-status {available|not-responding|unknown}] - 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.

Examples

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

```
cluster-1::> security key-manager external show-status
Node  Vserver  Key Server                                       Status
     ----  -------  ---------------------------------------------
-------------
     node1
           datavs
                    keyserver.datavs.com:5696
available
           cluster-1
                    10.0.0.10:5696
available
                    fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234
available
                    ks1.local:15696
available
     node2
           datavs
                    keyserver.datavs.com:5696
available
           cluster-1
                    10.0.0.10:5696
available
                    fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234
available
                    ks1.local:15696
available
     8 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 entires are displayed when external key management is not enabled for the 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 the key management servers for only the given Vserver.

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

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

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

Key Server
--------------------------------------------
keyserver.datavs.com:5696
Vserver: cluster-1
       Client Certificate: AdminClientCert
   Server CA Certificates: AdminServerCaCert
Key Server
--------------------------------------------
10.0.0.10:1234
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
               Key Server: keyserver.datavs.com:5696
                  Timeout: 25
                 Username: datavsuser
Vserver: cluster-1
       Client Certificate: AdminClientCert
   Server CA Certificates: AdminServerCaCert
               Key Server: 10.0.0.10:1234
                  Timeout: 25
                 Username:
Vserver: cluster-1
       Client Certificate: AdminClientCert
   Server CA Certificates: AdminServerCaCert
               Key Server: fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234
                  Timeout: 25
                 Username:
Vserver: cluster-1
       Client Certificate: AdminClientCert
   Server CA Certificates: AdminServerCaCert
               Key Server: ks1.local:1234
                  Timeout: 45
                 Username:
4 entries were displayed.
```

security key-manager external boot-interfaces modify

Modify external key manager logical interfaces

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

Description

This command enables cluster administrators to modify the IP address and route information that the external key manager uses at boot time to restore keys from external key servers.

Parameters

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

Use this parameter to modify information on the node that you specify.

`-address-type {ipv4|ipv6|ipv6z}` - Address Type (privilege: advanced)

Use this parameter to modify information for the address-type that you specify.

[-address <IP Address>] - Local Interface Address (privilege: advanced)

Use this parameter to modify the IP address that the system will use at boot time to restore keys from external key servers. This parameter implies `-override-default true` .

{ [-netmask <IP Address>] - Network Mask (privilege: advanced)

Use this parameter to modify the IP netmask that the system will use at boot time to restore keys from external key servers. This parameter can be used only with address-type ipv4. This parameter implies `-override-default true` .

| [-netmask-length <integer>] - Bits in Network Mask (privilege: advanced) }

Use this parameter to modify the IP netmask length that the system will use at boot time to restore keys from external key servers. This parameter implies `-override-default true` .

[-gateway <IP Address>] - Gateway (privilege: advanced)

Use this parameter to modify the IP gateway that the system will use at boot time to restore keys from external key servers. This parameter implies `-override-default true` .

[-port <Port Name>] - Network Port (privilege: advanced)

Use this parameter to modify the port that the system will use at boot time to restore keys from external key servers. The value that you specify cannot be a vlan or ifgrp port. This parameter implies `-override -default true` .

[-override-default {true|false}] - Override Default Setting? (privilege: advanced)

Use this parameter to modify the system's selection of boot time IP address and route information. When this value is `false` , the system will use the information associated with a node management LIF. When this value is `true` , then the administrator has chosen to override the defaults.

Examples

The following shows how to modify the port used by node "node2" at boot time to restore keys from external IPv4 key servers. In the example, IPv6 is not enabled in the cluster, so the `-address-type` parameter defaults to ipv4.

```
cluster-1::*> security key-manager external boot-interfaces modify -node
node2 -port e0d
```

The following example shows how to modify the IP address and gateway parameters used by node "node1" at boot time to restore keys from external IPv6 key servers.

```
cluster-1::*> security key-manager external boot-interfaces modify -node
node1 -address-type ipv6 -address fd20:8b1e:b255:814e:749e:11a3:3bff:5820
-gateway fd20:8b1e:b255:814e::1
```

security key-manager external boot-interfaces show

Show external key manager logical interfaces

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

Description

This command enables cluster administrators to view the IP address and route information that the external key manager uses at boot time to restore keys from external 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 (privilege: advanced)

Use this parameter to display information only about boot-time IP address and route information for the node that you specify.

[-address-type {ipv4|ipv6|ipv6z}] - Address Type (privilege: advanced)

Use this parameter to display information only about boot-time IP address and route information for the address-type that you specify.

[-address <IP Address>] - Local Interface Address (privilege: advanced)

Use this parameter to display information only about boot-time IP address and route information for the IP address that you specify.

[-netmask <IP Address>] - Network Mask (privilege: advanced)

Use this parameter to display information only about boot-time IP address and route information for the network mask that you specify.

[-netmask-length <integer>] - Bits in Network Mask (privilege: advanced)

Use this parameter to display information only about boot-time IP address and route information for the network mask length that you specify.

[-gateway <IP Address>] - Gateway (privilege: advanced)

Use this parameter to display information only about boot-time IP address and route information for the gateway that you specify.

[-port <Port Name>] - Network Port (privilege: advanced)

Use this parameter to display information only about boot-time IP address and route information for the port that you specify.

[-override-default {true|false}] - Override Default Setting? (privilege: advanced)

Use this parameter to display information only about boot-time IP address and route information with the override-default setting that you specify.

Examples

The following example shows how to display the IP address and route information that the external key manager uses at boot time to restore keys. In the example, IPv6 is not enabled in the cluster and, as a result, the command displays information for only the IPv4 address-type. he override-default value is false for all rows, which indicates that the system automatically configured the values based on the node management LIF configuration on the nodes.

```
cluster-1::*> security key-manager external boot-interfaces show
     Address Network                                  Override
Node     Type    Address/Mask       Gateway         Port  Default?
-------- ------- ------------------ --------------- ----- --------
node1
     ipv4    10.224.113.159/24  10.224.113.1    e0M   false
node2
     ipv4    10.224.113.160/24  10.224.113.1    e0M   false
2 entries were displayed.
```

The following example shows how to display the IP address and route information that the external key manager uses at boot time to restore keys. In the example, IPv6 is enabled in the cluster and, as a result, the command displays information for both the IPv4 and IPv6 address-types. The override-default value is false for most rows, which indicates that the system automatically configured the values based on the node management LIF configuration on the nodes. The override-default value for node1 and address-type ipv4 is true, which indicates an administrator has used the security key-manager external boot-interfaces modify command to override one or more fields, and that the values may differ from the corresponding node management LIF.

```
cluster-1::*> security key-manager external boot-interfaces show
         Address Network                                  Override
Node     Type    Address/Mask       Gateway         Port  Default?
-------- ------- ------------------ --------------- ----- --------
node1
     ipv4    10.224.113.159/24  10.224.113.1    e0d   true
         ipv6    fd20:8b1e:b255:814e:32bd:f35c:832c:5a09/64
                                    fd20:8b1e:b255:814e::1
                                                    e0M   false
node2
     ipv4    10.224.113.160/24  10.224.113.1    e0M   false
         ipv6    fd20:8b1e:b255:814e:749e:11a3:3bff:5820/64
                                    fd20:8b1e:b255:814e::1
                                                    e0M   false
4 entries were displayed.
```

Related Links

- security key-manager external boot-interfaces modify

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. Data 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 Data 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
00000000000000000200000000000001006268333f870860128fbe17d393e5083b0000000000
000000
```

security key-manager key migrate

Migrate keys from the admin Vserver's 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.

> This command currently only supports key migration from the Admin Vserver's onboard key manager to a Data Vserver's external key manager and vice versa.

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

Displays the key IDs stored in a key management server.

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.

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 'yes' 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 'no' 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.

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
Vserver: cluster-1
   Key Manager: onboard
          Node: node1
    Key Server: ""

Key Tag                                  Key Type  Restored
-------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
00000000000000000200000000000001000c11b3863f78c2273343d7ec5a67762e0000000000
000000
node1                                    NSE-AK    yes
```

```
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000000
000000
node1                                   NSE-AK    yes
    Key ID:
000000000000000002000000000000100e1f6b27094485d2d74408bca673b25eb0000000000
000000
node1                                   NSE-AK    yes
    Key ID:
000000000000000002000000000000100ea73be83ec42a7a2bd262f369cda83a40000000000
000000
Vserver: datavs
   Key Manager: external
          Node: node1
    Key Server: keyserver.datavs.com:5965
Key Tag                                 Key Type  Restored
-------------------------------------  --------  --------
eb9f8311-e8d8-487e-9663-7642d7788a75  VEK       yes
    Key ID:
000000000000000002000000000000004001cb18336f7c8223743d3e75c6a7726e0000000000
000000
9d09cbbf-0da9-4696-87a1-8e083d8261bb  VEK       yes
    Key ID:
000000000000000002000000000000004064f2e1533356a470385274a9c3ffb9770000000000
000000
40c3546e-600c-401c-b312-f01be52258dd  VEK       yes
    Key ID:
000000000000000002000000000000401e6f2b09744582d74d084cb6a372be5b0000000000
000000
9b195ecb-35ee-4d11-8f61-15a8de377ad7  VEK       yes
    Key ID:
000000000000000002000000000000040ea73be83ec42a7a2bd262f369cda83a40000000000
000000
Vserver: cluster-1
   Key Manager: onboard
          Node: node2
    Key Server: -
Key Tag                                 Key Type  Restored
-------------------------------------  --------  --------
node1                                   NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000000
000000
node1                                   NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000000
```

```
000000
node1                                   NSE-AK    yes
    Key ID:
000000000000000002000000000000100e1f6b27094485d2d74408bca673b25eb0000000000
000000
node1                                   NSE-AK    yes
    Key ID:
000000000000000002000000000000100ea73be83ec42a7a2bd262f369cda83a40000000000
000000
Vserver: datavs
   Key Manager: external
          Node: node2
    Key Server: keyserver.datavs.com:5965

Key Tag                                 Key Type  Restored
-------------------------------------  --------  --------
eb9f8311-e8d8-487e-9663-7642d7788a75  VEK       yes
    Key ID:
000000000000000002000000000000004001cb18336f7c8223743d3e75c6a7726e0000000000
000000
9d09cbbf-0da9-4696-87a1-8e083d8261bb  VEK       yes
    Key ID:
000000000000000002000000000000004064f2e1533356a470385274a9c3ffb9770000000000
000000
40c3546e-600c-401c-b312-f01be52258dd  VEK       yes
    Key ID:
000000000000000002000000000000401e6f2b09744582d74d084cb6a372be5b0000000000
000000
9b195ecb-35ee-4d11-8f61-15a8de377ad7  VEK       yes
    Key ID:
000000000000000002000000000000040ea73be83ec42a7a2bd262f369cda83a40000000000
000000
```

security key-manager key show

(DEPRECATED)-Display encryption key IDs stored in onboard key manager

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. Use security key-manager key query instead.

This command displays the key IDs of the authentication keys (NSE-AK) and SVM keys (SVM-KEK) that are available in onboard key management. This command is not supported for an external key management

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.

| [-detail]

If this parameter is specified, the command displays additional details about the key IDs.

| [-instance] }

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

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

If this parameter is specified, the command displays information only about key IDs that are located on the specified storage system.

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

If this parameter is specified, the command displays information only about key IDs that are managed by the specified key management. For example, use *onboard* for onboard key management.

[-key-id <text>] - Key Identifier

If this parameter is specified, the command displays information only about the specified key IDs.

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

If this parameter is specified, the command displays information only about key IDs that have the specified key tags.

[-key-location <text>] - Key Location

If this parameter is specified, the command displays information only about key IDs that are located on the specified key location. For example, use *local-cluster* for onboard key management.

[-used-by <Key Usage Type>] - Used By

If this parameter is specified, the command displays information only about key IDs that are associated with the specified application usage of the keys. For example, "NSE-AK" would display key IDs only for NSE drives.

[-restored {yes|no}] - Restored

If this parameter is specified, the command displays information only about key IDs that have the specified value of restored keys. If restored is *yes* , then the corresponding key is available (normal). If restored is *no* , use the security key-manager setup command to restore the key. See the man page for security key-manager setup for details.

Examples

The following example shows all keys stored in the onboard key manager:

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

Node: node1
Key Store: onboard
Used By
--------
NSE-AK
    Key ID:
000000000000000002000000000001001bc4c708e2a89a312e14b6ce6d4d49d40000000000
000000
NSE-AK
    Key ID:
000000000000000002000000000001005e89099721f8817e65e3aeb68be1bfca0000000000
000000
SVM-KEK
    Key ID:
000000000000000002000000000000a0046df92864d4cece662b93beb7f5366100000000000
000000

Node: node2
Key Store: onboard
Used By
--------
NSE-AK
    Key ID:
000000000000000002000000000001001bc4c708e2a89a312e14b6ce6d4d49d40000000000
000000
NSE-AK
    Key ID:
000000000000000002000000000001005e89099721f8817e65e3aeb68be1bfca0000000000
000000
SVM-KEK
    Key ID:
000000000000000002000000000000a0046df92864d4cece662b93beb7f5366100000000000
000000
6 entries were displayed.
```

The following example shows a detailed view of all keys stored in the onboard key manager:

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

Node: node1
Key Store: onboard
Key ID Key Tag         Used By    Stored In
Restored
------ --------------- ---------- ------------------------------------
--------
000000000000000002000000000001001bc4c708e2a89a312e14b6ce6d4d49d40000000000
000000
       -               NSE-AK     local-cluster                        yes
000000000000000002000000000001005e89099721f8817e65e3aeb68be1bfca0000000000
000000
       -               NSE-AK     local-cluster                        yes
000000000000000002000000000000a0046df92864d4cece662b93beb7f5366100000000000
000000
       -               SVM-KEK    local-cluster                        yes

Node: node2
Key Store: onboard
Key ID Key Tag         Used By    Stored In
Restored
------ --------------- ---------- ------------------------------------
--------
000000000000000002000000000001001bc4c708e2a89a312e14b6ce6d4d49d40000000000
000000
       -               NSE-AK     local-cluster                        yes
000000000000000002000000000001005e89099721f8817e65e3aeb68be1bfca0000000000
000000
       -               NSE-AK     local-cluster                        yes
000000000000000002000000000000a0046df92864d4cece662b93beb7f5366100000000000
000000
       -               SVM-KEK    local-cluster                        yes
6 entries were displayed.
```

Related Links

- security key-manager key query
- security key-manager setup

security key-manager onboard disable

Disable onboard key management

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 management configuration associated with the admin Vserver.

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
         management.
Do you want to continue? {y|n}: y
```

security key-manager onboard enable

Enable 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 Critieria (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 character long, and you are required to enter that passphrase each time a node reboots. CC mode cannot be enabled in a MetroCluster configuration.

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 onboard key management:

Re-enter the cluster-wide passphrase:

After configuring onboard key management, 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

Show salt and wrapped keys for the admin Vserver as a hex dump

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

Description

This command displays the backup information for onboard key management 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 management backup data for the admin Vserver:

```
cluster-1::> security key-manager onboard show-backup
--------------------------BEGIN BACKUP--------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAACgAAAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAAAA
IgAAAAAAAAAAoAAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAAAACQAAAAAAAAAAgAAAAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJs
b2IAAQAAAAMAAAAYAQAAAAAAAADA5/
ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3t
JA/LRzUQRHwv+1aWvAAAAAAAAAAAACIAAAAAAAAAAKAAAAAAAAAAACI8z/
bAAAAAAAAAAAAAAAAAgAAAAAAAAQAbxMcI4qiaMS4Uts5tTUnUAAAAAAAAAAAAAkAAA
AAAAAAIAAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5SmyjLSgoK/
qc8FAmMMcrRXY6uriulnL0WPB/
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBL
ZXkgQmxvYgABAAAAAwAAABgBAAAAAAAAAA1cNLLwAAAAAiAAAAAAAAAAACgAAAAAAAAAAA
Q5NxHQAAAAAAAAAAAAAAAAIAAAAAAAkAave0kD8tHNRBEfC/
7Vpa8AAAAAAAAAAAAIgAAAAAAAAAAoAAAAAAAAAAAJ4/
cQsAAAAAAAAAAAAAAAAAACAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAAACQA
AAAAAAAAgAAAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rr
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA
---------------------------END BACKUP---------------------------
```

security key-manager onboard sync

Sync onboard key management 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 onboard key management 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 onboard key management 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 Management 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 onboard key management 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 onboard key management 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.

Examples

The following example updates the cluster-wide passphrase used for onboard key management:

```
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