



security key-manager commands

ONTAP 9.5 commands

NetApp

February 11, 2024

Table of Contents

- security key-manager commands 1
 - security key-manager add 1
 - security key-manager create-key 1
 - security key-manager delete-key-database 3
 - security key-manager delete-kmip-config 4
 - security key-manager delete 4
 - security key-manager prepare-to-downgrade 5
 - security key-manager query 5
 - security key-manager restore 8
 - security key-manager setup 11
 - security key-manager show 13
 - security key-manager update-passphrase 15
 - security key-manager backup show 15
 - security key-manager config modify 17
 - security key-manager config show 17
 - security key-manager external boot-interfaces modify 18
 - security key-manager external boot-interfaces show 19
 - security key-manager key show 21

security key-manager commands

security key-manager add

Add a key management server

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

Description

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
```

security key-manager create-key

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 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: 000000000000000000200000000000100D0F7C2462D626B739FE81B89F29A092F.

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: 000000000000000002000000000001006268333F870860128FBE17D393E5083B.

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

security key-manager delete-key-database

Deletes the key hierarchy for onboard key manager

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

Description

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

security key-manager delete-kmip-config

Deletes the KMIP configuration

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

Description

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.

security key-manager delete

Delete a key management server

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

Description

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
```

security key-manager prepare-to-downgrade

Disables onboard keymanagement features for unsupported versions

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

Description

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

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 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:		
000000000000000000002000000000001001d71f3b2468d7e16a6e6972d3e66452000000000000000000		
301a4e57-9efb-11e7-b2bc-0050569c227f	VEK	yes
Key ID:		
000000000000000000002000000000005004d03aca5b72cd20b2f83eae1531c605e000000000000000000		

```
Node: node2
```

```
Key Manager: 10.0.0.10
```

```
Server Status: available
```

Key Tag	Key Type	Restored
-----	-----	-----
node1	NSE-AK	yes
Key ID:		
000000000000000000002000000000001001d71f3b2468d7e16a6e6972d3e66452000000000000000000		
301a4e57-9efb-11e7-b2bc-0050569c227f	VEK	no
Key ID:		
000000000000000000002000000000005004d03aca5b72cd20b2f83eae1531c605e000000000000000000		

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:
0000000000000000000020000000000001001d71f3b2468d7e16a6e6972d3e6645200000000000
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:
0000000000000000000020000000000005004d03aca5b72cd20b2f83eae1531c605e0000000000
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 restore](#)

security key-manager restore

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 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
-----
000000000000000000002000000000001001d71f3b2468d7e16a6e6972d3e6645200000000000
000000
000000000000000000002000000000005004d03aca5b72cd20b2f83eae1531c605e0000000000
000000
Node: node2
  Key Manager: 10.0.0.10
  Server Status: available

Key IDs
-----
000000000000000000002000000000001001d71f3b2468d7e16a6e6972d3e6645200000000000
000000
000000000000000000002000000000005004d03aca5b72cd20b2f83eae1531c605e0000000000
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
-----
000000000000000000002000000000001001d71f3b2468d7e16a6e6972d3e6645200000000000
000000
Node: node2
  Key Manager: 10.0.0.10
  Server Status: available

Key IDs
-----
000000000000000000002000000000001001d71f3b2468d7e16a6e6972d3e6645200000000000
000000

```

security key-manager setup

Configure key manager connectivity

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

Description

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 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 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 update-passphrase](#)

security key-manager show

Display key management servers

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

Description

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

security key-manager update-passphrase

Update cluster-wide passphrase

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

Description

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 setup](#)

security key-manager backup show

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 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:

[illegible]

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 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 {<netport>|<ifgrp>}`] - 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 {<netport>|<ifgrp>}`] - 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. The 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 show

Display Encryption Key IDs

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

Description

This command displays the key IDs of the authentication keys (NSE-AK) and vservers 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

Key ID	Used By
000000000000000000002000000000001001BC4C708E2A89A312E14B6CE6D4D49D4	NSE-AK
000000000000000000002000000000001005E89099721F8817E65E3AEB68BE1BFCA	NSE-AK
00000000000000000000200000000000A0046DF92864D4CECE662B93BEB7F536610	SVM-KEK

Node: node2

Key Store: onboard

Key ID	Used By
000000000000000000002000000000001001BC4C708E2A89A312E14B6CE6D4D49D4	NSE-AK
000000000000000000002000000000001005E89099721F8817E65E3AEB68BE1BFCA	NSE-AK
00000000000000000000200000000000A0046DF92864D4CECE662B93BEB7F536610	SVM-KEK

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

-----	-----	-----	-----

0000000000000000000020000000000001001BC4C708E2A89A312E14B6CE6D4D49D4			
--	--	--	--

-	NSE-AK	local-cluster	yes
---	--------	---------------	-----

0000000000000000000020000000000001005E89099721F8817E65E3AEB68BE1BFCA			
--	--	--	--

-	NSE-AK	local-cluster	yes
---	--------	---------------	-----

000000000000000000002000000000000A0046DF92864D4CECE662B93BEB7F536610			
--	--	--	--

-	SVM-KEK	local-cluster	yes
---	---------	---------------	-----

Node: node2

Key Store: onboard

Key ID	Key Tag	Used By	Stored In
--------	---------	---------	-----------

Restored

-----	-----	-----	-----

0000000000000000000020000000000001001BC4C708E2A89A312E14B6CE6D4D49D4			
--	--	--	--

-	NSE-AK	local-cluster	yes
---	--------	---------------	-----

0000000000000000000020000000000001005E89099721F8817E65E3AEB68BE1BFCA			
--	--	--	--

-	NSE-AK	local-cluster	yes
---	--------	---------------	-----

000000000000000000002000000000000A0046DF92864D4CECE662B93BEB7F536610			
--	--	--	--

-	SVM-KEK	local-cluster	yes
---	---------	---------------	-----

6 entries were displayed.

Related Links

- [security key-manager setup](#)

Copyright information

Copyright © 2024 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.