Adding a second controller to create an HA pair

Upgrading a stand-alone controller module to HA pair is a multistep process involving both hardware and software changes that must be performed in the proper order.

Before you begin

- An existing controller module must be installed, configured, and operating in Data ONTAP 8.x 7-Mode or Data ONTAP 7.3.x.
  This controller module is referred to as the *existing* controller module; the examples in this procedure have the console prompt existing_ctlr>.
  The controller module that is being added is referred to as the *new* controller module;the examples in this procedure have the console prompt new_ctlr>.
- The new controller module must be received from NetApp as part of the upgrade kit.
  This procedure does not apply to moving a controller module from a preexisting system or a system that was previously in an HA pair.
- Your system must have an empty slot available for the new controller module when upgrading to a single-chassis HA pair (a HA pair in which both controller modules reside in the same chassis.

  Note: This configuration is not supported on all systems.
- You must have rack space and cables for the new controller module when upgrading to a dual-chassis HA pair (an HA pair in which the controller modules reside in separate chassis.

  Note: This configuration is not supported on all systems.
- Each controller module must be connected to the network through its e0a port or, if your system has one, the e0M port.

About this task

This procedure does not apply to systems operating in clustered Data ONTAP.

This procedure can take over an hour, with additional time needed to initialize the disks. The time to initialize the disks depends on the size of the disks.

Steps

15. Setting up Storage Encryption on the new controller module on page 14

Preparing for the upgrade

To prepare for the upgrade to an HA pair, you must make sure that your system meets all requirements and that you have all required information.

Steps

1. Ensure that your system has at least three unowned disks for the new controller module by entering the following command on the existing controller module:

   `disk show -n`

   Two disks are required for file system installation and the third is a spare. These three disks are in addition to a spare disk for the existing controller module.

   If you are adding disks or disk shelves to your system, see the *Data ONTAP Storage Management Guide* for your version of Data ONTAP on the NetApp Support Site.

   Note: In Data ONTAP 8.x, you must set the `disk.auto_assign` option to `off` on the existing controller module before adding any new disks. See the *Data ONTAP Storage Management Guide for 7-Mode* on the NetApp Support Site for more information.

2. Ensure that you have network cables and storage cables ready.
3. Ensure that you have a serial port console available for the controller modules.
4. Review the *Site Requirements Guide* on the NetApp Support Site and gather all IP addresses and other network parameters for the new controller module.

Preparing to add a controller module when using Storage Encryption

If the existing controller module is configured for Storage Encryption, you must gather information from the system and rekey the self-encrypting disks (SEDs) before adding the new controller module.

About this task

Steps

1. Enter the following command and note the key IDs on all disk drives that are using Storage Encryption:

   `disk encrypt show`

   #### Example

   The command displays the status of each self-encrypting disk:

```
storage-system> disk encrypt show
Disk       Key ID                                                           Locked?
0c.00.1    080CF0C8000000000100000000000000A948EE8604F4598ADFFB185B5BB7FED3  Yes
0c.00.0    080CF0C8000000000100000000000000A948EE8604F4598ADFFB185B5BB7FED3  Yes
0c.00.3    080CF0C8000000000100000000000000A948EE8604F4598ADFFB185B5BB7FED3  Yes
0c.00.4    080CF0C8000000000100000000000000A948EE8604F4598ADFFB185B5BB7FED3  Yes
0c.00.2    080CF0C8000000000100000000000000A948EE8604F4598ADFFB185B5BB7FED3  Yes
0c.00.5    080CF0C8000000000100000000000000A948EE8604F4598ADFFB185B5BB7FED3  Yes
```

2. Enter the following command and note all the necessary certificate files (`client.pem`, `client_private.pem`, and *`ip_address_key_server`*`_CA.pem`) that have been installed:

keymgr list cert

Later in the procedure you need to install these same certificate files on the new partner controller module.

3. Enter the following command to identify the IP address of the key servers:

   key_manager show

   All external key management servers associated with the storage system are listed. Later in the procedure you need to add these same key servers on the new partner controller module.

   Example

   The following command displays all external key management servers associated with the storage system:

   ```
   storage-system> key_manager show
     172.18.99.175
   ```

4. Enter the following command and check that the key IDs listed match those shown by the `disk encrypt show` command in step 1:

   key_manager query

   Example

   The following command checks the status of all key management servers linked to the storage system and displays additional information:

   ```
   storage-system> key_manager query

   Key server 172.18.99.175 reports 4 keys.

   Key tag                          Key ID
   --------                         -------
   storage-system                   080CF0C80...
   storage-system                   080CF0C80...
   storage-system                   080CF0C80...
   storage-system                   080CF0C80...
   ```

5. Back up all data on all aggregates using standard methods for your site.

6. Enter the following command to reset the authentication key on the drives using Storage Encryption to their Manufacturing System ID (MSID):

   disk encrypt rekey 0x0 *

7. Examine the CLI command output to ensure that there are no `disk encrypt rekey` failures.

Preparing the netboot server

How you prepare to netboot depends on the version of Data ONTAP you are running.

Choices

- Preparing the netboot server in Data ONTAP 8.x on page 4
- Preparing the netboot server in Data ONTAP 7.3.x on page 5

Preparing the netboot server in Data ONTAP 8.x

You must download the correct Data ONTAP netboot image from the NetApp Support Site to the netboot server and know its IP address.

Before you begin

- You must have an attached computer with access to the existing storage system to copy files.
  See the *Data ONTAP System Administration Guide for 7-Mode* for more information about accessing files in the storage system's `/etc` directories.
- You must have access to the NetApp Support Site at *support.netapp.com*.
  This enables you to download the necessary system files.

About this task

- You must download the netboot image for the same version of Data ONTAP that is running on the new controller module. Both controller modules in the HA pair must run the same version of Data ONTAP.
- This procedure does not apply to systems operating in Cluster-Mode.

Steps

1. Identify the location of the root directory for `httpd` files or, if none is configured, configure the directory.

   This location is maintained in the `httpd.rootdir` option. You can display the value with the following command at the Data ONTAP prompt:

   ```
   existing_ctlr> options httpd.rootdir
   ```

   This directory is referred to as the *web-accessible directory* in the following steps.

   If you have created a root directory (for example, `vol0`), you can set the `httpd.rootdir` option to that directory with the following command at the Data ONTAP prompt:

   ```
   existing_ctlr> options httpd.rootdir /vol/vol0
   ```

2. Download and extract the file used for performing the netboot of your system:

   a. Download the appropriate `netboot.tgz` file for your platform from the NetApp Support Site to a web-accessible directory.
   b. Change to the web-accessible directory.
   c. Extract the contents of the `netboot.tgz` file to the target directory by entering the following command:

      `tar -zxvf netboot.tgz`

   Your directory listing should contain the following directory:
   `netboot/`

3. Download the `image.tgz` file from the NetApp Support Site to the web-accessible directory.

   Your directory listing should contain the following file and directory:
   `image.tgz netboot/`

4. Determine the IP address of the existing controller module.

   This address is referred to later in this procedure as *`ip-address-of-existing controller`*.

5. Ping *ip-address-of-existing controller* to ensure that the address is alive and reachable.

Preparing the netboot server in Data ONTAP 7.3.x

You must copy files from the existing controller module's `/etc` directories to the `httpd` root directory and know the existing controller module's IP address.

Before you begin

- You must have an attached computer with access to the existing storage system to copy files.
  See the *Data ONTAP System Administration Guide* for more information about accessing files in the storage system's `/etc` directories.
- You must have access to the NetApp Support Site at *support.netapp.com*.
  This enables you to download the necessary system files.

About this task

- Data ONTAP 7.3.x does not support all systems.
  See the *Hardware Universe* at *hwu.netapp.com* for supported systems.
- You must download the netboot image for the same version of Data ONTAP that is running on the existing controller module.
  Both controller modules in the HA pair must run the same version of Data ONTAP.

Steps

1. Copy the following boot image files from the controller module's `/etc/boot` and `/etc/software` directory to the root directory for httpd files:
   a. Determine the root directory for `httpd` files.

If `httpd` is...	Then...
Configured	Enter the following command at the existing controller module's Data ONTAP prompt to display the root directory: **`options httpd.rootdir`** The system displays the following output: `httpd.rootdir /vol/vol0 existing_ctlr>` In the preceding example, the location is `/vol/vol0`.

If `httpd` is...	Then...
Not configured	i. Enable `httpd` by entering the following command at the existing controller module's Data ONTAP prompt: **`options httpd.enable on`** ii. Verify that you can view the files in the web-accessible directory by entering the following command at the existing controller module's Data ONTAP prompt: **`options httpd`** The system displays the following output: `httpd.autoindex.enable on` iii. Set the root directory by entering the following command at the existing controller module's Data ONTAP prompt: **`options httpd.rootdir /vol/vol0`**

b. Copy the following files from the existing controller module's `/etc/boot` and `/etc/software` directories to the root directory identified in the previous step:

- From the `/etc/boot/` directory, copy the file with a name similar to `netapp-x86-64`.
- From the `/etc/software/` directory, copy the Data ONTAP image file with a name similar to `setup.exe`.

2. Enter the following command to determine the IP address of the existing controller module (referred to in this procedure as *ip-address-of-existing controller*):

`ifconfig -a`

Example

In the following example, the *`ip-address-of-existing controller`* is 172.22.133.8:

```
existing_ctlr> ifconfig -a
e0M: flags=948043 UP,BROADCAST,RUNNING,MULTICAST,TCPCKSUM  mtu 1500
inet 172.22.133.8 netmask 0xffffe000 broadcast 172.22.159.255
partner inet 172.22.130.194 (not in use)
ether 00:a0:98:09:08:8c (auto-100tx-fd-up) flowcontrol full
existing_ctlr>
```

Installing and cabling the new controller module

You must physically install the new controller module in the chassis and cable it.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have an I/O expansion module (IOXM) module in your system and are creating a single-chassis HA pair, you must uncable and remove the IOXM.

   You can then use the empty bay for the new controller module. However, the new configuration will not have the extra I/O provided by the IOXM.
3. If you have a 60xx system, move the NVRAM adapter in the existing controller to slot 1.

This is required for the system to operate in an HA pair.

4. Physically install the new controller module and, if necessary, additional fans:

If you are adding a controller module...	Then perform these steps...
To an empty bay to create a single-chassis HA pair and the platform is a 31xx or 6210 system	**a.** Install three additional fans in the chassis to cool the new controller module: **i.** Remove the bezel by using both hands to hold it by the openings on each side, and then pull the bezel away from the chassis until it releases from the four ball studs on the chassis frame. **ii.** Remove the blank plate that covers the bay that will contain the new fans. **iii.** Install the fans as described in the *Replacing a fan module* document for your system on the NetApp Support Site at *support.netapp.com*. **b.** Remove the blank plate in the rear of the chassis that covers the empty bay that will contain the new controller module. **c.** Gently push the controller module halfway into the chassis. See the system's *Hardware Overview* on the NetApp Support Site at *support.netapp.com* for an illustration.
To an empty bay to create a single-chassis HA pair and the platform is a 32xx or , FAS22xx system	**a.** Remove the blank plate in the rear of the chassis that covers the empty bay that will contain the new controller module. **b.** Gently push the controller module halfway into the chassis. To prevent the controller module from automatically booting, do not fully seat it in the chassis until later in this procedure. See the system's *Hardware Overview* on the NetApp Support Site at *support.netapp.com* for an illustration.
In a separate chassis from its HA partner to create a dual-chassis HA pair	Install the new system in the rack or system cabinet.

5. Cable the HA interconnect if you have a dual-chassis HA pair and cable the disk shelves as necessary.

   See the system's *Installation and Setup Instructions*, the *Clustered Data ONTAP High-Availability Configuration Guide* for your version of Data ONTAP, and, if applicable, the *Universal SAS and ACP Cabling Guide*.

6. Power up the existing controller module.

7. Depending on your configuration, power up the new controller module and interrupt the boot process:

If the new controller module is...	Then...
In the same chassis as the existing controller module	**a.** Push the controller module firmly into the bay. When fully seated, the controller module receives power and automatically boots. **b.** Interrupt the boot process by pressing Ctrl-C.
In a separate chassis from the existing controller module	**a.** Turn on the power supplies on the new controller module. **b.** Interrupt the boot process by pressing Ctrl-C.

   The system displays the LOADER prompt (LOADER>, LOADER-A>, or LOADER-B>).

   Note: If there is no LOADER prompt, record the error message and contact technical support. If the system displays the boot menu, reboot and attempt to interrupt the boot process again.

Configuring and cabling CNA ports (FAS80xx systems only)

If you are adding a controller module to a FAS80xx system, you must check the configuration of the CNA ports on the new controller module and, if necessary, change the defaults to match the CNA port configuration of the existing controller module.

Before you begin

You must have the SFP+ modules for the CNA ports.

Steps

1. If you have not already done so, enter Maintenance mode:
   a. Enter
      boot_ontap
      .
   b. Press Ctrl-C when you see the message `Press Ctrl-C for Boot Menu`.
   c. Answer **y** when prompted by the system.
   d. Select the Maintenance mode option from the displayed menu.
2. On the new controller module, issue the following command to check how the ports are currently configured:
   ucadmin show
   The system displays output similar to the following example:

```
*> ucadmin show
          Current Current   Pending  Pending
 Adapter  Mode    Type      Mode     Type      Status
 -------  ------- --------- -------  -------   ------
  0e      fc      initiator -        -         online
  0f      cna     target    -        -         online
  0g      cna     target    -        -         online
...
```

3. If the current SFP+ module does not match the desired use, replace it with the correct SFP+ module.
4. If the current configuration does not match the desired use, enter one of the following commands to change the configuration as needed:

If the desired use is for...	Then enter the following command...
FC initiator	**ucadmin modify -t initiator *adapter_name***
FC target	**ucadmin modify -t target *adapter_name***
Ethernet	**ucadmin modify -m cna *adapter_name***

5. If you have changed the settings, reboot the new controller module to implement the configuration changes.
6. After the new controller module reboots, verify the settings by entering the following command:
   ucadmin show -c
7. Cable the port.

Verifying and setting the HA state of the controller module and chassis

You must verify the HA state of the chassis and controller modules, and, if necessary, update the state to indicate that the system is in an HA pair. If you have a FAS20xx, 30xx, 31xx or 60xx system, you can skip this task.

Steps

1. Reboot the existing controller module and press Ctrl-C when prompted to do so, to display the boot menu.
2. At the boot menu, select the option for Maintenance mode boot.
3. After the system boots into Maintenance mode, enter the following command to display the HA state of the local controller module and chassis:

   `ha-config show`

   The HA state should be `ha` for all components.
4. If necessary, enter the following command to set the HA state of the controller module:

   `ha-config modify controller ha`

   Respond **`y`** when prompted to continue the operation.
5. If necessary, enter the following command to set the HA state of the chassis:

   `ha-config modify chassis ha`

   Respond **`y`** when prompted to continue the operation.
6. Exit Maintenance mode by entering the following command:

   `halt`
7. Boot the system by entering the following command from the boot loader prompt:

   `boot_ontap`
8. Repeat the preceding steps on the partner controller module and chassis, as necessary.

Booting and installing Data ONTAP on the new controller module

To assign an IP address, netboot the new controller module, and install the operating system on it, you must perform a specific sequence of steps.

About this task

This procedure includes initializing disks. The time required to initialize the disks depends on the size of the disks.

The system automatically assigns two disks to the new controller module. See the *Storage Management Guide* for your version of Data ONTAP for information about managing disks and assigning additional disks.

Steps

1. Enter the following commands at the boot environment prompt (LOADER>, LOADER-A>, or LOADER-B>) to configure the IP address of the new controller module:

If DHCP is...	Then enter the following command...
Available	**`ifconfig e0M -auto`**

If DHCP is...	Then enter the following command...
Not available	**ifconfig e0M -addr=*new_controller_ip_address* -mask=*255.255.xxx.xxx* -gw=*xxx.xxx.xxx.xxx* -dns=*xxx.xxx.xxx.xxx* -domain=*yourCompanyname.com***

2. Netboot the new controller module, using the appropriate commands and files for your version of Data ONTAP.

If your version of Data ONTAP is...	Enter the following command at the LOADER prompt:
7.3.x	**netboot http://*ip-address-of-existing controller*/netapp-x86-64** *ip-address-of-existing controller* is the IP address determined when you were preparing the netboot server.
8.x operating in 7-Mode	**netboot http://*ip-address-of-existing controller*/netboot/kernel** *ip-address-of-existing controller* is the IP address determined when you were preparing the netboot server.

The new controller module boots and the boot menu is displayed.

3. Select the appropriate option in the boot menu, depending on your version of Data ONTAP.

If your version of Data ONTAP is...	Then...
7.3.x	Depending on the type of root volume you require, select **4) Initialize all disks** or **4a)** for a flexible root volume.
8.x operating in 7-Mode	**a.** Select the option **Install new software first** from the boot menu and respond **y** when prompted for confirmation. This boot menu option downloads and installs the new Data ONTAP image to the boot device. **b.** During the software installation process, when you are prompted for the URL of the `image.tgz` file, enter the path as follows: **http://*ip-address-of-existing controller*/image.tgz** If necessary, enter the user name associated with the URL when prompted. After the software installation is complete, you are prompted to reboot the system. **c.** Respond **n** if prompted to restore the backup configuration. **d.** Respond **y** when you are prompted to reboot the system and use the new software. **e.** Reboot the system. The system reboots and displays the boot menu. **f.** Select option **4** to initialize all disks. **g.** Respond **y** when you are prompted to zero disks and install a new file system. **h.** Respond **y** again when you are warned that this will erase all data on the disks.

Setting up Data ONTAP on the new controller module

After the system completes disk initialization, it displays prompts for system setup. You must follow the setup prompts to enter configuration information for the new controller module.

Steps

1. Proceed through the prompts, entering the appropriate information for your site.

Example

The following example shows the first few setup prompts:

```
Please enter the new hostname []:[Respond appropriately for your site, for example
new_ctlr]
Do you want to configure virtual network interfaces? [n]:[Respond appropriately for your
site]
Please enter the IP address for Network Interface e0a
[ip_addr]:new_controller_ip_address
Please enter the netmask for Network Interface e0a [255.255.224.0]: [Respond
appropriately for your site]
:
:
```

When the setup process finishes, the Data ONTAP prompt should appear, showing the name assigned to the controller module (in the example, it is `new_ctlr`).

2. If you are running Data ONTAP 7.3.x, enter the following command with the `-r` and `-f` parameters to install the Data ONTAP operating system on the new controller module:

   `software update DOT-image-file.exe -r -f`

   `DOT-image-file` is the specific Data ONTAP image file that you downloaded from the NetApp Support Site. For example, the file name might be `7351_setup_q.exe`. In that case, you would issue the following command:

   ```
   new_ctlr>software update 7351_setup_q.exe.exe -r -f
   ```

   Note: The exact file name might differ from this example.

   The `-r` parameter will suppress the automatic reboot after the update. The `-f` parameter overwrites the existing image in the `/etc/software` directory.

   This step is not required for systems running Data ONTAP 8.x.

Enabling the cf.mode option or adding cf licenses

How you enable the high-availability functionality depends on the version of Data ONTAP you are running. Systems running software prior to Data ONTAP 8.2 use the cf license. Systems using Data ONTAP 8.2 or later use the `cf.mode` option.

Choices

- Enabling the cf.mode option on each controller module and installing licenses on the new controller (Data ONTAP 8.2) on page 11
- Adding cf licenses to both controller modules (pre-Data ONTAP 8.2) on page 12

Enabling the cf.mode option on each controller module and installing licenses on the new controller (Data ONTAP 8.2)

On systems running Data ONTAP 8.2, you must use the `options` command to set the HA mode to HA on both controller modules. Also, you must add licenses for the those Data ONTAP services licensed on the existing node so that each node has a matching set of licenses.

Steps

1. Enter the following command on each of the node consoles:

   `options cf.mode ha`

2. Add licenses for the existing controller module at the console for the new controller module:

   license add *license-key*

   The *license-key* is 28 digits in length.

3. Repeat the previous step for each required license so the new controller module has the same licenses as the existing controller module.

Adding cf licenses to both controller modules (pre-Data ONTAP 8.2)

On systems running versions of Data ONTAP prior to 8.2, you must use the `license add` command to add required licenses to both controller modules. Also, you must enable the licenses for the same Data ONTAP services on both nodes in an HA pair; otherwise, failover does not function properly.

Steps

1. Add the cf license for the new controller module by entering the following command at the new controller module's prompt:

   license add *XXXXXXX*

   Repeat this step for each required license.

2. Switch to the console for the existing controller module and add the cf license for this controller module:

   license add *XXXXXXX*

   Repeat this step for each required license.

Running setup on both controller modules to add the partner IP address

You must run setup on the controller modules and answer the prompts to add the IP address of the partner controller module.

Steps

1. Run setup on the existing controller module by entering the following command:

   setup

2. Proceed through the setup prompts, shown in *Setting up Data ONTAP on the new controller module*, and make the following changes:

   a. Enable a port on the existing controller module to take over the new partner's IP address during a failover.
   b. Enter the IP address of the new partner controller as the address to be taken over, as shown in the following example:

   #### Example

   ```
   Should interface e0a take over a partner IP address during failover? [y]:y
   Please enter the IP address or interface name to be taken over by e0a
   []:new_controller_ip_address
   ```

3. Repeat these steps on the new controller module.

4. Reboot both controller modules for the changes to take effect.

Rebooting both controller modules and enabling the HA pair

You must reboot both controller modules to implement the new configuration and issue commands to enable the HA pair on both controller modules.

Steps

1. Enable the new licenses or cf.mode option by rebooting the existing controller module and then the new controller module by entering the following command at the applicable prompt:

   `reboot`

2. After the controller modules finish rebooting, enable the HA pair by entering the following command at either controller module's prompt:

   `cf enable`

3. Verify that controller failover is enabled by entering the following command on each node console:

   `cf status`

   The system displays the following output if controller failover is enabled:
   `Controller Failover enabled, filer2 is up.`

Installing the firmware after adding a second controller module

After adding the controller module, you must install the latest firmware on the new controller module to ensure that the controller module and remote management device function properly with Data ONTAP.

Steps

1. Log in to the NetApp Support Site, select the most current version of firmware for your system from those listed at *support.netapp.com/NOW/cgi-bin/fw*, and then follow the instructions for downloading and installing the new firmware.
2. If your system uses an RLM and any version of Data ONTAP or an SP and Data ONTAP 8.1.x or earlier, select the most current version of firmware for your remote management device from those listed at *support.netapp.com/NOW/download/tools/rlm_fw* or *support.netapp.com/NOW/cgi-bin/fw*, and then follow the instructions for downloading and installing the new firmware.

   For instructions on downloading firmware for your remote management device, see the *Data ONTAP Upgrade and Revert/Downgrade Guide* for your version at *support.netapp.com*.

Cloning the configuration from the existing controller module to the new controller module

You must copy the configuration of the existing controller module to the new controller module to ensure that both nodes have matching configurations.

Before you begin

The `rsh` option must be enabled on the existing controller.

Steps

1. Clone the existing controller module's configuration data to the new controller module by entering the following command:

   `new_ctlr> config clone existing_controller_IP_address root:password`

2. Reboot the new controller module so that the cloned options take effect by entering the following command:

   new_ctlr> reboot

Verifying the configuration with the Config Advisor

The Config Advisor utility verifies that the controller modules are properly configured for failover. This utility checks licenses, network configurations, options, and so on, and provides output that shows when error conditions occur.

Steps

1. Go to the Config Advisor page on the NetApp Support Site at *support.netapp.com/NOW/download/tools/config_advisor/*.
2. Use the links and information on the page to download and run the tool.

Setting up Storage Encryption on the new controller module

If the existing system used Storage Encryption, you must configure the new controller module for Storage Encryption, including installing and setting up the key managers, certificates, and servers.

About this task

This procedure includes steps that are performed on both the existing controller module and the new controller module. Be sure to enter the command on the correct system.

Steps

1. On the *existing* controller module, enter the following commands to verify that the key server is still available:

   key_manager status

   key_manager query

   #### Example

   The following command checks the status of all key management servers linked to the storage system:

   ```
   storage-system> key_manager status
   Key server                      Status
   172.18.99.175                   Server is responding
   ```

   The following command checks the status of all key management servers linked to the storage system and displays additional information:

   ```
   storage-system> key_manager query
   Key server 172.18.99.175 is responding.

   Key server 172.18.99.175 reports 4 keys.

   Key tag                          Key ID
   --------                         -------
   storage-system                   080CF0C80...
   storage-system                   080CF0C80...
   storage-system                   080CF0C80...
   storage-system                   080CF0C80...
   ```

2. On the *new* controller module, complete the following steps to install the same SSL certificates that are on the existing controller module:

a. Copy the certificate files to a temporary location on the storage system.
b. Install the public certificate of the storage system by entering the following command at the storage system prompt:

   keymgr install cert *</path/>*client.pem
c. Install the private certificate of the storage system by entering the following command at the storage system prompt:

   keymgr install cert *</path/>*client_private.pem
d. Install the public certificate of the key management server by entering the following command at the storage system prompt:

   keymgr install cert *</path/key_management_server_ipaddress>*_CA.pem
e. If you are linking multiple key management servers to the storage system, repeat the preceding steps for each public certificate of each key management server.

3. On the *new* controller module, run the Storage Encryption setup wizard to set up and install the key servers.

You must install the same key servers that are installed on the existing controller module.

a. Enter the following command at the storage system prompt:

   key_manager setup
b. Complete the steps in the wizard to configure Storage Encryption.

Example

The following example shows how to configure Storage Encryption in Data ONTAP 8.1:

```
storage-system> key_manager setup
Found client certificate file client.pem.
Registration successful for client.pem.
Found client private key file client_private.pem.
Is this file protected by a passphrase? [no]:
Registration successful for client_private.pem.
Enter the IP address for a key server, 'q' to quit:  172.16.132.118
Enter the IP address for a key server, 'q' to quit:  172.16.132.211
Enter the IP address for a key server, 'q' to quit:  172.18.128.201
Enter the IP address for a key server, 'q' to quit:  q
Enter the TCP port number for kmip server [6001] :

You will now be prompted to enter a key tag name. The
key tag name is used to identify all keys belonging to this
Data ONTAP system. The default key tag name is based on the
system's hostname.

Would you like to use <storage-system> as the default key tag name? [yes]: yes

Registering 3 key servers...
Found client CA certificate file 172.16.132.118_CA.pem.
Registration successful for 172.16.132.118_CA.pem.
Found client CA certificate file 172.16.132.211_CA.pem.
Registration successful for 172.16.132.211_CA.pem.
Found client CA certificate file 172.18.128.201_CA.pem.
Registration successful for 172.18.128.201_CA.pem.
Registration complete.

Do you wish to enter or generate a passphrase for the system's
encrypting drives at this time? [yes]:  yes

Would you like the system to autogenerate a passphrase? [yes]:  yes

Key ID: 080CDCB200000000010000000000000003FE505B0C5E3E76061EE48E02A29822C

Make sure that you keep a copy of your passphrase, key ID, and key tag
name in a secure location in case it is ever needed for recovery purposes.

Should the system lock all encrypting drives at this time? yes
0c.00.2 successful rekey.
0c.00.4 successful rekey.
```

```
0c.00.0 successful rekey.
0c.00.3 successful rekey.
0c.00.2 successful lock.
0c.00.4 successful lock.
0c.00.0 successful lock.
0c.00.3 successful lock.
```

The following example shows how to configure Storage Encryption in Data ONTAP 8.1.1 and later:

```
storage-system*> key_manager setup
Found client certificate file client.pem.
Registration successful for client.pem.
Found client private key file client_private.pem.
Is this file protected by a passphrase? [no]:
Registration successful for client_private.pem.
Enter the IP address for a key server, 'q' to quit:  172.22.192.192
Enter the IP address for a key server, 'q' to quit:  q
Enter the TCP port number for kmip server [6001] :

You will now be prompted to enter a key tag name. The
key tag name is used to identify all keys belonging to this
Data ONTAP system. The default key tag name is based on the
system's hostname.

Would you like to use <storage-system> as the default key tag name? [yes]:

Registering 1 key servers...
Found client CA certificate file 172.22.192.192_CA.pem.
Registration successful for 172.22.192.192_CA.pem.
Registration complete.

You will now be prompted for a subset of your network configuration
setup.  These parameters will define a pre-boot network environment
allowing secure connections to the registered key server(s).

Enter network interface:  e0a
Enter IP address:  172.16.132.165
Enter netmask:   255.255.252.0
Enter gateway:  172.16.132.1

Do you wish to enter or generate a passphrase for the system's
encrypting drives at this time? [yes]:  yes

Would you like the system to autogenerate a passphrase? [yes]:  yes

Key ID: 080CDCB2000000000100000000000003FE505B0C5E3E76061EE48E02A29822C

Make sure that you keep a copy of your passphrase, key ID, and key tag
name in a secure location in case it is ever needed for recovery purposes.

Should the system lock all encrypting drives at this time? yes
Completed rekey on 4 disks: 4 successes, 0 failures, including 0 unknown key and 0
authentication failures.
Completed lock on 4 disks: 4 successes, 0 failures, including 0 unknown key and 0
authentication failures.
```

4. On the *existing* controller module, enter the applicable command to restore authentication keys either from all linked key management servers or from a specific one:
   - **key_manager restore -all**
   - **key_manager restore -key_server *key_server_ip_address***
5. On the *existing* controller module, rekey all of the disks by entering the following command at the prompt:

   key_manager rekey -keytag *key_tag*

   key_tag is the key tag name specified in the setup wizard in step 3.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Trademark information

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Customer Fitness, Cryptainer, CryptoShred, CyberSnap, Data Center Fitness, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, ExpressPod, FAServer, FastStak, FilerView, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, Snap Creator, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, VelocityStak, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the web at *www.ibm.com/legal/copytrade.shtml*.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.

Copyright information

Trademark information

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277