Manage controllers

SANtricity 11.8

NetApp
April 05, 2024

This PDF was generated from https://docs.netapp.com/us-en/e-series-santricity/sm-hardware/controller-states.html on April 05, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Manage controllers . . . 1

Controller states . . . 1

Considerations for assigning IP addresses . . . 1

Configure management port . . . 2

Configure NTP server addresses . . . 4

Configure DNS server addresses . . . 5

View controller settings . . . 6

Configure remote login (SSH) . . . 8

Place controller online . . . 10

Place controller offline . . . 10

Place controller in service mode . . . 11

Reset (reboot) controller . . . 11

Manage controllers

Controller states

You can place a controller into three different states: online, offline, and service mode.

Online state

The online state is the normal operating state of the controller. It means that the controller is operating normally and is available for I/O operations.

When you place a controller online, its status is set to optimal.

Offline state

The offline state is typically used to prepare a controller for replacement when there are two controllers in the storage array. A controller can enter the offline state in two ways: you can issue an explicit command or the controller can fail. A controller can exit the offline state only by issuing another explicit command or by replacing the failed controller. You can place a controller offline only if there are two controllers in the storage array.

When a controller is in the offline state, the following conditions are true:

- The controller is not available for I/O.
- You cannot manage the storage array through that controller.
- Any volumes currently owned by that controller are moved to the other controller.
- Cache mirroring is disabled and all volumes are changed to write through cache mode.

Service mode

Service Mode is typically used only by technical support to move all storage array volumes to one controller so that the other controller can be diagnosed. A controller must be manually placed in service mode and must be manually placed back online after the service operation is completed.

When a controller is in service mode, the following conditions are true:

- The controller is not available for I/O.
- Technical support can access the controller through the serial port or network connection to analyze potential problems.
- Any volumes currently owned by that controller are moved to the other controller.
- Cache mirroring is disabled and all volumes are changed to write through cache mode.

Considerations for assigning IP addresses

By default, controllers ship with DHCP enabled on both network ports. You can assign static IP addresses, use the default static IP addresses, or use DHCP-assigned IP addresses. You also can use IPv6 stateless auto-configuration.

> ⓘ IPv6 is disabled by default on new controllers, but you can configure the management port IP addresses using an alternate method, and then enable IPv6 on the management ports using System Manager.

When the network port is in a "link down" state, that is, disconnected from a LAN, the system reports its configuration as either static, displaying an IP address of 0.0.0.0 (earlier releases), or DHCP enabled with no IP address reported (later releases). After the network port is in a "link up" state (that is, connected to a LAN), it attempts to obtain an IP address through DHCP.

If the controller is unable to obtain a DHCP address on a given network port, it reverts to a default IP address, which might take up to 3 minutes. The default IP addresses are as follows:

```
Controller 1 (port 1): IP Address: 192.168.128.101
```

```
Controller 1 (port 2): IP Address: 192.168.129.101
```

```
Controller 2 (port 1): IP Address: 192.168.128.102
```

```
Controller 2 (port 2): IP Address: 192.168.129.102
```

When assigning IP addresses:

- Reserve Port 2 on the controllers for Customer Support usage. Do not change the default network settings (DHCP enabled).
- To set static IP addresses for E2800 and E5700 controllers, use SANtricity System Manager. To set static IP addresses for E2700 and E5600 controllers, use SANtricity Storage Manager. After a static IP address is configured, it remains set through all link down/up events.
- To use DHCP to assign the IP address of the controller, connect the controller to a network that can process DHCP requests. Use a permanent DHCP lease.

> ⓘ The default addresses are not persisted across link down events. When a network port on a controller is set to use DHCP, the controller attempts to obtain a DHCP address on every link up event, including cable insertions, reboots, and power cycles. Any time a DHCP attempt fails, the default static IP address for that port is used.

Configure management port

The controller includes an Ethernet port used for system management. If necessary, you can change its transmission parameters and IP addresses.

About this task

During this procedure, you select port 1 and then determine the speed and port addressing method. Port 1 connects to the network where the management client can access the controller and System Manager.

ⓘ Do not use port 2 on either controller. Port 2 is reserved for use by technical support.

Steps

1. Select **Hardware**.
2. If the graphic shows the drives, click **Show back of shelf**.

   The graphic changes to show the controllers instead of the drives.

3. Click the controller with the management port you want to configure.

   The controller's context menu appears.

4. Select **Configure management ports**.

   The Configure Management Ports dialog box opens.

5. Make sure port 1 is displayed, and then click **Next**.
6. Select the configuration port settings, and then click **Next**.

   Field details

Field	Description
Speed and duplex mode	Keep the Auto-negotiate setting if you want System Manager to determine the transmission parameters between the storage array and the network; or if you know the speed and mode of your network, select the parameters from the drop-down list. Only the valid speed and duplex combinations appear in the list.
Enable IPv4 / Enable IPv6	Select one or both options to enable support for IPv4 and IPv6 networks.

   If you select **Enable IPv4**, a dialog box opens for selecting IPv4 settings after you click **Next**. If you select **Enable IPv6**, a dialog box opens for selecting IPv6 settings after you click **Next**. If you select both options, the dialog box for IPv4 settings opens first, and then after you click **Next**, the dialog box for IPv6 settings opens.

7. Configure the IPv4 and/or IPv6 settings, either automatically or manually.

Field details

Field	Description
Automatically obtain configuration from DHCP server	Select this option to obtain the configuration automatically.
Manually specify static configuration	Select this option, and then enter the controller's IP address. (If desired, you can cut and paste addresses into the fields.) For IPv4, include the network subnet mask and gateway. For IPv6, include the routable IP address and router IP address. If you change the IP address configuration, you lose the management path to the storage array. If you use SANtricity Unified Manager to globally manage arrays in your network, open the user interface and go to **Manage › Discover**. If you use SANtricity Storage Manager, you must remove the device from the Enterprise Management Window (EMW), add it back to the EMW by selecting **Edit › Add Storage Array**, and then enter the new IP address.

8. Click **Finish**.

Results

The management port configuration is displayed in the controller settings, Management Ports tab.

Configure NTP server addresses

You can configure a connection to the Network Time Protocol (NTP) server so that the controller periodically queries the NTP server to update its internal time-of-day clock.

Before you begin

- An NTP server must be installed and configured in your network.
- You must know the address of the primary NTP server and an optional backup NTP server. These addresses can be fully qualified domain names, IPv4 addresses, or IPv6 addresses.

> If you enter one or more domain names for the NTP servers, you must also configure a DNS server to resolve the NTP server address. You need to configure the DNS server only on those controllers where you configured NTP and provided a domain name.

About this task

NTP enables the storage array to automatically synchronize the controller's clocks with an external host using Simple Network Time Protocol (SNTP). The controller periodically queries the configured NTP server, and then uses the results to update its internal time-of-day clock. If only one controller has NTP enabled, the alternate controller periodically synchronizes its clock with the controller that has NTP enabled. If neither controller has NTP enabled, the controllers periodically synchronize their clocks with each other.

You do not need to configure NTP on both controllers; however, doing so improves the storage array's ability to stay synchronized during hardware or communication failures.

Steps

1. Select **Hardware**.
2. If the graphic shows the drives, click **Show back of shelf**.

   The graphic changes to show the controllers instead of the drives.

3. Click the controller you want to configure.

   The controller's context menu appears.

4. Select **Configure NTP server**.

   The Configure Network Time Protocol (NTP) Server dialog box opens.

5. Select **I want to enable NTP on Controller** (**A** or **B**).

   Additional selections appear in the dialog box.

6. Select one of the following options:
   - **Automatically obtain NTP server addresses from DHCP server** — The detected NTP server addresses are shown.

     If the storage array is set to use a static NTP address, no NTP servers appear.

   - **Manually specify NTP server addresses** — Enter the primary NTP server address and a backup NTP server address. The backup server is optional. (These address fields appear after you select the radio button.) The server address can be a fully qualified domain name, IPv4 address, or IPv6 address.
7. **Optional:** Enter server information and authentication credentials for a backup NTP server.
8. Click **Save**.

Results

The NTP server configuration is displayed in the controller settings, **DNS / NTP** tab.

Configure DNS server addresses

Domain Name System (DNS) is used to resolve fully qualified domain names for the controllers and a Network Time Protocol (NTP) server. The management ports on the storage array can support IPv4 or IPv6 protocols simultaneously.

Before you begin

- A DNS server must be installed and configured in your network.
- You know the address of the primary DNS server and an optional backup DNS server. These addresses can be IPv4 addresses or IPv6 addresses.

About this task

This procedure describes how to specify a primary and backup DNS server address. The backup DNS server can be optionally configured to use if a primary DNS server fails.

> If you already configured the storage array's management ports with Dynamic Host Configuration Protocol (DHCP), and you have one or more DNS or NTP servers associated with the DHCP setup, then you do not need to manually configure DNS or NTP. In this case, the storage array should have already obtained the DNS/NTP server addresses automatically. However, you should still follow the instructions below to open the dialog box and make sure that the correct addresses are detected.

Steps

1. Select **Hardware**.
2. If the graphic shows the drives, click **Show back of shelf**.

   The graphic changes to show the controllers instead of the drives.

3. Select the controller to configure.

   The controller's context menu appears.

4. Select **Configure DNS server**.

   The Configure Domain Name System (DNS) Server dialog box opens.

5. Select one of the following options:
   - **Automatically obtain DNS server addresses from DHCP server** — The detected DNS server addresses are shown.

     > If the storage array is set to use a static DNS address, no DNS servers appear.

   - **Manually specify DNS server addresses** — Enter a primary DNS server address and a backup DNS server address. The backup server is optional. (These address fields appear after you select the radio button.) These addresses can be IPv4 addresses or IPv6 addresses.
6. Click **Save**.
7. Repeat these steps for the other controller.

Results

The DNS configuration is displayed in the controller settings, **DNS / NTP** tab.

View controller settings

You can view information about a controller, such as the status of the host interfaces, drive interfaces, and management ports.

Steps

1. Select **Hardware**.
2. If the graphic shows the drives, click **Show back of shelf**.

   The graphic changes to show the controllers instead of the drives.

3. Do one of the following actions to display the controller settings:

   - Click the controller to display the context menu, and then select **View settings**.
   - Select the controller icon (next to the **Shelf** drop-down list). For duplex configurations, select either **Controller A** or **Controller B** from the dialog box, and then click **Next**.

     The Controller Settings dialog box opens.

4. Select the tabs to move between property settings.

   Some tabs have a link for **Show more settings** at the top right.

Field details

Tab	Description
Base	Shows the controller status, model name, replacement part number, current firmware version, and the non-volatile static random access memory (NVSRAM) version.
Cache	Shows the cache settings of the controller, which include the data cache, processor cache, and the cache backup device. The cache backup device is used to back up data in the cache if you lose power to the controller. Status can be Optimal, Failed, Removed, Unknown, Write Protected, or Incompatible.
Host Interfaces	Shows the host interface information and the link status of each port. The host interface is the connection between the controller and the host, such as Fibre Channel or iSCSI. ⓘ The host interface card (HIC) location is either in the baseboard or in a slot (bay). "Baseboard" indicates that the HIC ports are built into the controller. "Slot" ports are on the optional HIC.
Drive Interfaces	Shows the drive interface information and the link status of each port. The drive interface is the connection between the controller and the drives, such as SAS.
Management Ports	Shows the management port details, such as the host name used to access the controller and whether a remote login has been enabled. The management port connects the controller and the management client, which is where a browser is installed for accessing System Manager.
DNS / NTP	Shows the addressing method and IP addresses for the DNS server and the NTP server, if these servers have been configured in System Manager. Domain Name System (DNS) is a naming system for devices connected to the Internet or a private network. The DNS server maintains a directory of domain names and translates them to Internet Protocol (IP) addresses. Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems in data networks.

5. Click **Close**.

Configure remote login (SSH)

By enabling remote login, you allow users from outside the local area network to start an SSH session and access settings on the controller.

For SANtricity versions 11.74 and later, you can also configure multifactor authorization (MFA) by requiring users to enter an SSH key and/or SSH password. For SANtricity versions 11.73 and earlier, this feature does *not* include an option for multifactor authorization with SSH keys and passwords.

> ! **Security risk** — For security reasons, only technical support personnel should use the Remote Login feature.

Steps

1. Select **Hardware**.
2. If the graphic shows the drives, click **Show back of shelf**.

   The graphic changes to show the controllers instead of the drives.

3. Click the controller for which you want to configure remote login.

   The controller’s context menu appears.

4. Select **Configure remote login (SSH)**. (For SANtricity versions 11.73 and earlier, this menu item is **Change remote login**.)

   The dialog box opens for enabling remote login.

5. Select the **Enable remote login** checkbox.

   This setting provides remote login with three options for authorization:

   - **Password only**. For this option, you are done and can click **Save**. If you have a duplex system, you can enable remote login on the second controller by following the previous steps.
   - **Either SSH key or password**. For this option, proceed to the next step.
   - **Both password and SSH key**. For this option, select the **Require authorized public key and password for remote login** checkbox and proceed to the next step.
6. Populate the **Authorized public key** field. This field contains a list of authorized public keys, in the format of the OpenSSH **authorized_keys** file.

   When populating the **Authorized public key** field, be aware of the following guidelines:

   - The **Authorized public key** field applies to both controllers and only needs to be configured on the first controller.
   - The **authorized_keys** file should contain only one key per line. Lines starting with # and empty lines are ignored. For more information about the file format, see Configuring Authorized Keys for OpenSSH.
   - An **authorized_keys** file should look similar to the following example:

   ```
   ssh-rsa
   AAAAB3NzaC1yc2EAAAADAQABAAABAQDJlG20rYTk4ok+xFjkPHYp/R0LfJqEYDLXA5AJ4
   9w3DvAWLrUg+1CpNq76WSqmQBmoG9jgbcAB5ABGdswdeMQZHilJcu29iJ3OKKv6SlCulA
   j1tHymwtbdhPuipd2wIDAQAB
   ```

7. When you’re done, click **Save**.
8. For duplex systems, you can enable remote login on the second controller by following the steps above. If

you are configuring the option for both a password and SSH key, be sure to select the **Require authorized public key and password for remote login** checkbox again.

9. After technical support is finished troubleshooting, you can disable remote login by returning to the Configure Remote Login dialog box and de-selecting the **Enable remote login** checkbox. If remote login is enabled on a second controller, a confirmation dialog opens and allows you to disable remote login on the second one as well.

   Disabling remote login terminates any current SSH sessions and rejects any new login requests.

Place controller online

If a controller is in the offline state or in service mode, you can place it back online.

Steps

1. Select **Hardware**.
2. If the graphic shows the drives, click **Show back of shelf**.

   The graphic changes to show the controllers instead of the drives.

3. Click a controller that is in either the offline state or service mode.

   The controller’s context menu appears.

4. Select **Place online**, and confirm that you want to perform the operation.

Results

Detection of a restored preferred path by the multipath driver can take up to 10 minutes.

Any volumes originally owned by this controller are automatically moved back to the controller as I/O requests are received for each volume. In some cases, you might need to manually redistribute the volumes with the **Redistribute volumes** command.

Place controller offline

If you are instructed to do so, you can place a controller offline.

Before you begin

- Your storage array must have two controllers. The controller that you are not placing offline must be online (in the optimal state).
- Make sure that no volumes are in use or that you have a multipath driver installed on all hosts using these volumes.

About this task

> Do not place a controller offline unless you are instructed to do so by the Recovery Guru or technical support.

Steps

1. Select **Hardware**.

2. If the graphic shows the drives, click **Show back of shelf**.

   The graphic changes to show the controllers instead of the drives.

3. Click the controller that you want to place offline.

   The controller’s context menu appears.

4. Select **Place offline**, and confirm that you want to perform the operation.

Results

It might take several minutes for System Manager to update the controller’s status to offline. Do not begin any other operations until after the status has been updated.

Place controller in service mode

If you are instructed to do so, you can place a controller in service mode.

Before you begin

- The storage array must have two controllers. The controller that you are not placing in service mode must be online (in the optimal state).
- Make sure that no volumes are in use or that you have a multipath driver installed on all hosts using these volumes.

> ⓘ Placing a controller in service mode might significantly reduce performance. Do not place a controller in service mode unless you are instructed to do so by technical support.

Steps

1. Select **Hardware**.
2. If the graphic shows the drives, click **Show back of shelf**.

   The graphic changes to show the controllers instead of the drives.

3. Click the controller that you want to place into service mode.

   The controller’s context menu appears.

4. Select **Place in service mode**, and confirm that you want to perform the operation.

Reset (reboot) controller

Some issues require a controller reset (reboot). You can reset the controller even if you don’t have physical access to it.

Before you begin

- The storage array must have two controllers. The controller that you are not resetting must be online (in the optimal state).
- Make sure that no volumes are in use or that you have a multipath driver installed on all hosts using these volumes.

Steps

1. Select **Hardware**.
2. If the graphic shows the drives, click **Show back of shelf**.

   The graphic changes to show the controllers instead of the drives.

3. Click the controller that you want to reset.

   The controller’s context menu appears.

4. Select **Reset**, and confirm that you want to perform the operation.

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.