Contents

Overview of the software setup process ..........................................................  6
  Setting up the software .................................................................................... 6
  Default storage system configuration ............................................................ 7
  The setup process ............................................................................................ 8
  Setup methods .................................................................................................. 9

Prerequisites to initial configuration .............................................................. 10
  Requirements for the administration host ....................................................... 10
  High-availability configuration requirements ................................................ 11
  Requirements for Windows domains ............................................................... 11
    Assigning domain administrator privileges ............................................... 11
    Creating a storage system domain account before setting up CIFS .......... 12
  Requirements for Active Directory authentication .......................................... 13
    DNS requirements for Active Directory ..................................................... 13
    Network infrastructure requirements for Active Directory ....................... 14
  Time services requirements ............................................................................. 15
  Switch configuration requirements for interface groups .............................. 15
  DHCP requirements for remote access ......................................................... 16
  Configuring dedicated management ports .................................................... 16
  Licensing requirements for systems that use array LUNs ............................. 17

Configuration information you need to gather ............................................. 18
  Software setup configuration worksheet ....................................................... 19
  Required storage system information .......................................................... 24
  Information required to set up network connections ...................................... 26
  Interface group information .......................................................................... 31
  HTTP information .......................................................................................... 33
  DNS services information ................................................................................ 34
  NIS services information ................................................................................ 35
  CIFS protocol information .............................................................................. 35
  Service processor information ....................................................................... 40
  Shelf Alternate Control Path Management configuration information .......... 41
  Information to collect before configuring Storage Encryption ...................... 42

Setting up your storage system for using native disk shelves .................... 44
Prerequisites for setup ............................................................... 44
Responding to setup command prompts ........................................ 45
Setting up CIFS ................................................................................ 51
Responding to sp setup command prompts ...................................... 54
Setting up Storage Encryption .......................................................... 57
  What Storage Encryption is .......................................................... 57
  Limitations of Storage Encryption ............................................... 58
Using SSL for secure key management communication ................... 58
Requirements for SSL certificates .................................................. 59
Installing SSL certificates on the storage system .............................. 59
Running the Storage Encryption setup wizard .................................... 60

Additional steps to set up a Data ONTAP system that uses both disks and array LUNs ................................................................. 61

Data ONTAP systems that can use array LUNs on storage arrays ...... 63
Setting up your system to use only array LUNs ................................. 64
Prerequisites for starting setup when using only array LUNs ............... 64
Providing ownership and system ID for Data ONTAP systems using array LUNs ................................................................................. 65

Installing Data ONTAP software on a system that uses only array LUNs ......................................................................................... 68
Data ONTAP installation stages .......................................................... 68
Obtaining Data ONTAP software images ........................................... 68
  Obtaining images for HTTP servers ........................................... 69
  Obtaining images for UNIX clients .............................................. 70
  Obtaining images for Windows clients ........................................ 71
Installing Data ONTAP software images ............................................ 73
  Installing software images from the /etc/software directory .......... 74
  Installing software images from an HTTP server ........................ 75

Commands for managing files in the /etc/software directory .......... 77

Required licenses for setting up a Data ONTAP system that uses array LUNs ................................................................. 77

Verifying software setup ........................................................................ 78
Verifying network connectivity .......................................................... 78
  Troubleshooting connections to new network interfaces .................. 79
Verifying host-name resolution .......................................................... 79
Verifying setup of dedicated management ports .................................. 80
Verifying that the storage system is available ....................................... 81
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing licenses</td>
<td>82</td>
</tr>
<tr>
<td>Preparing NFS clients to access the storage system</td>
<td>83</td>
</tr>
<tr>
<td>Enabling or disabling NFS on the storage system</td>
<td>83</td>
</tr>
<tr>
<td>Exporting file systems to NFS clients</td>
<td>84</td>
</tr>
<tr>
<td>Preparing CIFS clients to access the storage system</td>
<td>86</td>
</tr>
<tr>
<td>Creating a storage system DNS &quot;A&quot; record for CIFS client access</td>
<td>86</td>
</tr>
<tr>
<td>Ways to verify the configuration for HA pairs</td>
<td>87</td>
</tr>
<tr>
<td>Verifying the HA pair configuration</td>
<td>87</td>
</tr>
<tr>
<td>Configuring a node for non-HA (stand-alone) use</td>
<td>88</td>
</tr>
<tr>
<td>Setting up AutoSupport</td>
<td>90</td>
</tr>
<tr>
<td>Verifying SP connections</td>
<td>92</td>
</tr>
<tr>
<td>Preparing to use OnCommand System Manager</td>
<td>93</td>
</tr>
<tr>
<td>Verifying the existence of two paths to an array LUN</td>
<td>94</td>
</tr>
<tr>
<td>Verifying the existence of two paths: storage show disk command</td>
<td>94</td>
</tr>
<tr>
<td>Verifying the existence of two paths: storage array show-config command</td>
<td>95</td>
</tr>
<tr>
<td>Verifying path failover for array LUNs</td>
<td>96</td>
</tr>
<tr>
<td>Verifying path failover for array LUNs in a stand-alone system</td>
<td>96</td>
</tr>
<tr>
<td>Verifying path failover for array LUNs in an HA pair</td>
<td>96</td>
</tr>
<tr>
<td><strong>Data ONTAP documentation</strong></td>
<td>98</td>
</tr>
<tr>
<td><strong>Time zones</strong></td>
<td>100</td>
</tr>
<tr>
<td>Time zones by geographical region</td>
<td>100</td>
</tr>
<tr>
<td>GMT offset and miscellaneous time zones</td>
<td>106</td>
</tr>
<tr>
<td><strong>Supported languages</strong></td>
<td>109</td>
</tr>
<tr>
<td>Specifying the language code</td>
<td>109</td>
</tr>
<tr>
<td>Language choices</td>
<td>109</td>
</tr>
<tr>
<td><strong>Troubleshooting setup</strong></td>
<td>111</td>
</tr>
<tr>
<td>Troubleshooting boot failure after system power on</td>
<td>111</td>
</tr>
<tr>
<td>Checking disk ownership</td>
<td>112</td>
</tr>
<tr>
<td>Retrying system setup</td>
<td>112</td>
</tr>
<tr>
<td>Retrying CIFS setup</td>
<td>113</td>
</tr>
<tr>
<td><strong>Copyright information</strong></td>
<td>114</td>
</tr>
<tr>
<td><strong>Trademark information</strong></td>
<td>115</td>
</tr>
<tr>
<td><strong>How to send your comments</strong></td>
<td>116</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>117</td>
</tr>
</tbody>
</table>
Overview of the software setup process

You can set up Data ONTAP software to use native disks and array LUNs. The software setup process consists of satisfying prerequisites, gathering and entering configuration information at setup prompts, and verifying network connections, licenses, and configuration settings.

Setting up the software

The software setup process for your new storage system requires several steps after you have completed hardware setup. You must gather configuration information, power on the system, enter configuration information when the setup command runs, and verify the system configuration.

Before you begin

- You must have prepared the physical site for your new storage system and you must have racked and cabled storage system hardware according to the following documents:
  - Site Requirements Guide
  - Installation and Setup Instructions
  - Data ONTAP High Availability and MetroCluster Configuration Guide for 7-Mode

- Make sure that your serial console or laptop is connected to the storage controller through the IOIOI port.

- Make sure that storage system components and external switches are powered up in the correct order.
  The order is especially important the first time you boot the system to ensure that initial configuration is completed correctly.

- You must have ensured that your network and storage environment meet storage system requirements.

  Note: The Data ONTAP High Availability and MetroCluster Configuration Guide for 7-Mode also includes important information about HA configuration prerequisites and verification procedures that you need to consult during the software setup process.

About this task

If your storage system is intended for use with LUNs on a storage array, you have additional configuration requirements.
Steps

1. Gather system configuration information and record it in the worksheet provided.

2. Power on the new system.

3. Choose one of the following options depending on your storage system configuration:

<table>
<thead>
<tr>
<th>If you are setting up your storage system for using...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Native disk shelves</td>
<td>Enter the information you gathered when the <code>setup</code> command begins to run. You do not need to install Data ONTAP software.</td>
</tr>
<tr>
<td>Only array LUNs</td>
<td>In maintenance mode, perform tasks for setting up your system to access array LUNs. This includes entering the information that you gathered when the <code>setup</code> command begins to run and installing Data ONTAP software.</td>
</tr>
</tbody>
</table>

4. Verify that basic system functionality has been configured correctly.

5. Configure system features and provision those features as described in relevant documents of the Data ONTAP library.

Related concepts

- Prerequisites to initial configuration on page 10
- Configuration information you need to gather on page 18
- Setting up your storage system for using native disk shelves on page 44
- Verifying software setup on page 78
- Data ONTAP systems that can use array LUNs on storage arrays on page 63

Related tasks

- Setting up your system to use only array LUNs on page 64

Related information

Documentation: By Product Library: support.netapp.com/documentation/productsatoz/index.html

Default storage system configuration

Before your storage system was shipped to you, a series of tasks was performed to configure your storage system for use. These tasks simplify the setup process and ensure that you can run the `setup` script on systems with native disk shelves.

Storage systems that use only array LUNs require a number of prerequisite configuration steps and software installation before you run the setup script.
The following tasks were performed on storage systems containing native disk shelves:

- Your storage system was configured at the factory with an aggregate and FlexVol root volume.
  - For storage systems that have Data ONTAP 7.0 or later installed at the factory, the root volume is a FlexVol volume.
  - The root volume is installed at the factory on FAS systems and, starting with Data ONTAP 7.3, also on V-Series systems ordered with disk shelves.
- Licenses (such as CIFS and NFS) that you have purchased were installed on your system.
- Bootloader files and firmware updates, including primary and secondary BIOS images, were installed on the boot device that was shipped with your system.

Related concepts

_Data ONTAP systems that can use array LUNs on storage arrays_ on page 63

**The setup process**

On systems with preinstalled software, when your new system is powered on for the first time, the setup script runs. The software setup process collects information that enables the storage system to serve data in your environment.

**Note:** For a Data ONTAP system that is ordered without native disk shelves, you must perform prerequisite configuration steps before running the setup script.

When Data ONTAP software is installed on your new storage system, the following files are not populated:

- `/etc/rc`
- `/etc/exports`
- `/etc/hosts`
- `/etc/hosts.equiv`
- `/etc/nsswitch.conf`
- `/etc/resolv.conf`

During software setup, you can enter configuration values to populate these files and to configure the installed functionality of your system. Your system's hardware configuration and licenses determine which values and functionality you can enter.

You have the option to enter configuration values manually in the command-line interface, or have configuration values populated from information in a DHCP server, depending on the setup method.
you select. You can also choose to enter all initial configuration values during the setup process or to enter only essential networking values and complete the initial configuration at a later time.

If the storage system is properly configured with self-encrypting disks and is running a version of Data ONTAP that supports Storage Encryption, you can launch the Storage Encryption setup wizard after completion of the storage system setup wizard.

**Related tasks**

*Setting up Storage Encryption* on page 57

---

**Setup methods**

You can provide initial setup configuration values through the command-line interface. This method requires a serial console connection or a network connection.

The most common method to set up a new system is to enter configuration values at the storage system command-line interface in a serial console session.

When you boot your system for the first time, a DHCP broadcast is issued from the management port (e0M, if your system has one) or from the first onboard network interface (usually e0a). If there is no response to the DHCP broadcast, the `setup` command begins to run automatically on the system console. You can also elect to disregard a DHCP server response and enter configuration values at the command-line interface.

The `setup` script collects information to populate configuration files and to configure the installed functionality of your system. You might also be prompted to respond to `setup` commands for other system features.

**Note:** You cannot use OnCommand System Manager for initial setup of the storage system.
Prerequisites to initial configuration

Before you begin the software setup process, you must ensure that you have prepared your network and storage environment for your new storage system and installed licenses.

Requirements for the administration host

You should designate a Windows or UNIX client workstation as an administration host to limit access to the storage system's root file system, to provide a text editor to edit configuration files, or to provide the ability to administer a storage system remotely.

During the setup process, you are prompted to designate a workstation on the network as an administration host. For more information about administration hosts, see the Data ONTAP System Administration Guide for 7-Mode.

Windows and UNIX client workstations can serve as administration hosts, with these requirements and privileges:

- If you plan to use a Windows client to manage the storage system, the Windows client must support a secure protocol such as SSH or SSL.
  You can edit configuration files from any Windows client as long as you connect to the storage system as root or Administrator.

- If you plan to use a UNIX client to manage the storage system, the UNIX client must meet the following requirements:
  - Support a text editor that can display and edit text files containing lines ending with the newline character
  - Support a secure protocol such as SSH or SSL
  - Support the mounting of directories using the NFS protocol
  When connecting from a UNIX client, the administrator operates as root.

Attention: If you change the name or IP address of an administration host on a storage system that has already been set up and configured, the /etc/exports files are overwritten on system reboot.
High-availability configuration requirements

The different types of HA pair offer access to storage through two different controllers. Each type has its own benefits and requirements.

For information about preparing your environment for a new HA pair, see the Data ONTAP High Availability and MetroCluster Configuration Guide for 7-Mode.

Requirements for Windows domains

If you use Windows NT4-style authentication and are adding your system to a Windows domain, the storage system administrator account must have permissions to add the system to an Active Directory domain. It might also be necessary to create a domain account for your new system before initial setup.

Permissions for adding a storage system to an Active Directory domain are the same as permissions required for adding any Windows server.

**Note:** When you run the `cifs setup` command, a Windows directory account is automatically created, unless you intend to use Windows NT4-style authentication. To use Windows NT4-style authentication, you must create a domain account by using Windows tools before you run the `cifs setup` command. If you do not perform this action, the `cifs setup` command terminates, prompting you to create the domain account.

Assigning domain administrator privileges

Before adding a storage system to a Windows Active Directory domain, organizational unit (OU), or other Active Directory container object, you need to ensure that the storage system administrator account has sufficient privileges and permissions to add a Windows Active Directory server to that domain or object.

About this task

When the `cifs setup` program adds the storage system to an Active Directory environment, it creates an Active Directory domain computer object and joins the storage system’s computer account to that domain. Before this happens, you need to assign permissions to certain domain objects.

**Note:** This procedure applies to a Windows 2000 or 2003 Server. Details of this procedure might vary on other Windows server versions. For more information about the supported Windows operating systems, see the Interoperability Matrix.
Steps

1. In the Active Directory Users and Computers View menu, ensure that the Advanced Features menu item is selected.

2. In the Active Directory tree, select the OU for your storage system.

3. Select the user or group that can add the storage system to the domain.

4. In the Permissions list, ensure that the following check boxes are enabled:
   - Change Password
   - Write Public Information
   - Create Computer Objects

Related information

*Interoperability Matrix: support.netapp.com/matrix*

Creating a storage system domain account before setting up CIFS

You must create the storage system domain account before the `cifs setup` command is run if your security structure does not allow you to assign the necessary permissions to the setup program to create the storage system domain account, or if you intend to use Windows NT4-style authentication.

About this task

If you create the storage system domain account before the `cifs setup` command is run, you must follow these guidelines:

- You do not need to assign the Create Computer Objects permission.
- You can assign permissions specifically on the storage system domain account, instead of assigning them on the storage system container.

Steps

1. In the Active Directory Users and Computers View menu, ensure that the Advanced Features menu item is selected.

2. In the Active Directory tree, locate the Organizational Unit (OU) for your storage system, right-click and select **New > Computer**.

3. Enter the storage system (domain account) name.
   
   You must make a note of the storage system name you entered, to ensure that you enter it correctly when you run the `cifs setup` command later.
4. In the "Add this computer to the domain" field, specify the name of the storage system administrator account.

5. Right-click the computer account you just created, and select Properties from the pop-up menu.

6. Click the Security tab.

7. Select the user or group that adds the storage system to the domain.

8. In the Permissions list, ensure that the following check boxes are selected:
   - Change Password
   - Write Public Information

**After you finish**

When the cifs setup command is run, you see the prompt "Please enter the new hostname." Enter the storage system name you specified in Step 3.

**Requirements for Active Directory authentication**

If you are deploying your new system in an Active Directory domain with Kerberos or NTLM authentication, you need to ensure that DNS and network infrastructure are configured correctly before initial system setup.

**Note:** Kerberos 5 authentication depends upon the synchronization of time between the clients and the Kerberos Key Distribution Centers (KDCs).

**Related concepts**

*Time services requirements* on page 15

**Related tasks**

*Creating a storage system DNS "A" record for CIFS client access* on page 86

**Related information**

*Unified Windows and UNIX Authentication Using Microsoft Active Directory Kerberos:*

www.netapp.com/us/media/tr-3457.pdf

**DNS requirements for Active Directory**

Active Directory Kerberos requires that a standards-based DNS implementation be configured. The implementation must support service locator records.

Your DNS solution must have the following capabilities:
The DNS solution must be standards-based (RFC 1035).

Service locator records must be supported.

The following additional capabilities are recommended:

- Support for dynamic updates
- Support for incremental zone transfers

The following DNS solutions meet the requirements:

  This Active Directory integrated DNS provides the recommended capabilities. Service locator records are configured automatically.

- Berkeley Internet Name Domain (BIND) DNS
  If you use BIND DNS, you need to manually configure the service locator records.

**Network infrastructure requirements for Active Directory**

You should ensure that clients have reliable network connections with the storage system, DNS servers, time servers, and Active Directory domain controllers.

You must verify the following network infrastructure functionality:

- To ensure that clients can find the Active Directory LDAP and Kerberos servers, there must be reliable network connectivity between the clients and DNS servers containing the LDAP and Kerberos service records.
  If possible, this should be a high-bandwidth connection.

- Clients must have reliable connections to domain controllers that host both the LDAP and Kerberos services.
  If possible, this should be a high-bandwidth connection.

- When the enterprise contains more than one domain or utilizes universal groups, there must be adequate connectivity from domain controllers to a global catalog server.
  If possible, this should be a high-bandwidth connection.

- If the enterprise is located in multiple locations that have low-bandwidth connectivity, you should configure Active Directory sites.
  These sites group resources within a local high-bandwidth zone.

- If clients from other domains access resources on the storage system, there should be reliable connectivity between the storage system and all domain controllers with users who access resources on the storage system.
Time services requirements

You must configure your storage system for time service synchronization. Many services and applications depend on accurate time synchronization.

During CIFS setup, if the storage system is to be joined to an Active Directory domain, Kerberos authentication is used. Kerberos authentication requires the storage system's time and the domain controller's time to match (within 5 minutes). If the times do not match within 5 minutes, setup and authentication attempts fail.

By default, within Active Directory domains, all domain controllers synchronize to the domain controller that is configured as the PDC Emulator Master. Therefore, one of the following configurations is required:

- All storage systems are configured to synchronize to one of the domain controllers.
- Both the storage systems and the controller are configured to synchronize to a central time server.

For more information about time services supported by Data ONTAP, see the Data ONTAP System Administration Guide for 7-Mode.

Switch configuration requirements for interface groups

If you use interface groups, you must ensure that your switches support the interface group type required for your storage system before powering on for the first time.

<table>
<thead>
<tr>
<th>Interface group</th>
<th>Switch support requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic multimode</td>
<td>Link Aggregation Control Protocol (LACP)</td>
</tr>
<tr>
<td>Static multimode</td>
<td>Aggregates (but must not have control packet exchange for configuring an aggregate)</td>
</tr>
<tr>
<td>Single-mode</td>
<td>No special switch requirements</td>
</tr>
</tbody>
</table>

For more information about interface groups, see the Data ONTAP Network Management Guide for 7-Mode.
DHCP requirements for remote access

When you enable Dynamic Host Configuration Protocol (DHCP) to assign a static IP address to an onboard network interface during first-time setup, you can complete the configuration remotely by using an SSH client.

If your system includes an e0M interface, the system broadcasts a DHCP request through it. If a DHCP server responds, it assigns an IP address to the e0M interface. If your system does not have an e0M interface, the system uses the first onboard network interface (e0a) for the DHCP broadcast.

When you use DHCP to assign an IP address to the onboard interface, the storage system performs the following operations:

- Obtains the address from the DHCP server when the storage system is turned on
- Configures the onboard interface with the IP address
- Becomes accessible to an SSH client

**Attention:** When you use DHCP with a storage system, you must ensure that the DHCP server is configured to return a static IP address for the interface. If the server returns a dynamic IP address, the storage system displays an error message and continues to use the IP address permanently. This can result in an IP address conflict if the DHCP server assigns the IP address dynamically to other clients from time to time.

DHCPv6 servers are not currently supported.

Configuring dedicated management ports

Before running setup, you need to ensure that the e0M interfaces are serving only management traffic on a dedicated management LAN or that they are configured down after running setup.

**About this task**

You should not use the e0M interface for data traffic, as it can cause performance and routing problems. To configure dedicated management ports, follow steps 1–4 before running setup, and step 5 during setup.

**Note:** These steps apply to only storage systems that have an e0M dedicated management port.

**Steps**

1. Identify a dedicated management subnet on which to configure e0M addresses.
2. Ensure that no data clients have addresses on that subnet and that no storage system addresses that serve data are on that subnet.

3. Ensure that DNS and NIS do not advertise storage system addresses on that subnet.

4. Ensure that static routes that use gateway addresses on that subnet are never used for data traffic.

5. If you cannot meet these conditions, configure the dedicated management ports (e0M) down after running the `setup` command:
   a. Mount the NFS root volume.
   b. Append the command `ifconfig e0M down` to the `/etc/rc` file.

6. If you can meet these conditions, perform these additional steps:
   a. When configuring the e0M interface, partner it with the e0M interface on the HA partner. You can do this step while running the `setup` command.
   b. Set the following option to on to block data traffic on both HA partners:
      
      ```
      interface.blocked.mgmt_data_traffic on
      ```

      You must do this step after running the `setup` command.

   For more information about using the e0M interface to manage Data ONTAP, see the Data ONTAP System Administration Guide for 7-Mode and the Data ONTAP Network Management Guide for 7-Mode.

**Licensing requirements for systems that use array LUNs**

You must install a license to operate a Data ONTAP system that uses array LUNs.

If you order a Data ONTAP system with native disks, the factory installs the Data ONTAP software and the licenses would be available on your system. If you order your system without native disks, you must install the Data ONTAP software and licenses after running the setup program.

**Related concepts**

*Required licenses for setting up a Data ONTAP system that uses array LUNs* on page 77
Configuration information you need to gather

Before powering on your storage system for the first time, you should use the configuration worksheet to gather the information that the software setup process requires.

If you are configuring a storage system as part of a high-availability configuration, some types of information must be unique for each storage system in the configuration, and some types of information must be identical on both storage systems. Both nodes of the HA pair should have identical licenses installed.

For more information, see the *Data ONTAP High Availability and MetroCluster Configuration Guide for 7-Mode.*
**Software setup configuration worksheet**

You can use the configuration worksheet to record values that you will use during the software setup process.

<table>
<thead>
<tr>
<th>Category</th>
<th>Types of information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licenses</td>
<td>Usually Data ONTAP systems ordered with disks come with licenses preinstalled. You can use the <code>license show</code> command at the storage system command line to verify that the appropriate licenses are installed on your system or to configure additional licenses. You can find license keys for your initial or add-on software orders at the NetApp Support Site under <strong>My Support &gt; Software Licenses</strong>. For instance, you can search with the serial number of a system to find all license keys associated with the system. If you cannot locate your license keys from the Software Licenses page, you should contact your sales or support representative. Record your license keys here. You can install licenses for optional features either before or after running the <code>setup</code> script. <strong>Note:</strong> After you finish setting up Data ONTAP and can access the CLI, wait at least five minutes before trying the <code>license show</code> command to see which licenses are installed. For more information, see the knowledgebase article <strong>Data ONTAP 8.2 Licensing Overview and References</strong> on the NetApp Support Site and <strong>Data ONTAP System Administration Guide for 7-Mode</strong>.</td>
<td></td>
</tr>
<tr>
<td>Terminal server</td>
<td>TCP/IP address</td>
<td></td>
</tr>
<tr>
<td>(sometimes used for remote serial console port access)</td>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Types of information</td>
<td>Your values</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Storage system</td>
<td>Host name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time zone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Storage system location</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Language used for multiprotocol storage systems:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NFS Classic (v2 or v3) only—Language setting does not matter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NFS Classic (v2 or v3) and CIFS—Language of the clients</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NFS v4, with or without CIFS—<code>cl_lang.UTF-8</code>, where <code>cl_lang</code> is the language of the clients.</td>
<td></td>
</tr>
<tr>
<td>Administration host</td>
<td>Host name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>Interface groups</td>
<td>Name of the interface group (such as ig0)</td>
<td></td>
</tr>
<tr>
<td>(include information for each interface group)</td>
<td>Mode type (single, multi, or LACP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Load balancing type (IP based, MAC address based, port based, or round-robin based)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Number of links (number of physical interfaces to include in the interface group)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Link names (physical interface names such as e0a, e5a, or e9b)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP address for the interface group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subnet mask (IPv4) or subnet prefix length (IPv6) for the interface group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Partner interface group name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Media type for the interface group</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Types of information</td>
<td>Your values</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Ethernet interfaces (if not using interface groups)</td>
<td>Interface name (include information for each interface port, such as e0a, e5a)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPv4</td>
<td>Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subnet mask</td>
</tr>
<tr>
<td></td>
<td>IPv6 (not always used)</td>
<td>Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subnet prefix length</td>
</tr>
<tr>
<td></td>
<td>Partner IP address or interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Media type (network type)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Are jumbo frames supported?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MTU size for jumbo frames</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Flow control</td>
<td></td>
</tr>
<tr>
<td>e0M interface (if available)</td>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network mask</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Partner IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Flow control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The e0M management interface either should be on a separate subnet from the controller's other data ports or configured down.</td>
<td></td>
</tr>
<tr>
<td>Router (if used)</td>
<td>Gateway name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPv4 address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPv6 address</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>Location of HTTP directory</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>Domain name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Server address 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Server address 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Server address 3</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Types of information</td>
<td>Your values</td>
</tr>
<tr>
<td>----------</td>
<td>----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>NIS</td>
<td>Domain name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Server address 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Server address 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Server address 3</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Types of information</td>
<td>Your values</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CIFS</td>
<td>Windows domain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WINS servers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Multiprotocol or NTFS-only storage system?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Should CIFS create default <code>/etc/passwd</code> and <code>/etc/group</code> files?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NIS group caching</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hours to update the cache</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CIFS server name (if different from default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User authentication style:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(1) Active Directory domain authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Active Directory domains only)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(2) Windows NT 4 domain authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Windows NT or Active Directory domains)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(3) Windows Workgroup authentication using the storage system's local user accounts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(4) <code>/etc/passwd</code> and/or NIS/LDAP authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Joining the CIFS domain can be a long-running process. Avoid pressing Enter until the command prompt returns.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Active Directory domain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Domain name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time server names or IP addresses</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows user name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows user password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local administrator name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local administrator password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CIFS administrator or group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active Directory container (CLI setup only)</td>
<td></td>
</tr>
</tbody>
</table>
### Category

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SP (If not using DHCP, fill in the IP information.)</strong></td>
<td></td>
</tr>
<tr>
<td>SP (If not using DHCP, fill in the IP information.)</td>
<td></td>
</tr>
<tr>
<td>Supported on these systems:</td>
<td></td>
</tr>
<tr>
<td>FAS22xx</td>
<td></td>
</tr>
<tr>
<td>32xx</td>
<td></td>
</tr>
<tr>
<td>62xx</td>
<td></td>
</tr>
<tr>
<td>FAS80xx</td>
<td></td>
</tr>
<tr>
<td>MAC address</td>
<td></td>
</tr>
<tr>
<td>IPv4 Address</td>
<td></td>
</tr>
<tr>
<td>IPv4 Subnet mask</td>
<td></td>
</tr>
<tr>
<td>IPv4 Gateway</td>
<td></td>
</tr>
<tr>
<td>IPv6 (not always used)</td>
<td></td>
</tr>
<tr>
<td>IPv6 Address</td>
<td></td>
</tr>
<tr>
<td>IPv6 Subnet prefix length</td>
<td></td>
</tr>
<tr>
<td>IPv6 Gateway</td>
<td></td>
</tr>
<tr>
<td>AutoSupport mail host</td>
<td></td>
</tr>
<tr>
<td>AutoSupport recipients</td>
<td></td>
</tr>
<tr>
<td>ACP</td>
<td></td>
</tr>
<tr>
<td>Network interface name</td>
<td></td>
</tr>
<tr>
<td>Domain (subnet) for network interface</td>
<td></td>
</tr>
<tr>
<td>Netmask (subnet mask) for network interface</td>
<td></td>
</tr>
</tbody>
</table>

### Related tasks

*Responding to setup command prompts* on page 45

### Required storage system information

You must provide basic information about the storage system during the setup process. This information is required regardless of licensed features and usage.

**Note:** In Data ONTAP 8.0 and later, the following security measures are enforced:

- SecureAdmin is set up automatically on storage systems shipped with Data ONTAP 8.0 or later installed.
  For these systems, the following are the default security settings:
  - Secure protocols (including SSH and SSL/HTTPS) are enabled by default.
  - Nonsecure protocols (including RSH, Telnet, FTP, and HTTP) are disabled by default.
- A root password is required during the initial setup of a storage system shipped with Data ONTAP 8.0 or later installed.

You must provide the following storage system information:
<table>
<thead>
<tr>
<th>Information type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name (Hostname or Storage System Name)</td>
<td>The name by which the storage system is known on the network.&lt;br&gt; If the storage system is licensed for the NFS protocol, the name can be no longer than 32 characters.&lt;br&gt; If the storage system is licensed for the CIFS protocol, the name can be no longer than 15 characters.&lt;br&gt; The host name must be unique for each storage system in an HA pair.</td>
</tr>
<tr>
<td>Password (Administrative Password)</td>
<td>A password for the root account that the storage system requires before granting administrative access at the console or through a secure protocol. The password is required for initial setup.&lt;br&gt; The <code>security.passwd.rules.history</code> default is six passwords, and is enabled at first login. This option controls whether an administrator can reuse a password.&lt;br&gt; The following are the default password rules:&lt;br&gt;  - The password must be at least eight characters long.&lt;br&gt;  - The password must contain at least one number.&lt;br&gt;  - The password must contain at least two alphabetic characters.&lt;br&gt;  - The password must not contain the Ctrl-C or Ctrl-D key combination, or the two-character string <code>^C</code> or <code>^D</code>.</td>
</tr>
<tr>
<td>Time zone (Timezone)</td>
<td>The time zone in which the storage system resides. See <em>Time zones</em> on page 100 for a list of valid time zones.&lt;br&gt; The time zone must be identical on both storage systems in an HA pair.</td>
</tr>
</tbody>
</table>
### Information type

<table>
<thead>
<tr>
<th>Information type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage system location</td>
<td>A description of the physical location of the storage system. The text you enter during the storage system setup process is recorded in the SNMP location information. Use a description that identifies where to find your storage system (for example, &quot;Lab 5, Row 7, Rack B&quot;).</td>
</tr>
<tr>
<td>Language</td>
<td>The language used for multiprotocol storage systems if both the CIFS and NFS protocols are licensed. For a list of supported languages and their abbreviations, see <em>Supported languages</em> on page 109. The language must be identical on both storage systems in an HA pair.</td>
</tr>
<tr>
<td>Administration host</td>
<td>A client computer that is allowed to access the storage system through a secure protocol.</td>
</tr>
</tbody>
</table>

For more information about storage system security and passwords, see the *Data ONTAP System Administration Guide for 7-Mode*.

### Related tasks

- *Responding to setup command prompts* on page 45

---

**Information required to set up network connections**

You must provide basic information about the storage system's network connections during the setup process. This information is required regardless of licensed features and usage.

Some of the Internet Protocol information is required both for physical interfaces and for interface groups.

You must provide the following information about the storage system's network connections:

<table>
<thead>
<tr>
<th>Information type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network interface name</td>
<td>The name of the Ethernet (or GbE) interface, depending on what port the Ethernet card is installed in. Examples include e3a, e3b, e3c, and e3d (for an Ethernet quad-port adapter). Network interface names are automatically assigned by Data ONTAP as it discovers them.</td>
</tr>
<tr>
<td>Information type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Internet protocol</td>
<td>You are prompted to configure IPv6. If you enter n, further prompts are for IPv4 values only.</td>
</tr>
<tr>
<td></td>
<td>If you enter y to configure IPv6, you must also supply IPv4 configuration information for network interfaces in addition to IPv6 configuration information.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Enabling IPv6 during setup does not enable file access protocols (CIFS, NFS, FTP, or HTTP) over IPv6.</td>
</tr>
<tr>
<td></td>
<td>Enabling IPv6 during setup also enables IPv6 router advertisement. This can be disabled separately by setting the ip.v6.ra_enable option to off.</td>
</tr>
<tr>
<td></td>
<td>For more information about using file access protocols over IPv6, see the <em>Data ONTAP File Access and Protocols Management Guide for 7-Mode</em>. For more information about IPv4 and IPv6 support, see the <em>Data ONTAP Network Management Guide for 7-Mode</em>.</td>
</tr>
</tbody>
</table>

| IP address          | A unique address for each network interface.                                                                                               |
|                     | IPv4 example: 192.0.2.66                                                                                                                    |
|                     | IPv6 example: 2001:0DB8:85A3:0:0:8A2E:0370:99                                                                                               |

| Subnet mask (, IPv4 only) | The IPv4 subnet mask for the network to which each network interface is attached.                                                         |
|                          | Example: 255.255.255.0                                                                                                                     |

<p>| Subnet prefix length    | The number of bits used as the subnet mask for the specified interface.                                                                     |
|                         | For an IPv6 address, the prefix length must be less than or equal to 128 bits. The default value of prefix length is 64 bits.              |</p>
<table>
<thead>
<tr>
<th>Information type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner IP address (interface to take over)</td>
<td>If your storage system is configured for controller takeover, you must record the interface name or IP address belonging to the partner that this interface should take over during HA configuration takeover. Examples: e0a or 10.10.10.2</td>
</tr>
<tr>
<td></td>
<td>When configuring interface groups, you must specify the interface group name rather than the IP address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>When using the <code>ifconfig</code> command with IPv4, you can map the partner's interface to a local interface or the partner's IP address. When using IPv6, you must specify the partner interface, not an IP address. To use IPv6 in an HA pair, IPv6 must be enabled on both nodes.</td>
</tr>
<tr>
<td>Information type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Media type (network type)</td>
<td>If the network interface is Gigabit or 10 Gigabit Ethernet, you do not need to configure the media type because these interfaces support only one speed and duplex. If the network interface is 10/100 or 10/100/1000 Ethernet, you can select autonegotiation or you can explicitly configure the speed and duplex by using these media types:</td>
</tr>
</tbody>
</table>
|                                  | • auto  
  Autonegotiate speed and duplex  
• 100tx-fd  
  100Base-TX, full-duplex  
• 100tx  
  100Base-TX, half-duplex  
• tp-fd  
  10Base-T, full-duplex  
• tp  
  10Base-T, half-duplex  
If the network interface is 1/10 Gigabit Ethernet, you do not need to configure the media type because it supports only full-duplex and automatically negotiates the speed. The switch must be configured to match the media type values you select. |
<table>
<thead>
<tr>
<th>Information type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow control</td>
<td>The management of the flow of frames between two directly connected link-partners. You can use the following options:</td>
</tr>
</tbody>
</table>
|                          | • none  
|                          | No flow control                                                             |
|                          | • receive  
|                          | Ability to receive flow control frames                                       |
|                          | • send  
|                          | Ability to send flow control frames                                         |
|                          | • full  
<p>|                          | Ability to send and receive flow control frames                              |
| Router (routing gateway) | You can record the following information for the primary gateway to use for routing outbound network traffic: |
|                          | • Gateway name                                                              |
|                          | • IP address of the router for IPv4 routing                                 |
|                          | • IP address of the router for IPv6 routing                                 |</p>
<table>
<thead>
<tr>
<th>Information type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>e0M interface (if available)</td>
<td>The network interface of the management port (if included in your system). You must ensure that the e0M interfaces are serving only management traffic on a dedicated management LAN or that they are disabled (also called configured down). Do not use the e0M interface for data traffic, because it can cause performance and routing problems. You can use the e0M interface to access the storage system with protocols such as SSH and SNMP, as well as monitoring tools such as OnCommand Unified Manager. When configuring the e0M interface, you must partner it with the e0M interface on the HA partner. The e0M interface cannot be included in interface group or VLAN configurations. For more information about using the e0M interface, see the <em>Data ONTAP System Administration Guide for 7-Mode</em> and the <em>Data ONTAP Release Notes for 7-Mode</em>.</td>
</tr>
</tbody>
</table>

For more information about setting up network connections, see the *Data ONTAP Network Management Guide for 7-Mode* and the `ifconfig` man page.

**Interface group information**

During setup, you are prompted to enter the number of interface groups that you want to configure. You must then enter configuration information for each interface group name you specify.

The interface group information must be identical on both storage systems in a high-availability pair. You must provide the following interface group information:
<table>
<thead>
<tr>
<th>Information type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of interface group</td>
<td>Interface group names are user specified. An interface group's name should meet the following criteria:</td>
</tr>
<tr>
<td></td>
<td>• It must begin with a letter.</td>
</tr>
<tr>
<td></td>
<td>• It must not contain any spaces.</td>
</tr>
<tr>
<td></td>
<td>• It must not contain more than 15 characters.</td>
</tr>
<tr>
<td></td>
<td>• It must not already be in use for an interface group.</td>
</tr>
<tr>
<td>Interface group type</td>
<td>You must select one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• single [s]</td>
</tr>
<tr>
<td></td>
<td>Single-mode</td>
</tr>
<tr>
<td></td>
<td>• multi [m]</td>
</tr>
<tr>
<td></td>
<td>Static multimode</td>
</tr>
<tr>
<td></td>
<td>• lacp [l]</td>
</tr>
<tr>
<td></td>
<td>Dynamic multimode</td>
</tr>
<tr>
<td></td>
<td>• Port based [p]</td>
</tr>
<tr>
<td></td>
<td>Port based</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You must ensure that the value you select corresponds to your network switch configuration.</td>
</tr>
<tr>
<td>Load balancing type</td>
<td>You must select one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• IP based [i]</td>
</tr>
<tr>
<td></td>
<td>• MAC based [m]</td>
</tr>
<tr>
<td></td>
<td>• Round-robin based [r]</td>
</tr>
<tr>
<td></td>
<td>• Port based [p]</td>
</tr>
<tr>
<td></td>
<td>Load balancing is applicable only for multimode interface groups.</td>
</tr>
<tr>
<td></td>
<td>The recommended default is the IP address load-balancing method.</td>
</tr>
<tr>
<td>Information type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Number and names of links</td>
<td>You can record the number of physical interfaces to be included in the interface group and the name of each physical interface.</td>
</tr>
<tr>
<td>Internet Protocol information</td>
<td>You can record the following information:</td>
</tr>
<tr>
<td></td>
<td>• IP address (IPv4 or IPv6)</td>
</tr>
<tr>
<td></td>
<td>• Subnet mask (IPv4)</td>
</tr>
<tr>
<td></td>
<td>• Subnet prefix length (IPv6)</td>
</tr>
<tr>
<td></td>
<td>• Media type</td>
</tr>
<tr>
<td></td>
<td>For more information, see “Network information.”</td>
</tr>
<tr>
<td>Partner interface group name</td>
<td>You can record the interface group name (not the IP address) belonging to the high-availability partner that this interface should take over.</td>
</tr>
</tbody>
</table>

For more information about interface groups and assigning the correct configuration values for your environment, see the *Data ONTAP Network Management Guide for 7-Mode*.

**Related concepts**

*Switch configuration requirements for interface groups* on page 15

*Information required to set up network connections* on page 26

**HTTP information**

If your storage system is using HTTP, you must designate the location of the HTTP directory from which web files and directories are served or accept the default value.

Web browsers can access all of the files in the HTTP server's root directory (or other directory you designate). You can also connect a third-party HTTP server to your storage system.

**Note:** It is not necessary to specify the HTTP directory if you want to provide administrative access to your system using HTTPS.

You must provide the following HTTP information:
## Information type

**Location of the HTTP directory**

The directory where the web files and directories are stored. The default directory is `/home/http` in the storage system’s root volume.

The `/home/http` path can be used by both HTTP and HTTPS.

For more information about file access using HTTP, see the *Data ONTAP File Access and Protocols Management Guide for 7-Mode*.

## DNS services information

To configure your storage system to use the Domain Name System (DNS), you must provide DNS domain and server names.

You must provide the following DNS services information:

<table>
<thead>
<tr>
<th>Information type</th>
<th>Description</th>
</tr>
</thead>
</table>
| DNS domain       | The name of your network’s DNS domain.  
The DNS domain name must be identical on both storage systems in an HA pair.  
**Note:** The domain name cannot contain an underscore (_) and must consist of alphanumeric characters. If you use an underscore, you receive a bad domain name message. |
| DNS servers      | The IP addresses of your DNS servers.  
If your storage system does not use Active Directory services, you need the IP addresses of one or more DNS servers that provide host-name lookup services to the storage system.  
**Note:** If you are enabling IPv6, you can enter IPv6 DNS server addresses here.  
If you want to make Active Directory services available to CIFS, you need the IP addresses of DNS servers that support your Windows Active Directory domain. |

For more information about configuring DNS, see the *Data ONTAP Network Management Guide for 7-Mode*. 
NIS services information

If your network uses the Network Information Service (NIS), you must provide NIS domain and server names.

You must provide the following NIS services information:

<table>
<thead>
<tr>
<th>Information type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIS domain</td>
<td>The name of your NIS domain. The storage system can use an NIS domain to authenticate users and client computers. The NIS domain name must be identical on both storage systems if your network uses NIS. If multiprotocol access is enabled on the storage system, group caching is beneficial for CIFS access as well as NFS access. With multiprotocol access, user mapping of CIFS users to NFS users is performed. When a Windows user requests access to data with UNIX security style, the Windows user is first mapped to the corresponding UNIX user. The UNIX users’ groups must then be ascertained before the storage system can determine appropriate access. Failure to enable these two options together could lead to slow CIFS access to resources due to time spent on NIS group lookups. If multiprotocol access is for NTFS-security style volumes or qtrees, user mapping also occurs.</td>
</tr>
<tr>
<td>NIS servers</td>
<td>The host names of your preferred NIS servers. If your site uses NIS, you need the host names of your NIS servers. If you want NIS to broadcast to find a server, you need to enter an asterisk (*) when asked for the NIS server names. <strong>Note:</strong> If you are enabling IPv6, you can enter IPv6 NIS server addresses here.</td>
</tr>
</tbody>
</table>

For more information about configuring NIS, see the *Data ONTAP Network Management Guide for 7-Mode*.

CIFS protocol information

If your storage system is licensed for the CIFS protocol, the `cifs setup` command runs automatically when basic setup has finished. You must provide information about the Windows domain, WINS servers, the Active Directory service, and your configuration preferences.

You must provide the following CIFS protocol information:
<table>
<thead>
<tr>
<th>Information type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows domain</td>
<td>The name of your Windows domain. If your site uses Windows domains and the storage system belongs to one of these domains, record the name of the domain to which the storage system should belong.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Windows domain name value does not need to be identical on both storage systems in an HA pair. Each storage system in an HA pair can exist in a different domain and workgroup from its partner. If you have a multiprotocol environment and use UID to Secure ID (SID) mapping, the UNIX security information must be compatible between the two domains.</td>
</tr>
<tr>
<td>WINS servers</td>
<td>The servers that handle Windows Internet Name Service (WINS) name registrations, queries, and releases. If you choose to make the storage system visible through WINS, you can record up to four WINS IP addresses.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The WINS server value does not need to be identical on both storage systems in an HA pair. Each storage system in an HA pair can exist in a different domain and workgroup from its partner.</td>
</tr>
<tr>
<td>Multiprotocol or</td>
<td>The setup utility determines if your system includes licenses for multiple file access protocols (to serve data to NFS, Windows, HTTP, and other clients) or for NTFS only (to serve data to Windows clients only).</td>
</tr>
<tr>
<td>NTFS-only</td>
<td></td>
</tr>
<tr>
<td>CIFS server name</td>
<td>By default, the CIFS server is the same as the system host name. You can select a different name for the CIFS server, although the name can be no longer than 15 characters.</td>
</tr>
<tr>
<td>Information type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>User authentication for CIFS services</td>
<td>Data ONTAP CIFS services support four styles of user authentication:</td>
</tr>
</tbody>
</table>
| | 1. Active Directory domain authentication (Active Directory domains only)  
Users are authenticated with the domain controller in an Active Directory domain using Kerberos or NTLM authentication.  
If you select this option, you are also prompted for other Active Directory configuration parameters. |
| | 2. Windows NT 4 domain authentication (Windows NT or Active Directory domains)  
Users are authenticated with the domain controller in an Active Directory or an NT domain using NT-style NTLM authentication only. |
| | 3. Windows Workgroup authentication using the storage system's local user accounts  
Users are authenticated with the storage system’s local user database using NT-style NTLM authentication. A maximum of 97 local users are supported, and local users can be members of the local groups (local user and group SIDs are used). Local users and groups are managed with the `useradmin` command. |
| | 4. `/etc/passwd` and/or NIS/LDAP authentication  
Users are authenticated on the basis of user names and passwords that are stored in the UNIX directory stores. Even if local Windows users are created on the storage system by using the `useradmin` command, they are not used for session authentication. All authentication is done based on UNIX user information stored in the UNIX identity stores. |

You should select an authentication style appropriate to the storage system's environment and to the clients requesting the authenticated session.

<table>
<thead>
<tr>
<th>Information type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory domain name</td>
<td>You must enter the fully qualified domain name of the domain; for example, example.com.</td>
</tr>
<tr>
<td>Information type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active Directory time services</td>
<td>In Active Directory-based domains, it is essential that the storage system's time matches the domain controller's time so that Kerberos-based authentication system works correctly. If the time difference between the storage system and the domain controllers is more than 5 minutes, CIFS authentication fails.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> In Data ONTAP 8.0 and later, time service configuration is recommended to enable a storage system in Active Directory-based domains.</td>
</tr>
<tr>
<td></td>
<td>The time services configuration should be identical on both storage systems in a high-availability configuration.</td>
</tr>
<tr>
<td></td>
<td>When you configure Active Directory time services, you are prompted for the host name and IP address of the time server you wish to use, as well as for additional backup servers if desired.</td>
</tr>
<tr>
<td>Windows domain administrator user name (Windows user name)</td>
<td>The user name of a Windows domain administrator with sufficient privileges to add this storage system to the Windows domain. Joining a domain requires an administrator user name and password. This also applies to NT4 domains.</td>
</tr>
<tr>
<td>Windows domain administrator password (Windows 2000 administrator password)</td>
<td>The password for the domain administrator user account. Joining a domain requires an administrator user name and password. This requirement also applies to NT4 domains. The password is required for initial setup. The following are the password rules for this account; they are the same rules as for the root password:</td>
</tr>
<tr>
<td></td>
<td>• The password must be at least eight characters long.</td>
</tr>
<tr>
<td></td>
<td>• The password must contain at least one number.</td>
</tr>
<tr>
<td></td>
<td>• The password must contain at least two alphabetic characters.</td>
</tr>
<tr>
<td></td>
<td>• The password must not contain the Ctrl-C or Ctrl-D key combination, or the two-character string ^C or ^D.</td>
</tr>
<tr>
<td>CIFS administrator</td>
<td>You can specify an additional user or group to be added to the storage system's local “BUILTIN\Administrators” group, thus giving them administrative privileges as well.</td>
</tr>
<tr>
<td>Information type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active Directory</td>
<td>The Windows Active Directory container in which storage system accounts are placed. This can be either the default Computers container or a previously created organizational unit (OU) on which you have the necessary permission to join the storage system to the domain. All OUs for which you have appropriate permissions are displayed; the desired OU can be chosen from this list. If the user running the <code>setup</code> command does not have appropriate rights to the OU, which holds the storage system object, another user who has the necessary permissions can be designated during the &quot;join&quot; step.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>CIFS - Logged in as <code>administrator@EXAMPLE.COM</code>.</td>
</tr>
<tr>
<td></td>
<td>The user that you specified has permission to create the storage system's machine account in several (7) containers. Please choose where you would like this account to be created.</td>
</tr>
<tr>
<td></td>
<td>(1) CN=computers</td>
</tr>
<tr>
<td></td>
<td>(2) OU=java_users</td>
</tr>
<tr>
<td></td>
<td>(3) OU=Engineer,OU=java_users</td>
</tr>
<tr>
<td></td>
<td>(4) OU=Market,OU=java_users</td>
</tr>
<tr>
<td></td>
<td>(5) OU=Filers</td>
</tr>
<tr>
<td></td>
<td>(6) OU=Domain Controllers</td>
</tr>
<tr>
<td></td>
<td>(7) None of the above</td>
</tr>
<tr>
<td></td>
<td>Choose 7:</td>
</tr>
<tr>
<td></td>
<td>Selection (1-7)? [1]: 7</td>
</tr>
<tr>
<td></td>
<td>The user you specified, '<a href="mailto:Administrator@EXAMPLE.COM">Administrator@EXAMPLE.COM</a>', may create the filer's machine account in the container(s) listed above. To use another container, you must specify a user with the appropriate privileges.</td>
</tr>
<tr>
<td></td>
<td>Enter the name of the Windows user [:]'</td>
</tr>
</tbody>
</table>

For more information about CIFS configuration and authentication, see the *Data ONTAP File Access and Protocols Management Guide for 7-Mode*.

**Related tasks**

*Setting up CIFS* on page 51
Service processor information

If your system includes a Service Processor (SP), you must provide information about the SP's network interface and AutoSupport settings. The SP is a remote management device that enables you to access, monitor, and troubleshoot the storage system remotely.

You must gather network and AutoSupport information.

You can configure the SP to use DHCP or static addressing. If you are using an IPv4 address for the SP, you need the following network information:

<table>
<thead>
<tr>
<th>Information type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>Specifies an available IP address for the SP. If you are using IPv6 for static addressing, you need the IPv6 global address.</td>
</tr>
<tr>
<td>Network mask</td>
<td>Specifies the network mask of your network.</td>
</tr>
<tr>
<td>Subnet prefix length</td>
<td>Specifies the number of bits used as the subnet mask for the specified IPv6 interface.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Specifies the IP address for the gateway of your network.</td>
</tr>
<tr>
<td>Mail host</td>
<td>You must record the name or IP address of the preferred mail host. The mail host delivers SP alerts to the same destination as AutoSupport email.</td>
</tr>
</tbody>
</table>

The SP sends event notifications based on the following AutoSupport settings:

- `autosupport.to`
- `autosupport.mailhost`

You should set at least the `autosupport.to` option before configuring the SP. Data ONTAP automatically sends AutoSupport configuration to the SP, allowing the SP to send alerts and notifications through an AutoSupport message to your internal support organization. You are prompted to enter the name or the IP address of the AutoSupport mail host when you configure the SP.

**Note:** The SP does not rely on the storage system’s `autosupport.support.transport` option to send notifications. The SP uses the Simple Mail Transport Protocol (SMTP).
For information about configuring the SP, see the Data ONTAP System Administration Guide for 7-Mode.

Shelf Alternate Control Path Management configuration information

If you are planning to attach SAS disk shelves to your system, you should configure Shelf Alternate Control Path Management (ACP) during the software setup process. ACP is a protocol that enables Data ONTAP to manage and control a SAS-connected storage shelf subsystem.

ACP uses a separate network (alternate path) from the data path, so management communication is not dependent on the data path being intact and available.

Before you configure ACP on the storage system, you must cable ACP connections.

You can also configure ACP after initial setup, by using one of the following methods:

- Running the `acpadmin configure` command
- Running the Data ONTAP setup script
  You can run the `setup` command and enter ACP configuration information.
- Setting the `acp.enabled` option to `on`
  If the option has not previously been set, you are prompted for ACP configuration values.

You must provide the following ACP information:

<table>
<thead>
<tr>
<th>Information type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network interface name</td>
<td>The name of the Ethernet (or GbE) interface that is used exclusively for ACP traffic.</td>
</tr>
<tr>
<td>Domain (subnet) for network interface</td>
<td>The network name (an IP address ending in 0) for the private subnet to be used exclusively by ACP. The default is 192.168.0.0.</td>
</tr>
<tr>
<td>Netmask for network interface</td>
<td>The subnet mask for the ACP interface. The default is 255.255.252.0.</td>
</tr>
</tbody>
</table>

For more information about ACP configuration, see the Universal SAS and ACP Cabling Guide and the Data ONTAP Storage Management Guide for 7-Mode.
# Information to collect before configuring Storage Encryption

You must gather certain information to successfully set up Storage Encryption on your storage system.

<table>
<thead>
<tr>
<th>Information to collect</th>
<th>Details</th>
<th>Required</th>
<th>Optional</th>
</tr>
</thead>
</table>
| Network interface name                                      | You must provide the name of the network interface the storage system should use to communicate with external key management servers.  
**Note:** Do not configure 10 Gigabit network interfaces for communication with key management servers. | x        |          |
<p>| Network interface IP address                                | You must provide the IP address of the network interface.                                                                                                                                               | x        |          |
| Network interface subnet mask                               | You must provide the subnet mask of the network interface.                                                                                                                                             | x        |          |
| Network interface gateway IP address                        | You must provide the IP address for the network interface gateway.                                                                                                                                    | x        |          |
| IP address for external key management server               | You must link the storage system to at least one external key management server during setup.                                                                                                         | x        |          |
| IP address for additional external key management servers   | You can link the storage system to multiple additional external key management servers during setup for redundancy.                                                                                       |          | x        |
| Port number for each external key management server         | You must provide the port number that each key management server listens on. The port number must be the same for all key management servers.                                                          | x        |          |
| Public SSL certificate for storage system                   | You must provide a public SSL certificate for the storage system to link it to the external key management server.                                                                                       | x        |          |
| Private SSL certificate for storage system                  | You must provide a private SSL certificate for the storage system.                                                                                                                                    | x        |          |
| Public SSL certificate for external key management servers  | You must provide a public SSL certificate for each external key management server to link it to the storage controller.                                                                                | x        |          |</p>
<table>
<thead>
<tr>
<th>Information to collect</th>
<th>Details</th>
<th>Required</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key tag name</td>
<td>You can provide a name that is used to identify all keys belonging to a particular storage system. The default key tag name is the system's host name.</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
Setting up your storage system for using native disk shelves

When you power on a storage system for the first time, the `setup` command begins to run automatically and prompts you for configuration information. You must enter the information you collected in the configuration worksheet by responding to prompts on the command line.

After responding to prompts to designate an administration host machine, you can continue setting up your storage system by using the `setup` command (responding to prompts from the command-line interface).

If CIFS is licensed for your storage system, you are also prompted for CIFS configuration information.

If the storage system is properly configured with self-encrypting disks and is running a version of Data ONTAP that supports Storage Encryption, you can launch the Storage Encryption setup wizard after completion of the storage system setup wizard.

Prerequisites for setup

If your system does not boot up when you power it on for the first time, you must troubleshoot your hardware configuration before proceeding to software setup.

**Note:** You should carefully review the setup procedures and gather configuration information before powering on your system for the first time. After the setup script begins to run, you cannot return to previous steps to make corrections. If you make a mistake, you can wait until the setup process is complete, and then reboot your system and begin the setup process again by entering the `setup` command. Alternatively, you can enter Ctrl-C to interrupt the setup script and make any necessary changes, and then begin the setup process again.

Related tasks

- [Retrying system setup](#) on page 112
- [Troubleshooting boot failure after system power on](#) on page 111
Responding to setup command prompts

The setup command begins running at the storage system command prompt, where you must enter the information you gathered.

Before you begin

- You must have powered on your storage system components and external switches by following the instructions in the Installation and Setup Instructions for your hardware platform.
- You must have completed the configuration worksheet.
- You must have obtained license keys for your initial or add-on software orders at the NetApp Support Site under My Support > Software Licenses.
  You can record your license keys on the Configuration worksheet on page 19.

About this task

After the storage system boots, Data ONTAP begins discovering devices, interfaces, and licenses installed in the system. Data ONTAP displays messages on the console and starts the setup process, prompting you to enter setup information.

If the network has not been configured, Data ONTAP performs a DHCP broadcast on the e0M port at initial boot-up. If no DHCP server is found, the setup script begins running. Most customers use static IP addresses rather than dynamic IP addresses on the storage system.

Steps

1. Type y or press Enter at the following prompt:

   Are you sure you want to continue? [yes]

   Information about your storage controller and adapters is displayed.

2. Enter the new hostname at the following prompt:

   Please enter the new hostname

   You can name this host whatever you wish (for example, host1).

3. Type either y or n at the following prompt:

   Do you want to enable IPv6?
If you type... Then you are prompted to enter...

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>y</td>
<td>IPv6 configuration information in later steps.</td>
</tr>
<tr>
<td>n</td>
<td>IPv4 configuration information in later steps.</td>
</tr>
</tbody>
</table>

**Note:** If you are configuring IPv6 for this system's network interfaces, you must also enter IPv4 configuration information when prompted. If you are only configuring IPv4 for this system's network interfaces, you do not need to enter IPv6 information.

4. Type either **y** or **n** at the following prompt:
   **Do you want to configure interface groups?**

<table>
<thead>
<tr>
<th>If you type...</th>
<th>Then you are...</th>
</tr>
</thead>
<tbody>
<tr>
<td>y</td>
<td>Prompted to enter additional configuration information for each of the interface groups. These prompts are:</td>
</tr>
<tr>
<td></td>
<td>• Number of interface groups to configure?</td>
</tr>
<tr>
<td></td>
<td>• Name of interface group.</td>
</tr>
<tr>
<td></td>
<td>• Is <code>interface_group_name</code> a single [s], multi [m] or a lacp [l] interface group?</td>
</tr>
<tr>
<td></td>
<td>• Is <code>interface_group_name</code> to use IP-based [i], MAC-based [m], Round-robin based [r], or Port based [p] load balancing?</td>
</tr>
<tr>
<td></td>
<td>• Number of links for <code>interface_group_name</code></td>
</tr>
<tr>
<td></td>
<td>• Name of link for <code>interface_group_name</code></td>
</tr>
<tr>
<td></td>
<td>• IP address for <code>interface_group_name</code></td>
</tr>
<tr>
<td></td>
<td>• Netmask for <code>interface_group_name</code></td>
</tr>
<tr>
<td></td>
<td>• Should interface group <code>interface_group_name</code> take over a partner interface group during failover?</td>
</tr>
<tr>
<td></td>
<td>• Media type for <code>interface_group_name</code></td>
</tr>
<tr>
<td>n</td>
<td>Directed to the next prompt.</td>
</tr>
</tbody>
</table>

5. Enter the IP address for the network interface `interface_group_name` that connects the storage system to your network (for example, 192.168.1.1) at the following prompt:
   **Please enter the IP address for Network Interface**

6. Enter the netmask for the network interface `interface_group_name` (for example, 255.255.255.0) at the following prompt:
   **Please enter the netmask for Network Interface**
<table>
<thead>
<tr>
<th>If you are configuring...</th>
<th>Then go to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6</td>
<td>The next step</td>
</tr>
<tr>
<td>IPv4</td>
<td>Step 10</td>
</tr>
</tbody>
</table>

7. If IPv6 is enabled, enter the IPv6 address for the network interface that connects the storage system to your network (for example, 2001:0DB8:85A3:0:0:8A2E:0370:99) at the following prompt:
   Please enter the IPv6 address for Network Interface

8. If IPv6 is enabled, enter the number of bits used as the subnet mask for the network interface `interface_group_name` at the following prompt:
   Please enter the subnet prefix length for Network Interface [64]
   The default is 64.

9. Type either **y** or **n** at the following prompt:
   Should interface group `interface_group_name` take over a partner interface group during failover [n]?

<table>
<thead>
<tr>
<th>If you type...</th>
<th>Then you are...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>y</strong></td>
<td>Prompted to enter the IPv4 address or interface name to be taken over by e0a: Please enter the partner interface name to be taken over by <code>interface_group_name</code></td>
</tr>
<tr>
<td><strong>n</strong></td>
<td>Directed to the next prompt.</td>
</tr>
</tbody>
</table>

   **Note:** Both nodes of the HA pair should have identical licenses installed.

10. Enter the media type that this interface should use:
    Please enter media type for e0a {100tx-fd, tp-fd, 100tx, tp, auto (10/100/1000)} [auto]

11. Enter the flow control option that this interface should use:
    Please enter flow control for e0a {none, receive, send, full} [full]

12. Specify whether you want this interface to support jumbo frames:
    Do you want `interface_group_name` to support jumbo frames?

13. Continue to enter network parameter values for each network interface when prompted.

14. Enter the IP address and netmask for interface e0M, and indicate whether it should take over a partner IP address during failover.
    If you want to configure the e0M interface, partner it with the e0M interface on the HA partner.
    **Note:** The following warning message and prompts are displayed for the e0M interface:
15. Enter the primary gateway that is used to route outbound network traffic at the prompt:
   Please enter the name or IP address of the IPv4 default gateway.

16. If IPv6 is enabled, enter the primary gateway that is used to route outbound IPv6 network traffic:
   Please enter the name or IPv6 address of the IPv6 default gateway.

17. Enter the name or IP address of the administration host:
   Please enter the name or IP address of the administration host:
   The administration host is given root access to the filer's /etc files for system administration.
   To allow /etc root access to all NFS clients enter RETURN below.
   **Attention:** If you change the name or IP address of an administration host on a storage system that has already been set up and configured, the /etc/exports files are overwritten on system reboot.

18. Select a valid value for your time zone and enter it at the prompt:
   Please enter timezone
   GMT is the default setting. See Time zones on page 100 for a list of supported values. For example, enter US/Pacific to use the Pacific time zone. Time zone values are case sensitive.

19. Specify the actual physical location where the storage system resides (for example, Bldg. 4, Floor 2, Room 216):
   Where is the filer located?

20. Enter the language used for multiprotocol files at the prompt:
   What language will be used for multi-protocol files {type ? for list}?
   Language codes are case sensitive. For example, the language code for U.S. English is en_US.

21. Enter the root directory for HTTP files at the prompt:
   Enter the root directory for HTTP files [directory_path]
   This is the root directory for the files that the storage system serves through HTTP or HTTPS.
22. If you type **y** at the prompt, you need the DNS domain name and associated IP address:
   Do you want to run DNS resolver? [y]
   
   You might enter up to three name servers. Respond to the following prompts:
   
   a. Please enter DNS domain name.
   
   b. Please enter the IP address for first nameserver.
   
   c. Do you want another nameserver?

23. If you type **y** at the prompt, you are prompted to enter the name of the NIS domain and the NIS servers:
   Do you want to run NIS client? [n]
   
   When you have finished with the NIS prompts, you see an advisory message regarding AutoSupport and you are prompted to continue.

24. If you have an RLM installed in your system and you want to use it, type **y** at the prompt and enter the RLM values you collected:
   Would you like to configure the RLM LAN interface [y]?
   
   Respond to the following prompts:
   
   a. Type **n** when prompted to enable DHCP:
      Would you like to enable DHCP on the RLM LAN interface?
   
   b. Please enter the IP address for the RLM.
   
   c. Please enter the netmask for the RLM.
   
   d. Please enter the IP address for the RLM gateway.
   
   e. Specify whether you want to assign an IPv6 global address for the RLM.
   
   f. If you specified **y**, enter the IPv6 address, subnet prefix length, and the IPv6 address for the RLM gateway.
   
   g. Please enter the name or IP address of the mail host.

25. If you have an SP installed in your system and you want to use it, type **y** at the prompt and enter the SP values you collected:
   Would you like to configure the SP LAN interface [y]?
   
   Respond to the following prompts:
   
   a. Type **n** when prompted to enable DHCP:
      Would you like to enable DHCP on the SP LAN interface?
   
   b. Please enter the IP address for the SP.
   
   c. Please enter the netmask for the SP.
d. Please enter the IP address for the SP gateway.

e. Specify whether you want to assign an IPv6 global address for the SP.

f. If you specified y, enter the IPv6 address, subnet prefix length, and the IPv6 address for the SP gateway.

g. Please enter the name or IP address of the mail host.

26. If you are planning to attach SAS disk shelves to your system, type y at the prompt and enter the ACP values you collected:
Do you want to configure the Shelf Alternate Control Path Management interface for SAS shelves?

Respond to the following prompts:

a. Enter the network interface you want to use for the Alternate Control Path Management.

b. Please enter the domain for Network Interface.

c. Please enter the netmask for Network Interface.

27. Enter the new root password when you see the following prompt:

```
Setting the administrative (root) password for new_system_name...
New password: _______________________
Retype new password: _______________________
```

The password is required for initial setup. The following are the password rules:

- The password must be at least eight characters long.
- The password must contain at least one number.
- The password must contain at least two alphabetic characters.
- The password must not contain the Ctrl-C or Ctrl-D key combination, or the two-character string ^C or ^D.

28. When the setup script is complete, to transfer the information you have entered to the storage system, you are prompted to reboot the system:
Now type 'reboot' for changes to take effect.

**Attention:** If you do not enter the **reboot** command, the information you entered does not take effect and is lost.

29. If you are configuring a pair of storage systems in an HA pair and have not configured the other storage system, repeat these instructions to set up the other storage system in the configuration.
Result

After you complete setup and can access the CLI, wait for at least five minutes before using the license show command to see which licenses are installed on the system. You also can use the man license command to view the license (1) man page for more information.

Related concepts

Supported languages on page 109

Related tasks

Verifying network connectivity on page 78
Retrying system setup on page 112
Specifying the language code on page 109

Setting up CIFS

If you have a valid CIFS license installed, the \texttt{cifs setup} command starts running automatically after the \texttt{setup} command is complete. You respond to a series of prompts to set up CIFS.

Before you begin

A valid CIFS license is required to set up CIFS. You also must have filled out the appropriate CIFS-related information in the \textit{configuration worksheet} on page 19 so that you can enter the values when prompted.

About this task

You can use the default root password when setting up CIFS.

Note: Another way to set up CIFS is to use the CIFS Setup wizard in OnCommand System Manager instead of using the \texttt{cifs setup} command. If you want to include your system in an organizational unit (OU) other than the default \textquote{Computers}, you must use the \texttt{cifs setup} command.

Steps

1. If you want to configure Windows Internet Naming Service (WINS), enter \texttt{y} at the following prompt:
   \begin{quote}
   Do you want to make the system visible via WINS?
   \end{quote}
   WINS translates between IP addresses and symbolic names for network nodes and resources.
   If you answer \texttt{y}, respond to the following prompts:
2. Specify whether you want to configure the storage system for multiple protocols or for NTFS only:

| (1) NTFS-only filer          |
| (2) Multiprotocol filer     |

<table>
<thead>
<tr>
<th>If...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>You are using NTFS only for your storage system.</td>
<td>Enter 1 at the prompt.</td>
</tr>
<tr>
<td>You have purchased multiprotocol licenses for your storage system.</td>
<td>Enter 2 at the prompt.</td>
</tr>
</tbody>
</table>

3. Specify whether you want to change the name of the CIFS server at the following prompt:
Would you like to change this name? [n]

CIFS requires local /etc/passwd and /etc/group files. An /etc/groups file is already present, but a default /etc/passwd file does not exist and should be created. The default passwd file contains entries for 'root', 'pcuser', and 'nobody'.

The default name for this CIFS server is server_name. Would you like to change this name?

If you answer y, enter the new CIFS server name at the following prompt:
Enter the CIFS server name for the filer [n]

4. Select the style of user authentication appropriate to your environment:

<table>
<thead>
<tr>
<th>If you select...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Go to the next step.</td>
</tr>
<tr>
<td>2, 3, or 4</td>
<td>Go to Step 10 and then see CIFS protocol information on page 35 and the Data ONTAP File Access and Protocols Management Guide for 7-Mode for more information about CIFS setup for these authentication options.</td>
</tr>
</tbody>
</table>
Example

Data ONTAP CIFS services support four styles of user authentication. Choose the one from the list below that best suits your situation.

(1) Active Directory domain authentication (Active Directory domains only)
(2) Windows NT 4 domain authentication (Windows NT or Active Directory domains)
(3) Windows Workgroup authentication using the filer's local user accounts
(4) /etc/passwd and/or NIS/LDAP authentication

5. Enter the fully qualified domain name when you see the following prompt:
   What is the name of the Active Directory domain?

   **Attention:** Joining a CIFS domain can take a long time. Do not press the Enter key until the command prompt returns.

6. If you want to configure time services, enter `y` when you see the following prompt:
   Would you like to configure time services?

   If you answer **y**, respond to the following prompts:

   Example

   Enter the time server host(s) and/or addresses?
   Would you like to specify additional time servers?

7. Enter the name and password of a Windows account with sufficient privileges to add computers to the Active Directory domain:

   Enter the name of the Windows user.
   Password for *Windows_user_name*:

   If you enter a Windows user name and password, you are prompted to supply Active Directory container names. The user that you specify has permission to create machine accounts for the storage system in several containers.

8. Enter **y** at the prompt to create a local administrator account:
   Do you want to create the (name of filer) administrator account?

   If you answer **y**, enter the new password:

   Enter the new password for (administrator account).
   Retype the password.

   **Note:** The password is required. The following are the password rules:
The password must be at least eight characters long.

The password must contain at least one number.

The password must contain at least two alphabetic characters.

The password must not contain the Ctrl-C or Ctrl-D key combination, or the two-character string ^C or ^D.

9. If you would like to specify a user or group that can administer CIFS, enter y at the prompt:

Would you like to specify a user or group that can administer CIFS?

If you answer y, respond to the following prompt:
Enter the name of a user or group that will administer CIFS on the filer.

Result

After you complete this procedure, CIFS is configured and the name registrations are complete. You should see the following message:

CIFS local server is running.

Related concepts

Preparing CIFS clients to access the storage system on page 86

Related tasks

Retrying CIFS setup on page 113
Preparing to use OnCommand System Manager on page 93

Responding to sp setup command prompts

If your system includes a Service Processor, the sp setup command starts automatically after the setup command (or the cifs setup command, if CIFS is licensed on your system) completes running.

Before you begin

You must ensure that the SP is cabled to the locked-wrench port before running the sp setup command.

About this task

Consider configuring the autosupport.to option before configuring the SP. Data ONTAP automatically sends AutoSupport configuration to the SP, allowing the SP to send alerts and notifications through an AutoSupport message.
If you have enabled IPv6 for Data ONTAP, you have the option to configure the SP for only IPv4, for only IPv6, or for both IPv4 and IPv6. Disabling IPv6 on Data ONTAP also disables IPv6 on the SP.

Attention: If you disable both IPv4 and IPv6, and if DHCP is also not configured, the SP has no network connectivity.

The firewall for IPv6 is configured to accept a maximum of 10 Internet Control Message Protocol (ICMP) packets in a one-second interval. If your system has management software that frequently performs diagnostic checks, this limit can cause false positive errors to be generated. You should consider increasing the software's ping interval or tuning the software's report to expect the false positive errors caused by the ICMP limit.

Note: The SP firmware is updated automatically.

Steps

1. At the storage system prompt, enter one of the following commands:

<table>
<thead>
<tr>
<th>If...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have not run the setup command yet.</td>
<td>Enter the setup command. The sp setup command starts automatically after the setup command finishes running.</td>
</tr>
<tr>
<td>You already have run the setup command.</td>
<td>Enter the sp setup command.</td>
</tr>
</tbody>
</table>

2. When the SP setup asks you whether to configure the SP, enter y.

3. Do one of the following when the SP setup asks you whether to enable DHCP on the SP:

<table>
<thead>
<tr>
<th>If you want to use...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static addressing</td>
<td>Enter n.</td>
</tr>
<tr>
<td>DHCP addressing</td>
<td>Enter y.</td>
</tr>
</tbody>
</table>

Note: Because y is the default value, you must enter n if you are using static addressing on the SP.

Note: The SP supports DHCPv4 servers but not DHCPv6 servers.

4. If you have not enabled DHCP for the SP (Step 3), provide the following information when prompted for static IP information:

- The IP address for the SP

Note: Entering 0.0.0.0 for the static IP address disables IPv4 for the SP. If you enter 0.0.0.0 for the static IP address, you should enter 0.0.0.0 also for the netmask and the IP address for the SP gateway.
5. If you have enabled IPv6 for Data ONTAP, perform one of the following actions when you are prompted to configure IPv6 connections for the SP:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure IPv6 connections for the SP</td>
<td>Enter y.</td>
</tr>
<tr>
<td>Disable IPv6 connections for the SP</td>
<td>Enter n.</td>
</tr>
</tbody>
</table>

6. If you choose to configure IPv6 for the SP, provide the following IPv6 information when prompted by the SP setup:

- The IPv6 global address
  Even if no IPv6 global address is assigned for the SP, the link-local address is present on the SP. The IPv6 router-advertised address is also present if the `ip.v6.ra_enable` option is set to on.

- The subnet prefix for the SP

- The IPv6 gateway for the SP

**Note:** You cannot use the SP setup to enable or disable the IPv6 router-advertised address for the SP. However, when you use the `ip.v6.ra_enable` option to enable or disable the IPv6 router-advertised address for Data ONTAP, the same configuration applies to the SP.

For information about enabling IPv6 for Data ONTAP or information about global, link-local, and router-advertised addresses, see the *Data ONTAP Network Management Guide for 7-Mode*.

7. After SP setup is complete, reboot the SP.

**Example of configuring the SP**

The following example shows that the SP is configured for both IPv4 and IPv6 connections:

```
mysystem> sp setup
The Service Processor (SP) provides remote management capabilities including console redirection, logging and power control.
It also extends AutoSupport by sending additional system event alerts. Your AutoSupport settings are used for sending these alerts via email over the SP LAN interface.
Would you like to configure the SP? y
Would you like to enable DHCP on the SP LAN interface? n
Please enter the IP address of the SP []: 192.168.123.98
Please enter the netmask of the SP []: 255.255.255.0
```
Please enter the IP address for the SP gateway []: 192.168.123.1
Do you want to enable IPv6 on the SP? y
Do you want to assign IPv6 global address? y
Please enter the IPv6 address for the SP []: fd22:8b1e:b255:204::1234
Please enter the subnet prefix for the SP []: 64
Please enter the IPv6 Gateway for the SP []: fd22:81be:b255:204::1
Verifying mailhost settings for SP use...

The following example shows that the SP is configured to use DHCP and IPv6:

```
mysystem> sp setup
mysystem> sp setup
The Service Processor (SP) provides remote management capabilities including console redirection, logging and power control. It also extends AutoSupport by sending additional system event alerts. Your AutoSupport settings are used for sending these alerts via email over the SP LAN interface.
```
Would you like to configure the SP? y
Would you like to enable DHCP on the SP LAN interface? y
Do you want to enable IPv6 on the SP? y
Do you want to assign IPv6 global address? y
Please enter the IPv6 address for the SP []: fd22:8b1e:b255:204::1234
Please enter the subnet prefix for the SP []: 64
Please enter the IPv6 Gateway for the SP []: fd22:81be:b255:204::1
Verifying mailhost settings for SP use...

**Related tasks**

- *Setting up AutoSupport* on page 90
- *Verifying SP connections* on page 92

**Setting up Storage Encryption**

During initial setup, your storage system checks whether it is properly configured with self-encrypting disks and is running a version of Data ONTAP that supports Storage Encryption. If the check is successful, you can then launch the Storage Encryption setup wizard after completion of the storage system setup wizard.

**What Storage Encryption is**

Storage Encryption is an optional feature that you can enable for additional data protection. It is available on certain supported storage controllers and disk shelves that contain disks with built-in encryption functionality.

In a standard storage environment, data is written to disk in cleartext format. This makes the data vulnerable to potential exposure to unauthorized users when disks removed from a storage system are lost or stolen.

When you enable Storage Encryption, the storage system protects your data at rest by storing it on self-encrypting disks.
The authentication keys used by the self-encrypting disks are stored securely on external key management servers.

**Limitations of Storage Encryption**

You must keep certain limitations in mind when using Storage Encryption.

- **Storage Encryption is not supported with SnapLock.**
  If a SnapLock license is installed on the storage system, Storage Encryption functionality is unavailable. If Storage Encryption is enabled on a storage system, you cannot add a SnapLock license.

- For the latest information about which storage systems, disk shelves, and key management servers are supported with Storage Encryption, see the Interoperability Matrix.

- All disks in the storage system and optional attached disk shelves must have encryption functionality to be able to use Storage Encryption. You cannot mix regular non-encrypting disks with self-encrypting disks.

- **Storage Encryption is not supported with Flash Pool aggregates.**

- **Storage Encryption key_manager commands are only available for local nodes.**
  They are not available in takeover mode for partner nodes.

- **Do not configure Storage Encryption to use 10 Gigabit network interfaces for communication with key management servers.**
  This limitation does not apply to serving data.

- **Storage Encryption supports a maximum of 128 authentication keys per key management server.**
  You receive a warning when the number of stored authentication keys reaches 100. You cannot create new authentication keys when the number of stored authentication keys reaches the limit of 128. You must then delete unused authentication keys before you can create new ones.

**Related information**

*Interoperability Matrix: support.netapp.com/matrix*

**Using SSL for secure key management communication**

The storage system and key management servers use SSL connections to keep the communication between them secure. This requires you to obtain and install various SSL certificates for the storage system and each key management server before you can set up and configure Storage Encryption.

To avoid issues when installing SSL certificates, you should first synchronize the time between the following systems:

- The server creating the certificates
- The key management servers
- The storage system
Requirements for SSL certificates

Before obtaining and installing SSL certificates, you must understand what certificates are required and their requirements.

SSL certificates for Storage Encryption must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format and follow a strict naming convention. The following table describes the required certificate types and naming conventions:

<table>
<thead>
<tr>
<th>Certificate for...</th>
<th>Certificate type</th>
<th>Certificate file name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage system</td>
<td>Public</td>
<td>client.pem</td>
</tr>
<tr>
<td>Storage system</td>
<td>Private</td>
<td>client_private.pem</td>
</tr>
<tr>
<td>Key management server</td>
<td>Public</td>
<td>key_management_server_ipaddress_CA.pem</td>
</tr>
<tr>
<td></td>
<td></td>
<td>key_management_server_ipaddress must be identical to the IP address of the key management server that you use to identify it when running the Storage Encryption setup program.</td>
</tr>
</tbody>
</table>

These public and private certificates are required for the storage system and key management servers to establish secure SSL connections with each other and verify each other's identities.

The certificates for the storage system are only used by the storage system's KMIP client.

The private certificate can be passphrase protected during creation. In this case, the Storage Encryption setup program prompts you to enter the passphrase.

If your key management server does not accept self-signed certificates, you also need to include the necessary certificate authority (CA) public certificate.

In an HA pair, both nodes must use the same public and private certificates.

If you want multiple HA pairs that are connected to the same key management server to have access to each other's keys, all nodes in all HA pairs must use the same public and private certificates.

Installing SSL certificates on the storage system

You install the necessary SSL certificates on the storage system by using the `keymgr install cert` command. The SSL certificates are required for securing the communication between the storage system and key management servers.

Before you begin

You must have obtained the public and private certificates for the storage system and the public certificate for the key management server and named them as required.
Steps

1. Copy the certificate files to a temporary location on the storage system.

2. Install the public certificate of the storage system by entering the following command at the storage system prompt:
   
   ```
   keymgr install cert /path/client.pem
   ```

3. 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
   ```

4. 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
   ```

5. If you are linking multiple key management servers to the storage system, repeat Step 4 for each public certificate of each key management server.

Running the Storage Encryption setup wizard

You launch the Storage Encryption setup wizard by using the `key_manager setup` command. You should run the Storage Encryption setup wizard after you complete setup of the storage system and the storage volumes or when you need to change Storage Encryption settings after initial setup.

Steps

1. Enter the following command at the storage system prompt:
   
   ```
   key_manager setup
   ```

2. Complete the steps in the wizard to configure Storage Encryption.

Example

The following command launches the Storage Encryption setup wizard and shows an example of how to configure Storage Encryption:

```
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: 080CDCB2000000001000000000000003FE505B0C5E3E76061EE48E02A29822C

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.

Additional steps to set up a Data ONTAP system that uses both disks and array LUNs

For Data ONTAP systems that use both disks and array LUNs, you must configure the storage arrays to work with Data ONTAP once you complete the configuration of the native disk shelves.

The information that you need to connect storage arrays to Data ONTAP systems can be found in the FlexArray Virtualization Installation Requirements and Reference Guide and the Data ONTAP Storage Management Guide for 7-Mode.
Related concepts

Data ONTAP systems that can use array LUNs on storage arrays on page 63
Data ONTAP systems that can use array LUNs on storage arrays

V-Series ("V") systems and new FAS platforms released in Data ONTAP 8.2.1 and later can use array LUNs if the proper license is installed. In discussions in the Data ONTAP and FlexArray Virtualization documentation, these systems are collectively referred to as Data ONTAP systems when it is necessary to make it clear which information applies to them and what information applies to storage arrays.

**Note:** Starting with Data ONTAP 8.2.1, the capability of using LUNs on a storage array, formerly identified as V-Series functionality, has a new name—*Data ONTAP FlexArray Virtualization Software*. The capability of using array LUNs continues to be available as a licensed feature in Data ONTAP.

**Systems prior to Data ONTAP 8.2.1 that can use array LUNs**

The only systems released prior to Data ONTAP 8.2.1 that can use array LUNs are V-Series systems—systems with a "V" or "GF" prefix. A V-Series system is an open storage controller that virtualizes storage from storage array vendors, native disks, or both into a single heterogeneous storage pool.

**Note:** Almost all Data ONTAP platforms released prior to Data ONTAP 8.2.1 were released with FAS and V-Series equivalent models (for example, a FAS6280 and a V6280). (For a few systems, there were no "V" equivalent models.) Although both types of models could access native disks, only the V-Series systems (a "V" or "GF" prefix) could attach to storage arrays.

**Systems in Data ONTAP 8.2.1 and later that can use array LUNs**

Starting with Data ONTAP 8.2.1, the model for how platforms are released and the storage they can use changes. Attaching to storage arrays is no longer limited to V-Series systems.

Starting with Data ONTAP 8.2.1, all new platforms are released as a single hardware model. This single hardware model has a FAS prefix; there are no longer separate "V" and FAS models for new platforms. If the V_StorageAttach license package is installed on a new FAS model, it can attach to storage arrays. (This is the same license required on a V-Series system.)

**Important:** FAS systems released prior to Data ONTAP 8.2.1 cannot use LUNs on storage arrays, even if they are upgraded to Data ONTAP 8.2.1 or later; only the "V" equivalent of a platform can use array LUNs.
Setting up your system to use only array LUNs

Storage systems ordered without native disk shelves require some initial setup before Data ONTAP can be installed and the system is able to use array LUNs.

Steps

1. Prerequisites for starting setup when using only array LUNs on page 64
2. Providing ownership and system ID for Data ONTAP systems using array LUNs on page 65

Prerequisites for starting setup when using only array LUNs

Before you start the Data ONTAP setup script to assign LUN ownership to specific Data ONTAP systems, the storage administrator must have made array LUNs available to Data ONTAP and you must connect the hardware devices.

The following tasks must be completed before Data ONTAP can use the storage on a storage array:

- The storage array administrator must create LUNs and make them available to Data ONTAP. See the following documents for more information:
  - FlexArray Virtualization Installation Requirements and Reference Guide
  - FlexArray Virtualization Implementation Guide for Third-Party Storage
  - Storage array documentation.

  The process of making array LUNs available to Data ONTAP varies among storage array types.

- The storage array administrator must configure LUN security. LUN security limits access to particular array LUNs to only the hosts for which the LUNs are intended.

  Attention: Array LUNs that the storage array presented for use by Data ONTAP are visible in Data ONTAP displays. Data ONTAP prevents you from assigning two different Data ONTAP systems as the owner of a particular array LUN. But Data ONTAP cannot prevent you from assigning a Data ONTAP system as the owner of an array LUN that was not intended for Data ONTAP use. Using the disk assign command to write ownership information to a LUN which is not owned by a Data ONTAP system causes irreversible data corruption.

- You must connect your Data ONTAP system to the storage array. See the FlexArray Virtualization Installation Requirements and Reference Guide for instructions.

- Complete the Configuration worksheet.
The worksheet includes a definition of each parameter needed to set up the system on the network.

**Related tasks**

*Providing ownership and system ID for Data ONTAP systems using array LUNs* on page 65

## Providing ownership and system ID for Data ONTAP systems using array LUNs

If your system is using only array LUNs, you must provide information through the boot menu and the setup program to assign array LUN ownership to your system and identify your system on the network.

**About this task**

Filling out your system information on the configuration worksheet before starting setup helps you complete setup faster.

You must assign at least one array LUN to this system during initial setup. You can assign more array LUNs during initial setup or wait until after Data ONTAP is installed.

**Steps**

1. Power on the system to load the kernel from the boot device.
   
   The system boot process begins.

2. Interrupt the boot process by pressing Ctrl-C when you see the following message on the console: *Press Ctrl-C for boot menu*

3. Select Maintenance Mode.

4. Enter the following command to identify the LUNs on the storage array that you can configure this system to own:

   ```bash
disk show -v
   ```

   You see a list of all LUNs available on the storage array port to which the Data ONTAP system is physically connected.

5. Enter the following command to assign the LUNs on the storage array that you want this system to own (you must assign at least one array LUN):

   ```bash
disk assign {disk_name | all | -n count} [-p pool] [-c block|zoned]
   ```

   **Attention:** Using the `disk assign` command to write ownership information to a LUN which is not owned by a Data ONTAP system causes irreversible data corruption.
• `disk_name | all | -n count` identifies the array LUNs assigned to this system. It is a required option.
  - `disk_name` specifies, by LUN name, the array LUNs to be assigned. In most cases, you identify the name of the specific array LUNs that this system is to own, in the following form:
  - `all` causes all array LUNs that are made available on the storage array to the array LUN neighborhood to be assigned to this system.
  - `-n count` causes the number of unassigned array LUNs specified by count to be assigned to this system.

• `-p pool`
  If you are not going to be deploying SyncMirror, you do not need to enter the pool parameter. The pool parameter defaults to 0 (zero). For details about SyncMirror, see the Data ONTAP Data Protection Online Backup and Recovery Guide for 7-Mode.
  In the following example, the `disk assign` command is used to assign `storeAlun1` and `storeAlun2` to pool 0 and `storeBlun1` `storeBlun2` to pool 1:
  ```
disk assign storeAlun1 storeAlun2 -p 0
disk assign storeBlun1 storeBlun2 -p 1
```

• `-c block | zoned`
  In Data ONTAP 8.1, you must use block. Zoned checksum (ZCS) type is not supported.
  In Data ONTAP 8.1.1 and later, the default and recommended checksum type for array LUNs is block. Advanced zone checksum type (AZCS), which provides more functionality than ZCS in previous releases, is an alternative to block checksum (BCS) type. However, for Data ONTAP systems that use array LUNs, AZCS is not recommended for high-performance random work loads. If you want to specify AZCS for an array LUN, specify zoned.

  **Note:** This caution does not apply to disks. With array LUNs, AZCS could be used for data recovery, archive, or similar work loads. AZCS uses three percent of the device capacity.

6. Enter the following command, and then review the list of array LUNs to confirm that all array LUNs you expected to be assigned to this system (the local system) are shown with the ID of this system:

   ```
disk show -v
```
   The local system ID is shown and the array LUNs (disks) exported on the port are shown.

7. Enter the following commands to halt and then reboot the system:

   ```
halt
boot
```

8. When you see the following message on the console, interrupt the boot process by pressing Ctrl-C:
Press Ctrl-C for Boot Menu

The boot options menu appears.

9. Select the following to create the root volume with one of the array LUNs that you assigned to this storage system:
   Clean configuration and initialize all disks.

10. Enter the following when the system prompts you whether you want to install a new file system:
   y

11. The system responds with the following message:
   This will erase all the data on the disks, are you sure?
   Enter: y

   The storage system creates a FlexVol root volume named “vol0” in an aggregate named “aggr0” (the system automatically creates the aggregate). After these are created on one of the assigned array LUNs, the system prompts for setup information.

   If you entered multiple array LUNs with the disk assign command, an array LUN is automatically selected. The system first tries to select an array LUN with a block checksum, if one is available, and then it selects the smallest array LUN.

12. The system displays the following prompt:
   Would you like to continue setup through the Web interface?
   Enter: n

13. Answer the prompts in the setup program, using the information that you recorded in the Configuration worksheet.

After you finish

After the setup program is complete, you need to install the Data ONTAP software, protocols, the license for accessing LUNs on storage arrays, and Data ONTAP features.

Related concepts

Prerequisites for starting setup when using only array LUNs on page 64

Related tasks

Responding to setup command prompts on page 45
Installing Data ONTAP software on a system that uses only array LUNs

When setting up a new storage system that uses only array LUNs, you must complete the setup program before you install the Data ONTAP software and licenses. During setup, you must provide system information and assign at least one array LUN to the system.

About this task

If you order your storage system with native disk shelves, the factory installs Data ONTAP for you.

Data ONTAP installation stages

You need to install Data ONTAP on a storage system that is going to use only array LUNs and was ordered without native disk shelves.

Installing Data ONTAP on a storage system that uses only array LUNs is a three-stage process:

1. Obtaining the installation image.
2. Installing the software.
3. Installing licenses on the system.

Obtaining Data ONTAP software images

You must copy a software image from the NetApp Support Site to your storage system using UNIX or Windows client connections. Alternatively, you can copy software images to an HTTP server on your network, and then storage systems can access the images using the software command.

To upgrade the storage system to the latest release of Data ONTAP, you need access to software images. Software images, firmware version information, and the latest firmware for your storage system model are available on the NetApp Support Site. Note the following important information:

- Software images are specific to storage system models.
  Be sure to obtain the correct image for your system.

- Software images include the latest version of system firmware that was available when a given version of Data ONTAP was released.

Related information

Download Software: support.netapp.com/NOW/cgi-bin/software
Obtaining images for HTTP servers

If you have an HTTP server that is accessible to your storage system, you can copy Data ONTAP software images to the HTTP server and use the `software` command to download and install Data ONTAP software images to your storage system.

For more information, see the software (1) man page.

Copying the software image to the HTTP server

You must copy the software image file to the HTTP server. This task prepares the HTTP server to serve software images to storage systems in your environment.

**Step**

1. Copy the software image (for example, `821_q_image.tgz`) from the NetApp Support Site or another system to the directory on the HTTP server from which the file is served.

Copying software images from the HTTP server without installing the images

You can copy software images to your storage system without immediately installing them. You might copy them, for instance, if you want to perform the installation later.

**Step**

1. Enter the following command from the storage system console:

   ```
   software get url -f filename
   ```

   `url` is the HTTP location from which you want to copy the Data ONTAP software images.

   Use the following URL syntax if you need to specify a user name, password, host, and port to access files on the HTTP server using Basic Access Authentication (RFC2617):

   ```
   http://username:password@host:port/path
   ```

   Use the `-f` flag to overwrite an existing software file of the same name in the storage system's `/etc/software` directory. If a file of the same name exists and you do not use the `-f` flag, the download fails and you are prompted to use `-f`.

   `filename` is the file name you specify for the software file being downloaded to your storage system. If no destination file name is specified, Data ONTAP uses the file name listed in the URL from which you are downloading and places the copy in the `/etc/software` directory on the storage system.

**Example**

In the following example, the `software get` command uses a new destination file name:
software get http://www.example.com/downloads/x86-64/821_q_image.tgz
821_mailboxes_q.tgz

You see a message similar to the following:

```
software: copying to /etc/software/821_mailboxes_q.tgz
software: 100% file read from location.
software: /etc/software/821_mailboxes_q.tgz has been copied.
```

### Obtaining images for UNIX clients

If you are using a UNIX client to copy a Data ONTAP software image to your storage system, you need access to both the storage system's console and the system's upgrade host. If the upgrade host does not have a web connection, you must also have access to a client system that can reach the NetApp Support Site.

### Mounting the storage system on your client

Before you copy a software image to your storage system, you must mount the system on your UNIX upgrade host.

#### Steps

1. As root user, mount the storage system’s root file system to the client’s `/mnt` directory by using the following command:
   ```
   mount system:/vol/vol0 /mnt
   
   system is the name of the storage system.
   
   /mnt is the directory on the client where you want to mount the storage system’s root file system.
   ```

2. Change to the `/mnt` directory by using the following command on your UNIX client console:
   ```
   cd /mnt
   
   /mnt is the directory on the client where you mounted the storage system’s root file system.
   ```

3. To acquire Data ONTAP files, download the Data ONTAP files by using a web browser from the NetApp Support Site.

### Obtaining software images for UNIX clients

You can use a web browser to copy the software image from the NetApp Support Site to a UNIX client.

#### About this task

You can copy the software image directly to your upgrade host. If your upgrade host does not have web access, you can copy the software image to portable storage media attached to a different client, then copy the image from portable storage to the upgrade host.
Steps

1. Use a web browser to log in to the NetApp Support Site.

2. Navigate to the Download Software area.

3. In the Software Download table, click the Select Platform list box in the Data ONTAP product row.

4. Select your storage system type from the list, and then click Go.

5. Follow the prompts to reach the software download page.

6. After you choose the software image that corresponds to your platform, complete one of the following actions, depending on your web environment:

<table>
<thead>
<tr>
<th>If you are connecting to the NetApp Support Site from...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>An upgrade host</td>
<td>Save the image to the .../etc/software directory on the mountpoint that you chose when you mounted the storage system on your client.</td>
</tr>
<tr>
<td>Another UNIX client</td>
<td>a. Save the image to portable storage media.</td>
</tr>
<tr>
<td></td>
<td>b. Connect the portable storage media to your upgrade host.</td>
</tr>
<tr>
<td></td>
<td>c. Copy the image to the .../etc/software directory on the mountpoint that you chose when you mounted the storage system on your client.</td>
</tr>
</tbody>
</table>

7. Continue with the installation procedures.

Related concepts

*Installing Data ONTAP software images* on page 73

Obtaining images for Windows clients

If you are using a Windows client to copy a Data ONTAP software image to your storage system, you need access to both the storage system's console and the system's upgrade host. If the upgrade
host does not have a web connection, you must also have access to a client system that can reach the NetApp Support Site.

**Mapping the storage system to your Windows host**

Before you copy a software image to your storage system, you must map the root directory of the system to your Windows upgrade host.

**Before you begin**

The CIFS service must be running, and the Administrator user must be defined in CIFS as having authority to access the C$ directory.

**Steps**

1. Log in to your client as Administrator, or log in using an account that has full control on the storage system C$ directory.

2. Map a drive to the C$ directory of your storage system.

   **Note:** On some computers, firewall software might not permit you to map a drive to the C$ directory of a storage system. To complete this procedure, disable the firewall until you no longer need access to the storage system through your laptop.

3. Copy the software image from the NetApp Support Site.

**Obtaining software images for Windows clients**

You can use a web browser to copy the software image from the NetApp Support Site to a Windows client.

**About this task**

You can copy the software image directly to your upgrade host. If your upgrade host does not have web access, you can copy the software image to portable storage media attached to a different client, then copy the image from portable storage to the upgrade host.

**Steps**

1. Use a web browser to log in to the NetApp Support Site.

2. Navigate to the Download Software area.

3. In the Software Download table, click the **Select Platform** list box in the Data ONTAP product row.

4. Select your storage system type from the list and click **Go**.

5. Follow the prompts to reach the software download page.
6. After you have chosen the software image that corresponds to your platform, complete one of the following actions, depending on your web environment:

<table>
<thead>
<tr>
<th>If you are connecting to the NetApp Support Site from...</th>
<th>Then do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>An upgrade host</td>
<td>Save the image to the \etc\software directory on the mountpoint that you chose previously, when you mounted the storage system on your client.</td>
</tr>
</tbody>
</table>
| Another Windows client                                  | a. Save the image to portable storage media.  
|                                                        | b. Connect the portable storage media to your upgrade host.  
|                                                        | c. Copy the image to the \etc\software directory on the mountpoint that you chose previously, when you mounted the storage system on your client. |

7. Continue with the installation procedures.

**Related concepts**

*Installing Data ONTAP software images* on page 73

**Installing Data ONTAP software images**

You should use the `software update` command to extract and install the system files on a storage system.

You can use the `software update` command to install a software image you have already copied to your storage system, or to copy and install the image from an HTTP server.

You must know the location of and have access to the software image. The `software update` command requires one of the following as an argument:

- The name of the software image you copied to the `/etc/software` directory
- The URL of the HTTP server that you configured to serve software images

The `software update` command enables you to perform several operations at one time. For example, if you use an HTTP server to distribute software images, you can copy an image from the HTTP server, extract and install the system files, download the files to the boot device, and reboot your system with one command.

For more information about the `software update` command and its options, see the `software(1)` man page.
Installing software images from the /etc/software directory

To install software images, the new software image must be present in the /etc/software directory on your storage system.

**Step**

1. From the storage system prompt, enter the following command:

   ```
   software update file options
   ```

   - `file` is the name of the software image you copied to the /etc/software directory.
   - `options` is one or more of the following:
     - The `-d` option prevents the `download` command from being run automatically after the system files are installed.
     - The `-f` option overwrites the existing image in the /etc/software directory.
     - The `-r` option prevents the system from rebooting automatically after the `download` command has finished (default).
     - The `-R` option causes the system to reboot automatically after the `download` command has finished.

**Example**

Use the following commands to copy and install the Data ONTAP software image:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then you can enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the new system files from the /etc/software directory</td>
<td><code>software update my_new_setup_i.tgz -d</code></td>
</tr>
<tr>
<td>Download the new system files to the boot device immediately after installing them</td>
<td><code>software update my_new_setup_i.tgz</code></td>
</tr>
<tr>
<td>Perform an upgrade on a single system and reboot immediately</td>
<td><code>software update my_new_setup_i.tgz -R</code></td>
</tr>
</tbody>
</table>

When you use the `software update` command without the options, a message similar to the following appears on your storage system console:

```software: You can cancel this operation by hitting Ctrl-C in the next 6 seconds.
software: Depending on system load, it might take many minutes
software: to complete this operation. Until it finishes, you will
software: not be able to use the console.```
software: copying to <filename>
software: 100% file read from location.
software: /etc/software/<filename> has been copied.
software: installing software, this could take a few minutes...
software: Data ONTAP Package Manager Verifier 1
software: Validating metadata entries in /etc/boot/NPM_METADATA.txt
software: Checking sha1 checksum of file checksum file: /etc/boot/NPM_FCSUM-pc.sha1.asc
software: Checking sha1 file checksums in /etc/boot/NPM_FCSUM-pc.sha1.asc
software: installation of <filename> completed.

software: Reminder: You might need to upgrade Volume SnapMirror destination
software: filers associated with this filer. Volume SnapMirror can not mirror
software: if the version of ONTAP on the source filer is newer than that on
software: the destination filer.
Mon Oct 2 13:26:17 PDT [filer: download.request:notice]

After you finish
Complete the installation by downloading to HA pairs or single systems.

Installing software images from an HTTP server
To install software images, you must know the URL of an HTTP server in your environment that is configured to serve software images.

Step
1. From the storage system prompt, enter the following command:

   `software update url options`

   - `url` is the URL of the HTTP server and subdirectory.
   - `options` is one or more of the following:
     - The `-d` option prevents the `download` command from being run automatically after the system files are installed.
     - The `-f` option overwrites the existing image in the `/etc/software` directory.
     - The `-r` option prevents the system from rebooting automatically after the `download` command has finished (default).
     - The `-R` option causes the system to reboot automatically after the `download` command has finished.
You can use the following commands to copy and install the Data ONTAP software image:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then you can enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy and install the image from your HTTP server</td>
<td><code>software update http://www.example.com/downloads/x86-64/my_new_setup_i.tgz -d</code></td>
</tr>
<tr>
<td>Copy and install the image from your HTTP server and overwrite an existing image</td>
<td><code>software update http://www.example.com/downloads/x86-64/my_new_setup_i.tgz -d -f</code></td>
</tr>
<tr>
<td>Copy and install the image from your HTTP server, then download the new system</td>
<td><code>software update http://www.example.com/downloads/x86-64/my_new_setup_i.tgz</code></td>
</tr>
<tr>
<td>files to the boot device immediately after installing them</td>
<td></td>
</tr>
<tr>
<td>Copy and install the image from your HTTP server to a single system, then</td>
<td><code>software update http://www.example.com/downloads/x86-64/my_new_setup_i.tgz -R</code></td>
</tr>
<tr>
<td>download the new system files and reboot immediately</td>
<td></td>
</tr>
</tbody>
</table>

When you use the `software update` command without the options, a message similar to the following appears on your storage system console:

```
software: You can cancel this operation by hitting Ctrl-C in the next 6 seconds.
software: Depending on system load, it might take many minutes
software: to complete this operation. Until it finishes, you will
software: not be able to use the console.
software: copying to <filename>
software: 100% file read from location.
software: /etc/software/<filename> has been copied.
software: installing software, this could take a few minutes...
software: Data ONTAP Package Manager Verifier 1
software: Validating metadata entries in /etc/boot/NPM_METADATA.txt
software: Checking shal checksum of file checksum file: /etc/boot/NPM_FCSUM-pc.sha1.asc
software: Checking shal file checksums in /etc/boot/NPM_FCSUM-pc.sha1.asc
software: installation of <filename> completed.
software: Reminder: You might need to upgrade Volume SnapMirror destination
software: filers associated with thisfiler. Volume SnapMirror can not mirror
software: if the version of ONTAP on the source filer is newer than that on
software: the destination filer.
Mon Oct 2 13:26:17 PDT [filer: download.request:notice]
```
After you finish

Complete the installation by downloading to HA pairs or single systems.

Commands for managing files in the /etc/software directory

After you have copied Data ONTAP system files to the /etc/software directory on your storage system, you can manage them from the storage system console by using the software command.

You use the software command to manage files in the /etc/software directory:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then use the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>List the contents of the /etc/software directory</td>
<td>software list</td>
</tr>
<tr>
<td>Delete files from the /etc/software directory</td>
<td>software delete</td>
</tr>
</tbody>
</table>

For more information, see the software(1) command man page.

Required licenses for setting up a Data ONTAP system that uses array LUNs

After installing the Data ONTAP software, you must install the license for using LUNs on storage arrays and, in some circumstances, a protocol license.

There is a different license key for Data ONTAP 8.2 and later and for releases prior to Data ONTAP 8.2. For Data ONTAP 8.2 and later, you need to use the V_StorageAttach license package.

You can install other licenses at the same time you install the license for using array LUNs, or you can install them later. The protocol license requirements are as follows:

<table>
<thead>
<tr>
<th>For installation from a...</th>
<th>This protocol license is required...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows client</td>
<td>CIFS</td>
</tr>
<tr>
<td>UNIX client</td>
<td>NFS</td>
</tr>
</tbody>
</table>

For more information about storage system licensing, see the Data ONTAP System Administration Guide for 7-Mode and the license (1) man page.

Related tasks

Managing licenses on page 82
Verifying software setup

As soon as hardware and software setup is complete, you should verify network connections, licensed functionality, and other relevant configurations in your environment.

Verifying network connectivity

You can use the `ping` command to verify that your clients can connect to the IP addresses you configured on the storage system during setup.

About this task

You must perform these tasks from a network client system.

**Note:** The `ping` command can take an IPv6 address as an argument; it is no longer necessary to enter `ping6 IPv6_address`.

For more information, see the *Data ONTAP Network Management Guide for 7-Mode*.

Steps

1. To verify network connectivity to an IP address, enter the following command:

   `ping IP_address`

   *IP_address* is the IP address that the storage system assigned to that interface during setup.

   **Example**

   You can use either the `ping6` or `ping` command to test the IPv6 connections for a storage system with an interface named e0a installed at 2001:0DB8:85A3:0:0:8A2E:0370:99:

   `ping6 2001:0DB8:85A3:0:0:8A2E:0370:99`

   The following command tests the IPv4 network connections for a storage system with an interface named e0a installed at 192.0.2.66:

   `ping 192.0.2.66`

2. Repeat the test once for each interface that is installed in the storage system.

Result

You should be able to reach your new storage system from clients on your network. If you cannot, use the recommended troubleshooting procedures.
Troubleshooting connections to new network interfaces

There are several ways to identify a problem when new network interfaces do not respond to a ping command.

Steps

1. Check to make sure that the interface is securely attached to the network.

2. Check to make sure that the media type is set correctly if the interface is using a multiport Ethernet card with different port speeds.

3. Check to make sure that the routers function properly with correct routing information if the ping command is issued from a network not directly attached to the interface.

4. If you received a response from the IP address ping but not the host-name ping, check to see whether there is a problem with host-name resolution.

Related tasks

Verifying host-name resolution on page 79

Verifying host-name resolution

You should ensure that host names you configured during the setup process are resolved into IP addresses.

About this task

When you run the setup command, the storage system generates a host name for each interface by appending the name of the interface to the storage system host name. You must ensure that these automatically generated host names are resolved into IP addresses.

For example, the interface name for the first interface on a storage system named "mysystem" might be mysystem-e0a; the second interface might be mysystem-e0b.

For more information about host-name resolution, see your Data ONTAP Network Management Guide for 7-Mode.

Steps

1. Depending on what you use for host-name resolution, perform one of the following actions from a client system:
If you use... | Then add an entry in...
---|---
DNS or NIS for name resolution | Your DNS or NIS databases for each of the storage system interfaces.
The following example shows how the entries might look for a storage system with four interfaces:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Interface Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.16.3.145</td>
<td>mysystem-e0a</td>
</tr>
<tr>
<td>192.16.3.146</td>
<td>mysystem-e0b</td>
</tr>
<tr>
<td>192.16.3.147</td>
<td>mysystem-f0</td>
</tr>
<tr>
<td>192.16.3.148</td>
<td>mysystem-a5</td>
</tr>
</tbody>
</table>

/etc/hosts files for name resolution | Each host's /etc/hosts file for each of the storage system interfaces.

2. To verify host-name resolution for a network interface, enter the following command:

```
ping hostname-interface
```

*hostname* is the host name that you assign to the storage system when you run the setup command.

*interface* is one of the interface names that the storage system assigns when you run the setup command.

Example

The following command tests the network connections for a storage system that has the host name "mysystem" with an interface named e0a installed.

```
ping mysystem-e0a
```

3. Repeat the test once for each interface that is installed in the storage system.

Result

If you receive a response from the IP-address ping but not the host-name ping, there might be a problem with name resolution.

**Verifying setup of dedicated management ports**

You need to verify that data traffic is blocked on the dedicated management ports (e0M interfaces), or that they are configured down.

**Steps**

1. Verify whether data traffic is blocked on the e0M interfaces by entering the following command:

```
options interface.blocked.mgmt_data_traffic
```
Example

```
mysystem> options interface.blocked.mgmt_data_traffic
interface.blocked.mgmt_data_traffic off (value might be overwritten in takeover)
```

The current setting of the option is displayed (on or off).

2. If this option is set to off, set it to on, first on the local host and again on the HA partner:

```
options interface.blocked.mgmt_data_traffic on
```

Now the data traffic is blocked on e0M on both HA partners.

3. If you are not using the e0M interfaces, configure them down:
   a. Mount the NFS root volume.
   b. Append the command `ifconfig e0M down` to the `/etc/rc` file.

Verifying that the storage system is available

You can use the `exportfs` command to verify that the root path and root directory are available to clients.

About this task

After setup is complete, the storage system is online, and the following entities should exist on the storage system:

- `/vol/vol0` (a virtual root path)
- `/vol/vol0/home` (a directory)

Note that `/vol` is not a directory—it is a special virtual root path under which the storage system mounts its volumes. You cannot mount `/vol` to view all the volumes on the storage system; you must mount each storage system volume separately. NFS and CIFS protocols provide the following access characteristics for the `/vol` virtual root path:

- For NFS
  `/vol/vol0` is exported to the administration host for root access; `/vol0/home` is exported to the administration host for root access and to all clients for general access.

- For CIFS
  By default, `/vol/vol0` is shared as `C$` and `/vol/vol0/etc/` is shared as `ETC$`. These two shares are created with "Full Control" given to the Builtin Administrators group and with no access given to any other users or groups. By default, the Builtin Administrators group members are the local administrator account, the Domain Administrator's group (if the storage system belongs to a domain), and any user or group that you configured with Administrative access.
during CIFS setup. The /vol/vol0/home directory is shared as HOME with "Full Control" access granted to the group Everyone.

Step

1. To verify that the /vol/vol0 path and /vol/vol0/home directory entities exist on your storage system, enter the following command at the storage system command line:

   ```
   exportfs
   ```

   You should see a listing that includes lines similar to the following:

   ```
   /vol/vol0 -sec=sys,rw=admin_host,root=admin_host,nosuid
   /vol/vol0/home -sec=sys,rw,root=admin_host,nosuid
   ```

Managing licenses

You can use the `license show` command at the storage system command line to verify that the appropriate protocol and service licenses are installed on your system or to configure additional licenses.

About this task

Data ONTAP licenses are issued as packages, each of which contains a bundle of features or a single feature. A package requires a license key, and installing the key enables you to access all features in the package.

For more information about storage system licensing, see your Data ONTAP System Administration Guide for 7-Mode and the license (1) man page. Also see the knowledgebase article Data ONTAP 8.2 Licensing Overview and References on the NetApp Support Site.

   **Note:** If you see the License database is not available at this time message, wait at least five minutes after rebooting the system and the CLI is available, and then try the `license` commands again.

Step

1. Enter the appropriate `license` command to manage your licenses:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Enter this command at the storage system prompt...</th>
</tr>
</thead>
<tbody>
<tr>
<td>View existing licenses</td>
<td><code>license show</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   Result: You see information about installed licenses, such as the license package name and the license type.
If you want to... Enter this command at the storage system prompt...

<table>
<thead>
<tr>
<th>Add one or more licenses</th>
<th>license add license_key1 license_key2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result: The new license key is enabled and added for specific Data ONTAP features or packages.</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting: The license add: invalid license key &quot;key&quot; reason: &quot;License serial-number does not belong to this node., skipping&quot; message displays when the system serial number does not match the serial number that is embedded in the license key. Issue the sysconfig command to verify the system serial number and use the license key for that system only. You can verify the correct license keys for that serial number on the NetApp Support Site under My Support &gt; Software Licenses. If you continue to have problems, contact technical support.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remove a license</th>
<th>license delete license_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result: The license of a package is deleted from the storage system.</td>
<td></td>
</tr>
</tbody>
</table>

Preparing NFS clients to access the storage system

To make storage system data available to NFS clients, you need to export the storage system's file system. You must also mount the file system on your NFS clients.

For more information about NFS configuration, see your Data ONTAP File Access and Protocols Management Guide for 7-Mode and your NFS client documentation.

You need a license to use the NFS protocol. For more information about licenses, see the Data ONTAP System Administration Guide for 7-Mode.

Enabling or disabling NFS on the storage system

Enabling or disabling NFS on the storage system includes managing the NFS license and the NFS server. You can use the license show command to manage the NFS license and the nfs command to manage the NFS server.

Steps

1. Check whether NFS is currently licensed on the storage system by entering the following command:

   license

2. Perform one of the following actions:
If NFS is... Enter the following command...

| Not licensed and you want to license it | license add nfs_license_key |
| Licensed and you want to remove the license | license delete nfs |

3. Check whether the NFS server is currently running on the storage system by entering the following command:

   nfs status

4. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If the NFS server is... Enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not running and you want to enable it nfs on</td>
</tr>
<tr>
<td>Running and you want to disable it nfs off</td>
</tr>
</tbody>
</table>

After you finish

If you installed an NFS license and enabled the NFS server, you must now configure exports before NFS clients can access data on the storage system.

Exporting file systems to NFS clients

Before NFS clients can mount file systems, you need to export those file systems by adding them to the storage system's /etc/exports file.

Before you begin

NFS must be licensed and the NFS service must be enabled before you can export file systems to NFS clients. For more information about configuring NFS licenses, see the Data ONTAP File Access and Protocols Management Guide for 7-Mode.

About this task

Security styles of file systems (UNIX, NTFS, and Mixed) are all available for exporting and can be mounted by NFS clients. However, for accessing a volume with NTFS effective security style (NTFS volume or mixed volume with NTFS effective security style), file access is granted based on NTFS permissions. To properly ascertain file permissions, UNIX user names are mapped to corresponding Windows user names, and access is granted based on NTFS permissions granted to the mapped Windows user.
Steps

1. Determine valid path names for directories by entering the following command at the storage system prompt:

```
qtree status
```

**Example**

The following display shows sample output from the `qtree status` command:

<table>
<thead>
<tr>
<th>Volume</th>
<th>Tree</th>
<th>Style</th>
<th>Oplocks</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>vol0</td>
<td>home</td>
<td>unix</td>
<td>enabled</td>
<td>normal</td>
</tr>
<tr>
<td>vol1snap</td>
<td>qtree1</td>
<td>unix</td>
<td>enabled</td>
<td>normal</td>
</tr>
<tr>
<td>vol2eng</td>
<td>team1</td>
<td>mixed</td>
<td>enabled</td>
<td>normal</td>
</tr>
<tr>
<td>vol2mkt</td>
<td>nt</td>
<td>ntfs</td>
<td>enabled</td>
<td>normal</td>
</tr>
</tbody>
</table>

2. From the `qtree` command output, convert the first two entries into valid path names by using the following format:

```
/Volume/Tree
```

**Example**

```
/vol0/home
/vol1snap/qtree1
/vol2eng/team1
```

3. Use a text editor from an NFS client to open the `/etc/exports` file on the storage system.

4. Add the storage system directories to the `/etc/exports` file by using the following format:

**Example**

```
/vol/vol0/home -sec=sys, rw, root=admin_host
/vol/vol1snap/qtree1 -sec=sys, rw, root=admin_host
/vol/vol2eng/team1 -sec=sys, rw=10.0.0.0/24:172.17.0.0/16, root=admin_host
/vol/vol2mkt/nt -sec=sys, rw=netgroup1:netgroup2, root=admin_host: 10.0.0.100
```

For information about specifying entries and access permissions in the `/etc/exports` file, see the chapter about file access using NFS in the `Data ONTAP File Access and Protocols Management Guide for 7-Mode`.

5. Save the file and exit the text editor.
6. To make your changes to the /etc/exports file effective immediately, issue the `exportfs` command with the reload option:

```
exportfs -r
```

## Preparing CIFS clients to access the storage system

If you are in an Active Directory domain, you must ensure that DNS is correctly configured to ensure CIFS client access.

Once setup is complete, the storage system establishes CIFS client connectivity by automatically registering with the master browser. If cross-subnet browsing is configured correctly, the storage system is now visible to all CIFS clients. For more information about cross-subnet browsing, see Microsoft networking documentation.

**Note:** Although CIFS visibility has been established, you must configure shares with share access permissions before any storage system data can become accessible to CIFS clients. For information about how to make a test share available to CIFS clients, see the *Data ONTAP File Access and Protocols Management Guide for 7-Mode*.

You also need to provide information to Windows client users about how to access data on the storage system for their particular Windows version.

## Creating a storage system DNS "A" record for CIFS client access

In Active Directory domains, you must create a storage system DNS "A" record on the DNS server before providing access to CIFS clients.

### About this task

The storage system's DNS "A" record can be created manually or registered dynamically.

### Steps

1. To configure the dynamic update of DNS through the storage system, set one of the following options:
   ```
   dns.update.enable on
   ```
   ```
   dns.update.enable secure
   ```
   You must use the `secure` command if your DNS supports secure updates.

2. To disable dynamic update of DNS, set the `dns.update.enable` option to `off`. 
Ways to verify the configuration for HA pairs

There are two ways you can check your high-availability configuration before placing the pair online: running the Config Advisor tool or using the command-line interface. You also need to review the requirements for configuring your HA pair.

When you configure HA pair, the following configuration information needs to be the same on both systems:

- Parameters
- Network interfaces
- Configuration files
- Licenses and option settings

You must set `options cf.mode to ha` for HA pairs.

Note: The values for domain controllers and WINS servers no longer need to be identical on both storage systems in an HA pair. You can have each storage system exist in a different domain or a different workgroup, or both. However, if you have a multiprotocol environment and use UID-to-SID mapping, the UNIX security information must be compatible between the two domains. For example, if you have a UID of 119, it must map to the same Windows account for both storage systems.

For more information about verifying your configuration and managing storage systems in an HA pair, see your *Data ONTAP High Availability and MetroCluster Configuration Guide for 7-Mode*.

Verifying the HA pair configuration

You can go to the NetApp Support Site and download the Config Advisor tool to check for common configuration errors.

About this task

Config Advisor is a configuration validation and health check tool for NetApp systems. It can be deployed at both secure sites and non-secure sites for data collection and system analysis.

Note: Support for Config Advisor is limited, and available only online.

Steps

1. Log in to the NetApp Support Site at `support.netapp.com` and go to Downloads > Utility ToolChest.
2. Click Config Advisor (WireGauge renamed).
3. Follow the directions on the web page for downloading, installing, and running the utility.

4. After running Config Advisor, review the tool's output and follow the recommendations to address any issues discovered.

### Configuring a node for non-HA (stand-alone) use

By default, storage controllers are configured for use in HA mode. To use a controller in stand-alone mode, you must disable the controller failover functionality and change the node to non-HA mode.

**Before you begin**

You must determine the current configuration of the storage controller because the controller failover and HA mode states can vary. You can use the `cf status` command to determine the current configuration.

You must also confirm that all loops and disk shelves in the system contain disks that belong to only one of the two nodes you intend to isolate. If any disk shelves or loops contain a mix of disks belonging to both nodes, you must move data.

**About this task**

When a storage controller is shipped from the factory or when Data ONTAP is reinstalled using option four of the Data ONTAP boot menu (Clean configuration and initialize all disks), HA mode is enabled by default, and the system's nonvolatile memory (NVRAM or NVMEM) is split. If you plan to use the controller in standalone mode, you must configure the node as non-HA. Reconfiguring the node as non-HA mode enables full use of the system's nonvolatile memory.

**Note:** Configuring the node as standalone removes the availability benefits of the HA configuration and creates a single point of failure.

For information on using the boot menu to manage the storage system, see the *Data ONTAP System Administration Guide for 7-Mode*.

**Choices**

- If the `cf status` output displays `Non-HA mode`, then the node is configured for non-HA mode and you are finished:

  **Example**

  ```
  node > cf status
  Non-HA mode.
  ```

- If the `cf status` output directs you to reboot, you must reboot the node to enable full use of the system's nonvolatile memory:
**Example**

```bash
node> cf status
Non-HA mode. Reboot to use full NVRAM.
```

1. Reboot the node using the following command:

    ```bash
    node> reboot
    ```

   After the node reboots, you are finished.

- **If the** `cf status` **output displays** `Controller Failover enabled`, **you must disable both controller failover and HA mode and then reboot the node to enable full use of the system's nonvolatile memory:**

**Example**

```bash
node> cf status
Controller Failover enabled
```

1. Disable controller failover using the following command:

    ```bash
    node> cf disable
    ```

2. Set the mode to non-HA by using the following command:

    ```bash
    node> options cf.mode non_ha
    ```

3. Open the `/etc/rc` file with a text editor and remove references to the partner node in the `ifconfig` entries, as shown in the following example:

    **Example**

    Original entry:

    ```bash
    ifconfig e0 199.9.204.254 partner 199.9.204.255
    ```

    Edited entry:

    ```bash
    ifconfig e0 199.9.204.254
    ```

4. Reboot the node by using the following command:

    ```bash
    node> reboot
    ```

   After the node reboots, you are finished.

- **If the** `cf status` **output displays** `Controller Failover disabled`, **then the HA mode is still enabled, so you must set the HA mode to non-HA and reboot the node to enable full use of the system's nonvolatile memory:**
Example

```
node> cf status
Controller Failover disabled
```

1. Set the mode to non-HA by using the following command:
   ```
   node> options cf.mode non_ha
   ```

2. Reboot the node by using the following command:
   ```
   node> reboot
   ```

After the node reboots, you are finished.

After you finish
Reconfigure the hardware.

Setting up AutoSupport

You can control whether and how AutoSupport information is sent to technical support and your internal support organization, and then test that the configuration is correct.

About this task
For more information about the following commands, see the man pages.

Steps
1. Ensure that AutoSupport is enabled by setting the `autosupport.enable` option to `on`.

2. If you want technical support to receive AutoSupport messages, set the following options:
   a. Set `autosupport.support.enable` to `on`.

   b. Select a transport protocol for messages to technical support by setting `autosupport.support.transport` to `smtp`, `http`, or `https`.

   c. If you chose HTTP or HTTPS as the transport protocol and you use a proxy, set `autosupport.proxy.url` to the URL of your proxy.

3. If you want your internal support organization or a support partner to receive AutoSupport messages, perform the following actions:
   a. Identify the recipients in your organization by setting the following options:
<table>
<thead>
<tr>
<th>Set this option...</th>
<th>To this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>autosupport.to</td>
<td>Up to five comma-separated individual email addresses or distribution lists in your internal support organization that will receive key AutoSupport messages</td>
</tr>
<tr>
<td>autosupport.noteto</td>
<td>Up to five comma-separated individual email addresses or distribution lists in your internal support organization that will receive a shortened version of key AutoSupport messages designed for cell phones and other mobile devices</td>
</tr>
<tr>
<td>autosupport.partner.to</td>
<td>Up to five comma-separated individual email addresses or distribution lists in your support partner organization that will receive all AutoSupport messages</td>
</tr>
</tbody>
</table>

b. Check that addresses are correctly configured by listing the destinations using the autosupport destinations show command.

4. If you are sending messages to your internal support organization or you chose SMTP transport for messages to technical support, configure SMTP by setting the following options:

   • Set autosupport.mailhost to one or more mail hosts, separated by commas. You can set a maximum of five.

   • Set autosupport.from to the email address that sends the AutoSupport message.

   • Set autosupport.max_smtp_size to the email size limit of your SMTP server.

5. If you want AutoSupport to specify a fully qualified domain name when it sends connection requests to your SMTP mail server, configure DNS.

   For information about configuring DNS, see the *Data ONTAP Network Management Guide for 7-Mode*.

6. Optional: Change the following settings:

<table>
<thead>
<tr>
<th>If you want to do this...</th>
<th>Then set the following options...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide private data by removing, masking, or encoding sensitive data in the messages</td>
<td>Set autosupport.content to minimal. If you change from complete to minimal, all AutoSupport history and all associated files are deleted.</td>
</tr>
<tr>
<td>Stop sending performance data in periodic AutoSupport messages</td>
<td>Set autosupport.performance_data.enable to disable.</td>
</tr>
</tbody>
</table>
7. Check the overall configuration using the `options autosupport` command.

8. Test that AutoSupport messages are being sent and received:
   a. Use the `options autosupport.doit test` command.
   b. Confirm that NetApp is receiving your AutoSupport messages by checking the email addresses that were specified in the `autosupport.to` option.
      An automated response from the NetApp mail handler should have been sent to these email addresses.
   c. Optional: Confirm that the AutoSupport message is being sent to your internal support organization or to your support partner by checking the email of any address that you configured for the `autosupport.to`, `autosupport.noteto`, or `autosupport.partner` options.

Verifying SP connections

You can use this procedure to verify that the Service Processor (SP) is set up correctly and connected to the network.

Before you begin

You must have configured AutoSupport before configuring the SP. Data ONTAP automatically sends the AutoSupport configuration to the SP, allowing the SP to send alerts and notifications through an AutoSupport message. AutoSupport is enabled by default when you configure your storage system for the first time.

About this task

For more information about AutoSupport and using the SP to manage remote storage systems, see the *Data ONTAP System Administration Guide for 7-Mode*. For more information about the `sp` commands, see the man pages.

Steps

1. At the storage system prompt, enter the following command to verify that the SP network configuration is correct:
   ```
   sp status
   ```
   You also can use the `system node service-processor network show` command to verify the SP network configuration.

2. At the storage system prompt, enter the following command to verify that the SP AutoSupport function is working properly:
   ```
   sp test autosupport
   ```
Note: The SP uses the same mail host information that Data ONTAP uses for AutoSupport. The `sp test autosupport` command requires that you set up the `autosupport.to` option properly.

The following message is a sample of the output Data ONTAP displays:
Sending email messages via SMTP server at mailhost@companyname.com. If `autosupport.enable` is on, then each email address in `autosupport.to` should receive the test message shortly.

### Example of displaying the configuration information

The following example displays the SP status and configuration information:

```
mysystem> sp status
Service Processor      Status: Online
   Firmware Version:   1.2
   Mgmt MAC Address:   00:A0:98:01:7D:5B
   Ethernet Link:      up
   Using DHCP:         no
IPv4 configuration:
   IP Address:         192.168.123.98
   Netmask:            255.255.255.0
   Gateway:            192.168.123.1
IPv6 configuration:
   Global IP:          fd22:8b1e:b255:204::1234
   Prefix Length:      64
   Gateway:            fd22:81be:b255:204::1
   Router Assigned IP: fd22:8b1e:b255:204:2a0:98ff:fe01:7d5b
   Prefix Length:      64
   Link Local IP:      fe80::2a0:98ff:fe00:7d1b
   Prefix Length:      64
```

### Preparing to use OnCommand System Manager

Before you can use OnCommand System Manager to monitor and manage Data ONTAP, you need to verify network connectivity and enable SNMP.

**About this task**

OnCommand System Manager 2.2 and later works with Data ONTAP 8.2.

**Steps**

1. Use the `ping` command to verify that clients using System Manager can connect to the IP addresses you configured on the storage system during setup.

2. Enable SNMP by using the following command: `options snmp.enable on`

For more information about using SNMP and diagnosing network problems, see the *Data ONTAP Network Management Guide for 7-Mode*. 
After you finish

You can use System Manager to configure and manage iSCSI networks, Fibre Channel fabrics and Fibre Channel over Ethernet in a SAN environment. You also can use System Manager for managing CIFS and NFS clients. For more information, see the OnCommand System Manager Help For Use With Data ONTAP 7-Mode.

Related tasks

Verifying network connectivity on page 78

Verifying the existence of two paths to an array LUN

If the primary path to any array LUN fails, Data ONTAP automatically maps each port of the Data ONTAP system to a secondary path. You must ensure that there are two paths to each array LUN so that the Data ONTAP system can continue to work when running on a single path.

Verifying the existence of two paths: storage show disk command

You should verify that your Data ONTAP system is configured with two paths to an array LUN so that there is a secondary path in case the primary path fails or is taken offline.

Steps

1. Enter the following command to show the primary and secondary paths to array LUNs:
   
   `storage show disk -p all`

   The system displays information similar to the following:

<table>
<thead>
<tr>
<th>PRIMARY ADAPTER</th>
<th>PORT</th>
<th>SECONDARY ADAPTER</th>
<th>PORT</th>
<th>SHELF BAY</th>
</tr>
</thead>
<tbody>
<tr>
<td>vnmc4500s32:4.127L1</td>
<td>-</td>
<td>vnmc4500s33:19.127L1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>vnmc4500s32:4.127L12</td>
<td>-</td>
<td>vnmc4500s33:19.127L12</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>vnmc4500s33:19.127L2</td>
<td>-</td>
<td>vnmc4500s32:4.127L2</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>vnmc4500s33:19.127L13</td>
<td>-</td>
<td>vnmc4500s32:4.127L13</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

   Note: When you use the `all` variable, adapters are displayed, but unassigned LUNs are not visible.

2. Determine whether a primary path and a secondary path to the array LUNs are shown.

   If you do not see a primary and secondary path, check the zoning, host group configuration, and cabling.

   Note: Do not continue with testing until you see two paths.
For information about troubleshooting pathing, see the *FlexArray Virtualization Installation Requirements and Reference Guide*

3. Look at the adapters shown to see whether all paths are on a single adapter.

If you see both paths through one port (for example, both paths through the 0c port), this is an indication that the back-end zoning is redundantly crossed. This is not a supported configuration.

**Note:** Data ONTAP changes the path to array LUNs, as necessary, for load balancing. Therefore, the primary and secondary paths for a given array LUN can change when the `storage show disk` command is issued at different times.

### Verifying the existence of two paths: storage array show-config command

You should verify that your Data ONTAP system is configured with two paths to an array LUN so that there is a secondary path in case the primary path fails or is taken offline.

**Step**

1. Enter the following command to show the primary and secondary paths to array LUNs:

   ```
   storage array show-config
   ```

   You see information similar to the following:

   ```
<table>
<thead>
<tr>
<th>LUN Group</th>
<th>Array Name</th>
<th>Array Target Ports</th>
<th>Switch Port</th>
<th>Initiator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group 0 (4 LUNS) HP_V210</td>
<td>50:00:1f:e1:50:0a:86:6d</td>
<td>vnmc4300s35:11</td>
<td>0b</td>
<td></td>
</tr>
<tr>
<td>50:00:1f:e1:50:0a:86:68</td>
<td>vnbr4100s31:1</td>
<td>0a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>50:00:1f:e1:50:0a:86:6c</td>
<td>vnmc4300s35:6</td>
<td>0d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group 1(50 LUNS) HP_V200</td>
<td>50:00:1f:e1:50:0d:14:6d</td>
<td>vnbr4100s31:5</td>
<td>0a</td>
<td></td>
</tr>
<tr>
<td>50:00:1f:e1:50:0d:14:68</td>
<td>vnmc4300s35:3</td>
<td>0d</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
   ```

   This example shows output from a Data ONTAP system that is connected to two storage arrays. Each LUN group consists of LUNs that share the same two paths. Group 0 contains a total of 4 LUNs on the HP_V210 array and Group 1 contains 50 LUNs on the HP_V200 array.

   Array LUNs that are not configured with two paths are shown as one or more LUNs with a single path, similar to the following example.

   ```
<table>
<thead>
<tr>
<th>LUN Group</th>
<th>Array Name</th>
<th>Array Target Ports</th>
<th>Switch Port</th>
<th>Initiator</th>
</tr>
</thead>
<tbody>
<tr>
<td>(4 LUNS) HP_V210</td>
<td>50:00:1f:e1:50:0a:86:6d</td>
<td>vnmc4300s35:11</td>
<td>0b</td>
<td></td>
</tr>
</tbody>
</table>
   ```
Verifying path failover for array LUNs

You want to demonstrate that the Data ONTAP system continues to work when running with a single path, for example, when a switch or storage array port is taken offline. You can test path failover by physically removing fibre cables or taking ports offline using Data ONTAP commands.

The procedure you use to test path failover differs slightly, depending on whether you are testing a stand-alone system or an HA pair.

Verifying path failover for array LUNs in a stand-alone system

It is important to demonstrate that a stand-alone Data ONTAP system continues to operate on a single path.

Steps

1. Set your privilege level to advanced:
   ```
   priv set advanced
   ```
2. Set port 0a offline by using the following command:
   ```
   fcadmin offline 0a
   ```
3. Show the number of disks seen on each adapter using the following command:
   ```
   sysconfig
   ```
   No disks will be assigned to adapter 0a.
4. Show the primary and secondary paths by using the following command:
   ```
   storage show disk -p
   ```
5. Return port 0a to online:
   ```
   fcadmin online 0a
   ```

Verifying path failover for array LUNs in an HA pair

It is important to demonstrate that controller failover and then path failover occur in an HA pair so that the system can to continue to operate on a single path.

Steps

1. Set your privilege level to advanced:
   ```
   priv set advanced
   ```
   You need to enter this command on the local and partner node.
2. On the local node, enter the following command to set port 0a offline (assuming that the redundant port pair is 0a and 0c):
   `fcadmin offline 0a`

3. Verify that only one path is available on the port pair:
   `storage show disk -p`

4. Enter the following command to initiate HA pair takeover:
   `cf takeover`

5. On the partner node, enter the following command:
   `cf giveback`

6. After the partner node is back online, repeat Steps 1, 2, and 3 on the partner node.
# Data ONTAP documentation

Product documentation for Data ONTAP is available online and in printed format.

Documentation is available on the NetApp Support Site. See the Release Notes for new features, enhancements, and known issues for Data ONTAP.

<table>
<thead>
<tr>
<th>For information about...</th>
<th>Go to the NetApp Support Site for the...</th>
</tr>
</thead>
<tbody>
<tr>
<td>New features, enhancements, known issues, and late-breaking news for your version of Data ONTAP software</td>
<td>Data ONTAP Release Notes for 7-Mode for your version of Data ONTAP.</td>
</tr>
<tr>
<td>Setting up and verifying software configuration</td>
<td>Data ONTAP Software Setup Guide for 7-Mode</td>
</tr>
<tr>
<td>Upgrading, downgrading, or reverting the Data ONTAP release</td>
<td>Data ONTAP Upgrade and Revert/Downgrade Guide for 7-Mode</td>
</tr>
<tr>
<td>Managing all aspects of your system</td>
<td>Documentation for your version of Data ONTAP. See the Data ONTAP Documentation Map for 7-Mode for an overview.</td>
</tr>
</tbody>
</table>
| Cabling, configuring, backing up and recovering data, and disk ownership | Data ONTAP System Administration Guide for 7-Mode  
Data ONTAP Data Protection Online Backup and Recovery Guide for 7-Mode  
Data ONTAP Storage Management Guide for 7-Mode  
FlexArray Virtualization Installation Requirements and Reference Guide |
<p>| Using high-availability configurations | Data ONTAP High Availability and MetroCluster Configuration Guide for 7-Mode |
| Setting up and managing network configurations of storage systems | Data ONTAP Network Management Guide for 7-Mode |
| Managing CIFS and NFS protocols | Data ONTAP File Access and Protocols Management Guide for 7-Mode |
| Configuring and managing Fibre Channel and iSCSI configurations, and creating and managing LUNs and initiator groups with the FC service | Data ONTAP SAN Administration Guide for 7-Mode |
| The most current information about your system hardware | Hardware Information Library page |</p>
<table>
<thead>
<tr>
<th>For information about...</th>
<th>Go to the NetApp Support Site for the...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware configuration options available for your system</td>
<td>Hardware Universe</td>
</tr>
<tr>
<td>Troubleshooting your system</td>
<td>Hardware Platform Monitoring Guide</td>
</tr>
<tr>
<td>Testing field-replaceable units and diagnosing and correcting system hardware problems</td>
<td>Diagnostics Guide or System-Level Diagnostics Guide depending on your storage system</td>
</tr>
<tr>
<td>Configuring Remote Management using SP after initial setup</td>
<td>Data ONTAP System Administration Guide for 7-Mode</td>
</tr>
<tr>
<td>Managing your disk shelves</td>
<td>Installation and Service Guide for your disk shelf model</td>
</tr>
<tr>
<td>Managing Storage Encryption</td>
<td>Data ONTAP Storage Management Guide for 7-Mode</td>
</tr>
<tr>
<td>Monitoring and managing Data ONTAP using OnCommand System Manager</td>
<td>OnCommand System Manager Help for Use With Data ONTAP 7-Mode</td>
</tr>
</tbody>
</table>

**Related information**

*Documentation: By Product Library: support.netapp.com/documentation/productsatoz/index.html*

*Hardware Universe: https://hwu.netapp.com/*
Time zones

You must select a valid time zone value from the lists provided, record it in the configuration worksheet, and enter the value at the `setup` prompt.

Data ONTAP uses time zones defined by the standard UNIX zoneinfo database. You can set your system time zone by using one of the following types of terms:

- A geographic region, usually expressed as `area/location`
- Greenwich Mean Time (GMT) or the difference in hours from GMT
- A valid alias; that is, a term defined by the standard to refer to a geographic region or GMT
- A system-specific or other term not associated with a geographic region or GMT

The following are examples of valid aliases:

<table>
<thead>
<tr>
<th>Alias</th>
<th>Standard reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jamaica</td>
<td>US/Eastern</td>
</tr>
<tr>
<td>Navajo</td>
<td>US/Mountain</td>
</tr>
<tr>
<td>UCT</td>
<td>GMT</td>
</tr>
<tr>
<td>UTC</td>
<td></td>
</tr>
<tr>
<td>Universal</td>
<td></td>
</tr>
<tr>
<td>Zulu</td>
<td></td>
</tr>
</tbody>
</table>

In most cases, you should select an appropriate geographical or GMT term unless you have special requirements in your environment.

If you need to change your selected time zone after setup is complete, you can use the `timezone` command.

For more information about time zones in Data ONTAP, see the `timezone(1)` and `zoneinfo(5)` man pages.

Time zones by geographical region

The names of geographical time zones that are valid in Data ONTAP combine an area and location, in which the latter can be a major city, region, or other geographical feature. You should find the most accurate combination for you and enter it at the `setup` prompt.

The following tables list the time zones by geographical region:
### Africa

<table>
<thead>
<tr>
<th>Africa/Abidjan</th>
<th>Africa/Djibouti</th>
<th>Africa/Maputo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa/Accra</td>
<td>Africa/Douala</td>
<td>Africa/Maseru</td>
</tr>
<tr>
<td>Africa/Addis_Ababa</td>
<td>Africa/Freetown</td>
<td>Africa/Mbabane</td>
</tr>
<tr>
<td>Africa/Algiers</td>
<td>Africa/Gaborone</td>
<td>Africa/Mogadishu</td>
</tr>
<tr>
<td>Africa/Asmera</td>
<td>Africa/Harare</td>
<td>Africa/Monrovia</td>
</tr>
<tr>
<td>Africa/Bamako</td>
<td>Africa/Johannesburg</td>
<td>Africa/Nairobi</td>
</tr>
<tr>
<td>Africa/Bangui</td>
<td>Africa/Kampala</td>
<td>Africa/Ndjamena</td>
</tr>
<tr>
<td>Africa/Banjul</td>
<td>Africa/Khartoum</td>
<td>Africa/Niamey</td>
</tr>
<tr>
<td>Africa/Bissau</td>
<td>Africa/Kigali</td>
<td>Africa/Nouakchott</td>
</tr>
<tr>
<td>Africa/Blantyre</td>
<td>Africa/Kinshasa</td>
<td>Africa/Ouagadougou</td>
</tr>
<tr>
<td>Africa/Brazzaville</td>
<td>Africa/Lagos</td>
<td>Africa/Porto-Nov</td>
</tr>
<tr>
<td>Africa/Bujumbura</td>
<td>Africa/Libreville</td>
<td>Africa/Sao_Tome</td>
</tr>
<tr>
<td>Africa/Cairo</td>
<td>Africa/Lome</td>
<td>Africa/Timbuktu</td>
</tr>
<tr>
<td>Africa/Casablanca</td>
<td>Africa/Luanda</td>
<td>Africa/Tripoli</td>
</tr>
<tr>
<td>Africa/Conakry</td>
<td>Africa/Lumumbashi</td>
<td>Africa/Tunis</td>
</tr>
<tr>
<td>Africa/Dakar</td>
<td>Africa/Lusaka</td>
<td>Africa/Windhoek</td>
</tr>
<tr>
<td>Africa/Dar_es_Salaam</td>
<td>Africa/Malabo</td>
<td></td>
</tr>
</tbody>
</table>

### America

<table>
<thead>
<tr>
<th>America/Adak</th>
<th>America/Grenada</th>
<th>America/Noronha</th>
</tr>
</thead>
<tbody>
<tr>
<td>America/Anchorage</td>
<td>America/Guadeloupe</td>
<td>America/Panama</td>
</tr>
<tr>
<td>America/Anguilla</td>
<td>America/Guatemala</td>
<td>America/Pangnirtung</td>
</tr>
<tr>
<td>America/Antigua</td>
<td>America/Guayaquil</td>
<td>America/Paramaribo</td>
</tr>
<tr>
<td>America/Aruba</td>
<td>America/Guyana</td>
<td>America/Phoenix</td>
</tr>
<tr>
<td>America/Asuncion</td>
<td>America/Halifax</td>
<td>America/Port_of_Spain</td>
</tr>
<tr>
<td>America/Atka</td>
<td>America/Havana</td>
<td>America/Port-au-Prince</td>
</tr>
<tr>
<td>America/Barbados</td>
<td>America/Indiana</td>
<td>America/Porto_Acre</td>
</tr>
<tr>
<td>America/Belize</td>
<td>America/Indianapolis</td>
<td>America/Puerto_Rico</td>
</tr>
<tr>
<td>America/Bogota</td>
<td>America/Inuvik</td>
<td>America/Rainy_River</td>
</tr>
<tr>
<td>America/Boise</td>
<td>America/Iqaluit</td>
<td>America/Rankin_Inlet</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>America/Buenos_Aires</td>
<td>America/Jamaica</td>
<td>America/Regina</td>
</tr>
<tr>
<td>America/Caracas</td>
<td>America/Jujuy</td>
<td>America/Rosario</td>
</tr>
<tr>
<td>America/Catamarca</td>
<td>America/Juneau</td>
<td>America/Santiago</td>
</tr>
<tr>
<td>America/Cayenne</td>
<td>America/Knox_IN</td>
<td>America/Santo_Domingo</td>
</tr>
<tr>
<td>America/Cayman</td>
<td>America/La_Paz</td>
<td>America/Sao_Paulo</td>
</tr>
<tr>
<td>America/Chicago</td>
<td>America/Lima</td>
<td>America/Scoresbysund</td>
</tr>
<tr>
<td>America/Cordoba</td>
<td>America/Los_Angeles</td>
<td>America/Shiprock</td>
</tr>
<tr>
<td>America/Costa_Rica</td>
<td>America/Louisville</td>
<td>America/St_Johns</td>
</tr>
<tr>
<td>America/Cuiaba</td>
<td>America/Maceio</td>
<td>America/St_Kitts</td>
</tr>
<tr>
<td>America/Curacao</td>
<td>America/Managua</td>
<td>America/St_Lucia</td>
</tr>
<tr>
<td>America/Dawson</td>
<td>America/Manaus</td>
<td>America/St_Thomas</td>
</tr>
<tr>
<td>America/Dawson_Creek</td>
<td>America/Martinique</td>
<td>America/St_Vincent</td>
</tr>
<tr>
<td>America/Denver</td>
<td>America/Mazatlan</td>
<td>America/Swift_Current</td>
</tr>
<tr>
<td>America/Detroit</td>
<td>America/Mendoza</td>
<td>America/Tegucigalpa</td>
</tr>
<tr>
<td>America/Dominica</td>
<td>America/Menominee</td>
<td>America/Thule</td>
</tr>
<tr>
<td>America/Edmonton</td>
<td>America/Mexico_City</td>
<td>America/Thunder_Bay</td>
</tr>
<tr>
<td>America/El_Salvador</td>
<td>America/Miquelon</td>
<td>America/Tijuana</td>
</tr>
<tr>
<td>America/Ensenada</td>
<td>America/Montevideo</td>
<td>America/Tortola</td>
</tr>
<tr>
<td>America/Fort_Wayne</td>
<td>America/Montreal</td>
<td>America/Vancouver</td>
</tr>
<tr>
<td>America/Fortaleza</td>
<td>America/Montserrat</td>
<td>America/Virgin</td>
</tr>
<tr>
<td>America/Glace_Bay</td>
<td>America/Nassau</td>
<td>America/Whitehorse</td>
</tr>
<tr>
<td>America/Godthab</td>
<td>America/New_York</td>
<td>America/Winnipeg</td>
</tr>
<tr>
<td>America/Goose_Bay</td>
<td>America/Nipigon</td>
<td>America/Yakutat</td>
</tr>
<tr>
<td>America/Grand_Turk</td>
<td>America/Nome</td>
<td>America/Yellowknife</td>
</tr>
</tbody>
</table>

**Antarctica**

<table>
<thead>
<tr>
<th>Antarctica/Casey</th>
<th>Antarctica/Mawson</th>
<th>Antarctica/Palmer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antarctica/DumontDUrville</td>
<td>Antarctica/McMurdo</td>
<td>Antarctica/South_Pole</td>
</tr>
</tbody>
</table>
### Asia

<table>
<thead>
<tr>
<th>Asia/Aden</th>
<th>Asia/Irkutsk</th>
<th>Asia/Qatar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia/Alma-Ata</td>
<td>Asia/Ishigaki</td>
<td>Asia/Rangoon</td>
</tr>
<tr>
<td>Asia/Amman</td>
<td>Asia/Istanbul</td>
<td>Asia/Riyadh</td>
</tr>
<tr>
<td>Asia/Anadyr</td>
<td>Asia/Jakarta</td>
<td>Asia/Saigon</td>
</tr>
<tr>
<td>Asia/Aqtau</td>
<td>Asia/Jayapura</td>
<td>Asia/Seoul</td>
</tr>
<tr>
<td>Asia/Aqtobe</td>
<td>Asia/Jerusalem</td>
<td>Asia/Shanghai</td>
</tr>
<tr>
<td>Asia/Ashkhabad</td>
<td>Asia/Kabul</td>
<td>Asia/Singapore</td>
</tr>
<tr>
<td>Asia/Baghdad</td>
<td>Asia/Kamchatka</td>
<td>Asia/Taipei</td>
</tr>
<tr>
<td>Asia/Bahrain</td>
<td>Asia/Karachi</td>
<td>Asia/Tashkent</td>
</tr>
<tr>
<td>Asia/Baku</td>
<td>Asia/Kashgar</td>
<td>Asia/Tbilisi</td>
</tr>
<tr>
<td>Asia/Bangkok</td>
<td>Asia/Katmandu</td>
<td>Asia/Tehran</td>
</tr>
<tr>
<td>Asia/Beirut</td>
<td>Asia/Krasnoyarsk</td>
<td>Asia/Tel_Aviv</td>
</tr>
<tr>
<td>Asia/Bishkek</td>
<td>Asia/Kuala_Lumpur</td>
<td>Asia/Thimbu</td>
</tr>
<tr>
<td>Asia/Brunei</td>
<td>Asia/Kuching</td>
<td>Asia/Tokyo</td>
</tr>
<tr>
<td>Asia/Calcutta</td>
<td>Asia/Kuwait</td>
<td>Asia/Ujung_Pandang</td>
</tr>
<tr>
<td>Asia/Chungking</td>
<td>Asia/Macao</td>
<td>Asia/Ulan_Bator</td>
</tr>
<tr>
<td>Asia/Colombo</td>
<td>Asia/Magadan</td>
<td>Asia/Urumqi</td>
</tr>
<tr>
<td>Asia/Dacca</td>
<td>Asia/Manila</td>
<td>Asia/Vientiane</td>
</tr>
<tr>
<td>Asia/Damascus</td>
<td>Asia/Muscat</td>
<td>Asia/Vladivostok</td>
</tr>
<tr>
<td>Asia/Dubai</td>
<td>Asia/Nicosia</td>
<td>Asia/Yakutsk</td>
</tr>
<tr>
<td>Asia/Dushanbe</td>
<td>Asia/Novosibirsk</td>
<td>Asia/Yekaterinburg</td>
</tr>
<tr>
<td>Asia/Gaza</td>
<td>Asia/Omsk</td>
<td>Asia/Yerevan</td>
</tr>
<tr>
<td>Asia/Harbin</td>
<td>Asia/Phnom_Penh</td>
<td></td>
</tr>
<tr>
<td>Asia/Hong_Kong</td>
<td>Asia/Pyongyang</td>
<td></td>
</tr>
</tbody>
</table>

### Atlantic

<table>
<thead>
<tr>
<th>Atlantic/Azores</th>
<th>Atlantic/Faeroe</th>
<th>Atlantic/South_Georgia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atlantic/Bermuda</td>
<td>Atlantic/Jan_Mayen</td>
<td>Atlantic/St_Helena</td>
</tr>
<tr>
<td>Atlantic/Canary</td>
<td>Atlantic/Madeira</td>
<td>Atlantic/Stanley</td>
</tr>
<tr>
<td>Atlantic/Cape_Verde</td>
<td>Atlantic/Reykjavik</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------</td>
<td></td>
</tr>
</tbody>
</table>

**Australia**

<table>
<thead>
<tr>
<th>Australia/ACT</th>
<th>Australia/LHI</th>
<th>Australia/Queensland</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia/Adelaide</td>
<td>Australia/Lindeman</td>
<td>Australia/South</td>
</tr>
<tr>
<td>Australia/Brisbane</td>
<td>Australia/Lord Howe</td>
<td>Australia/Sydney</td>
</tr>
<tr>
<td>Australia/Broken_Hill</td>
<td>Australia/Melbourne</td>
<td>Australia/Tasmania</td>
</tr>
<tr>
<td>Australia/Canberra</td>
<td>Australia/NSW</td>
<td>Australia/Victoria</td>
</tr>
<tr>
<td>Australia/Darwin</td>
<td>Australia/North</td>
<td>Australia/West</td>
</tr>
<tr>
<td>Australia/Hobart</td>
<td>Australia/Perth</td>
<td>Australia/Yancowinna</td>
</tr>
</tbody>
</table>

**Brazil**

<table>
<thead>
<tr>
<th>Brazil/Acre</th>
<th>Brazil/East</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazil/DeNoronha</td>
<td>Brazil/West</td>
</tr>
</tbody>
</table>

**Canada**

<table>
<thead>
<tr>
<th>Canada/Atlantic</th>
<th>Canada/Eastern</th>
<th>Canada/Pacific</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada/Central</td>
<td>Canada/Mountain</td>
<td>Canada/Saskatchewan</td>
</tr>
<tr>
<td>Canada/East- Saskatchewan</td>
<td>Canada/Newfoundland</td>
<td>Canada/Yukon</td>
</tr>
</tbody>
</table>

**Chile**

<table>
<thead>
<tr>
<th>Chile/Continental</th>
<th>Chile/EasterIsland</th>
</tr>
</thead>
</table>

**Europe**

<table>
<thead>
<tr>
<th>Europe/Amsterdam</th>
<th>Europe/Kiev</th>
<th>Europe/San_Marino</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe/Andorra</td>
<td>Europe/Kuybyshev</td>
<td>Europe/Sarajevo</td>
</tr>
<tr>
<td>Europe/Athens</td>
<td>Europe/Lisbon</td>
<td>Europe/Simferopol</td>
</tr>
<tr>
<td>Europe/Belfast</td>
<td>Europe/Ljubljana</td>
<td>Europe/Skopje</td>
</tr>
<tr>
<td>Europe/Belgrade</td>
<td>Europe/London (BST)</td>
<td>Europe/Sofia</td>
</tr>
<tr>
<td>Europe/Berlin</td>
<td>Europe/Luxembourg</td>
<td>Europe/Stockholm</td>
</tr>
<tr>
<td>Europe/Bratislava</td>
<td>Europe/Madrid</td>
<td>Europe/Tallinn</td>
</tr>
<tr>
<td>Time zones</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Europe/Brussels</th>
<th>Europe/Malta</th>
<th>Europe/Tirane</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe/Bucharest</td>
<td>Europe/Minsk</td>
<td>Europe/Vaduz</td>
</tr>
<tr>
<td>Europe/Budapest</td>
<td>Europe/Monaco</td>
<td>Europe/Vatican</td>
</tr>
<tr>
<td>Europe/Chisinau</td>
<td>Europe/Moscow</td>
<td>Europe/Vienna</td>
</tr>
<tr>
<td>Europe/Copenhagen</td>
<td>Europe/Oslo</td>
<td>Europe/Vilnius</td>
</tr>
<tr>
<td>Europe/Dublin</td>
<td>Europe/Paris</td>
<td>Europe/Warsaw</td>
</tr>
<tr>
<td>Europe/Gibraltar</td>
<td>Europe/Prague</td>
<td>Europe/Zagreb</td>
</tr>
<tr>
<td>Europe/Helsinki</td>
<td>Europe/Riga</td>
<td>Europe/Zurich</td>
</tr>
<tr>
<td>Europe/Istanbul</td>
<td>Europe/Rome</td>
<td></td>
</tr>
</tbody>
</table>

**Indian (Indian Ocean)**

<table>
<thead>
<tr>
<th>Indian/Antananarivo</th>
<th>Indian/Comoro</th>
<th>Indian/Mauritius</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indian/Chagos</td>
<td>Indian/Kerguelen</td>
<td>Indian/Mayotte</td>
</tr>
<tr>
<td>Indian/Christmas</td>
<td>Indian/Mahe</td>
<td>Indian/Reunion</td>
</tr>
<tr>
<td>Indian/Cocos</td>
<td>Indian/Maldives</td>
<td></td>
</tr>
</tbody>
</table>

**Mexico**

<table>
<thead>
<tr>
<th>Mexico/BajaNorte</th>
<th>Mexico/BajaSur</th>
<th>Mexico/General</th>
</tr>
</thead>
</table>

**Pacific**

<table>
<thead>
<tr>
<th>Pacific/Apia</th>
<th>Pacific/Johnston</th>
<th>Pacific/Ponape</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pacific/Auckland</td>
<td>Pacific/Kiritimati</td>
<td>Pacific/Port_Moresby</td>
</tr>
<tr>
<td>Pacific/Chatham</td>
<td>Pacific/Kosrae</td>
<td>Pacific/Rarotonga</td>
</tr>
<tr>
<td>Pacific/Easter</td>
<td>Pacific/Kwajalein</td>
<td>Pacific/Saipan</td>
</tr>
<tr>
<td>Pacific/Efate</td>
<td>Pacific/Majuro</td>
<td>Pacific/Samoa</td>
</tr>
<tr>
<td>Pacific/Enderbury</td>
<td>Pacific/Marquesas</td>
<td>Pacific/Tahiti</td>
</tr>
<tr>
<td>Pacific/Fakaofo</td>
<td>Pacific/Midway</td>
<td>Pacific/Tarawa</td>
</tr>
<tr>
<td>Pacific/Fiji</td>
<td>Pacific/Nauru</td>
<td>Pacific/Tongatapu</td>
</tr>
<tr>
<td>Pacific/Funafuti</td>
<td>Pacific/Niue</td>
<td>Pacific/Truk</td>
</tr>
<tr>
<td>Pacific/Galapagos</td>
<td>Pacific/Norfolk</td>
<td>Pacific/Wake</td>
</tr>
</tbody>
</table>
GMT offset and miscellaneous time zones

If you are not using a standard geographical time zone, you must select a GMT value or other valid term and enter it at the setup prompt.

Tables in this section contain the following valid time zone values:

- Time zones defined by GMT offset (how many hours different they are from Greenwich Mean Time)
- Time zones that are not associated with a geographical region
- Regional time zones that are not grouped by major land mass

### GMT

<table>
<thead>
<tr>
<th>GMT</th>
<th>GMT+9</th>
<th>GMT-5</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMT+1</td>
<td>GMT+10</td>
<td>GMT-6</td>
</tr>
<tr>
<td>GMT+2</td>
<td>GMT+11</td>
<td>GMT-7</td>
</tr>
<tr>
<td>GMT+3</td>
<td>GMT+12</td>
<td>GMT-8</td>
</tr>
<tr>
<td>GMT+4</td>
<td>GMT+13</td>
<td>GMT-9</td>
</tr>
<tr>
<td>GMT+5</td>
<td>GMT-1</td>
<td>GMT-10</td>
</tr>
<tr>
<td>GMT+6</td>
<td>GMT-2</td>
<td>GMT-11</td>
</tr>
<tr>
<td>GMT+7</td>
<td>GMT-3</td>
<td>GMT-12</td>
</tr>
<tr>
<td>GMT+8</td>
<td>GMT-4</td>
<td></td>
</tr>
</tbody>
</table>

### Etc

<table>
<thead>
<tr>
<th>Etc/GMT</th>
<th>Etc/GMT+11</th>
<th>Etc/GMT-9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Etc/GMT+0</td>
<td>Etc/GMT+12</td>
<td>Etc/GMT-10</td>
</tr>
<tr>
<td>Etc/GMT+1</td>
<td>Etc/GMT0</td>
<td>Etc/GMT-11</td>
</tr>
<tr>
<td>Etc/GMT+2</td>
<td>Etc/GMT-0</td>
<td>Etc/GMT-12</td>
</tr>
<tr>
<td>Time zones</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Etc/GMT+3</td>
<td>Etc/GMT-1</td>
<td>Etc/GMT-13</td>
</tr>
<tr>
<td>Etc/GMT+4</td>
<td>Etc/GMT-2</td>
<td>Etc/GMT-14</td>
</tr>
<tr>
<td>Etc/GMT+5</td>
<td>Etc/GMT-3</td>
<td>Etc/Greenwich</td>
</tr>
<tr>
<td>Etc/GMT+6</td>
<td>Etc/GMT-4</td>
<td>Etc/UTC</td>
</tr>
<tr>
<td>Etc/GMT+7</td>
<td>Etc/GMT-5</td>
<td>Etc/Universal</td>
</tr>
<tr>
<td>Etc/GMT+8</td>
<td>Etc/GMT-6</td>
<td>Etc/UTC</td>
</tr>
<tr>
<td>Etc/GMT+9</td>
<td>Etc/GMT-7</td>
<td>Etc/Zulu</td>
</tr>
<tr>
<td>Etc/GMT+10</td>
<td>Etc/GMT-8</td>
<td></td>
</tr>
</tbody>
</table>

**Miscellaneous**

<table>
<thead>
<tr>
<th>Time zones</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Arctic/Longyearbyen</td>
<td>HST</td>
</tr>
<tr>
<td>CET</td>
<td>Iceland</td>
</tr>
<tr>
<td>CST6CDT</td>
<td>Iran</td>
</tr>
<tr>
<td>Cuba</td>
<td>Israel</td>
</tr>
<tr>
<td>EET</td>
<td>Japan</td>
</tr>
<tr>
<td>Egypt</td>
<td>Kwajalein</td>
</tr>
<tr>
<td>Eire</td>
<td>Libya</td>
</tr>
<tr>
<td>EST</td>
<td>MET</td>
</tr>
<tr>
<td>EST5EDT</td>
<td>MST</td>
</tr>
<tr>
<td>Factory</td>
<td>MST7MDT</td>
</tr>
<tr>
<td>GB</td>
<td>Navajo</td>
</tr>
<tr>
<td>GB-Eire</td>
<td>NZ</td>
</tr>
<tr>
<td>Greenwich</td>
<td>NZ-CHAT</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>Poland</td>
</tr>
</tbody>
</table>

**System V**

<table>
<thead>
<tr>
<th>Time zones</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SystemV/AST4</td>
<td>SystemV/EST5EDT</td>
</tr>
<tr>
<td>SystemV/AST4ADT</td>
<td>SystemV/HST10</td>
</tr>
<tr>
<td>SystemV/CST6</td>
<td>SystemV/MST7</td>
</tr>
<tr>
<td>SystemV/CST6CDT</td>
<td>SystemV/MST7MDT</td>
</tr>
<tr>
<td>SystemV/EST5</td>
<td>SystemV/PST8</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>

108 | Software Setup Guide
Supported languages

You must select a supported language from the list provided and record its abbreviation in the configuration worksheet.

Specifying the language code

When you enter language codes during setup, you might need to specify a suffix, such as UTF-8.

Step

1. When prompted during setup, enter the code that corresponds to the appropriate language. To use UTF-8 as the NFS character set, append UTF-8 to the abbreviation:

   Example
   
   ko.UTF-8

Language choices

When you respond to the setup prompt for language used for multiprotocol files, you need to enter the language code abbreviation.

   Note: You can also view supported languages and their abbreviations by entering the vol lang command at the storage system prompt.

The following table lists the language choices:¹

<table>
<thead>
<tr>
<th>Language</th>
<th>Abbreviation</th>
<th>Language</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arabic</td>
<td>ar</td>
<td>Norwegian</td>
<td>no</td>
</tr>
<tr>
<td>Croatian</td>
<td>hr</td>
<td>Polish</td>
<td>pl</td>
</tr>
<tr>
<td>Czech</td>
<td>cs</td>
<td>Portuguese</td>
<td>pt</td>
</tr>
<tr>
<td>Danish</td>
<td>da</td>
<td>POSIX</td>
<td>C</td>
</tr>
<tr>
<td>Dutch</td>
<td>nl</td>
<td>Romanian</td>
<td>ro</td>
</tr>
<tr>
<td>English</td>
<td>en</td>
<td>Russian</td>
<td>ru</td>
</tr>
<tr>
<td>English (U.S.)</td>
<td>en_US</td>
<td>Simplified Chinese</td>
<td>zh</td>
</tr>
</tbody>
</table>

¹ To use UTF-8 as the NFS character set, you must append .UTF-8 to the language code.
<table>
<thead>
<tr>
<th>Language</th>
<th>Abbreviation</th>
<th>Language</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finnish</td>
<td>fi</td>
<td>Simplified Chinese (GBK)</td>
<td>zh.GBK</td>
</tr>
<tr>
<td>French</td>
<td>fr</td>
<td>Slovak</td>
<td>sk</td>
</tr>
<tr>
<td>German</td>
<td>de</td>
<td>Slovenian</td>
<td>sl</td>
</tr>
<tr>
<td>Hebrew</td>
<td>he</td>
<td>Spanish</td>
<td>es</td>
</tr>
<tr>
<td>Hungarian</td>
<td>hu</td>
<td>Swedish</td>
<td>sv</td>
</tr>
<tr>
<td>Italian</td>
<td>it</td>
<td>Traditional Chinese euc-tw</td>
<td>zh_TW</td>
</tr>
<tr>
<td>Japanese euc-j</td>
<td>ja</td>
<td>Traditional Chinese Big 5</td>
<td>zh_TW.BIG5</td>
</tr>
<tr>
<td>Japanese PCK (sjis)</td>
<td>ja_JP.PCK</td>
<td>Turkish</td>
<td>tr</td>
</tr>
<tr>
<td>Korean</td>
<td>ko</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting setup

Setup problems might be related to software configuration or hardware issues.

Troubleshooting boot failure after system power on

If your system does not boot when you power it on, you can troubleshoot the problem by following a series of steps.

Steps

1. Look for a description of the problem on the console.
   You must follow any instructions provided on the console.

2. Check all cables and connections, making sure they are secure.

3. Ensure that power is supplied and is reaching your system from the power source.

4. Ensure that the power supplies on your controller and disk shelves are working:

<table>
<thead>
<tr>
<th>If the LEDs on a power supply are...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illuminated</td>
<td>Proceed to the next step.</td>
</tr>
<tr>
<td>Not illuminated</td>
<td>Remove the power supply and reinstall it, making sure that it connects with the backplane.</td>
</tr>
</tbody>
</table>

5. Verify disk shelf compatibility with your version of Data ONTAP and ensure that the disk shelf IDs are unique.
   For more information, see the *Hardware Universe*.

6. If your system has SAS, SSD, or SATA disks in shelves, go to Step 7; otherwise, ensure that the Fibre Channel disk shelf speed is correct.

7. Check *disk ownership* on page 112 to ensure that the disks are assigned to the system.

8. Turn off your controller and disk shelves, and then turn on the controller and disk shelves.
   For information about LED responses, check the quick reference card that came with the disk shelf or the hardware guide for your disk shelf.

9. Exit Maintenance mode by entering the following command:
   `halt`
10. Enter the following command at the firmware prompt to reboot the storage system:

```
boot
```

<table>
<thead>
<tr>
<th>If your system...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boots successfully</td>
<td>Proceed to set up the software.</td>
</tr>
<tr>
<td>Does not boot successfully</td>
<td>Contact technical support. The system might not have</td>
</tr>
<tr>
<td></td>
<td>the boot image downloaded on the boot device. Also</td>
</tr>
<tr>
<td></td>
<td>verify that you have run all the system-level</td>
</tr>
<tr>
<td></td>
<td>diagnostics, the cables are securely connected, and</td>
</tr>
<tr>
<td></td>
<td>that hardware components are properly installed in</td>
</tr>
<tr>
<td></td>
<td>the storage system.</td>
</tr>
</tbody>
</table>

11. If you suspect hardware problems, see the *System-Level Diagnostics Guide* for information about running diagnostics using the `sldiag` commands, and contact technical support.

### Checking disk ownership

When you are troubleshooting boot failure, you must check disk ownership to ensure that the disks are assigned to the system.

**Steps**

1. Boot into maintenance mode and select option 5.

   If you cannot boot into the 1-5 menu, you probably have an issue with the boot image. Contact technical support.

2. Verify that disks are assigned to the system by entering `disk show`.

3. Validate that storage is attached to the system, and verify any changes that you made, by entering `disk show -v`.

### Retrying system setup

You can rerun the `setup` command, if you make an inadvertent mistake during the initial setup process or want to change the storage system configuration.

**About this task**

After the `setup` script begins to run, you cannot return to previous steps to make corrections. If you make a mistake, you must complete the setup process and reboot your system, then begin the setup process again by entering the `setup` command. When you have corrected your setup errors and are prompted to reboot your system, type `source/etc/rc` instead of `reboot` for the changes to take effect.
Steps

1. Enter the setup command and follow the prompts.

2. When you are ready to reboot the system, enter the source/etc/rc command.

   If your system boots successfully, your system is successfully set up. If your system does not boot successfully, contact technical support. The system might not have the boot image downloaded on the boot device.

Retrying CIFS setup

You can rerun the cifs setup command, if you make an inadvertent mistake during the initial CIFS setup process or want to change the CIFS configuration.

About this task

If you need to terminate the cifs setup command while it is in progress, press Ctrl-C. You can then enter the cifs restart command to restart CIFS using your old configuration information.

Steps

1. Enter the following command to stop the CIFS service:
   
   `cifs terminate`

2. Enter the cifs setup command and follow the prompts to reconfigure CIFS.

3. When you are ready to reboot the system, enter the following command:
   
   `reboot`

   If your system boots successfully, your system is successfully set up. If your system does not boot successfully, contact technical support.

   For more information about configuring CIFS, see the Data ONTAP File Access and Protocols Management Guide for 7-Mode.
Copyright information

Copyright © 1994–2014 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to
restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer
Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).
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.
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
Index

A
abbreviations
  language codes 109
ACP
  configuration requirements for SAS-attached shelves 41
Active Directory
  assigning administrator privileges 11
  authentication requirements 13
  configuration requirements 35
  DNS requirements 13
  domain administrator 35
  network infrastructure requirements 14
  preparing CIFS clients to access 86
  time service requirements 15
administration hosts
  configuration requirements 24
  Windows or UNIX requirements 10
administrative passwords
  configuration requirements 24
administrator privileges
  assigning 11
Alternate Control Path
  See ACP
array LUNs
  Data ONTAP installation stages 68
  prerequisites to Data ONTAP setup 64
  setting up storage systems for 64
  systems running Data ONTAP that can use 63
authentication
  Active Directory 13
  Windows NT4 11
AutoSupport
  configuration information 40
  setup 90
  verifying SP function for 92
B
BIND DNS
  authentication requirements 13
  blocking data traffic
    dedicated management ports 80
C
certificates
  installing SSL, on storage systems 59
  SSL requirements 59
checking disk ownership
  troubleshooting boot failure 112
CIFS
  configuration requirements 35
  creating a domain account before setting up 12
  creating DNS "A" records 86
  domain administrator 35
  mapping root directory to host 72
  preparing clients to access storage system 86
  retrying CIFS setup 113
  setting up 51
  /vol/vol0 access as C$ 81
  /vol/vol0/home access as HOME 81
cifs setup command
  setting up CIFS 35
  using to set up CIFS 51
clients
  accessing storage system 86
  exporting file systems to NFS clients 84
  obtaining software images for UNIX 70
  obtaining software images for Windows 72
codes
  language 109
command-line interface
  configuring 9
commands
  cifs setup 51
  disabling HA mode 88
  enabling non-HA mode 88
  exportfs 81
  for managing files in /etc/software directory 77
  for obtaining software images for HTTP servers 69
  license add 82
  responding to setup prompts 45
  software update 73
  sp setup 54
  sp status 92
  sp test autosupport 92
Common Internet File System
  See CIFS
Config Advisor
  checking for common configuration errors with 87
downloading and running 87  
verifying configuration 87
configuration  
additional steps for systems that use both disks and array LUNs 61  
CIFS information 35  
dedicated management ports 16  
e0M interfaces 16, 80  
HTTP information 33  
information to gather 18  
interface groups 31  
network information required 26  
NIS services information 35  
prerequisites 10  
Service Processor information 40  
storage system information 24  
storage system, default 7  
switch, requirements for interface groups 15  
time zones 100  
verifying high-availability pairs 87
configuration worksheet  
how to enter configuration values 44  
software setup 19
connections  
troubleshooting network 79  
verifying network 78

D
Data ONTAP software  
documentation 98  
installation stages on Data ONTAP systems 68  
installing on systems that use only array LUNs 68  
responding to setup command prompts 45  
setup overview 6
Data ONTAP software images  
about obtaining 68  
installing 73  
requirements for obtaining, UNIX client 70  
requirements for obtaining, Windows client 71
Data ONTAP system files  
installation overview 73  
installation procedure for HTTP 75  
installation procedure from /etc/software 74
Data ONTAP systems  
prerequisite configuration steps 7  
setting up array LUNs 65, 68
data traffic  
blocking on e0M interfaces 80  
e0M restrictions 16

E

dedicated management ports  
configuring 16  
configuring down 80
DHCP  
configuration requirements 16
DHCPv6 servers  
not supported 16
directories  
installing software images from /etc/software 74  
specifying HTTP 33  
disabling  
NFS 83  
disk assign command  
assigning LUNs to systems 65  
disk ownership  
checking 112  
disk shelves, native  
setting up storage system 44
DNS  
authentication requirements 13  
configuration requirements 34  
creating "A" records for CIFS client access 86  
verifying host-name resolution 79
documentation roadmap  
finding information 98
domain accounts  
administrator requirements 35  
authentication 11  
creating before setting up CIFS 12  
domain administrator privileges  
assigning 11
Domain Name System  
See DNS
Dynamic Host Configuration Protocol  
See DHCP

e0M interface  
configuration requirements 26  
configuring down 80  
configuring to use 16  
restrictions 16, 45  
enabling  
NFS 83
/etc/exports file  
exporting data to NFS clients 84
/etc/hosts  
verifying host name resolution 79
/etc/software directory
commands for managing files in 77
installing software images from 74
exportfs command
  verifying storage availability 81
exporting file systems
  NFS clients 84

F
files
  commands for managing in /etc/software directory 77

G
geographical time zones
  list of 100
Greenwich Mean Time (GMT)
  time zones, offset 106

H
HA mode
  disabling 88
HA pairs
  changing nodes to stand-alone 88
  verifying path failover for array LUNs in 96
  See also high-availability configurations
hardware setup
  after completing 6
  system fails to boot up 44
  troubleshooting system failure to boot up 111
high-availability configurations
  about 11
  verifying configuration 87
high-availability pairs
  configuration requirements 18
  storage system information 24
host names
  configuration requirements 24
  resolution 79
hosts, administration
  Windows or UNIX requirements 10
HTTP servers
  configuration requirements 33
  copying software image to 69
  copying software images from, without installing 69
  installing software images from 75
  obtaining software images for 69

I
images
  copying software from HTTP server without installing 69
  copying software to HTTP server 69
  installing software, from /etc/software directory 74
  installing software, from HTTP server 75
  obtaining for Windows clients 72
  obtaining software, for HTTP servers 69
  obtaining UNIX client software 70
installation
  of Data ONTAP, stages 68
installing
  Data ONTAP on system using only array LUN 68
  software images from /etc/software directory 74
  software images from HTTP server 75
  SSL certificates on storage systems 59
interface groups
  configuration requirements 15, 31
Internet protocol
  configuration requirements 26
IP addresses
  verifying 78

K
Kerberos
  authentication requirements 13
  DNS requirements 13
  time service requirements 15
key management servers
  introduction to using SSL for secure communication 58

L
languages
  configuration requirements 24
  list of codes 109
  specifying codes 109
  supported by Data ONTAP 109
license show command
  using to display license information 82
licenses
  CIFS 35
  default storage system configuration 7
  enabling or disabling NFS 83
  managing 82
  NFS 83
protocol, required 77
limitations
Storage Encryption 58
LUN ownership
assigning 65
LUNs (array)
systems running Data ONTAP that can use 63
LUNs, array
configuring for Data ONTAP systems 61
verifying path failover for, in HA pairs 96
See also LUNs (array)

M
management ports
configuration requirements 26
configuring eOM interfaces 16
managing
licenses 82

N
native disk shelves
default storage system configuration 7
setting up storage system 44
NetApp Support Site
about obtaining Data ONTAP software images from 68
network connections
configuration information required 26
infrastructure requirements 14
setup methods 9
verifying 78
verifying SP 92
Network File System
See NFS
Network Information Services
See NIS
network interfaces
troubleshooting 79
NFS
enabling or disabling 83
exporting data to 84
preparing to access storage system 83
/vol/vol0 access 81
/vol/vol0/home access 81
NIS
configuration information 35
verifying host-name resolution 79
Non-HA mode
enabling 88
NTLM
authentication requirements 13

O
obtaining software images
for UNIX clients 70
for Windows clients 72
OnCommand System Manager
preparing to use 93
See also System Manager
organizational units (OU)
assigning administrator privileges 11
configuration requirements 35

P
passwords
administrative, configuration requirements 24
path failover
verifying for array LUNs in HA pairs 96
path failover for array LUNs
overview 96
verifying in a stand-alone system 96
paths to an array LUN
validating 94, 95
ping command
using to verify network connectivity 78
prerequisites
initial configuration 10
OnCommand System Manager 93
setup 44
privileges, administrator
assigning 11
product documentation
finding information 98
protocol licenses
managing 82
required 77

R
rebooting
CIFS setup 113
system setup 112
remote access
DHCP requirements 16
remote LAN module
See RLM
requirements
Active Directory authentication 13
configuration for HA pairs 11
DHCP 16
DNS for Active Directory 13
network infrastructure 14
switch configuration for interface groups 15
time services 15
Windows domains 11

RLM
setting up 45
root directories
mapping to Windows host 72

S
SAS-attached storage shelves
configuring ACP 41
secure communication
introduction to using SSL for 58
serial console connections
setup methods 9
servers
copying from HTTP without installing 69
copying software image to HTTP 69
enabling or disabling NFS 83
installing software images from HTTP 75
obtaining software images for HTTP 69
service locator records
authentication requirements 13
Service processor
See SP
setting up
Storage Encryption 57
setup
array LUN setup, prerequisites 64
AutoSupport 90
CIFS 51
collecting storage system information 8
methods 9
overall process 6
overview 6
preparing to use OnCommand System Manager 93
prerequisites 44
retrying 112
retrying CIFS 113
software configuration worksheet 19
SP 54
storage system with native disk shelves 44
verifying 78
setup command
about 44
default storage system configuration 7
language choices 109
setting up Data ONTAP 45
setup wizards
running the Storage Encryption 60
Shelf Alternate Control Path Management
configuration information for SAS-attached shelves 41
software images
about obtaining 68
copying from HTTP server without installing 69
copying to HTTP server 69
installing 73
installing from /etc/software directory 74
installing from HTTP server 75
obtaining for HTTP servers 69
obtaining for UNIX clients 70
obtaining for Windows clients 72
requirements for obtaining, UNIX client 70
requirements for obtaining, Windows client 71
software setup
configuration worksheet 19
for storage system 44
overall process 6
overview 6
prerequisites 44
process, about 8
retrying 112
verifying 78
software update command
installing software images 73
SP
configuration information 40
setting up 45, 54
verifying SP connections 92
sp setup command
setting up SP 54
sp status command
verifying SP connections 92
sp test autosupport command
verifying SP AutoSupport 92
SSL certificates
installing on storage systems 59
requirements 59
SSL connections
introduction to using for secure key management communication 58
stand-alone operation
changing an HA pair node to 88
stand-alone systems
   verifying path failover for array LUNs 96
storage array show-config command
   verifying secondary path to an array LUN 95
Storage Encryption
   explained 57
   information to collect before configuring 42
   installing SSL certificates for 59
   introduction to using SSL for secure key management communication 58
   limitations 58
   running the setup wizard 60
   setting up 57
   SSL certificates requirements 59
storage shelves
   configuring ACP for SAS 41
storage show disk command
   verifying secondary path to an array LUN 94
storage systems
   configuration information 24
   creating a domain account 12
   creating DNS "A" records 86
   default configuration 7
   DNS services information 34
   mapping to a drive 72
   mounting on your UNIX host 70
   preparing CIFS clients to access 86
   preparing NFS clients to access 83
   setting up with native disk shelves 44
   software setup process 6
   verifying availability 81
storage systems using array LUNs
   assigning LUNs for 65
switches
   configuration requirements 15
system files
   commands for managing in /etc/software directory 77
System Manager
   not supported for setup 9
   setting up CIFS 51
system power on
   troubleshooting boot failure 111
systems
   mounting on your UNIX host 70
systems that use array LUNs
   licensing requirements for 17

T
time services
   requirements 15
time zones
   configuration requirements 24
   geographical regions 100
   GMT offset 106
   selecting values 100
troubleshooting
   boot failure after system power on 111
   network connections 79
   overview 111
   retrying CIFS setup 113
   retrying system setup 112
troubleshooting boot failure
   checking disk ownership 112
two paths to an array LUN
   verifying 94

U
UID-to-SID mapping
   high-availability configuration requirements 87
UNIX clients
   mounting the system on 70
   obtaining software images for 70
   requirements for obtaining software images 70
   requirements to manage storage system 10
utils
   checking for common configuration errors with Config Advisor 87
downloading and running Config Advisor 87

V
V-Series functionality
   name change to FlexArray Virtualization 63
V-Series systems
   See LUNs (array)
verifying
   dedicated management ports (e0M) 80
   host-name resolution 79
   licenses 82
   network connections 78
   path failover for array LUNs in HA pairs 96
   secondary path to an array LUN 94, 95
   software setup 78
   SP setup and connections 92
   storage availability and licensing 81
verifying path failover for array LUNs in stand-alone systems 96
/vol directory about 81
/vol/vol0 directory
   CIFS access as C$ 81
   NFS access 81
   verifying 81
/vol/vol0/home directory
   CIFS access as HOME 81
   NFS access 81
   verifying 81

W

Windows Active Directory domain
   assigning administrator privileges 11
Windows clients

obtaining software images for 72
requirements for obtaining software images 71
requirements to manage storage system 10
Windows domains
   assigning administrator privileges 11
   configuration requirements 35
Windows hosts
   mapping root directory to 72
Windows NT4
   authentication requirements 11, 12
WINS servers
   configuration requirements 35
wizards
   running the Storage Encryption setup 60
worksheets
   software setup configuration 19