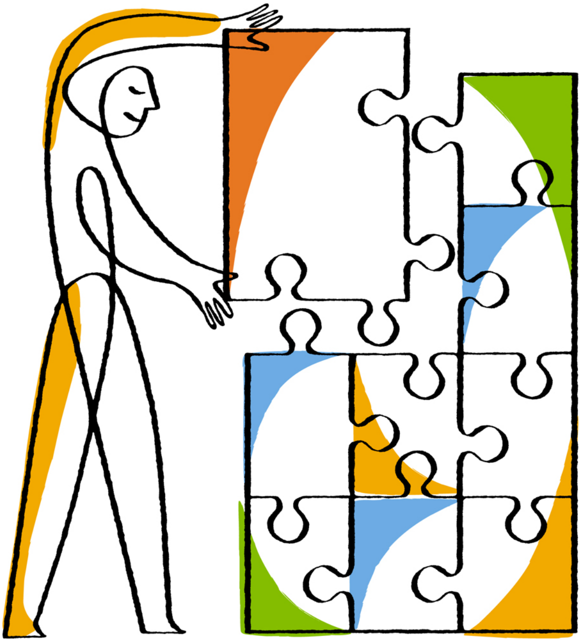
Data ONTAP® 8.2

Software Setup Guide

For 7-Mode



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) 4-NETAPP
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 210-06051_A0
April 2013

Contents

Overview of the software setup process

You can set up Data ONTAP software to use native or third-party storage systems. The software setup process consists of satisfying prerequisites, gathering configuration information, entering configuration information at setup prompts, and verifying initial configuration parameters.

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*
- You must have plugged in the monitor cable to the DB-9 connector, which is attached to the console port labeled IOIOI.
- 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 third-party storage (a V-Series system configuration), 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 the following option depending on your storage system configuration:

If you are setting up your storage system for using...	Then...
Native disk shelves	Enter the information you gathered when the `setup` command begins to run. You do not need to install the Data ONTAP software.
Only third-party storage	Perform V-Series system configuration tasks in maintenance mode, install the Data ONTAP software, and enter the information you gathered when the `setup` command begins to run.

4. Verify that basic system functionality has been configured correctly.
5. Configure system features and provision your 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

Related tasks

Setting up your system to use only third-party storage 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.

V-Series systems that use only third-party storage 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.

About 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 V-Series system ordered without native disk shelves, you must perform prerequisite configuration steps and install the software 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 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 59

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/NOW/products/interoperability

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 14

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.

  Windows 2000 and Windows Server 2003, 2008, and 2012 Active Directory requires service locator records for finding the domain controllers, global catalog servers, Kerberos servers, LDAP servers, and the KPASSWD servers.

The following additional capabilities are recommended:

- Support for dynamic updates
- Support for incremental zone transfers

The following DNS solutions meet the requirements:

- Microsoft Server 2000, 2003, 2008, and 2012 DNS

  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.

Interface group	**Switch support requirements**
Dynamic multimode	Link Aggregation Control Protocol (LACP)
Static multimode	Aggregates (but must not have control packet exchange for configuring an aggregate)
Single-mode	No special switch requirements

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*.

Requirements for creating array LUNs for V-Series systems

The storage administrator must create LUNs on the storage array and make them available to Data ONTAP before you set up your V-Series system and install Data ONTAP software on it. You provide information through the boot menu and the setup program to assign array LUN ownership.

V-Series system licensing requirements

You must install a license to operate a V-Series system. The license must be installed within 72 hours of running setup or the system shuts down.

If you ordered your V-Series system with native disks, the factory installed Data ONTAP software and licenses for you. If you ordered your system without native disks, you must install the Data ONTAP software and licenses after running the setup program.

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*.

Configuration worksheet

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

Category	Types of information	Your values
Licenses	Usually your storage system comes with the licenses preinstalled. You can use the `license show` 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 **My Support > Software Licenses**. 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 `setup` script. **Note:** After you finish setting up Data ONTAP and can access the CLI, wait at least five minutes before trying the `license show` command to see which licenses are installed. For more information, see the knowledgebase article *Data ONTAP 8.2 Licensing Overview and References* on the NetApp Support Site.	
Terminal server (sometimes used for remote serial console port access)	TCP/IP address	
	Port	

Category	**Types of information**	**Your values**
Storage system	Host name	
	Password	
	Time zone	
	Storage system location	
	Language used for multiprotocol storage systems: • NFS Classic (v2 or v3) only—Language setting does not matter • NFS Classic (v2 or v3) and CIFS—Language of the clients • Name of the interface group (such as ig0NFS v4, with or without CIFS—**`cl_lang.UTF-8`**, where **`cl_lang`** is the language of the clients.	
Administration host	Host name	
	IP address	
Interface groups (include information for each interface group)	Name of the interface group (such as ig0)	
	Mode type (single, multi, or LACP)	
	Load balancing type (IP based, MAC address based, or round-robin based)	
	Number of links (number of physical interfaces to include in the interface group)	
	Link names (physical interface names such as e0a, e5a, or e9b)	
	IP address for the interface group	
	Subnet mask (IPv4) or subnet prefix length (IPv6) for the interface group	
	Partner interface group name	
	Media type for the interface group	

Category	**Types of information**		**Your values**
Ethernet interfaces (if not using interface groups)	Interface name (include information for each interface port, such as e0a, e5a)		
	IPv4	Address	
		Subnet mask	
	IPv6 (not always used)	Address	
		Subnet prefix length	
	Partner IP address or interface		
	Media type (network type)		
	Are jumbo frames supported?		
	MTU size for jumbo frames		
	Flow control		
e0M interface (if available)	IP address		
	Network mask		
	Partner IP address		
	Flow control		
	Note: The e0M management interface either should be on a separate subnet from the controller's other data ports or configured down.		
Router (if used)	Gateway name		
	IPv4 address		
	IPv6 address		
HTTP	Location of HTTP directory		
DNS	Domain name		
	Server address 1		
	Server address 2		
	Server address 3		

Category	**Types of information**	**Your values**
NIS	Domain name	
	Server address 1	
	Server address 2	
	Server address 3	

Category	**Types of information**		**Your values**
CIFS	Windows domain		
	WINS servers	1	
		2	
		3	
	Multiprotocol or NTFS-only storage system?		
	Should CIFS create default `/etc/passwd` and `/etc/group` files?		
	NIS group caching	Enable?	
		Hours to update the cache	
	CIFS server name (if different from default)		
	User authentication style: (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 storage system's local user accounts (4) /etc/passwd and/or NIS/LDAP authentication **Note:** Joining the CIFS domain can be a long-running process. Avoid pressing Enter until the command prompt returns.		
	Windows Active Directory domain	Domain name	
		Time server names or IP addresses	
		Windows user name	
		Windows user password	
		Local administrator name	
		Local administrator password	
	CIFS administrator or group		
	Active Directory container (CLI setup only)		

Category	**Types of information**		**Your values**
SP (If not using DHCP, fill in the IP information.) Supported on these systems: FAS22xx 32xx 62xx	MAC address		
	IPv4	Address	
		Subnet mask	
		Gateway	
	IPv6 (not always used)	Address	
		Subnet prefix length	
		Gateway	
	AutoSupport mail host		
	AutoSupport recipients		
RLM (If not using DHCP, fill in the IP information.) Supported on these systems: 31xx 6040 6080	MAC address		
	IPv4	Address	
		Subnet mask	
		Gateway	
	IPv6 (not always used)	Address	
		Subnet prefix length	
		Gateway	
	AutoSupport mail host		
	AutoSupport recipients		
ACP	Network interface name		
	Domain (subnet) for network interface		
	Netmask (subnet mask) for network interface		

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:

Information type	**Description**
Host name (Hostname or Storage System Name)	The name by which the storage system is known on the network. If the storage system is licensed for the NFS protocol, the name can be no longer than 32 characters. If the storage system is licensed for the CIFS protocol, the name can be no longer than 15 characters. The host name must be unique for each storage system in an HA pair.
Password (Administrative Password)	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. The `security.passwd.rules.history` default is six passwords, and is enabled at first login. This option controls whether an administrator can reuse a password. The following are the default 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*.

Information type	**Description**
Time zone (Timezone)	The time zone in which the storage system resides. See *Time zones* on page 98 for a list of valid time zones. The time zone must be identical on both storage systems in an HA pair.
Storage system location	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, "Lab 5, Row 7, Rack B").
Language	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 *Supported languages* on page 107. The language must be identical on both storage systems in an HA pair.
Administration host	A client computer that is allowed to access the storage system through a secure protocol.

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

Network information

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:

Information type	**Description**
Network interface name	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.
Internet protocol	You are prompted to configure IPv6. If you enter **n**, further prompts are for IPv4 values only. If you enter **y** to configure IPv6, you must also supply IPv4 configuration information for network interfaces in addition to IPv6 configuration information. **Note:** Enabling IPv6 during setup does not enable file access protocols (CIFS, NFS, FTP, or HTTP) over IPv6. Enabling IPv6 during setup also enables IPv6 router advertisement. This can be disabled separately by setting the `ip.v6.ra_enable` option to `off`. For more information about using file access protocols over IPv6, see the *Data ONTAP File Access and Protocols Management Guide for 7-Mode*. For more information about IPv4 and IPv6 support, see the *Data ONTAP Network Management Guide for 7-Mode*.
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 (Network Mask, IPv4 only)	The IPv4 subnet mask for the network to which each network interface is attached. Example: 255.255.255.0
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.

Information type	**Description**
Partner IP address (Interface to Take Over)	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 When configuring interface groups, you must specify the interface group name rather than the IP address. **Note:** When using the `ifconfig` 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.
Media type (Network Type)	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: • **`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 The switch must be configured to match the media type values you select.

Information type	**Description**
Flow control	The management of the flow of frames between two directly connected link-partners. You can use the following options: • **`none`** No flow control • **`receive`** Ability to receive flow control frames • **`send`** Ability to send flow control frames • **`full`** 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
e0M interface (if available)	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 configured down. Do not use the e0M interface for data traffic, as 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. **Note:** The e0M interface cannot be included in interface group or VLAN configurations. For more information about using the e0M interface, see the *Data ONTAP System Administration Guide for 7-Mode* and the *Data ONTAP Release Notes for 7-Mode*.

For more information about these parameters, see the *Data ONTAP Network Management Guide for 7-Mode* and the `ifconfig` man page.

Interface group information

If you want to use interface groups, you should plan for them before installation and create them during the software setup process.

Interface groups were referred to as "virtual network interfaces" or "virtual interfaces (vifs)" in the Data ONTAP 7.2 and 7.3 release families.

During setup, you are first 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.

> **Note:** The interface group information must be identical on both storage systems in a high-availability pair.

You must provide the following interface group information:

Information type	**Description**
Name of interface group	You must assign a name for the interface group, for example, ig0. Interface group names are user specified. An interface group's name should meet the following criteria: • It must begin with a letter. • It must not contain any spaces. • It must not contain more than 15 characters. • It must not already be in use for an interface group.

Information type	**Description**
Interface group type	You must select one of the following values: • `single [s]` Single-mode • `multi [m]` Static multimode • `lacp [l]` Dynamic multimode **Note:** You must ensure that the value you select corresponds to your network switch configuration. For more information, see “Switch configuration requirements for interface groups.”
Load balancing type	You must select one of the following values: • `IP based [i]` • `MAC based [m]` • `Round-robin based [r]` **Note:** Load balancing is applicable only for multimode interface groups. It is best to use the IP address load-balancing method with dynamic multimode interface groups.
Number and names of links	You can record the number of physical interfaces to be included in the interface group and the name of each physical interface.
Internet Protocol information	You can record the following information: • IP address (IPv4 or IPv6) • Subnet mask (IPv4) • Subnet prefix length (IPv6) • Media type For more information, see “Network information.”
Partner interface group name	You can record the interface group name (not the IP address) belonging to the high-availability partner that this interface should take over.

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
Network information 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	Description
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:

Information type	**Description**
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:

Information type	**Description**
NIS domain	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.
NIS servers	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. **Note:** If you are enabling IPv6, you can enter IPv6 NIS server addresses here.

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:

Information type	Description
Windows domain	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. **Note:** 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.
WINS servers	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. **Note:** 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.
Multiprotocol or NTFS-only	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).
CIFS server name	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.

Information type	Description
User authentication for CIFS services	Data ONTAP CIFS services support four styles of user authentication: **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.
Active Directory domain name	You must enter the fully qualified domain name of the domain; for example, example.com.

Information type	Description
Active Directory time services	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. **Note:** In Data ONTAP 8.0 and later, time service configuration is recommended to enable a storage system in Active Directory-based domains. The time services configuration should be identical on both storage systems in a high-availability configuration. 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.
Windows domain administrator user name (Windows user name)	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.
Windows domain administrator password (Windows 2000 administrator password)	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: • 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*.
CIFS administrator	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.

<table>
<tr><th>Information type</th><th>Description</th></tr>
<tr><td>Active Directory container</td><td>
<p>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 "join" step.</p>
<p>Example:</p>
<p><code>CIFS - Logged in as administrator@EXAMPLE.COM.</code></p>
<p><code>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.</code></p>
<pre>
(1) CN=computers
(2) OU=java_users
(3) OU=Engineer,OU=java_users
(4) OU=Market,OU=java_users
(5) OU=Filers
(6) OU=Domain Controllers
(7) None of the above
</pre>
<p>Choose 7:</p>
<pre>
Selection (1-7)? [1]: 7
The user you specified,
'Administrator@EXAMPLE.COM', 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.

Enter the name of the Windows user []:'
</pre>
</td></tr>
</table>

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

Related tasks

Responding to cifs setup command prompts on page 51

Remote LAN Module information

If your storage system has a Remote LAN Module (RLM), you must provide information about the RLM's network interface and network connections. The RLM provides remote platform management capabilities, including remote access, monitoring, troubleshooting, logging, and alerting features.

If you are running RLM firmware version 4.0 or later, and you have enabled IPv6 for Data ONTAP, you have the option to configure the RLM for only IPv4, for only IPv6, or for both IPv4 and IPv6.

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

You must provide the following RLM information:

Information type	**Description**
Media Access Control (MAC) address	If you are using DHCP addressing, you can record the MAC address of the RLM. You can obtain the address from the MAC address label on the RLM or by using the `sysconfig -v` command (if you configure the RLM after initial system setup). **Note:** You do not need to record IP and gateway addresses if you are using DHCP addressing for the RLM. DHCPv6 servers are not currently supported.
IP address	You can record an available IP address for the RLM. **Note:** You can enter an IPv4 address, an IPv6 address, or both depending on how you configured your storage system.
Network mask	You must record the IPv4 network mask of your network.
Subnet prefix length	You must record the number of bits used as the subnet mask for the specified IPv6 interface.
Gateway	You must record the IP address for the gateway of your network. **Note:** You can enter an IPv4 address, an IPv6 address, or both depending on how you configured your RLM.

Information type	**Description**
Mail host	You must record the name or IP address of the preferred mail host. The mail host delivers RLM alerts to the same destination as AutoSupport email.

For more information about configuring your RLM, see the *Data ONTAP System Administration Guide for 7-Mode*.

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:

Information type	**Description**
IP address	Specifies an available IP address for the SP. If you are using IPv6 for static addressing, you need the IPv6 global address.
Network mask	Specifies the network mask of your network.
Subnet prefix length	Specifies the number of bits used as the subnet mask for the specified IPv6 interface.
Gateway	Specifies the IP address for the gateway of your network. **Note:** If you are using IPv6 for static addressing, you must use the IPv6 gateway.
Mail host	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.

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 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.

> **Note:** ACP connections must be cabled before you enter ACP configuration parameters on the storage system.

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

- 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:

Information type	**Description**
Network interface name	The name of the Ethernet (or GbE) interface that is used exclusively for ACP traffic.
Domain (subnet) for network interface	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.
Netmask for network interface	The subnet mask for the ACP interface. The default is 255.255.252.0.

For more information about ACP configuration, see the *Universal SAS and ACP Cabling Guide*.

Information to collect before configuring Storage Encryption

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

Information to collect	**Details**	**Required**	**Optional**
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	
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	

Information to collect	Details	Required	Optional
Key tag name	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.		x

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 110

Troubleshooting if the system does not boot when powered on on page 109

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:
  - Storage system components and external switches must be 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.
  - 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.
- 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. For more information about licenses, see the *Data ONTAP System Administration Guide for 7-Mode* and the knowledgebase article *Data ONTAP 8.2 Licensing Overview and References* on the NetApp Support Site.

About this task

You should supply an appropriate response from the configuration worksheet.

If the network has not been configured, Data ONTAP does 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. Choose the following option that describes your configuration:

If you are...	Then...
Using a DHCP server to assign IP addresses to your storage system	Allow the DHCP search to finish.
Not using a DHCP server to assign IP addresses to your storage system	Press Ctrl-C to skip the DHCP search, then go to the next step.

2. Type **y** or press Enter at the following prompt:

```
The setup command will rewrite the /etc/rc, /etc/exports,
/etc/hosts, /etc/hosts.equiv, /etc/dgateways, /etc/nsswitch.conf,
and /etc/resolv.conf files, saving the original contents of
these files in .bak files (e.g. /etc/exports.bak).
```

```
Are you sure you want to continue? [yes]
```

Information about your storage controller and adapters is displayed.

3. Enter the new hostname at the prompt:
   `Please enter the new hostname`

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

4. Type either **`y`** or **`n`** at the following prompt:
   `Do you want to enable IPv6?`

If you type...	Then you are prompted to enter...
`y`	IPv6 configuration information in later steps.
`n`	IPv4 configuration information in later steps.

> **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.

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

If you type...	Then you are...
`y`	Prompted to enter additional configuration information for each of the interface groups. These prompts are: • `Number of interface groups to configure?` • `Name of interface group`. • `Is` *`interface_group_name`* `a single [s], multi [m] or a lacp [l] interface group?` • `Is` *`interface_group_name`* `to use IP=based [i], MAC-based [m], Round-robin based [r], or Port based [p] load balancing?` • `Number of links for` *`interface_group_name`* • `Name of link for` *`interface_group_name`* If you have additional links, you should also enter their names here. • `IP address for` *`interface_group_name`* • `Netmask for` *`interface_group_name`* • `Should interface group` *`interface_group_name`* `take over a partner interface group during failover?` • `Media type for` *`interface_group_name`*
`n`	Directed to the next prompt.

6. Enter the IP address for the network interface *`interface_group_name`* at the prompt:
   `Please enter the IP address for Network Interface`

You must enter the correct IP address for the network interface that connects the storage system to your network (for example, 192.168.1.1).

7. Enter the netmask for the network interface `interface_group_name` at the prompt:
   ```
   Please enter the netmask for Network Interface
   ```
   After entering the IP address, you need to enter the netmask for your network (for example, 255.255.255.0):

If you are configuring...	Then go to...
IPv6	The next step
IPv4	Step 10

8. Enter the IPv6 address for the network interface `interface_group_name` at the prompt:
   ```
   Please enter the IPv6 address for Network Interface
   ```
   Enter the correct IPv6 address for the network interface that connects the storage system to your network (for example, 2001:0DB8:85A3:0:0:8A2E:0370:99). You see this prompt only if IPv6 is enabled.

9. 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. You see this prompt only if IPv6 is enabled.

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

If you type...	Then you are...
y	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 interface_group_name` **Note:** Both nodes of the HA pair should have identical licenses installed.
n	Directed to the next prompt.

11. 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]
    ```
12. Enter the flow control option that this interface should use:
    ```
    Please enter flow control for e0a {none, receive, send, full} [full]
    ```
13. Specify whether you want this interface to support jumbo frames:
    ```
    Do you want interface_group_name to support jumbo frames?
    ```
14. Continue to enter network parameter values for each network interface when prompted.

15. 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:

    ```
    e0M is a Data ONTAP dedicated management port.

    NOTE: Dedicated management ports cannot be used for data protocols
    (NFS, CIFS, iSCSI, NDMP or Snap*), and if they are configured they
    should be on an isolated management LAN.
    The default route will use dedicated mgmt ports only as the last
    resort, since data protocol traffic will be blocked by default.

    Please enter the IP address for Network Interface e0M.
    Please enter the netmask for Network Interface e0M.
    Should interface e0M take over a partner IP address during failover?
    Please enter the IPv4 address or interface name to be taken over by
    e0M.
    ```

16. 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.`

17. 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.`

    You see this prompt only if IPv6 is enabled.

18. 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.

19. 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 98 for a list of supported values. For example, enter **`US/Pacific`** to use the Pacific time zone. Time zone values are case sensitive.

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

21. Enter the language used for multiprotocol files at the prompt:
    `What language will be used for multi-protocol files {type ? for list}?`

See *Supported languages* on page 107 for a list of supported values and *Specifying the language code* on page 107 for how to enter the language code. Language codes are case sensitive. For example, the language code for US English is **`en_US`**.

22. 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.

23. 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?`

24. 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.

25. 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.`

26. 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.`

27. 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.`

28. 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*.

29. When setup is complete, to transfer the information you have entered to the storage system, enter the following command, as directed by the prompt on the screen:
`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.

30. 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.

After you finish

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 tasks

Verifying network connectivity on page 78
Retrying system setup on page 110

Responding to cifs setup command prompts

If you have a valid CIFS license installed, the `cifs setup` command starts running automatically after the `setup` command is complete. Otherwise, you can use the `license add` command to install the CIFS license.

About this task

Each step displays the `cifs setup` command prompt. You should supply an appropriate response from the configuration worksheet.

> **Note:** You can use the CIFS Setup wizard in OnCommand System Manager to set up CIFS instead of using the `cifs setup` command. If you want to include your system in an organizational unit (OU) other than the default "Computers", you must use the `cifs setup` command.

During CIFS setup, you are prompted for the root password. When you enter the current password, it is not accepted. If you want to continue using the same password, you can enter Ctrl-C to stop the setup script and set the password history to `0`. If you want to use a different root password, you can change the password at the prompt. If you modify the password history to `0` to use the existing password, you need to reset it to the old value after completing CIFS setup.

Steps

1. If you want to configure Windows Internet Naming Service (WINS), enter **y** at the following prompt:
   `Do you want to make the system visible via WINS?`

   WINS translates between IP addresses and symbolic names for network nodes and resources.

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

   ```
   You can enter up to 4 IPv4 WINS addresses.
   IPv4 address(es) of your WINS name server(s):
   Would you like to specify additional WINS name servers [n]?
   ```

2. Specify whether you want to configure the storage system for multiple protocols or for NTFS only:

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

If...	Then...
You are using NTFS only for your storage system.	Enter **1** at the prompt.
You have purchased multiprotocol licenses for your storage system.	Enter **2** at the prompt.

You can find license keys for your initial or add-on software orders at the NetApp Support Site under **My Support** > **Software Licenses**. For more information about installing software licenses, see the *Data ONTAP System Administration Guide for 7-Mode* and the knowledgebase article *Data ONTAP 8.2 Licensing Overview and References* on the NetApp Support Site.

3. Enter the root password when you see the following prompt:

```
CIFS requires local /etc/passwd and /etc/group files and default
files
will be created. The default passwd file contains entries for 'root',
'pcuser', and 'nobody'.
Enter the password for the root user []:
Retype the password []:
```

If you have not changed the password history settings before beginning CIFS setup, you must enter a new root password to continue with the setup.

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

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

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

If you select...	Then...
1	Go to the next step.
2, **3**, or **4**	Go to Step 10, then see *CIFS protocol information* on page 34 and the *Data ONTAP File Access and Protocols Management Guide for 7-Mode* for more information about CIFS setup for these authentication options.

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
```

6. 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.

7. 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?
   ```

8. 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.

9. 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.
   ```

   Important: 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*.

10. 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.
```

After you finish

If you have modified the password history settings, change the password history option back to the default value or to a value that was previously set by the administrator:

`options security.passwd.rules.history 6`

Related concepts

Preparing CIFS clients to access the storage system on page 86

Related tasks

Retrying CIFS setup on page 111

Preparing to use OnCommand System Manager on page 92

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.

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.

Steps

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

If...	Then...
You have not run the `setup` command yet.	Enter the **`setup`** command. The `sp setup` command starts automatically after the `setup` command finishes running.
You already have run the `setup` command.	Enter the **`sp setup`** command.

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:

If you want to use...	Then...
Static addressing	Enter **`n`**. **Note:** Because **`y`** is the default value, you must enter **`n`** if you are using static addressing on the SP.
DHCP addressing	Enter **`y`**. **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.
   - The netmask for the SP
   - The IP address for the SP gateway
   - The name or IP address of the mail host to use for AutoSupport (if you use the `setup` command)
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:

If you want to...	Then...
Configure IPv6 connections for the SP	Enter **y**.
Disable IPv6 connections for the SP	Enter **n**.

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*.

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 use
   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
   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 use
   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 87

Verifying SP connections on page 89

Responding to rlm setup command prompts

If your system includes an RLM, the `rlm setup` command starts automatically after the `setup` command (or the `cifs setup` command if CIFS is licensed on your system) completes running. You can configure the RLM to use either a static or DHCP address.

About this task

For each step, you should supply an appropriate response from the configuration worksheet.

It is best to configure AutoSupport before configuring the RLM. Data ONTAP automatically sends AutoSupport configuration to the RLM, allowing the RLM to send alerts and notifications through an AutoSupport message.

Note: If you are running RLM firmware version 4.0 or later, and you have enabled IPv6 for Data ONTAP, you have the option to configure the RLM for only IPv4, for only IPv6, or for both IPv4 and IPv6. Disabling IPv6 on Data ONTAP also disables IPv6 on the RLM. If you disable both IPv4 and IPv6, and if DHCP is not configured, the RLM has no network connectivity.

Steps

1. When the RLM setup asks you whether to configure the RLM, enter **y**.

   If you answer **n** here, you can configure the RLM at a later time.

2. Perform one of the following steps when the RLM setup asks you whether to enable DHCP on the RLM:

If you want to enable...	Then...
DHCP addressing	Enter **y**.
Static addressing	Enter **n**.

3. If you have not enabled DHCP for the RLM, provide the following information when prompted for static IP information:

    - The IP address for the RLM

        Note: Entering **`0.0.0.0`** for the static IP address disables IPv4 for the RLM.

    - The netmask for the RLM
    - The IP address for the RLM gateway
    - The name or IP address of the mail host to use for AutoSupport (if you use the `setup` command)

4. If you enabled IPv6 for Data ONTAP and your RLM firmware version is 4.0 or later, the RLM supports IPv6, and the RLM setup asks you whether to configure IPv6 connections for the RLM:

    - To configure IPv6 connections for the RLM, enter **`y`**.
    - To disable IPv6 connections for the RLM, enter **`n`**

    Note: You can use the `rlm status` command to find the RLM version information. If you need to update the RLM version, use the `rlm update` command. For more information about the RLM firmware version, see the RLM firmware download page on the NetApp Support Site.

5. Enter the following IPv6 information at the RLM setup prompt:

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

    Note: You cannot use the RLM setup to enable or disable the IPv6 router-advertised address for the RLM. 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 RLM.

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*.

Example

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

```
      The Remote LAN Module (RLM) 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 RLM LAN interface.
Would you like to configure the RLM? y
Would you like to enable DHCP on the RLM LAN interface? n
Please enter the IP address for the RLM []:192.168.123.98
Please enter the netmask for the RLM []:255.255.255.0
Please enter the IP address for the RLM gateway []:192.168.123.1
```

```
Do you want to enable IPv6 on the RLM ? y
Do you want to assign IPv6 global address? y
Please enter the IPv6 address for the RLM []:fd22:8b1e:b255:204::1234
Please enter the subnet prefix for the RLM []: 64
Please enter the IPv6 Gateway for the RLM []:fd22:81be:b255:204::1
Verifying mailhost settings for RLM use...
```

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

```

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

Related tasks

Setting up AutoSupport on page 87
Verifying RLM connections on page 90

Related information

NetApp Support Site: support.netapp.com

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 Pools.
- 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/NOW/products/interoperability

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:

Certificate for...	**Certificate type**	**Certificate file name**
Storage system	Public	`client.pem`
Storage system	Private	`client_private.pem`
Key management server	Public	*`key_management_server_ipaddress`*`_CA.pem` *`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.

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 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:

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

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

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

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

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

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

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

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

Key ID:
080CDCB20000000001000000000000003FE505B0C5E3E76061EE48E02A29822C

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 required to set up V-Series systems using native disk shelves and third-party storage

For V-Series systems using both native disk shelves and third-party storage, you have completed the configuration of the native disk shelves, but you must now configure your third-party storage.

The information that you need to connect third-party storage to Data ONTAP is given in the *V-Series Installation Requirements and Reference Guide* and the *Data ONTAP Storage Management Guide for 7-Mode*.

Setting up your system to use only third-party storage

V-Series systems ordered without native disk shelves require some initial setup before Data ONTAP is installed and the system becomes operational.

Steps

1. *Prerequisites to starting setup when using only third-party storage* on page 64
2. *Providing array LUN ownership and system ID for V-Series systems* on page 65

Prerequisites to starting setup when using only third-party storage

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

Tasks that must be completed before Data ONTAP can use the storage on a third-party storage array are as follows:

- The storage array administrator must create LUNs and make them available to Data ONTAP. See the following documents for more information:
  - *V-Series Installation Requirements and Reference Guide*
  - *V-Series 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 prevents a V-Series system from accessing array LUNs for a non V-Series host and the reverse.

  > **Attention:** Although Data ONTAP provides controls to prevent one V-Series system from owning an array LUN that is assigned to another V-Series system, there are no controls to prevent you from assigning V-Series ownership of an array LUN owned by a non V-Series host. Using the `disk assign` command to write ownership information to a LUN owned by a non V-Series system causes irreversible data corruption.
- You must connect your V-Series system to the storage array. See the *V-Series Installation Requirements and Reference Guide* for instructions.
- Complete the Configuration worksheet.

The worksheet includes a definition of each parameter that you need to enter to set up the system on the network.

Related tasks

Providing array LUN ownership and system ID for V-Series systems on page 65

Providing array LUN ownership and system ID for V-Series systems

If your system is using only third-party storage, 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:

   ```
   disk show -v
   ```

   You see a list of all LUNs available on the storage array port to which the V-Series 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):

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

   > **Attention:** This step causes irreversible data corruption when performed on an array LUN that is being used by or that will be used by a non V-Series host.

   - `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 V-Series 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 pool1:

  ```
  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 V-Series systems using third party storage, 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 to starting setup when using only third-party storage on page 64

Related tasks

Responding to setup command prompts on page 45

Installing Data ONTAP software on a V-Series system that uses third-party storage

When setting up a new V-Series system that uses only third-party storage, 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 V-Series system with native disk shelves, the factory installs Data ONTAP for you.

Data ONTAP installation stages

You need to install Data ONTAP only on V-Series systems that were ordered without native disk shelves.

Installing Data ONTAP on a V-Series system 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

System Firmware + Diagnostics Download: support.netapp.com/NOW/cgi-bin/fw

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, `820_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/x86-64/820_q_image.tgz
   811_mailboxes_q.tgz
   ```

You see a message similar to the following:

```
software: copying to /etc/software/820_mailboxes_q.tgz
software: 100% file read from location.
software: /etc/software/820_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:

If you are connecting to the NetApp Support Site from...	Then...
An upgrade host	Save the image to the `.../etc/software` directory on the mountpoint that you chose when you mounted the storage system on your client.
Another UNIX 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 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

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:

If you are connecting to the NetApp Support Site from...	Then do this...
An upgrade host	Save the image to the `\etc\software` directory on the mountpoint that you chose previously, when you mounted the storage system on your client.

If you are connecting to the NetApp Support Site from...	Then do this...
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:

If you want to...	**Then you can enter...**
Install the new system files from the `/etc/software` directory	**`software update my_new_setup_i.tgz -d`**
Download the new system files to the boot device immediately after installing them	**`software update my_new_setup_i.tgz`**
Perform an upgrade on a single system and reboot immediately	**`software update -R my_new_setup_i.tgz`**

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.
```

```
Mon Oct 2 13:26:17 PDT [filer: rc:info]: 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.

   #### Example

   You can use the following commands to copy and install the Data ONTAP software image:

If you want to...	Then you can enter...
Copy and install the image from your HTTP server	**`software update http://www.example.com/downloads/x86-64/my_new_setup_i.tgz -d -f`**

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

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.
Mon Oct 2 13:26:17 PDT [filer: rc:info]: 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.

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:

If you want to...	Then use the following command...
List the contents of the `/etc/software` directory	`software list`
Delete files from the `/etc/software` directory	`software delete`

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

Required licenses for setting up a V-Series system

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

For a V-Series system to use array LUNs, the license must be installed within 72 hours of running setup or the system shuts down. 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 as you are installing the license for using array LUNs or later. Protocol license requirements are as follows:

For installation from a...	This protocol license is required...
Windows client	CIFS
UNIX client	NFS

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: Beginning with Data ONTAP 7.3.3, 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:
	`192.16.3.145 mysystem-e0a`
	`192.16.3.146 mysystem-e0b`
	`192.16.3.147 mysystem-f0`
	`192.16.3.148 mysystem-a5`

`/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:

If you want to...	Enter this command at the storage system prompt...
View existing licenses	**`license show`** 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...
Add one or more licenses	**`license add`** ***`license_key1 license_key2`*** Result: The new license key is enabled and added for specific Data ONTAP features or packages. Troubleshooting: The `license add: invalid license key "`*`key`*`" reason: "License serial-number does not belong to this node., skipping"` 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 > Software Licenses**. If you continue to have problems, contact technical support.
Remove a license	**`license delete`** ***`license_name`*** Result: The license of a package is deleted from the storage system.

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`***

If NFS is...	Enter the following command...
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:

If the NFS server is...	Enter the following command...
Not running and you want to enable it	**`nfs on`**
Running and you want to disable it	**`nfs off`**

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:

```
Volume          Tree      Style    Oplocks    Status
------          ----      -----    -------    -------
vol0            home      unix     enabled    normal
vol1snap        qtree1    unix     enabled    normal
vol2eng         team1     mixed    enabled    normal
vol2mkt         nt        ntfs     enabled    normal
```

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`.

Verifying the configuration for HA pairs

There are two ways you can check your high-availability configuration before placing the pair online: running the HA Configuration Checker (formerly the Cluster Configuration Checker) or using the command-line interface.

When you configure HA pair pairs, 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*.

Related information

HA Configuration Checker: support.netapp.com/NOW/download/tools/cf_config_check

Setting up AutoSupport

You can control whether and how AutoSupport information is sent to NetApp 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 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 NetApp 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:

Set this option	To this
`autosupport.to`	Up to five comma-separated individual email addresses or distribution lists in your internal support organization that will receive key AutoSupport messages
`autosupport.noteto`	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
`autosupport.partner.to`	Up to five comma-separated individual email addresses or distribution lists in your support partner organization that will receive all AutoSupport messages

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:

If you want to do this...	Set the following options...
Hide private data by removing, masking, or encoding sensitive data in the messages	Set `autosupport.content` to `minimal`. **Note:** If you change from `complete` to `minimal`, all AutoSupport history and all associated files are deleted.
Stop sending performance data in periodic AutoSupport messages	Set `autosupport.performance_data.enable` to `disable`.

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 address that technical support has on file for the system owner, who should have received an automated response from the NetApp mail handler.
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
```

Verifying RLM connections

You can use this procedure to verify that the Remote LAN Module (RLM) is set up correctly and connected to the network.

Before you begin

You must have configured AutoSupport before configuring the RLM. Data ONTAP automatically sends the AutoSupport configuration to the RLM, allowing the RLM 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

The RLM network interface is not used for serving data, so it does not show up in the output for the `ifconfig` command.

For more information about AutoSupport and about using the RLM to manage remote storage systems, see your *Data ONTAP System Administration Guide for 7-Mode*.

Steps

1. To verify that AutoSupport is enabled and AutoSupport options are valid, enter the following command:

   `options autosupport`

   The AutoSupport options should be set as follows:

   ```
   autosupport.enable on
   autosupport.support.enable on
   autosupport.mailhost name or IP address of mailhost
   autosupport.to name or email address of alert recipients
   ```

2. Enter the following command to verify the configuration of the RLM interface:

   `rlm status`

   Note: It might take a few minutes for the new RLM network settings to take effect.

3. Enter the following command to verify that the RLM AutoSupport function is working properly:

   `rlm test autosupport`

   Note: The RLM uses the same mail host information that Data ONTAP uses for AutoSupport. You must ensure that the `autosupport.to` option is set properly before issuing this command.

   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.
   ```

   The RLM should send an email within a few minutes. If the test fails, you should verify storage system connectivity and check whether the mail host and recipients are valid.

Example for displaying configuration information

The following example displays the RLM status and configuration information:

```
storage-system> rlm status
    Remote LAN Module    Status: Online
        Part Number:        110-00030
        Revision:           A0
        Serial Number:      123456
        Firmware Version:   4.0
        Mgmt MAC Address:   00:A0:98:01:7D:5B
        Ethernet Link:      up, 100Mb, full duplex, auto-neg complete
        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 fails, Data ONTAP automatically maps each storage system port to a secondary path. You want to ensure that there are two paths to each array LUN so that the V-Series 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 V-Series 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 LUNs:

   `storage show disk -p` ***`all`***

   The system displays information similar to the following:

   ```
   PRIMARY     PORT             SECONDARY  PORT           SHELF BAY
   ADAPTER
   -------------------- ---- ------------------------- ---- ---
   vnmc4500s32:4.127L1    -    vnmc4500s33:19.127L1   -     -    -   0a
   vnmc4500s32:4.127L12   -    vnmc4500s33:19.127L12  -     -    -   0a
   vnmc4500s33:19.127L2   -    vnmc4500s32:4.127L2    -     -    -   0c
   vnmc4500s33:19.127L13  -    vnmc4500s32:4.127L13   -     -    -   0c
   ```

   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 zoning, host group configuration, and cabling.

   Note: Do not continue with testing until you see two paths.

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 V-Series 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 LUNs:

   `storage array show-config`

   You see information similar to the following.

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

   This example shows output from a V-Series system connected to two storage arrays. Each LUN group is comprised 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.

   ```
   LUN Group Array Name Array Target Ports    Switch Port  Initiator
           (4 LUNS) HP_V210 50:00:1f:e1:50:0a:86:6d  vnmc4300s35:11 0b
   ```

Verifying path failover for array LUNs

You want to demonstrate that the V-Series system continues to work when running with a single path, for example, when a switch or 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 V-Series 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 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. You can also order printed copies from this web site. See the *Release Notes* for new features, enhancements, and known issues for Data ONTAP 8.1.1.

For information about...	**Go to the NetApp Support Site for the...**
New features, enhancements, known issues, and late-breaking news for your version of Data ONTAP software	*Data ONTAP Release Notes for 7-Mode* for your version of Data ONTAP.
Setting up and verifying software configuration	*Data ONTAP Software Setup Guide for 7-Mode*
Upgrading, downgrading, or reverting the Data ONTAP release	*Data ONTAP Upgrade and Revert/Downgrade Guide for 7-Mode*
Managing all aspects of your system	Documentation for your version of Data ONTAP. See the *Data ONTAP Documentation Map for 7-Mode* for an overview.
Cabling, configuring, and disk ownership	*Data ONTAP High Availability and MetroCluster Configuration Guide for 7-Mode* *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* *V-Series Installation Requirements and Reference Guide*
Setting up and managing network configurations of storage systems	*Data ONTAP Network Management Guide for 7-Mode*
Configuring and managing the FC protocol, 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
Hardware configuration options available for your system	*Hardware Universe*

For information about...	Go to the NetApp Support Site for the...
Troubleshooting your system	*Hardware Platform Monitoring Guide*
Testing field-replaceable units and diagnosing and correcting system hardware problems	*Diagnostics Guide* or *System-Level Diagnostics Guide* depending on your storage system
Configuring Remote Management after initial setup	*Data ONTAP System Administration Guide for 7-Mode*
Managing your disk shelves	*Installation and Service Guide* for your disk shelf model
Managing Storage Encryption	*Data ONTAP Storage Management Guide for 7-Mode*
Monitoring and managing Data ONTAP using OnCommand System Manager	*OnCommand System Manager Help for Use With Data ONTAP 7-Mode*

Related information

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

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:

Alias	**Standard reference**
Jamaica	US/Eastern
Navajo	US/Mountain
UCT	GMT
UTC	
Universal	
Zulu	

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

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

America

America/Adak	America/Grenada	America/Noronha
America/Anchorage	America/Guadeloupe	America/Panama
America/Anguilla	America/Guatemala	America/Pangnirtung
America/Antigua	America/Guayaquil	America/Paramaribo
America/Aruba	America/Guyana	America/Phoenix
America/Asuncion	America/Halifax	America/Port_of_Spain
America/Atka	America/Havana	America/Port-au-Prince
America/Barbados	America/Indiana	America/Porto_Acre
America/Belize	America/Indianapolis	America/Puerto_Rico

America/Bogota	America/Inuvik	America/Rainy_River
America/Boise	America/Iqaluit	America/Rankin_Inlet
America/Buenos_Aires	America/Jamaica	America/Regina
America/Caracas	America/Jujuy	America/Rosario
America/Catamarca	America/Juneau	America/Santiago
America/Cayenne	America/Knox_IN	America/Santo_Domingo
America/Cayman	America/La_Paz	America/Sao_Paulo
America/Chicago	America/Lima	America/Scoresbysund
America/Cordoba	America/Los_Angeles	America/Shiprock
America/Costa_Rica	America/Louisville	America/St_Johns
America/Cuiaba	America/Maceio	America/St_Kitts
America/Curacao	America/Managua	America/St_Lucia
America/Dawson	America/Manaus	America/St_Thomas
America/Dawson_Creek	America/Martinique	America/St_Vincent
America/Denver	America/Mazatlan	America/Swift_Current
America/Detroit	America/Mendoza	America/Tegucigalpa
America/Dominica	America/Menominee	America/Thule
America/Edmonton	America/Mexico_City	America/Thunder_Bay
America/El_Salvador	America/Miquelon	America/Tijuana
America/Ensenada	America/Montevideo	America/Tortola
America/Fort_Wayne	America/Montreal	America/Vancouver
America/Fortaleza	America/Montserrat	America/Virgin
America/Glace_Bay	America/Nassau	America/Whitehorse
America/Godthab	America/New_York	America/Winnipeg
America/Goose_Bay	America/Nipigon	America/Yakutat
America/Grand_Turk	America/Nome	America/Yellowknife

Antarctica

Antarctica/Casey	Antarctica/Mawson	Antarctica/Palmer

Antarctica/DumontDUrville
Antarctica/McMurdo
Antarctica/South_Pole

Asia

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

Atlantic

Atlantic/Azores	Atlantic/Faeroe	Atlantic/South_Georgia
Atlantic/Bermuda	Atlantic/Jan_Mayen	Atlantic/St_Helena
Atlantic/Canary	Atlantic/Madeira	Atlantic/Stanley
Atlantic/Cape_Verde	Atlantic/Reykjavik	

Australia

Australia/ACT	Australia/LHI	Australia/Queensland
Australia/Adelaide	Australia/Lindeman	Australia/South
Australia/Brisbane	Australia/Lord Howe	Australia/Sydney
Australia/Broken_Hill	Australia/Melbourne	Australia/Tasmania
Australia/Canberra	Australia/NSW	Australia/Victoria
Australia/Darwin	Australia/North	Australia/West
Australia/Hobart	Australia/Perth	Australia/Yancowinna

Brazil

Brazil/Acre	Brazil/East
Brazil/DeNoronha	Brazil/West

Canada

Canada/Atlantic	Canada/Eastern	Canada/Pacific
Canada/Central	Canada/Mountain	Canada/Saskatchewan
Canada/East- Saskatchewan	Canada/Newfoundland	Canada/Yukon

Chile

Chile/Continental	Chile/EasterIsland

Europe

Europe/Amsterdam	Europe/Kiev	Europe/San_Marino
Europe/Andorra	Europe/Kuybyshev	Europe/Sarajevo

Europe/Athens	Europe/Lisbon	Europe/Simferopol
Europe/Belfast	Europe/Ljubljana	Europe/Skopje
Europe/Belgrade	Europe/London (BST)	Europe/Sofia
Europe/Berlin	Europe/Luxembourg	Europe/Stockholm
Europe/Bratislava	Europe/Madrid	Europe/Tallinn
Europe/Brussels	Europe/Malta	Europe/Tirane
Europe/Bucharest	Europe/Minsk	Europe/Vaduz
Europe/Budapest	Europe/Monaco	Europe/Vatican
Europe/Chisinau	Europe/Moscow	Europe/Vienna
Europe/Copenhagen	Europe/Oslo	Europe/Vilnius
Europe/Dublin	Europe/Paris	Europe/Warsaw
Europe/Gibraltar	Europe/Prague	Europe/Zagreb
Europe/Helsinki	Europe/Riga	Europe/Zurich
Europe/Istanbul	Europe/Rome	

Indian (Indian Ocean)

Indian/Antananarivo	Indian/Comoro	Indian/Mauritius
Indian/Chagos	Indian/Kerguelen	Indian/Mayotte
Indian/Christmas	Indian/Mahe	Indian/Reunion
Indian/Cocos	Indian/Maldives	

Mexico

Mexico/BajaNorte	Mexico/BajaSur	Mexico/General

Pacific

Pacific/Apia	Pacific/Johnston	Pacific/Ponape
Pacific/Auckland	Pacific/Kiritimati	Pacific/Port_Moresby
Pacific/Chatham	Pacific/Kosrae	Pacific/Rarotonga
Pacific/Easter	Pacific/Kwajalein	Pacific/Saipan

Pacific/Efate	Pacific/Majuro	Pacific/Samoa
Pacific/Enderbury	Pacific/Marquesas	Pacific/Tahiti
Pacific/Fakaofo	Pacific/Midway	Pacific/Tarawa
Pacific/Fiji	Pacific/Nauru	Pacific/Tongatapu
Pacific/Funafuti	Pacific/Niue	Pacific/Truk
Pacific/Galapagos	Pacific/Norfolk	Pacific/Wake
Pacific/Gambier	Pacific/Noumea	Pacific/Wallis
Pacific/Guadalcanal	Pacific/Pago_Pago	Pacific/Yap
Pacific/Guam	Pacific/Palau	
Pacific/Honolulu	Pacific/Pitcairn	

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

GMT	GMT+9	GMT-5
GMT+1	GMT+10	GMT-6
GMT+2	GMT+11	GMT-7
GMT+3	GMT+12	GMT-8
GMT+4	GMT+13	GMT-9
GMT+5	GMT-1	GMT-10
GMT+6	GMT-2	GMT-11
GMT+7	GMT-3	GMT-12
GMT+8	GMT-4	

Etc

Etc/GMT	Etc/GMT+11	Etc/GMT-9
Etc/GMT+0	Etc/GMT+12	Etc/GMT-10
Etc/GMT+1	Etc/GMT0	Etc/GMT-11
Etc/GMT+2	Etc/GMT-0	Etc/GMT-12
Etc/GMT+3	Etc/GMT-1	Etc/GMT-13
Etc/GMT+4	Etc/GMT-2	Etc/GMT-14
Etc/GMT+5	Etc/GMT-3	Etc/Greenwich
Etc/GMT+6	Etc/GMT-4	Etc/UTC
Etc/GMT+7	Etc/GMT-5	Etc/Universal
Etc/GMT+8	Etc/GMT-6	Etc/UTC
Etc/GMT+9	Etc/GMT-7	Etc/Zulu
Etc/GMT+10	Etc/GMT-8	

Miscellaneous

Arctic/Longyearbyen	HST	Portugal
CET	Iceland	PRC
CST6CDT	Iran	PST8PDT
Cuba	Israel	ROC
EET	Japan	ROK
Egypt	Kwajalein	Singapore
Eire	Libya	Turkey
EST	MET	UCT
EST5EDT	MST	Universal
Factory	MST7MDT	UTC
GB	Navajo	WET
GB-Eire	NZ	W-SU
Greenwich	NZ-CHAT	Zulu
Hong Kong	Poland	

System V

SystemV/AST4	SystemV/EST5EDT	SystemV/PST8PDT
SystemV/AST4ADT	SystemV/HST10	SystemV/YST9
SystemV/CST6	SystemV/MST7	SystemV/YST9YDT
SystemV/CST6CDT	SystemV/MST7MDT	
SystemV/EST5	SystemV/PST8	

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]

Language	Abbreviation	Language	Abbreviation
Arabic	ar	Norwegian	no
Croatian	hr	Polish	pl
Czech	cs	Portuguese	pt
Danish	da	POSIX	C
Dutch	nl	Romanian	ro
English	en	Russian	ru
English (U.S.)	en_US	Simplified Chinese	zh

[1] To use UTF-8 as the NFS character set, you must append .UTF-8 to the language code.

Language	**Abbreviation**	**Language**	**Abbreviation**
Finnish	fi	Simplified Chinese (GBK)	zh.GBK
French	fr	Slovak	sk
German	de	Slovenian	sl
Hebrew	he	Spanish	es
Hungarian	hu	Swedish	sv
Italian	it	Traditional Chinese euc-tw	zh_TW
Japanese euc-j	ja	Traditional Chinese Big 5	zh_TW.BIG5
Japanese PCK (sjis)	ja_JP.PCK	Turkish	tr
Korean	ko		

Troubleshooting setup

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

Troubleshooting if the system does not boot when powered 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. Make sure that the power supplies on your controller and disk shelves are working:

If the LEDs on a power supply are...	Then...
Illuminated	Proceed to the next step.
Not illuminated	Remove the power supply and reinstall it, making sure that it connects with the backplane.

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 shelves, go to step 7; otherwise ensure that the Fibre Channel disk shelf speed is correct.
7. Check disk ownership to ensure that the disks are assigned to the system:
   a) 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 or the CF card. Contact technical support.

   b) Verify that disks are assigned to the system by entering **`disk show`**.

   c) Validate that storage is attached to the system, and verify any changes you made, by entering **`disk show -v`**.
8. Turn off your controller and disk shelves, and then turn on the 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. Use the onboard diagnostics to check that Fibre Channel disks in the storage system are operating properly:

a) Turn on your system and press Ctrl-C.

Enter **`boot_diags`** at the LOADER> prompt.

b) Enter **`fcal`** in the Diagnostic Monitor program that starts at boot.

c) Enter **`73`** at the prompt to show all disk drives.

d) Exit the Diagnostic Monitor by entering **`99`** at the prompt, as needed.

e) Enter the **`exit`** command to return to LOADER.

f) Start Data ONTAP by entering **`autoboot`** at the prompt.

10. Use the onboard diagnostics to check that SAS disks in the storage system are operating properly:

a) Enter **`boot_diags`** at the LOADER> prompt.

b) Enter **`mb`** in the Diagnostic Monitor program.

c) Enter **`6`** to select the SAS test menu.

d) Enter **`42`** to scan and show disks on the selected SAS.

This displays the number of SAS disks.

e) Enter **`72`** to show the attached SAS devices.

f) Exit the Diagnostic Monitor by entering **`99`** at the prompt, as needed.

g) Enter the **`exit`** command to return to LOADER.

h) Start Data ONTAP by entering **`autoboot`** at the prompt.

11. Try booting your system again:

If your system...	Then...
Boots successfully	Proceed to set up the software.
Does not boot successfully	Contact technical support. The system might not have the boot image downloaded on the boot device.

Depending on your storage controller model, see the *Diagnostics Guide* or *System-Level Diagnostics Guide* for more information about running diagnostics.

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 © 1994–2013 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, Cryptainer, CryptoShred, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, FAServer, FastStak, FilerView, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, 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, 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, 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