## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deciding whether to use this guide</td>
<td>4</td>
</tr>
<tr>
<td>Cluster setup workflows</td>
<td>5</td>
</tr>
<tr>
<td>Setting up the cluster</td>
<td>6</td>
</tr>
<tr>
<td>Completing the cluster setup worksheet</td>
<td>6</td>
</tr>
<tr>
<td>Creating the cluster on the first node</td>
<td>11</td>
</tr>
<tr>
<td>Joining a node to the cluster</td>
<td>12</td>
</tr>
<tr>
<td>Synchronizing the system time across the cluster</td>
<td>13</td>
</tr>
<tr>
<td>Commands for managing symmetric authentication on NTP servers</td>
<td>14</td>
</tr>
<tr>
<td>Deciding where to send important event notifications</td>
<td>15</td>
</tr>
<tr>
<td>Configuring important EMS events to send email notifications</td>
<td>16</td>
</tr>
<tr>
<td>Configuring important EMS events to forward notifications to a syslog server</td>
<td>16</td>
</tr>
<tr>
<td>Configuring SNMP traphosts to receive event notifications</td>
<td>17</td>
</tr>
<tr>
<td>Provisioning an SVM by using a preconfigured ONTAP template</td>
<td>18</td>
</tr>
<tr>
<td>Additional system configuration tasks to complete</td>
<td>21</td>
</tr>
<tr>
<td>Copyright information</td>
<td>22</td>
</tr>
<tr>
<td>Trademark information</td>
<td>23</td>
</tr>
<tr>
<td>How to send comments about documentation and receive update notifications</td>
<td>24</td>
</tr>
<tr>
<td>Index</td>
<td>25</td>
</tr>
</tbody>
</table>
Deciding whether to use the Software Setup Guide

This guide describes how to set up and configure ONTAP.

You should use this guide if the cluster setup for your configuration is not supported by OnCommand System Manager GUI wizard (for example, a MetroCluster configuration or IPv6-only configuration).

You should use the System Manager GUI wizard whenever possible to set up the cluster.

Cluster management using System Manager

If you want additional configuration information, you should see the following documentation:

- Software express upgrade
- Upgrade, revert, or downgrade
- ONTAP concepts
Cluster setup workflows

After installing the hardware, you should use the System Manager GUI wizard whenever possible to set up the cluster. You should only use the CLI Cluster Setup wizard if the GUI wizard does not support the cluster setup (for example, a MetroCluster configuration or IPv6-only configuration).

Related information
- Fabric-attached MetroCluster installation and configuration
- Stretch MetroCluster installation and configuration
- FlexArray virtualization installation requirements and reference
Setting up the cluster

Setting up the cluster involves setting up each node, creating the cluster on the first node, and joining any remaining nodes to the cluster.

Steps

1. Completing the cluster setup worksheet on page 6
   The cluster setup worksheet enables you to record the values that you need during the cluster setup process. If a default value is provided, you can use that value or else enter your own.

2. Creating the cluster on the first node on page 11
   You use the Cluster Setup wizard to create the cluster on the first node. The wizard helps you to configure the cluster network that connects the nodes (if the cluster consists of two or more nodes), create the cluster admin storage virtual machine (SVM), add feature license keys, and create the node management interface for the first node.

3. Joining a node to the cluster on page 12
   After creating a new cluster, you use the Cluster Setup wizard to join each remaining node to the cluster one at a time. The wizard helps you to configure each node's node management interface.

4. Synchronizing the system time across the cluster on page 13
   Synchronizing the time ensures that every node in the cluster has the same time, and prevents CIFS and Kerberos failures.

5. Deciding where to send important event notifications on page 15
   Before you configure important EMS event notifications, you need to decide whether to send the notifications to an email address, a syslog server, or an SNMP traphost.

Completing the cluster setup worksheet

The cluster setup worksheet enables you to record the values that you need during the cluster setup process. If a default value is provided, you can use that value or else enter your own.

System defaults (for clusters configured to use network switches)

The system defaults are the default values for the private cluster network. It is best to use these default values. However, if they do not meet your requirements, you can use the table to record your own values.

You only need to consider the system defaults for clusters that are connected using network switches. Single-node clusters and two-node switchless clusters do not use a cluster network.

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Default</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private cluster network ports</td>
<td>Network and LIF management</td>
<td></td>
</tr>
<tr>
<td>MTU size for cluster ports</td>
<td>9000 bytes</td>
<td></td>
</tr>
<tr>
<td>Every node in the cluster must have the same MTU size as the cluster interconnect switches.</td>
<td>255.255.0.0</td>
<td></td>
</tr>
</tbody>
</table>
### Types of information

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Default</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster interface IP addresses (for each cluster network port on each node)</td>
<td>169.254.x.x</td>
<td></td>
</tr>
<tr>
<td>The IP addresses for each node must be on the same subnet.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Cluster information

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster name</td>
<td></td>
</tr>
<tr>
<td>The name must begin with a letter, and it must be fewer than 44 characters. The name can include the following special characters: . _ ~</td>
<td></td>
</tr>
<tr>
<td>Cluster base license key</td>
<td></td>
</tr>
<tr>
<td>The cluster base license key is not required to complete setup. However, it must be installed before you can install any feature licenses. To find your cluster base license key:</td>
<td></td>
</tr>
<tr>
<td>1. Go to the NetApp Support Site.</td>
<td></td>
</tr>
<tr>
<td>2. Click My Support &gt; Software Licenses.</td>
<td></td>
</tr>
</tbody>
</table>

### Feature license keys

You can find license keys for your initial or add-on software orders at the NetApp Support Site under My Support > Software Licenses.
### Admin storage virtual machine (SVM)

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster administrator password</td>
<td>The password for the admin account that the cluster requires before granting cluster administrator access to the console or through a secure protocol. The default rules for passwords are as follows:</td>
</tr>
<tr>
<td></td>
<td>• A password must be at least eight characters long.</td>
</tr>
<tr>
<td></td>
<td>• A password must contain at least one letter and one number.</td>
</tr>
<tr>
<td>Cluster management interface port</td>
<td>The physical port that is connected to the data network and enables the cluster administrator to manage the cluster.</td>
</tr>
<tr>
<td>Cluster management interface IP address</td>
<td>A unique IPv4 or IPv6 address for the cluster management interface. The cluster administrator uses this address to access the admin SVM and manage the cluster. Typically, this address should be on the data network. You can obtain this IP address from the administrator responsible for assigning IP addresses in your organization. Example: 192.0.2.66</td>
</tr>
</tbody>
</table>
### Types of information

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster management interface netmask (IPv4)</td>
<td></td>
</tr>
<tr>
<td>The subnet mask that defines the range of valid IPv4 addresses on the cluster management network.</td>
<td></td>
</tr>
<tr>
<td>Example: 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>Cluster management interface netmask length (IPv6)</td>
<td></td>
</tr>
<tr>
<td>If the cluster management interface uses an IPv6 address, then this value represents the prefix length that defines the range of valid IPv6 addresses on the cluster management network.</td>
<td></td>
</tr>
<tr>
<td>Example: 64</td>
<td></td>
</tr>
<tr>
<td>Cluster management interface default gateway</td>
<td></td>
</tr>
<tr>
<td>The IP address for the router on the cluster management network.</td>
<td></td>
</tr>
<tr>
<td>DNS domain name</td>
<td></td>
</tr>
<tr>
<td>The name of your network's DNS domain.</td>
<td></td>
</tr>
<tr>
<td>The domain name must consist of alphanumeric characters. To enter multiple DNS domain names, separate each name with either a comma or a space.</td>
<td></td>
</tr>
<tr>
<td>Name server IP addresses</td>
<td></td>
</tr>
<tr>
<td>The IP addresses of the DNS name servers.</td>
<td></td>
</tr>
<tr>
<td>Separate each address with either a comma or a space.</td>
<td></td>
</tr>
</tbody>
</table>

### Node information (for each node in the cluster)

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical location of the controller</td>
<td></td>
</tr>
<tr>
<td>A description of the physical location of the controller. Use a description that identifies where to find this node in the cluster (for example, “Lab 5, Row 7, Rack B”).</td>
<td></td>
</tr>
<tr>
<td>Node management interface port</td>
<td></td>
</tr>
<tr>
<td>The physical port that is connected to the node management network and enables the cluster administrator to manage the node.</td>
<td></td>
</tr>
<tr>
<td>Types of information</td>
<td>Your values</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Node management interface IP address</td>
<td>A unique IPv4 or IPv6 address for the node management interface on the management network. If you defined the node management interface port to be a data port, then this IP address should be a unique IP address on the data network. You can obtain this IP address from the administrator responsible for assigning IP addresses in your organization. Example: 192.0.2.66</td>
</tr>
<tr>
<td>Node management interface netmask (IPv4)</td>
<td>The subnet mask that defines the range of valid IP addresses on the node management network. If you defined the node management interface port to be a data port, then the netmask should be the subnet mask for the data network. Example: 255.255.255.0</td>
</tr>
<tr>
<td>Node management interface netmask length (IPv6)</td>
<td>If the node management interface uses an IPv6 address, then this value represents the prefix length that defines the range of valid IPv6 addresses on the node management network. Example: 64</td>
</tr>
<tr>
<td>Node management interface default gateway</td>
<td>The IP address for the router on the node management network.</td>
</tr>
<tr>
<td>System configuration backup destination address (single-node clusters only)</td>
<td>The remote URL where the cluster configuration backups will be uploaded. You can specify either an HTTP or FTP address. <strong>Note:</strong> The web server that serves the remote URL must have PUT operations enabled.</td>
</tr>
<tr>
<td>User name for the configuration backup destination address (single-node clusters only)</td>
<td>The user name required to log in to the remote URL and upload the configuration backup file.</td>
</tr>
<tr>
<td>Password for the configuration backup destination address (single-node clusters only)</td>
<td>The password for the remote URL, if the user name requires a password.</td>
</tr>
</tbody>
</table>
NTP server information

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP server addresses</td>
<td>The IP addresses of the Network Time Protocol (NTP) servers at your site. These servers are used to synchronize the time across the cluster.</td>
</tr>
</tbody>
</table>

Creating the cluster on the first node

You use the Cluster Setup wizard to create the cluster on the first node. The wizard helps you to configure the cluster network that connects the nodes (if the cluster consists of two or more nodes), create the cluster admin storage virtual machine (SVM), add feature license keys, and create the node management interface for the first node.

Before you begin

The cluster setup worksheet should be completed, the storage system hardware should be installed and cabled, and the console should be connected to the node on which you intend to create the cluster.

Steps

1. Power on all nodes.

2. Connect to the console of the first node.

   The node boots, and then the Cluster Setup wizard starts on the console.

   Welcome to the cluster setup wizard....

3. Follow the instructions on the screen to assign an IP address to the node.

   Note: AutoSupport is enabled by default.

4. If using the GUI wizard to perform setup, follow the instructions to complete setup in your web browser. If using the CLI wizard to perform setup, press Enter to continue.

   Use your web browser to complete cluster setup by accessing https://10.63.11.29

   Otherwise, press Enter to complete cluster setup using the command line interface:

   Do you want to create a new cluster or join an existing cluster? {create, join}:

5. Create a new cluster:

   create

6. Accept the system defaults or enter your own values.

7. After setup is completed, verify that the cluster is active and the first node is healthy by entering the ONTAP CLI command:

   cluster show
Example

The following example shows a cluster in which the first node (cluster1-01) is healthy and eligible to participate:

<table>
<thead>
<tr>
<th>Node</th>
<th>Health</th>
<th>Eligibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster1-01</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>

You can access the Cluster Setup wizard to change any of the values you entered for the admin SVM or node SVM by using the `cluster setup` command.

After you finish

If the cluster consists of two or more nodes, you should join each remaining node to the cluster. If you used the setup GUI, however, it is not necessary to perform the join flow on each subsequent node.

For more information on setting up a cluster using the setup GUI, see the OnCommand System Manager online help.

Joining a node to the cluster

After creating a new cluster, you use the Cluster Setup wizard to join each remaining node to the cluster one at a time. The wizard helps you to configure each node’s node management interface.

Before you begin

The cluster must be created on the first node.

About this task

You can only join one node to the cluster at a time. When you start to join a node to the cluster, you must complete the join, and the node must be part of the cluster before you can start to join the next node.

Note: If you use the GUI System Manager wizard, you need not perform the join flow on each subsequent node.

Steps

1. Power on all nodes.
   
   The node boots, and then the Cluster Setup wizard starts on the console.

   Welcome to the cluster setup wizard....
   
   Do you want to create a new cluster or join an existing cluster? {create, join}:

2. Join the node to the cluster:

   join

3. Follow the instructions on the screen to set up the node and join it to the cluster.

4. After setup is completed, verify that the node is healthy and eligible to participate in the cluster:

   cluster show
The following example shows a cluster after the second node (cluster1-02) has been joined to the cluster:

```
cluster1::> cluster show
```

<table>
<thead>
<tr>
<th>Node</th>
<th>Health</th>
<th>Eligibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster1-01</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>cluster1-02</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>

You can access the Cluster Setup wizard to change any of the values you entered for the admin SVM or node SVM by using the `cluster setup` command.

5. Repeat this task for each remaining node.

### Synchronizing the system time across the cluster

Synchronizing the time ensures that every node in the cluster has the same time, and prevents CIFS and Kerberos failures.

**Before you begin**

A Network Time Protocol (NTP) server should be set up at your site. Beginning in ONTAP 9.5, you can set up your NTP server with symmetric authentication.

**About this task**

You synchronize the time across the cluster by associating the cluster with one or more NTP servers.

**Steps**

1. Verify that the system time and time zone is set correctly for each node.
   
   All nodes in the cluster should be set to the same time zone.
   
   a. Use the `cluster date show` command to display the current date, time, and time zone for each node.

   **Example**

   ```
   cluster1::> cluster date show
   ```

<table>
<thead>
<tr>
<th>Node</th>
<th>Date</th>
<th>Time zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster1-01</td>
<td>01/06/2015 09:35:15</td>
<td>America/New_York</td>
</tr>
<tr>
<td>cluster1-02</td>
<td>01/06/2015 09:35:15</td>
<td>America/New_York</td>
</tr>
<tr>
<td>cluster1-03</td>
<td>01/06/2015 09:35:15</td>
<td>America/New_York</td>
</tr>
<tr>
<td>cluster1-04</td>
<td>01/06/2015 09:35:15</td>
<td>America/New_York</td>
</tr>
</tbody>
</table>

   4 entries were displayed.

   b. Optional: Use the `cluster date modify` command to change the date or time zone for all of the nodes.

   **Example**

   This example changes the time zone for the cluster to be GMT:

   ```
   cluster1::> cluster date modify -timezone GMT
   ```
2. Use the `cluster time-service ntp server create` command to associate the cluster with your NTP server.

   - To set up your NTP server without symmetric authentication enter the following command:
     ```bash
     cluster time-service ntp server create -server server_name
     ```
   - To set up your NTP server with symmetric authentication, enter the following command:
     ```bash
     cluster time-service ntp server create -server server_ip_address -key-id key_id
     ```
     **Note:** Symmetric authentication is available beginning in ONTAP 9.5. It is not available in ONTAP 9.4 or earlier.

**Example**

This example assumes that DNS has been configured for the cluster. If you have not configured DNS, you must specify the IP address of the NTP server:

```bash
cluster1::> cluster time-service ntp server create -server ntp1.example.com
```

3. Verify that the cluster is associated with an NTP server:

   ```bash
   cluster time-service ntp server show
   ```

**Example**

```bash
cluster1::> cluster time-service ntp server show
Server               Version
--------------------  -----------
ntp1.example.com     auto
```

**Related information**

*System administration*

**Commands for managing symmetric authentication on NTP servers**

Beginning in ONTAP 9.5, Network Time Protocol (NTP) version 3 is supported. NTPv3 includes symmetric authentication using SHA-1 keys which increases network security.

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure an NTP server without symmetric authentication</td>
<td><code>cluster time-service ntp server create -server server_name</code></td>
</tr>
<tr>
<td>Configure an NTP server with symmetric authentication</td>
<td><code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code></td>
</tr>
<tr>
<td>Enable symmetric authentication for an existing NTP server</td>
<td><code>cluster time-service ntp server modify -server server_name -key-id key_id</code></td>
</tr>
<tr>
<td>An existing NTP server can be modified to enable authentication by adding the required key-id.</td>
<td><code>cluster time-service ntp server modify -server server_name -key-id key_id</code></td>
</tr>
<tr>
<td>To do this...</td>
<td>Use this command...</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Configure a shared NTP key</td>
<td><code>cluster time-service ntp key create</code></td>
</tr>
<tr>
<td></td>
<td><code>-id shared_key_id</code></td>
</tr>
<tr>
<td></td>
<td><code>-type shared_key_type</code></td>
</tr>
<tr>
<td></td>
<td><code>-value shared_key_value</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Shared keys are referred to by an ID. The ID, its type, and value must be identical on both the node and the NTP server</td>
</tr>
<tr>
<td>Configure an NTP server with an unknown key ID</td>
<td><code>cluster time-service ntp server create</code></td>
</tr>
<tr>
<td></td>
<td><code>-server server_name</code></td>
</tr>
<tr>
<td></td>
<td><code>-key-id key_id</code></td>
</tr>
<tr>
<td>Configure a server with a key ID not configured</td>
<td><code>cluster time-service ntp server create</code></td>
</tr>
<tr>
<td>on the NTP server.</td>
<td><code>-server server_name</code></td>
</tr>
<tr>
<td></td>
<td><code>-key-id key_id</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The key ID, type, and value must be identical to the key ID, type, and value configured on the NTP server.</td>
</tr>
<tr>
<td>Disable symmetric authentication</td>
<td><code>cluster time-service ntp server modify</code></td>
</tr>
<tr>
<td></td>
<td><code>-server server_name</code></td>
</tr>
<tr>
<td></td>
<td><code>-authentication disabled</code></td>
</tr>
</tbody>
</table>

### Deciding where to send important event notifications

Before you configure important EMS event notifications, you need to decide whether to send the notifications to an email address, a syslog server, or an SNMP traphost.

**About this task**

If your environment already contains a syslog server for aggregating the logged events from other systems, such as servers and applications, then it is easier to use that syslog server also for important event notifications from storage systems.

If your environment does not already contain a syslog server, then it is easier to use email for important event notifications.

If you already forward event notifications to an SNMP traphost, then you might want to monitor that traphost for important events.

- Set EMS to send event notifications.

<table>
<thead>
<tr>
<th>If you want...</th>
<th>Refer to this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>The EMS to send important event notifications to an email address</td>
<td><a href="#">Configuring important EMS events to send email notifications</a> on page 16</td>
</tr>
<tr>
<td>The EMS to forward important event notifications to a syslog server</td>
<td><a href="#">Configuring important EMS events to forward notifications to a syslog server</a> on page 16</td>
</tr>
<tr>
<td>If you want the EMS to forward event notifications to an SNMP traphost</td>
<td><a href="#">Configuring SNMP traphosts to receive event notifications</a> on page 17</td>
</tr>
</tbody>
</table>
**Configuring important EMS events to send email notifications**

To receive email notifications of the most important events, you must configure the EMS to send email messages for events that signal important activity.

**Before you begin**

DNS must be configured on the cluster to resolve the email addresses.

**About this task**

You can perform this task any time the cluster is running by entering the commands on the ONTAP command line.

**Steps**

1. Configure the event SMTP mail server settings:

   ```
   event config modify --mail-server mailhost.your_domain --mail-from cluster_admin@your_domain
   ```

2. Create an email destination for event notifications:

   ```
   event notification destination create --name storage-admins --email your_email@your_domain
   ```

3. Configure the important events to send email notifications:

   ```
   event notification create --filter-name important-events --destinations storageadmins
   ```

**Configuring important EMS events to forward notifications to a syslog server**

To log notifications of the most severe events on a syslog server, you must configure the EMS to forward notifications for events that signal important activity.

**Before you begin**

DNS must be configured on the cluster to resolve the syslog server name.

**About this task**

If your environment does not already contain a syslog server for event notifications, you must first create one. If your environment already contains a syslog server for logging events from other systems, then you might want to use that one for important event notifications.

You can perform this task any time the cluster is running by entering the commands on the ONTAP command line.

**Steps**

1. Create a syslog server destination for important events:

   ```
   event notification destination create --name syslog-ems --syslog syslog-server-address
   ```

2. Configure the important events to forward notifications to the syslog server:

   ```
   event notification create --filter-name important-events --destinations syslog-ems
   ```
Configuring SNMP traphosts to receive event notifications

To receive event notifications on an SNMP traphost, you must configure a traphost.

Before you begin

• SNMP and SNMP traps must be enabled on the cluster.
  
  **Note:** SNMP and SNMP traps are enabled by default.

• DNS must be configured on the cluster to resolve the traphost names.

About this task

If you do not already have an SNMP traphost configured to receive event notifications (SNMP traps), you must add one.

You can perform this task any time the cluster is running by entering the commands on the ONTAP command line.

Step

1. If your environment does not already have an SNMP traphost configured to receive event notifications, add one:

   ```
   system snmp traphost add -peer-address snmp_traphost_name
   ```

   All event notifications that are supported by SNMP by default are forwarded to the SNMP traphost.
Provisioning an SVM by using a preconfigured ONTAP template

Starting with ONTAP 9.3, you can create and provision an SVM by using a preconfigured template. You must provide values for the parameters that are defined in the template.

Before you begin

All of the required feature licenses must be installed on the cluster.

About this task

The VserverEnvironmentSetup template is the preconfigured template that you can use for configuring SVMs. The VserverEnvironmentSetup template enables you to set up the following configurations:

- Security style, language setting, and IPspace of the SVM
- Protocols
- Data LIFs
- Network routes
- DNS configuration
- Active Directory configuration
- NIS configuration
- LDAP client and server configuration
- CIFS server

The VserverEnvironmentSetup template is a read-only template. You cannot modify the default parameter values of this template. If you want to modify the default values of any of the parameters in the template, you must copy the template, and then modify the default values of the parameters.

Steps

1. View and note down the values for the parameters that are defined in the template for creating and configuring the SVM:

   template parameter show

Example

```bash
cluster1::> template parameter show

Template: VserverEnvironmentSetup
Permission: readonly

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default Value</th>
<th>Read Only</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vserver</td>
<td>string</td>
<td>-</td>
<td>no</td>
<td>Vserver Name</td>
</tr>
<tr>
<td>security_style</td>
<td>string</td>
<td>unix</td>
<td>no</td>
<td>Vserver Security Style</td>
</tr>
<tr>
<td>language</td>
<td>string</td>
<td>C.UTF-8</td>
<td>no</td>
<td>Vserver Language</td>
</tr>
<tr>
<td>ipspace</td>
<td>string</td>
<td>Default</td>
<td>no</td>
<td>Vserver IPSpace</td>
</tr>
<tr>
<td>protocols</td>
<td>enum</td>
<td>-</td>
<td>no</td>
<td>Protocols to configure</td>
</tr>
<tr>
<td>Allowed Values:</td>
<td>nfs, cifs, iscsi, fcp</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data_lif</td>
<td>array of lifInfoStruct</td>
<td>-</td>
<td>yes</td>
<td>Data LIF Info Struct</td>
</tr>
<tr>
<td>data_lif[#].ipaddr</td>
<td>IPAddress</td>
<td>-</td>
<td>no</td>
<td>IP Addr</td>
</tr>
</tbody>
</table>
```
2. Optional: If you want to modify the default value of any parameter in the template, customize the existing template:

   a. Copy the template:

```
template copy -name template_name -destination_name new_template_name
```

**Example**

```
cluster1::> template copy -name VserverEnvironmentSetup -destination-name template1
```

The new template is a read/write template.

b. Modify the default value of the parameter that you want to change:

```
template parameter modify -template template_name -name parameter_name -default-value new_default_value
```

**Example**

```
cluster1::> template parameter modify -template template1 -name security_style -default-value ntfs
```

3. Provision the SVM by specifying values for the parameters in the template:

```
template provision -name template_name
```

**Example**

```
cluster-1::> template provision -name template1
Press Ctrl+C to abort.
*************
* Setup of vserver *
*************
Vserver Name: vs0
Vserver Language [C.UTF-8]:
Vserver Security Style [ntfs]:
Vserver IPSpace [Default]:

*************
* Setup of network.interface *
*************
Enter number of instances for object network.interface: 2
(1/2)LIF Protocol: nfs
```
(1/2) IP Addr: 1.1.1.1
(1/2) NetMask: 255.255.255.0
(1/2) Node Name: node1-vsim1
(1/2) Port: e0c
(2/2) LIF Protocol: nfs
(2/2) IP Addr: 1.1.1.1
(2/2) NetMask: 255.255.255.0
(2/2) Node Name: node1-vsim1
(2/2) Port: e0c

***************************
* Setup of network.routes *
***************************
Enter number of instances for object network.routes: 1
(1/1) Gateway: 1.1.1.1

*************************
* Setup of access.dns *
*************************
Search Domain: netapp.com
DNS IP Addresses List: 1.1.1.1

************************
* Setup of security.nis *
*************************
NIS Domains: netapp.com
NIS IP Address: 1.1.1.1

********************
* Setup of security *
********************
LDAP Client Config: ldapconfig
LDAP Server IP: 1.1.1.1
LDAP Base DN: dc=examplebasedn

********************
* Setup of protocols *
********************
Protocols to configure: nfs
[Job 15] Configuring vserver for vs0 (100%)
## Additional system configuration tasks to complete

After setting up a cluster, you can use either OnCommand System Manager or the ONTAP command-line interface (CLI) to continue configuring the cluster.

<table>
<thead>
<tr>
<th>System configuration task</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure networking:</td>
<td></td>
</tr>
<tr>
<td>• Create broadcast domains</td>
<td>Network and LIF management</td>
</tr>
<tr>
<td>• Create subnets</td>
<td></td>
</tr>
<tr>
<td>• Create IP spaces</td>
<td></td>
</tr>
<tr>
<td>Set up the Service Processor</td>
<td>System administration</td>
</tr>
<tr>
<td>Lay out your aggregates</td>
<td>Disk and aggregate management</td>
</tr>
<tr>
<td>Create and configure data storage virtual machines (SVMs)</td>
<td>Cluster management using System Manager</td>
</tr>
<tr>
<td></td>
<td>NFS configuration</td>
</tr>
<tr>
<td></td>
<td>SMB/CIFS management</td>
</tr>
<tr>
<td></td>
<td>SAN administration</td>
</tr>
</tbody>
</table>
Trademark information

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

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.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

• NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
• Telephone: +1 (408) 822-6000
• Fax: +1 (408) 822-4501
• Support telephone: +1 (888) 463-8277
Index

A
- about this guide
  - deciding whether to use the Software Setup Guide 4
- alert events
  - configuring EMS to send email notifications 16
  - configuring to forward notifications to syslog server 16
- AutoSupport
  - noteto configuration with email addresses 16

C
- cluster setup
  - information to gather for 6
  - introduction to the process for 6
  - workflows 5
- Cluster Setup wizard
  - using to create a cluster on the first node 11
  - using to join nodes to the cluster 12
- clusters
  - creating on the first node 11
  - joining a node to 12
  - synchronizing the system time 13
  - system configuration tasks to complete after setup 21
- commands
  - for managing symmetric authentication on NTP servers 14
- comments
  - how to send feedback about documentation 24
- critical events
  - configuring EMS to send email notifications 16
  - configuring to forward notifications to syslog server 16

D
- documentation
  - how to receive automatic notification of changes to 24
  - how to send feedback about 24

E
- emergency events
  - configuring EMS to send email notifications 16
  - configuring to forward notifications to syslog server 16
- EMS
  - configuring to forward notifications to syslog server 16
  - configuring to send email notifications 16
  - configuring to send SNMP traps 17
  - deciding where to send important event notifications 15
- event notifications
  - configuring EMS for email 16
  - configuring for syslog server 16
  - forwarding to SNMP traphosts 17
- events
  - deciding where to send important notifications 15
- express guides
  - deciding where to send important EMS event notifications 15

F
- feedback
  - how to send comments about documentation 24

G
- guides
  - requirements for using the Software Setup Guide 4

I
- important events
  - configuring EMS for email notifications 16
  - configuring for syslog server 16
  - forwarding to SNMP traphosts 17
- information
  - how to send feedback about improving documentation 24

M
- managing symmetric authentication on NTP servers
  - commands for 14

N
- Network Time Protocol (NTP)
  - enabling for the cluster 13
  - nodes
    - joining to a cluster 12
    - synchronizing system time across the cluster 13
    - using the Cluster Setup wizard to create the cluster on the first 11
- NTP
  - See Network Time Protocol
- NTP servers
  - commands for managing symmetric authentication on 14

P
- provisioning SVMs
  - by using a template 18

S
- setup
  - completing the worksheet for cluster 6
- SNMP traphosts
configuring EMS for 17
Software Setup Guide
requirements for using 4
suggestions
how to send feedback about documentation 24
system configuration
tasks to complete after cluster setup 21
system time
synchronizing across the cluster 13

T
templates
for configuring an SVM 18
for creating an SVM 18

for provisioning an SVM 18
time
system, synchronizing across the cluster 13
traphosts, SNMP
configuring EMS for 17
Twitter
how to receive automatic notification of
documentation changes 24

W
workflows
for cluster setup 5
worksheets
completing the cluster setup 6