



ONTAP® 9

Software Setup Guide

November 2018 | 215-11142_GO
doccomments@netapp.com

Updated for ONTAP 9.5

 **NetApp**®

Contents

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

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.

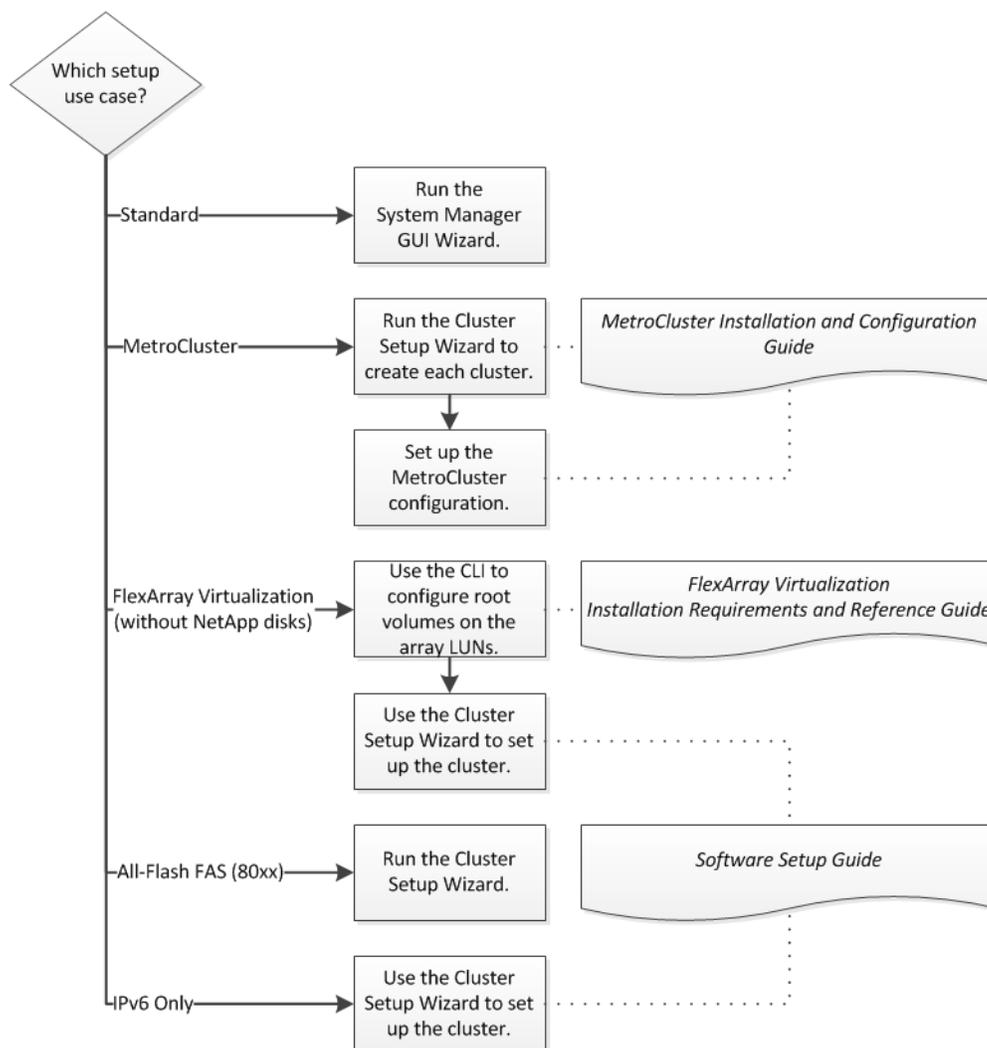
Cluster management using System Manager

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 trap host.

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.

Types of information	Default	Your values
Private cluster network ports	<i>Network and LIF management</i>	
MTU size for cluster ports Every node in the cluster must have the same MTU size as the cluster interconnect switches.	9000 bytes	
Cluster network netmask	255.255.0.0	

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

Cluster information

Types of information	Your values
<p>Cluster name</p> <p>The name must begin with a letter, and it must be fewer than 44 characters. The name can include the following special characters:</p> <p>. - _</p>	
<p>Cluster base license key</p> <p>The cluster base license key is not required to complete setup. However, it must be installed before you can install any feature licenses.</p> <p>To find your cluster base license key:</p> <ol style="list-style-type: none"> 1. Go to the NetApp Support Site. NetApp Support 2. Click My Support > Software Licenses. 	

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**.

Types of information	Your values
Feature license keys	

Admin storage virtual machine (SVM)

Types of information	Your values
<p>Cluster administrator password</p> <p>The password for the admin account that the cluster requires before granting cluster administrator access to the console or through a secure protocol.</p> <p>The default rules for passwords are as follows:</p> <ul style="list-style-type: none"> • A password must be at least eight characters long. • A password must contain at least one letter and one number. 	
<p>Cluster management interface port</p> <p>The physical port that is connected to the data network and enables the cluster administrator to manage the cluster.</p>	
<p>Cluster management interface IP address</p> <p>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.</p> <p>You can obtain this IP address from the administrator responsible for assigning IP addresses in your organization.</p> <p>Example: 192.0.2.66</p>	

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

Node information (for each node in the cluster)

Types of information	Your values
<p>Physical location of the controller</p> <p>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").</p>	
<p>Node management interface port</p> <p>The physical port that is connected to the node management network and enables the cluster administrator to manage the node.</p>	

Types of information	Your values
<p>Node management interface IP address</p> <p>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.</p> <p>You can obtain this IP address from the administrator responsible for assigning IP addresses in your organization.</p> <p>Example: 192.0.2.66</p>	
<p>Node management interface netmask (IPv4)</p> <p>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.</p> <p>Example: 255.255.255.0</p>	
<p>Node management interface netmask length (IPv6)</p> <p>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.</p> <p>Example: 64</p>	
<p>Node management interface default gateway</p> <p>The IP address for the router on the node management network.</p>	
<p>System configuration backup destination address (single-node clusters only)</p> <p>The remote URL where the cluster configuration backups will be uploaded. You can specify either an HTTP or FTP address.</p> <p>Note: The web server that serves the remote URL must have PUT operations enabled.</p>	
<p>User name for the configuration backup destination address (single-node clusters only)</p> <p>The user name required to log in to the remote URL and upload the configuration backup file.</p>	
<p>Password for the configuration backup destination address (single-node clusters only)</p> <p>The password for the remote URL, if the user name requires a password.</p>	

NTP server information

Types of information	Your values
NTP server addresses The IP addresses of the Network Time Protocol (NTP) servers at your site. These servers are used to synchronize the time across the cluster.	

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:

```
cluster1::> cluster show
Node           Health Eligibility
-----
cluster1-01    true   true
```

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
```

Example

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

```
cluster1::> cluster show
Node           Health Eligibility
-----
cluster1-01   true   true
cluster1-02   true   true
```

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
Node           Date           Time zone
-----
cluster1-01   01/06/2015 09:35:15 America/New_York
cluster1-02   01/06/2015 09:35:15 America/New_York
cluster1-03   01/06/2015 09:35:15 America/New_York
cluster1-04   01/06/2015 09:35:15 America/New_York
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:
`cluster time-service ntp server create -server server_name`
 - To set up your NTP server with symmetric authentication, enter the following command:
`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:

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

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

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

Example

```
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.

To do this...	Use this command...
Configure an NTP server without symmetric authentication	<code>cluster time-service ntp server create -server server_name</code>
Configure an NTP server with symmetric authentication	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>
Enable symmetric authentication for an existing NTP server An existing NTP server can be modified to enable authentication by adding the required key-id.	<code>cluster time-service ntp server modify -server server_name -key-id key_id</code>

To do this...	Use this command...
Configure a shared NTP key	<pre>cluster time-service ntp key create -id <i>shared_key_id</i> -type <i>shared_key_type</i> - value<i>shared_key_value</i></pre> <p>Note: 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</p>
Configure an NTP server with an unknown key ID	<pre>cluster time-service ntp server create -server <i>server_name</i> -key-id <i>key_id</i></pre>
Configure a server with a key ID not configured on the NTP server.	<pre>cluster time-service ntp server create -server <i>server_name</i> -key-id <i>key_id</i></pre> <p>Note: The key ID, type, and value must be identical to the key ID, type, and value configured on the NTP server.</p>
Disable symmetric authentication	<pre>cluster time-service ntp server modify -server <i>server_name</i> - authentication disabled</pre>

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 trap host.

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 trap host, then you might want to monitor that trap host for important events.

- Set EMS to send event notifications.

If you want...	Refer to this...
The EMS to send important event notifications to an email address	Configuring important EMS events to send email notifications on page 16
The EMS to forward important event notifications to a syslog server	Configuring important EMS events to forward notifications to a syslog server on page 16
If you want the EMS to forward event notifications to an SNMP trap host	Configuring SNMP trap hosts to receive event notifications on page 17

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
storage_admins
```

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

```
cluster1::> template parameter show

  Template: VserverEnvironmentSetup
Permission: readonly

Parameter          Type          Default Value  Read Only  Description
-----
vserver            string        -              no         Vserver Name
security_style     string        unix           no         Vserver Security Style
language           string        C.UTF-8       no         Vserver Language
ipspace            string        Default       no         Vserver IPspace
protocols          enum          -              no         Protocols to configure
  Allowed Values: nfs, cifs, iscsi, fcp
data_lif           array of lifInfoStruct
data_lif[#].ipaddr IPAddress     -              yes        Data LIF Info Struct
data_lif[#].ipaddr IPAddress     -              no         IP Addr
```

```

data_lif[#].netmask IPAddress - no NetMask
data_lif[#].protocol string - no LIF Protocol
data_lif[#].homenode string - no Node Name
data_lif[#].homeport string - no Port
gateway array of IPAddress - yes Gateway
gateway[#] IPAddress - no Gateway
search_domain string - no Search Domain
dns_server string - no DNS IP Addresses List
ad_admin_name string - no AD Admin Name
ad_admin_passwd string *** no AD Admin Passwd
ad_domain string - no AD Domain
ad_ou string CN=Computers no Organizational Name
wg_name string - no WG Name
nis_domain string - no NIS Domains
nis_ipaddr string - no NIS IP Address
ldap_server string - no LDAP Server IP
ldap_base_dn string - no LDAP Base DN
client_config string - no LDAP Client Config
cifs_server string - no CIFS Server Name
26 entries were displayed.

```

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 templatel
```

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 templatel -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 templatel
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: nodel-vsml
(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: nodel-vsml
(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.

System configuration task	Resource
Configure networking: <ul style="list-style-type: none">• Create broadcast domains• Create subnets• Create IP spaces	<i>Network and LIF management</i>
Set up the Service Processor	<i>System administration</i>
Lay out your aggregates	<i>Disk and aggregate management</i>
Create and configure data storage virtual machines (SVMs)	<i>Cluster management using System Manager</i> <i>NFS configuration</i> <i>SMB/CIFS management</i> <i>SAN administration</i>

Copyright information

Copyright © 2018 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

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.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

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*](mailto: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](#)