NetApp Element 11.5

Setup Guide

November 2019 | 215-14519_2019-11_en-us
doccomments@netapp.com

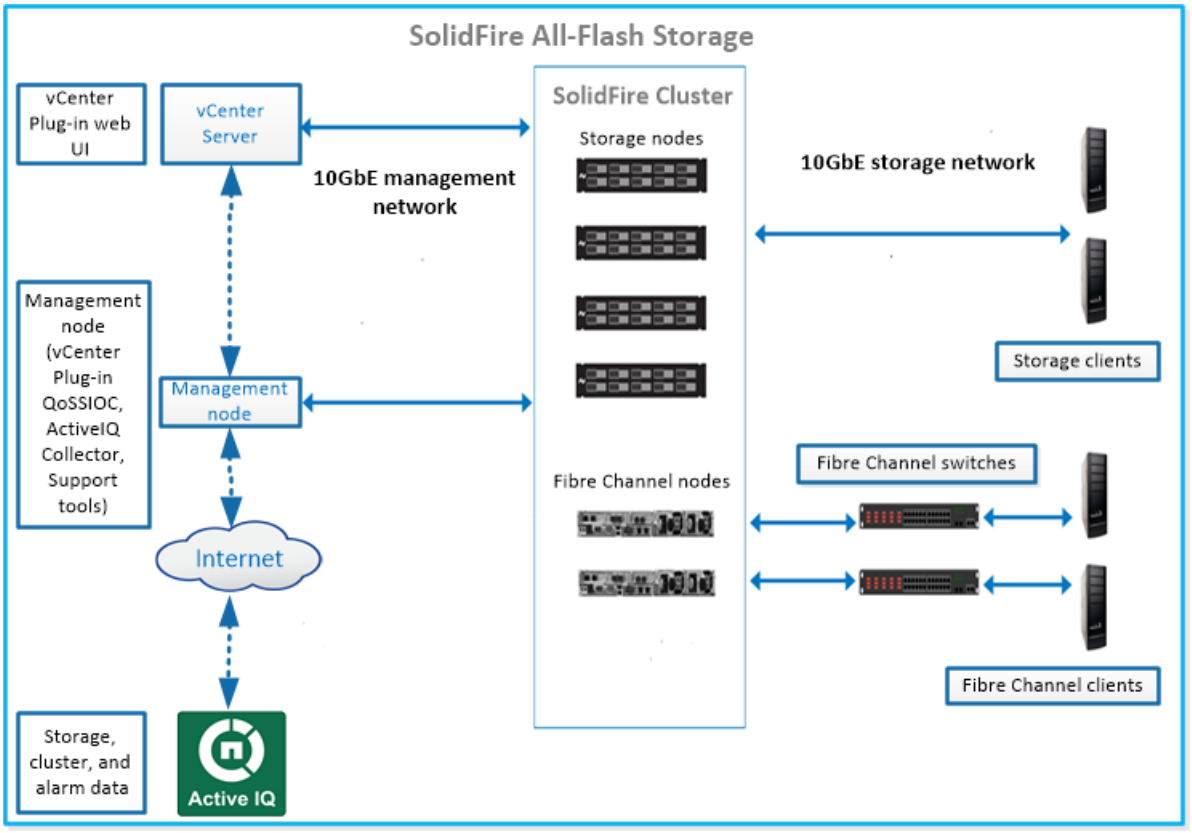
NetApp®

Contents

SolidFire storage system

A SolidFire all-flash storage system is comprised of discrete hardware components (drive and nodes) that are combined into a single pool of storage resources through NetApp Element software running independently on each node. This unified cluster presents as a single storage system for use by external clients and is managed as a single entity through the Element software UI, API and other management tools.

Using the NetApp Element software user interface, you can set up and monitor SolidFire cluster storage capacity and performance, and manage storage activity across a multi-tenant infrastructure.



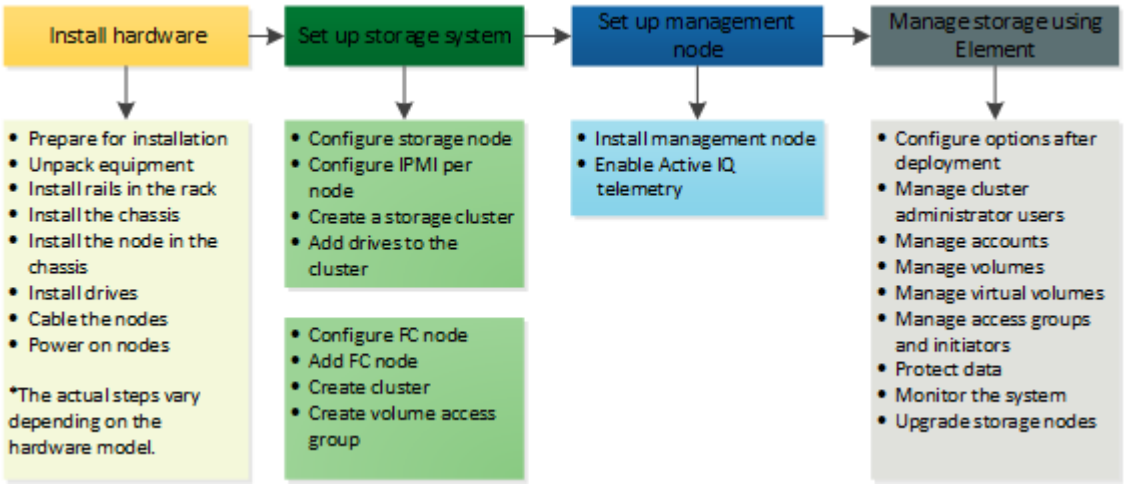
A SolidFire all-flash storage system includes the following components:

- Nodes: Physical hardware that provides the storage resources for a cluster. There are two types of nodes:
  - Storage nodes: Servers containing a collection of drives.
  - Fibre Channel (FC) nodes: Used to connect FC clients via a Fibre Channel switch.
- Cluster: The hub of the SolidFire storage system comprised of a least four nodes.
- Management node: Enables you to upgrade and provide system services including monitoring and telemetry, manage cluster assets and settings, run system tests and utilities, and provide NetApp Support access for troubleshooting. The management node (mNode) is a virtual machine that runs in tandem with an Element software-based storage cluster.

- Active IQ: A web-based tool that provides continually updated historical views of cluster-wide data. You can set up alerts for specific events, thresholds, or metrics. Active IQ enables you to monitor system performance and capacity, as well as stay informed about cluster health.
- Drives are used in storage nodes and store data for the cluster. A storage node contains two types of drives:
  - Volume metadata drives store information that defines the volumes and other objects within a cluster.
  - Block drives store data blocks for application volumes.

Setup overview

Before you get started, you might want to understand the sequence of installing and setting up NetApp Element software.



Determining which SolidFire components to install

You might want to check which SolidFire components, such as the management node, Active IQ and the NetApp Monitoring Agent (NMA), that you should install, depending on configuration and deployment choices.

About this task

The following table lists the additional components and indicates whether you should install them.

Component	Standalone SolidFire storage cluster	NetApp HCI cluster
Management node	Recommended	Installed by default, required
Active IQ	Recommended*	Recommended*
NetApp Monitoring Agent	Not supported	Recommended

*Active IQ is required for capacity-licensed SolidFire storage clusters.

Steps

1. Determine which components should be installed.
2. Complete the installation according to the procedure:

   Installing a management node on page 16

   Enabling SolidFire Active IQ on page 21

   For NetApp Monitoring Agent information, see the deployment information.

   HCI Documentation Center

Setting up an Element storage system

Setting up a NetApp Element software storage system involves configuring a storage node, creating a storage cluster, and adding drives to the cluster. If you use a Fibre Channel network, you can configure a Fibre Channel node.

Steps

1. Configuring a storage node on page 8
   You must configure individual nodes before you can add them to a cluster. When you install and cable a node in a rack unit and power it on, the terminal user interface (TUI) displays the fields necessary to configure the node. Ensure that you have the necessary configuration information for the node before proceeding.
2. Creating a storage cluster on page 11
   You can create a storage cluster after you have configured all of the individual nodes. When you create a cluster, a cluster administrator user account is automatically created for you. The cluster administrator has permission to manage all cluster attributes and can create other cluster administrator accounts.
3. Accessing the Element software user interface on page 12
   You can access the Element UI by using the management virtual IP (MVIP) address of the primary cluster node.
4. Adding drives to a cluster on page 12
   When you add a node to the cluster or install new drives in an existing node, the drives automatically register as available. You must add the drives to the cluster by using either the Element UI or API before they can participate in the cluster.
5. Configuring a Fibre Channel node on page 13
   Fibre Channel nodes enable you to connect the cluster to a Fibre Channel network fabric. Fibre Channel nodes are added in pairs, and operate in active-active mode (all nodes actively process traffic for the cluster). Clusters running Element software version 9.0 and later support up to four nodes; clusters running previous versions support a maximum of two nodes.

Configuring a storage node

You must configure individual nodes before you can add them to a cluster. When you install and cable a node in a rack unit and power it on, the terminal user interface (TUI) displays the fields necessary to configure the node. Ensure that you have the necessary configuration information for the node before proceeding.

Alternatively, you can configure these settings by accessing the node via the Element UI using the Dynamic Host Configuration Protocol (DHCP) 1G management IP address displayed in the TUI. The DHCP address is located in the menu bar at the top of the TUI.

You cannot add a node with DHCP assigned IP addresses to a cluster. You can use the DHCP IP address to initially configure the node in the Element UI, TUI, or API. During this initial configuration, you can add the static IP address information so that you can add the node to a cluster.

After initial configuration, you can access the node using the node's management IP address. You can then change the node settings, add it to a cluster, or use the node to create a cluster. You can also configure a new node using Element software API methods.

Note: Beginning in Element version 11.0, nodes can be configured with IPv4, IPv6, or both addresses for their management network. This applies to both storage nodes and management nodes, except for management node 11.3 and later which does not support IPv6. When you create

a cluster, only a single IPv4 or IPv6 address can be used for the MVIP and the corresponding address type must be configured on all nodes.

Related tasks

Configuring the node using the TUI on page 9
Configuring the node using the node UI on page 10
Creating a storage cluster on page 11
You can create a storage cluster after you have configured all of the individual nodes. When you create a cluster, a cluster administrator user account is automatically created for you. The cluster administrator has permission to manage all cluster attributes and can create other cluster administrator accounts.

Related references

Node states on page 10

Configuring the node using the TUI

You can use the terminal user interface (TUI) to perform initial configuration for new nodes.

About this task

You should configure the Bond1G and Bond10G interfaces for separate subnets. Bond1G and Bond10G interfaces configured for the same subnet causes routing problems when storage traffic is sent via the Bond1G interface. If you must use the same subnet for management and storage traffic, manually configure management traffic to use the Bond10G interface. You can do this for each node using the Cluster Settings page of the Element UI.

If you later change the IP address using the TUI, the top banner does not immediately display the change. If you restart the node, the banner displays the newly assigned IP address.

Steps

1. Attach a keyboard and monitor to the node and then power on the node.

   The TUI appears on the tty1 terminal with the Network Settings tab. If a DHCP server is running on the network with available IP addresses, the 1GbE address appears in the Address field.

   Note: If the node cannot reach your configuration server, the TUI displays an error message. Check your configuration server connection or the networking connection to resolve the error.

2. Use the on-screen navigation to configure the 1G and 10G network settings for the node.

   Tip: To enter text, press **Enter** on the keyboard to open edit mode. After you enter text, press **Enter** again to close the edit mode. To navigate between fields, use the arrow keys.

3. Enter **s** to save the settings, and then enter **y** to accept the changes.
4. Enter **c** to navigate to the **Cluster** tab.
5. Use the on-screen navigation to configure the cluster settings for the node.

   All the nodes in a cluster must have identical cluster names. Cluster names are case-sensitive.

6. Enter **s** to save the settings, and then enter **y** to accept the changes.

   The node is put in a pending state and can be added to an existing cluster or a new cluster.

Related tasks

Creating a storage cluster on page 11

You can create a storage cluster after you have configured all of the individual nodes. When you create a cluster, a cluster administrator user account is automatically created for you. The cluster administrator has permission to manage all cluster attributes and can create other cluster administrator accounts.

Configuring the node using the node UI

You can configure nodes using the Node Configuration user interface.

About this task

- You can configure the node to have either an IPv4 or IPv6 address.
- You need the DHCP address displayed in the TUI to access a node. You cannot use DHCP addresses to add a node to a cluster.

  Attention: You should configure the Bond1G and Bond10G interfaces for separate subnets. Bond1G and Bond10G interfaces configured for the same subnet causes routing problems when storage traffic is sent via the Bond1G interface. If you must use the same subnet for management and storage traffic, manually configure management traffic to use the Bond10G interface. You can do this for each node using the Cluster Settings page of the ElementNetApp Element software UI.

Steps

1. In a browser window, enter the DHCP IP address of a node.

   You must add the extension `:442` to access the node; for example, `https://172.25.103.6:442`.

   The Network Settings tab opens with the Network Settings – Bond1G section.
2. Enter the 1G network settings.
3. Click **Save Changes**.
4. Click **Bond10G** to display the settings for the 10G network settings.
5. Enter the 10G network settings.
6. Click **Save Changes**.
7. Click **Cluster Settings**.
8. Enter the hostname for the 10G network.
9. Click **Save Changes**.

Related tasks

Configuring the node using the TUI on page 9

Node states

A node can be in one of several states depending on the level of configuration.

- Available: The node has no associated cluster name and is not yet part of a cluster.
- Pending: The node is configured and can be added to a designated cluster.
  Authentication is not required to access the node.
- Pending Active: The system is in the process of installing compatible Element software on the node. When complete, the node will move to the Active state.

- Active: The node is participating in a cluster.
  Authentication is required to modify the node.

In each of these states, some fields are read only.

Creating a storage cluster

You can create a storage cluster after you have configured all of the individual nodes. When you create a cluster, a cluster administrator user account is automatically created for you. The cluster administrator has permission to manage all cluster attributes and can create other cluster administrator accounts.

Before you begin

- You have installed the management node.
- You have configured all of the individual nodes.

About this task

During new node configuration, 1G or 10G Management IP (MIP) addresses are assigned to each node. You must use one of the node IP addresses created during configuration to open the Create a New Cluster page. The IP address you use depends on the network you have chosen for cluster management.

Note: When creating a new cluster, if you are using storage nodes that reside in a shared chassis, you might want to consider designing for chassis-level failure protection using the protection domains feature. Protection domains are automatically enabled with the appropriate node and chassis distribution.

Steps

1. In a browser window, enter a node MIP address.
2. In **Create a New Cluster**, enter the following information:
   - Management VIP: Routable virtual IP on the 1GbE or 10GbE network for network management tasks.

     Note: You can create a new cluster using IPv4 or IPv6 addressing.

   - iSCSI (storage) VIP: Virtual IP on the 10GbE network for storage and iSCSI discovery.

     Note: You cannot change the MVIP, SVIP, or cluster name after you create the cluster.

   - User name: The primary cluster administrator user name for authenticated access to the cluster. You must save the user name for future reference.

     Note: You can use uppercase and lowercase letters, special characters, and numbers for the user name and password.

   - Password: Password for authenticated access to the cluster. You must save the password for future reference.

   Two-way data protection is enabled by default. You cannot change this setting.
3. Read the End User License Agreement, and click **I Agree**.
4. Optional: In the Nodes list, ensure that the check boxes for nodes that should not be included in the cluster are not selected.

5. Click **Create Cluster**.

   The system might take several minutes to create the cluster depending on the number of nodes in the cluster. On a properly configured network, a small cluster of five nodes should take less than one minute. After the cluster is created, the Create a New Cluster window is redirected to the MVIP URL address for the cluster and displays the Element UI.

Accessing the Element software user interface

You can access the Element UI by using the management virtual IP (MVIP) address of the primary cluster node.

Before you begin

You must ensure that popup blockers and NoScript settings are disabled in your browser.

About this task

You can access the UI using IPv4 or IPv6 addressing, depending on configuration during cluster creation.

Steps

1. Choose one of the following:
   - IPv6: Enter `https://[IPv6 MVIP address]` For example:

     ```
     https://[fd20:8b1e:b256:45a::1234]/
     ```

   - IPv4: Enter `https://<IPv4 MVIP address>` For example:

     ```
     https://10.123.456.789/
     ```

2. For DNS, enter the host name.
3. Click through any authentication certificate messages.

Adding drives to a cluster

When you add a node to the cluster or install new drives in an existing node, the drives automatically register as available. You must add the drives to the cluster by using either the Element UI or API before they can participate in the cluster.

About this task

Drives are not displayed in the Available Drives list when the following conditions exist:

- Drives are in Active, Removing, Erasing, or Failed state.
- The node of which the drive is a part of is in Pending state.

Steps

1. From the Element user interface, select **Cluster > Drives**.
2. Click **Available** to view the list of available drives.
3. Do one of the following:

- To add individual drives, click the **Actions** icon for the drive you want to add and click **Add**.
- To add multiple drives, select the check boxes of the drives to add, click **Bulk Actions**, and click **Add**.

Configuring a Fibre Channel node

Fibre Channel nodes enable you to connect the cluster to a Fibre Channel network fabric. Fibre Channel nodes are added in pairs, and operate in active-active mode (all nodes actively process traffic for the cluster). Clusters running Element software version 9.0 and later support up to four nodes; clusters running previous versions support a maximum of two nodes.

You must ensure that the following conditions are met before you configure a Fibre Channel node:

- At least two Fibre Channel nodes are connected to Fibre Channel switches.
- All SolidFire Fibre Channel ports should be connected to your Fibre Channel fabric. The four SolidFire Bond10G network connections should be connected in one LACP bond group at the switch level. This will enable the best overall performance from the Fibre Channel systems.

Network and cluster configuration steps are the same for Fibre Channel nodes and storage nodes.

When you create a new cluster with Fibre Channel nodes and SolidFire storage nodes, the worldwide port name (WWPN) addresses for the nodes are available in the Element UI. You can use the WWPN addresses to zone the Fibre Channel switch.

WWPNs are registered in the system when you create a new cluster with nodes. In the Element UI, you can find the WWPN addresses from the WWPN column of the FC Ports tab, which you access from the Cluster tab.

Related tasks

Adding Fibre Channel nodes to a cluster on page 13
Creating a new cluster with Fibre Channel nodes on page 14

Adding Fibre Channel nodes to a cluster

You can add Fibre Channel nodes to a cluster when more storage is needed or during cluster creation. Fibre Channel nodes require initial configuration when they are first powered on. After the node is configured, it appears in the list of pending nodes and you can add it to a cluster.

About this task

The software version on each Fibre Channel node in a cluster must be compatible. When you add a Fibre Channel node to a cluster, the cluster installs the cluster version of Element on the new node as needed.

Steps

1. Select **Cluster** > **Nodes**.
2. Click **Pending** to view the list of pending nodes.
3. Do one of the following:
   - To add individual nodes, click the **Actions** icon for the node you want to add.
   - To add multiple nodes, select the check box of the nodes to add, and then **Bulk Actions**.

Note:

If the node you are adding has a different version of Element than the version running on the cluster, the cluster asynchronously updates the node to the version of Element running on the cluster master. After the node is updated, it automatically adds itself to the cluster. During this asynchronous process, the node will be in a pendingActive state.

4. Click **Add**.

   The node appears in the list of active nodes.

Creating a new cluster with Fibre Channel nodes

You can create a new cluster after you have configured the individual Fibre Channel nodes. When you create a cluster, a cluster administrator user account is automatically created for you. The cluster administrator has permission to manage all cluster attributes and can create other cluster administrator accounts.

Before you begin

You have configured the individual Fibre Channel nodes.

About this task

During new node configuration, 1G or 10G Management IP (MIP) addresses are assigned to each node. You must use one of the node IP addresses created during configuration to open the Create a New Cluster page. The IP address you use depends on the network you have chosen for cluster management.

Steps

1. In a browser window, enter a node MIP address.
2. In **Create a New Cluster**, enter the following information:
   - Management VIP: Routable virtual IP on the 1GbE or 10GbE network for network management tasks.
   - iSCSI (storage) VIP: Virtual IP on the 10GbE network for storage and iSCSI discovery.

     Note: You cannot change the SVIP after you create the cluster.

   - User name: The primary Cluster Admin user name for authenticated access to the cluster. You must save the user name for future reference.

     Note: You can use uppercase and lowercase letters, special characters, and numbers for the user name.

   - Password: Password for authenticated access to the cluster. You must save the user name for future reference.

   Two-way data protection is enabled by default. You cannot change this setting.
3. Read the End User License Agreement, and click **I Agree**.
4. Optional: In the Nodes list, ensure that the check boxes for nodes that should not be included in the cluster are not selected.
5. Click **Create Cluster**.

   The system might take several minutes to create the cluster depending on the number of nodes in the cluster. On a properly configured network, a small cluster of five nodes should take less than one minute. After the cluster is created, the Create a New Cluster window is redirected to the MVIP URL address for the cluster and displays the web UI.

Zoning for Fibre Channel nodes

When you create a new cluster with Fibre Channel nodes and SolidFire storage nodes, the worldwide port name (WWPN) addresses for the nodes are available in the web UI. You can use the WWPN addresses to zone the Fibre Channel switch.

WWPNs are registered in the system when you create a new cluster with nodes. In the Element UI, you can find the WWPN addresses from the WWPN column of the FC Ports tab, which you access from the Cluster tab.

Creating a volume access group for Fibre Channel clients

Volume access groups enable communication between Fibre Channel clients and volumes on a SolidFire storage system. Mapping Fibre Channel client initiators (WWPN) to the volumes in a volume access group enables secure data I/O between a Fibre Channel network and a SolidFire volume.

About this task

You can also add iSCSI initiators to a volume access group; this gives the initiators access to the same volumes in the volume access group.

Steps

1. Click **Management** > **Access Groups**.
2. Click **Create Access Group**.
3. Enter a name for the volume access group in the **Name** field.
4. Select and add the Fibre Channel initiators from the **Unbound Fibre Channel Initiators** list.

   Note: You can add or delete initiators at a later time.

5. Optional: Select and add an iSCSI initiator from the **Initiators** list.
6. To attach volumes to the access group, perform the following steps:
   a. Select a volume from the **Volumes** list.
   b. Click **Attach Volume**.
7. Click **Create Access Group**.

Setting up a management node

You can install the NetApp Element software management node (mNode). The management node is a virtual machine that runs in tandem with an Element software-based storage cluster. It is used to upgrade and provide system services including monitoring and telemetry, manage cluster assets and settings, run system tests and utilities, and enable NetApp Support access for troubleshooting.

Steps

1. Installing a management node on page 16
   You can manually install the management node for your cluster running NetApp Element software using the appropriate image for your configuration. This manual process is intended for SolidFire all-flash storage administrators and NetApp HCI administrators who are not using the NetApp Deployment Engine for management node installation.
2. Configuring a storage NIC (eth1) on page 20
   If you are using a second NIC for storage, you can SSH in to the management node or use the vCenter console and run a curl command to set up the network for eth1.
3. Enabling SolidFire Active IQ on page 21
   You can manually enable SolidFire Active IQ during the management node installation for your cluster running NetApp Element software.

Installing a management node

You can manually install the management node for your cluster running NetApp Element software using the appropriate image for your configuration. This manual process is intended for SolidFire all-flash storage administrators and NetApp HCI administrators who are not using the NetApp Deployment Engine for management node installation.

Before you begin

- Your cluster version must be running NetApp Element software 11.3 or later.
- Your installation uses IPv4. The management node 11.3 does not support IPv6.

  Note: You can use the management node 11.1 if you need IPv6 support.
- You have permissions to download software from the NetApp Support Site.
- You have identified the management node image type that is correct for your platform. See the following table for guidance:

Platform	Installation image type
Microsoft Hyper-V	`.iso`
KVM	`.iso`
VMware vSphere	`.iso`, `.ova`
Citrix XenServer	`.iso`
OpenStack	`.iso`

About this task

Prior to completing this procedure, you should have an understanding of persistent volumes and whether or not you want to use them. Persistent volumes allow management node data to be stored on a specified storage cluster so that data can be preserved in the event of management node loss or removal.

Steps

1. Download the OVA or ISO for your installation from the NetApp Support Site:
   - Element software: *https://mysupport.netapp.com/products/p/element_software.html*
   - NetApp HCI: *https://mysupport.netapp.com/products/p/hci.html*
   a. Select the version number of the software to download.
   b. Click **Go**.
   c. Read and click through the required prompts, accept the EULA, and select the management node image you want to download.
2. If you downloaded the OVA, follow these steps:
   a. Deploy the OVA.
   b. If your storage cluster is on a separate subnet from your management node (eth0) and you want to use persistent volumes, add a second network interface controller (NIC) to the VM on the storage subnet (eth1) or ensure that the management network can route to the storage network..
3. If you downloaded the ISO, follow these steps:
   a. Create a new 64-bit virtual machine from your hypervisor with the following configuration:
      - Six virtual CPUs
      - 12GB RAM
      - 400GB virtual disk, thin provisioned
      - One virtual network interface with internet access and access to the storage MVIP.
      - (Optional for SolidFire all-flash storage) One virtual network interface with management network access to the storage cluster. If your storage cluster is on a separate subnet from your management node (eth0) and you want to use persistent volumes, add a second network interface controller (NIC) to the VM on the storage subnet (eth1) or ensure that the management network can route to the storage network.

      Attention: Do not power on the virtual machine prior to the step indicating to do so later in this procedure.

   b. Attach the ISO to the virtual machine and boot to the `.iso` install image.

      Note: Installing a management node using the image might result in 30-second delay before the splash screen appears.
4. Power on the virtual machine for the management node after the installation completes.
5. Using the terminal user interface (TUI), create a management node admin user.

   Tip: To enter text, press **Enter** three times on the keyboard to open edit mode. After you enter text, press **Enter** again to close the edit mode. To navigate between fields, use the arrow keys.

6. Configure the management node network (eth0).

   Note: If you have a second NIC on eth1, see instructions on configuring a second NIC.

   Configuring a storage NIC (eth1)

7. SSH into the management node.

8. Using SSH, run the following command to gain root privileges. Enter your password when prompted:

   ```
   sudo su
   ```

9. Ensure time is synced (NTP) between the management node and the storage cluster.

   Note: In vSphere, the **Synchronize guest time with host** box should be checked in the VM options. Do not disable this option if you make future changes to the VM.

10. Configure the management node setup command:

    Note: You might be prompted to enter passwords or other information if you do not include them in the command. If your cluster is behind a proxy server, you must configure the proxy settings so you can reach a public network.

    ```
    /sf/packages/mnode/setup-mnode --mnode_admin_user [username] --
    storage_mvip [mvip] --storage_username [username] --telemetry_active
    [true]
    ```

    a. Replace the value in `[ ]` brackets (including the brackets) for each of the following required parameters:

       Note: The abbreviated form of the command name is in parentheses `( )` and can be substituted for the full name.

       --mnode_admin_user (-mu) [username]

       The username for the management node administrator account. This is likely to be the username for the user account you used to log into the management node.

       --storage_mvip (-sm) [MVIP address]

       The MVIP (management virtual IP address) of the storage cluster running Element software.

       --storage_username (-su) [username]

       The storage cluster administrator username for the cluster specified by the `--storage_mvip` parameter.

       --telemetry_active (-t) [true]

       Retain the value `true` that enables data collection for analytics by Active IQ.

    b. (Optional): Add password or Active IQ endpoint parameters to the command. You will be prompted to enter these passwords in a secure prompt if you do not include them in the command:

       --mnode_admin_password (-mp) [password]

       The password of the management node administrator account. This is likely to be the password for the user account you used to log into the management node.

       --storage_password (-sp) [password]

       The password of the storage cluster administrator specified by the `--storage_username` parameter.

--remote_host (-rh) [AIQ_endpoint]

The endpoint where Active IQ telemetry data is sent to be processed. If the parameter is not included, the default endpoint is used.

c. (Optional): Add the following persistent volume parameters:

Attention: Do not modify or delete the account and volumes created for persistent volumes functionality or a loss in management capability will result.

--use_persistent_volumes (-pv) [true/false, default: false]

Enable or disable persistent volumes. Enter the value `true` to enable persistent volumes functionality.

--persistent_volumes_account (-pva) [account_name]

If `--use_persistent_volumes` is set to `true`, use this parameter and enter the storage account name that will be used for persistent volumes.

Note: Use a unique account name for persistent volumes that is different from any existing account name on the cluster. It is critically important to keep the account for persistent volumes separate from the rest of your environment.

--persistent_volumes_mvip (-pvm) [mvip]

Enter the MVIP (management virtual IP address) of the storage cluster running Element software that will be used with persistent volumes. This is only required if multiple storage clusters are managed by the management node. If multiple clusters are not managed, the default cluster MVIP will be used.

d. Configure a proxy server:

--use_proxy (-up) [true/false, default: false]

Enable or disable the use of the proxy. This parameter is required to configure a proxy server.

--proxy_hostname_or_ip (-pi) [host]

The proxy hostname or IP. This is required if you want to use a proxy. If you specify this, you will be prompted to input `--proxy_port`.

--proxy_username (-pu) [username]

The proxy username. This parameter is optional.

--proxy_password (-pp) [password]

The proxy password. This parameter is optional.

--proxy_port (-pq) [port, default: 0]

The proxy port. If you specify this, you will be prompted to input the proxy host name or IP (`--proxy_hostname_or_ip`).

--proxy_ssh_port (-ps) [port, default: 443]

The SSH proxy port. This defaults to port 443.

11. (Optional) Use parameter help if you need additional information about each parameter:

--help (-h)

Returns information about each parameter. Parameters are defined as required or optional based on initial deployment. Upgrade and redeployment parameter requirements might vary.

12. Run the `setup-mnode` command.

13. Use the mNode API to add assets:

a. Using a browser, go to the storage MVIP and log in.

This action causes certificate to be accepted for the next step.

b. Using a browser, go to `https://<ManagementNodeIP>/mnode`.

c. Add a vCenter controller asset to the management node known assets for HCI monitoring (NetApp HCI installations only) and Hybrid Cloud Control (HCC):

d. Click **Authorize** and enter your MVIP user name and password credentials. Close the pop-up window.

e. Run **GET /assets** to pull the base asset ID needed to add the vCenter/controller asset.

f. Run **POST /assets/{ASSET_ID}/controllers** to add a controller asset with vCenter credentials.

g. For NetApp HCI or to access cloud services options in HCC, add a compute asset to the management node known assets:

Attention: You must perform this step or Cloud Services options will not be available from HCC.

h. Click **Authorize** and enter your MVIP user name and password credentials. Close the pop-up window.

i. Run **GET /assets** to pull the base asset ID needed to add the compute asset.

j. Run **POST/assets/{asset_id}/compute-nodes** to add a compute asset with credentials for the compute asset. The type is `ESXi Host`.

Configuring a storage NIC (eth1)

If you are using a second NIC for storage, you can SSH in to the management node or use the vCenter console and run a curl command to set up the network for eth1.

Before you begin

- You know your eth0 configuration details.
- Your cluster version is running NetApp Element software 11.3 or later.
- You have deployed a management node 11.3 or later.

Steps

1. Open an SSH or vCenter console.
2. Replace the values in the following command template (represented by `$`) for each of the required parameters for eth0 and eth1:

Note: The `cluster` object in the following template is optional and can be used for management node host name renaming. The `- -insecure` and the `-k` options should not be used in production environments.

```
curl -u $mnode-username:$mnode-password --insecure -X POST \
  https://$mnode_management_IP:442/json-rpc/10.0 \
  -H 'Content-Type: application/json' \
  -H 'cache-control: no-cache' \
  -d '  {
        "params": {
                "network": {
                        "eth0": {
                                "address": "$eth0_ip_mnode_management_IP",
                                "dns-nameservers": "$dns_ip_or_hostname",
                                "netmask": "$eth0_net_mask",
                                "gateway": "$gateway_IP",
```

```
                                "gatewayV6": ""
                        },
                        "eth1": {
                                "address": "$eth1_ip",
                                "netmask": "$eth1_netmask",
                                "status": "Up",
                                "method": "static",
                                "mtu": "9000"
                        }
      },
                "cluster": {
                        "name": "$desired_mNode_vm_hostname"
                }
        },
        "method": "SetConfig"
}
'
```

3. Run the command.

Enabling SolidFire Active IQ

You can manually enable SolidFire Active IQ during the management node installation for your cluster running NetApp Element software.

Before you begin

- Your cluster version must be running NetApp Element software 11.3 or later.

Step

1. Follow the instructions in management node installation information. The `--telemetry_active` parameter used in the setup script enables data collection for analytics by Active IQ.

   Installing a management node

Configuring a Fibre Channel node

Fibre Channel nodes enable you to connect the cluster to a Fibre Channel network fabric. Fibre Channel nodes are added in pairs, and operate in active-active mode (all nodes actively process traffic for the cluster). Clusters running Element software version 9.0 and later support up to four nodes; clusters running previous versions support a maximum of two nodes.

You must ensure that the following conditions are met before you configure a Fibre Channel node:

- At least two Fibre Channel nodes are connected to Fibre Channel switches.
- All SolidFire Fibre Channel ports should be connected to your Fibre Channel fabric. The four SolidFire Bond10G network connections should be connected in one LACP bond group at the switch level. This will enable the best overall performance from the Fibre Channel systems.

Network and cluster configuration steps are the same for Fibre Channel nodes and storage nodes.

When you create a new cluster with Fibre Channel nodes and SolidFire storage nodes, the worldwide port name (WWPN) addresses for the nodes are available in the Element UI. You can use the WWPN addresses to zone the Fibre Channel switch.

WWPNs are registered in the system when you create a new cluster with nodes. In the Element UI, you can find the WWPN addresses from the WWPN column of the FC Ports tab, which you access from the Cluster tab.

Related tasks

Adding Fibre Channel nodes to a cluster on page 13
Creating a new cluster with Fibre Channel nodes on page 14

Adding Fibre Channel nodes to a cluster

You can add Fibre Channel nodes to a cluster when more storage is needed or during cluster creation. Fibre Channel nodes require initial configuration when they are first powered on. After the node is configured, it appears in the list of pending nodes and you can add it to a cluster.

About this task

The software version on each Fibre Channel node in a cluster must be compatible. When you add a Fibre Channel node to a cluster, the cluster installs the cluster version of Element on the new node as needed.

Steps

1. Select **Cluster > Nodes**.
2. Click **Pending** to view the list of pending nodes.
3. Do one of the following:
   - To add individual nodes, click the **Actions** icon for the node you want to add.
   - To add multiple nodes, select the check box of the nodes to add, and then **Bulk Actions**.

   Note:

   If the node you are adding has a different version of Element than the version running on the cluster, the cluster asynchronously updates the node to the version of Element running on the

cluster master. After the node is updated, it automatically adds itself to the cluster. During this asynchronous process, the node will be in a pendingActive state.

4. Click **Add**.

   The node appears in the list of active nodes.

Creating a new cluster with Fibre Channel nodes

You can create a new cluster after you have configured the individual Fibre Channel nodes. When you create a cluster, a cluster administrator user account is automatically created for you. The cluster administrator has permission to manage all cluster attributes and can create other cluster administrator accounts.

Before you begin

You have configured the individual Fibre Channel nodes.

About this task

During new node configuration, 1G or 10G Management IP (MIP) addresses are assigned to each node. You must use one of the node IP addresses created during configuration to open the Create a New Cluster page. The IP address you use depends on the network you have chosen for cluster management.

Steps

1. In a browser window, enter a node MIP address.
2. In **Create a New Cluster**, enter the following information:
   - Management VIP: Routable virtual IP on the 1GbE or 10GbE network for network management tasks.
   - iSCSI (storage) VIP: Virtual IP on the 10GbE network for storage and iSCSI discovery.

     Note: You cannot change the SVIP after you create the cluster.

   - User name: The primary Cluster Admin user name for authenticated access to the cluster. You must save the user name for future reference.

     Note: You can use uppercase and lowercase letters, special characters, and numbers for the user name.

   - Password: Password for authenticated access to the cluster. You must save the user name for future reference.

   Two-way data protection is enabled by default. You cannot change this setting.
3. Read the End User License Agreement, and click **I Agree**.
4. Optional: In the Nodes list, ensure that the check boxes for nodes that should not be included in the cluster are not selected.
5. Click **Create Cluster**.

   The system might take several minutes to create the cluster depending on the number of nodes in the cluster. On a properly configured network, a small cluster of five nodes should take less than one minute. After the cluster is created, the Create a New Cluster window is redirected to the MVIP URL address for the cluster and displays the web UI.

Zoning for Fibre Channel nodes

When you create a new cluster with Fibre Channel nodes and SolidFire storage nodes, the worldwide port name (WWPN) addresses for the nodes are available in the web UI. You can use the WWPN addresses to zone the Fibre Channel switch.

WWPNs are registered in the system when you create a new cluster with nodes. In the Element UI, you can find the WWPN addresses from the WWPN column of the FC Ports tab, which you access from the Cluster tab.

Creating a volume access group for Fibre Channel clients

Volume access groups enable communication between Fibre Channel clients and volumes on a SolidFire storage system. Mapping Fibre Channel client initiators (WWPN) to the volumes in a volume access group enables secure data I/O between a Fibre Channel network and a SolidFire volume.

About this task

You can also add iSCSI initiators to a volume access group; this gives the initiators access to the same volumes in the volume access group.

Steps

1. Click **Management > Access Groups**.
2. Click **Create Access Group**.
3. Enter a name for the volume access group in the **Name** field.
4. Select and add the Fibre Channel initiators from the **Unbound Fibre Channel Initiators** list.

   Note: You can add or delete initiators at a later time.
5. Optional: Select and add an iSCSI initiator from the **Initiators** list.
6. To attach volumes to the access group, perform the following steps:
   a. Select a volume from the **Volumes** list.
   b. Click **Attach Volume**.
7. Click **Create Access Group**.

Contacting NetApp Support

If you need help with or have questions or comments about NetApp products, contact NetApp Support.

- Web:
  mysupport.netapp.com
- Phone:
  - 888.4.NETAPP (888.463.8277) (US and Canada)
  - 00.800.44.638277 (EMEA/Europe)
  - +800.800.80.800 (Asia/Pacific)

Where to find product documentation and other information

You can learn more about using and managing NetApp HCI and SolidFire all-flash storage from the resources available in the Documentation Centers and Resources pages for both products.

In the Documentation Centers, you can also find information about hardware installation and maintenance, additional content resources available, links to known issues and resolved issues, and the latest release notes. On the Resources pages, you can find links to data sheets, technical reports, white papers, and videos.

- *NetApp HCI Documentation Center*
- *NetApp HCI Resources page*
- *SolidFire and Element 11.3 Documentation Center*
- *SolidFire Resources page*

Copyright

Trademark

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