Configure SolidFire system options after deployment

Element Software

NetApp
June 10, 2024

Table of Contents

Configure SolidFire system options after deployment

After you set up your SolidFire system, you might want to perform some optional tasks.

If you change credentials in the system, you might want to know the impact on other components.

Additionally, you can configure settings for multi-factor authentication, external key management, and Federal Information Processing Standards (FIPS) security. You should also look at updating passwords when needed.

Find more information

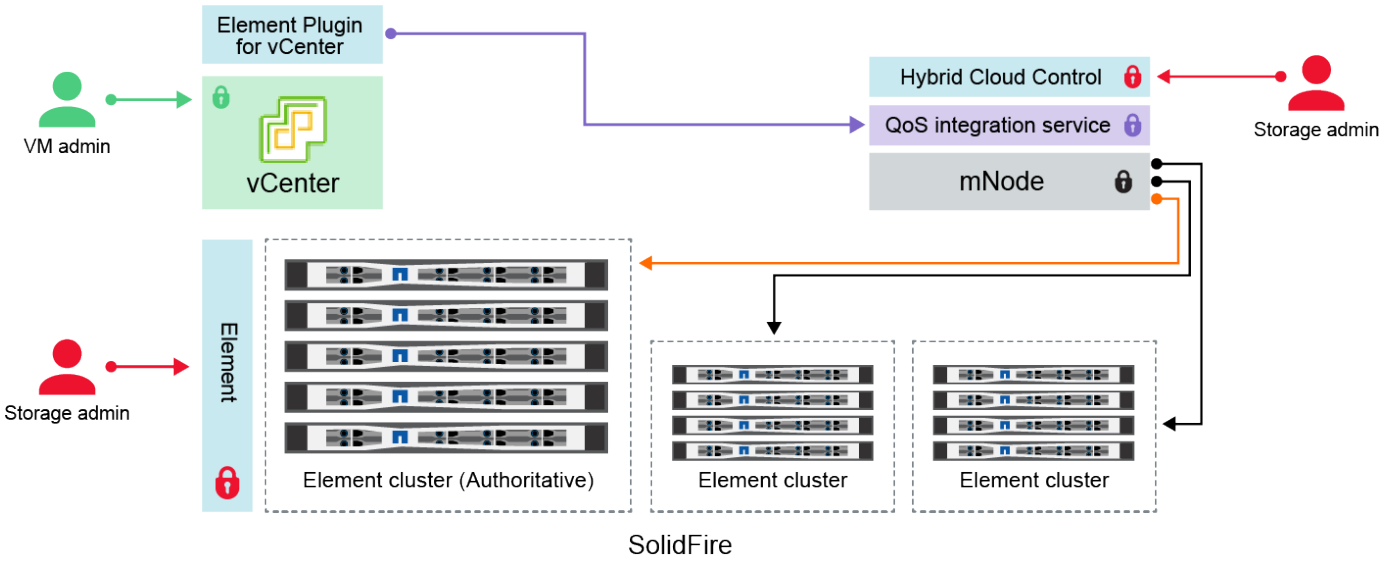
- Change credentials in NetApp HCI and NetApp SolidFire
- Change the Element software default SSL certificate
- Change the IPMI password for nodes
- Enable multi-factor authentication
- Get started with external key management
- Create a cluster supporting FIPS drives

Change credentials in NetApp HCI and NetApp SolidFire

Depending on the security policies in the organization that deployed NetApp HCI or NetApp SolidFire, changing credentials or passwords is commonly part of the security practices. Before you change passwords, you should be aware of the impact on other software components in the deployment.

If you change credentials for one component of a NetApp HCI or NetApp SolidFire deployment, the following table provides guidance as to the impact on other components.

NetApp SolidFire component interactions:



Credential Type and Icon	Usage by Admin	See these instructions
Element credentials 	**Applies to**: NetApp HCI and SolidFire Admins use these credentials to log into: • Element user interface on the Element storage cluster • Hybrid Cloud Control on the management node (mnode) When Hybrid Cloud Control manages multiple storage clusters, it accepts only the admin credentials for the storage clusters, known as the *authoritative cluster* that the mnode was initially set up for. For storage clusters later added to Hybrid Cloud Control, the mnode securely stores admin credentials. If credentials for subsequently added storage clusters are changed, the credentials must also be updated in the mnode using the mnode API.	• Update the storage cluster admin passwords. • Update the storage cluster admin credentials in the mnode using the modifyclusteradmin API.

Credential Type and Icon	Usage by Admin	See these instructions
vSphere Single Sign-on credentials 	**Applies to**: NetApp HCI only Admins use these credentials to log into the VMware vSphere Client. When vCenter is part of the NetApp HCI installation, credentials are configured in the NetApp Deployment Engine as the following: • username@vsphere.local with the specified password, and • administrator@vsphere.local with the specified password. When an existing vCenter is used to deploy NetApp HCI, the vSphere Single Sign-on credentials are managed by the IT VMware admins.	Update vCenter and ESXi credentials.
Baseboard management controller (BMC) credentials 	**Applies to**: NetApp HCI only Administrators use these credentials to log in to the BMC of the NetApp compute nodes in a NetApp HCI deployment. The BMC provides basic hardware monitoring and virtual console capabilities. BMC (sometimes referred to as *IPMI*) credentials for each NetApp compute node are stored securely on the mnode in NetApp HCI deployments. NetApp Hybrid Cloud Control uses BMC credentials in a service account capacity to communicate with the BMC in the compute nodes during compute node firmware upgrades. When the BMC credentials are changed, the credentials for the respective compute nodes must be updated also on the mnode to retain all Hybrid Cloud Control functionality.	• Configure IPMI for each node on NetApp HCI. • For H410C, H610C, and H615C nodes, change default IPMI password. • For H410S and H610S nodes, change default IPM password. • Change BMC credentials on the management node.
ESXi credentials 	**Applies to**: NetApp HCI only Admins can log into ESXi hosts using either SSH or the local DCUI with a local root account. In NetApp HCI deployments, the username is 'root' and the password was specified during the initial installation of that compute node in NetApp Deployment Engine. ESXi root credentials for each NetApp compute node are stored securely on the mnode in NetApp HCI deployments. NetApp Hybrid Cloud Control uses the credentials in a service account capacity to communicate with ESXi hosts directly during compute node firmware upgrades and health checks. When the ESXi root credentials are changed by a VMware admin, the credentials for the respective compute nodes must be updated on the mnode to retain Hybrid Cloud Control functionality.	Update credentials for vCenter and ESXi hosts.

Credential Type and Icon	Usage by Admin	See these instructions
QoS integration password 	**Applies to**: NetApp HCI and optional in SolidFire Not used for interactive logins by admins. The QoS integration between VMware vSphere and Element Software is enabled via: • Element Plug-in for vCenter Server, and • QoS service on the mnode. For authentication, the QoS service uses a password that is exclusively used in this context. The QoS password is specified during the initial installation of the Element Plug-in for vCenter Server, or auto-generated during NetApp HCI deployment. No impact on other components.	Update QoSSIOC credentials in the NetApp Element Plug-in for vCenter Server. The NetApp Element Plug-in for vCenter Server SIOC password is also known as the *QoSSIOC password*. Review the Element Plug-in for vCenter Server KB article.
vCenter Service Appliance credentials 	**Applies to**: NetApp HCI only if set up by NetApp Deployment Engine Admins can log into the vCenter Server appliance virtual machines. In NetApp HCI deployments, the username is 'root' and the password was specified during the initial installation of that compute node in the NetApp Deployment Engine. Depending on the VMware vSphere version deployed, certain admins in the vSphere Single Sign-on domain can also log in to the appliance. No impact on other components.	No changes needed.
NetApp Management Node admin credentials 	**Applies to**: NetApp HCI and optional in SolidFire Admins can log into the NetApp management node virtual machines for advanced configuration and troubleshooting. Depending on the management node version deployed, login via SSH is not enabled by default. In NetApp HCI deployments, the username and password was specified by the user during the initial installation of that compute node in NetApp Deployment Engine. No impact on other components.	No changes needed.

Find more information

- Change the Element software default SSL certificate
- Change the IPMI password for nodes

- Enable multi-factor authentication
- Get started with external key management
- Create a cluster supporting FIPS drives

Change the Element software default SSL certificate

You can change the default SSL certificate and private key of the storage node in the cluster using the NetApp Element API.

When a NetApp Element software cluster is created, the cluster creates a unique self-signed Secure Sockets Layer (SSL) certificate and private key that is used for all HTTPS communication via the Element UI, per-node UI, or APIs. Element software supports self-signed certificates as well as certificates that are issued and verified by a trusted Certificate Authority (CA).

You can use the following API methods to get more information about the default SSL certificate and make changes.

- **GetSSLCertificate**

  You can use the GetSSLCertificate method to retrieve information about the currently installed SSL certificate including all certificate details.

- **SetSSLCertificate**

  You can use the SetSSLCertificate method to set the cluster and per-node SSL certificates to the certificate and private key you supply. The system validates the certificate and private key to prevent an invalid certificate from being applied.

- **RemoveSSLCertificate**

  The RemoveSSLCertificate method removes the currently installed SSL certificate and private key. The cluster then generates a new self-signed certificate and private key.

> The cluster SSL certificate is automatically applied to all new nodes added to the cluster. Any node removed from the cluster reverts to a self-signed certificate and all user-defined certificate and key information is removed from the node.

Find more information

- Change the management node default SSL certificate
- What are the requirements around setting custom SSL certificates in Element Software?
- SolidFire and Element Software Documentation
- NetApp Element Plug-in for vCenter Server

Change default IPMI password for nodes

You can change the default Intelligent Platform Management Interface (IPMI) administrator password as soon as you have remote IPMI access to the node. You might want to do this if there were any installation updates.

For details about configuring IPM access for nodes, see Configure IPMI for each node.

You can change the IPM password for these nodes:

- H410S nodes
- H610S nodes

Change the default IPMI password for H410S nodes

You should change the default password for the IPMI administrator account on each storage node as soon as you configure the IPMI network port.

What you'll need

You should have configured the IPMI IP address for each storage node.

Steps

1. Open a web browser on a computer that can reach the IPMI network and browse to the IPMI IP address for the node.
2. Enter the user name `ADMIN` and password `ADMIN` in the login prompt.
3. Upon logging in, click the **Configuration** tab.
4. Click **Users**.
5. Select the `ADMIN` user and click **Modify User**.
6. Select the **Change Password** check box.
7. Enter a new password in the **Password** and **Confirm Password** fields.
8. Click **Modify**, and then click **OK**.
9. Repeat this procedure for any other H410S nodes with default IPMI passwords.

Change the default IPMI password for H610S nodes

You should change the default password for the IPMI administrator account on each storage node as soon as you configure the IPMI network port.

What you'll need

You should have configured the IPMI IP address for each storage node.

Steps

1. Open a web browser on a computer that can reach the IPMI network and browse to the IPMI IP address for the node.
2. Enter the user name `root` and password `calvin` in the login prompt.
3. Upon logging in, click the menu navigation icon at the top left of the page to open the sidebar drawer.
4. Click **Settings**.
5. Click **User Management**.
6. Select the **Administrator** user from the list.
7. Enable the **Change Password** check box.
8. Enter a new, strong password in the **Password** and **Confirm Password** fields.

9. Click **Save** at the bottom of the page.
10. Repeat this procedure for any other H610S nodes with default IPMI passwords.

Find more information

- SolidFire and Element Software Documentation
- NetApp Element Plug-in for vCenter Server

Copyright information

Trademark information