Technical Report

NetApp HCI Security Hardening Guide

Guidelines for Secure Deployment of NetApp HCI

James Bradshaw, NetApp HCI Product Team, NetApp

December 2020 | TR-4860

Abstract

This technical report provides guidance and configuration settings for NetApp HCI to help organizations meet prescribed security objectives for information system confidentiality, integrity, and availability.

TABLE OF CONTENTS

Introduction

The evolution of the current threat landscape presents an organization with unique challenges for protecting its most valuable assets: data and information. The advanced and dynamic threats and vulnerabilities that organizations face are ever-increasing in sophistication. Coupled with an increase in the effectiveness of obfuscation and surveillance techniques on the part of potential intruders, system managers must address the security of data and information proactively. This guide seeks to assist operators and administrators in that task by leveraging the confidentiality, integrity, and availability integral to the NetApp HCI Solution.

NetApp HCI Security Solutions

NetApp HCI eliminates the pain points of legacy IT operations that lead to infrastructure silos. Check out the NetApp HCI Solutions Catalog where you will find a number of validated solutions to help simplify your multi-application, multi-cloud environment.

NetApp has partnered with Coalfire and HyTrust to provide solutions to fully validated multitenant solution that integrates with HyTrust CloudControl (HTCC) and DataControl to meet the key security measures for FISMA as defined in NIST SP 800-53 Revision 4 and Payment Card Industry Data Security Standard (PCI DSS) V3.2.1.

Security Based HCI Solutions

- NetApp HCI - NIST Security Controls for FISMA with HyTrust for Multitenant Infrastructure
- NetApp HCI Verified Reference Architecture for PCI DSS 3.2.1

System Management

NetApp HCI provides multiple options to manage all components in the HCI stack. This section describes each method and best practice for your NetApp HCI environment.

Out-Of-Band Management

All NetApp HCI nodes provide additional out-of-band management capabilities through a dedicated management port. NetApp H410C, H410S, H610S, and H615C nodes also allow for baseboard management controller (BMC) access through a dedicated port.

See the following guidelines for hardware appliance nodes:

- You should change default passwords, and NetApp recommends user access to AD/LDAP for better user control and auditing.
- If the appliance has a BMC, be aware that the BMC management port allows low-level hardware access. Connect the BMC management port only to a secure, trusted, internal management network. If no such network is available, leave the BMC management port unconnected or blocked unless a BMC connection is requested by technical support.
- If the appliance supports remote management of the controller hardware over Ethernet using the Intelligent Platform Management Interface (IPMI) standard, block untrusted traffic on port 623.

Command-Line Management

VMware

By default, SSH is disabled in vCenter and vSphere. It is best practice to leave the SSH protocol disabled if not in use.

Enable or Disable SSH for vCenter

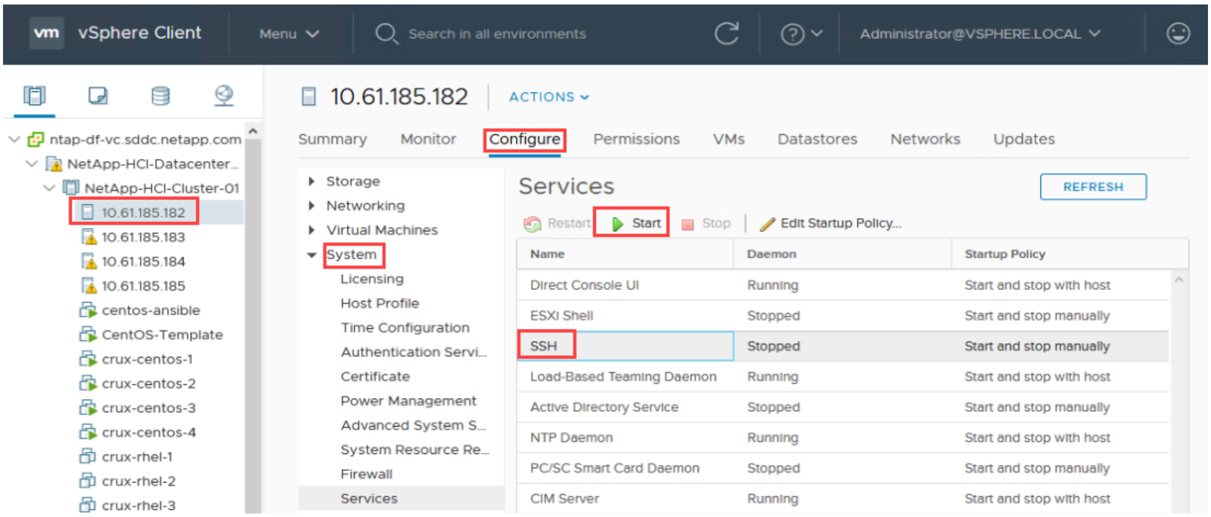
To enable the vCenter Server Appliance (VCSA) in the vCenter Server Appliance Management Interface (VAMI), use the following steps:

1. Log in to the VAMI as root.
2. Click Access and then Edit.
3. Edit the access settings for the VCSA.

For more information, see Enable or Disable SSH and Bash Shell Access.

Enable or Disable SSH for vSphere

To enable SSH for an ESXi host, log into vCenter and select Host > Configure > System > SSH > Start.



Services

Name	Daemon	Startup Policy
Direct Console UI	Running	Start and stop with host
ESXi Shell	Stopped	Start and stop manually
SSH	Stopped	Start and stop manually
Load-Based Teaming Daemon	Running	Start and stop with host
Active Directory Service	Stopped	Start and stop manually
NTP Daemon	Running	Start and stop with host
PC/SC Smart Card Daemon	Stopped	Start and stop manually
CIM Server	Running	Start and stop with host

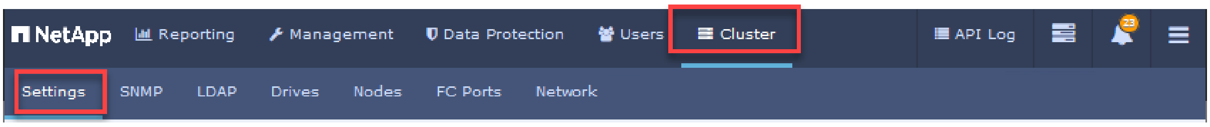
For more information, see: Using ESXi Shell in ESXi 5.x, 6.x, and 7.x (2004746).

Element

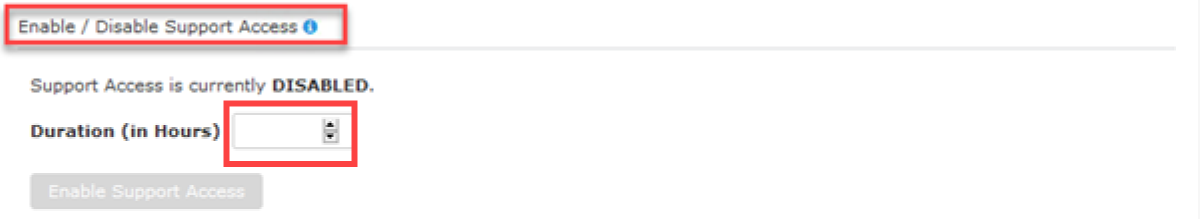
By default, SSH is disabled. SSH is enabled and disabled with the Support Access option in the Element UI. Support access is enabled to allow temporary access to the Element storage cluster by NetApp.

To enable SSH for Element Storage, complete the following steps:

1. Log into Element.
2. Select Cluster > Settings.
3. Enter the time duration in the Enable / Disable Support Access section in the form of hours.



Support access can only be enabled for a minimum of 1 hour and a maximum of 24 hours. If you require a duration longer than 24 hours, you can use the Element API to set the desired time.



Enable / Disable Support Access

Support Access is currently **DISABLED**.

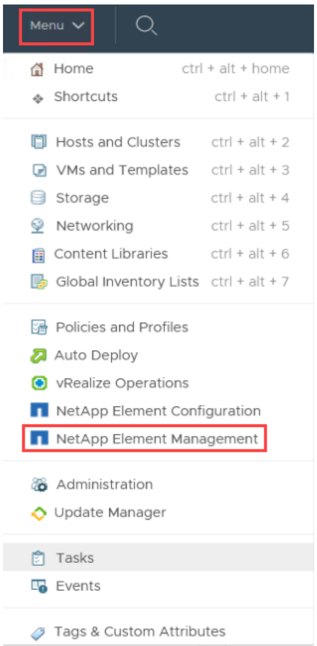
Duration (in Hours)

Graphical User Interface (GUI) Options

NetApp Element Plug-in for vCenter Server (VCP)

Administrators have the option to use the built-in NetApp Element Plug-in for vCenter Server (VCP), which is a web-based tool integrated with the VMware vSphere Web Client user interface (UI). The plug-in is an extension and alternative scalable, user-friendly interface for VMware vSphere that can manage and monitor storage clusters running NetApp Element software.

You can use the plug-in user interface to discover and configure clusters and to manage, monitor, and allocate storage from cluster capacity to configure datastores and virtual datastores (for virtual volumes). A cluster appears on the network as a single local group that is represented to hosts and administrators by virtual IP addresses. You can also monitor cluster activity with real-time reporting, including error and alert messaging for any event that might occur while performing various operations.


Menu
Home ctrl + alt + home
Shortcuts ctrl + alt + 1
Hosts and Clusters ctrl + alt + 2
VMs and Templates ctrl + alt + 3
Storage ctrl + alt + 4
Networking ctrl + alt + 5
Content Libraries ctrl + alt + 6
Global Inventory Lists ctrl + alt + 7
Policies and Profiles
Auto Deploy
vRealize Operations
NetApp Element Configuration
NetApp Element Management
Administration
Update Manager
Tasks
Events
Tags & Custom Attributes

NetApp Element Software User Interface

Element is the storage operating system at the heart of an Element cluster. Element software runs independently on all nodes in the cluster and enables the nodes of the cluster to combine resources and present as a single storage system to external clients. Element software is responsible for cluster all coordination, scale, and management of a system. The Element software user interface is built upon the Element API and served through HTTPS from the cluster’s MVIP. Additionally, each node has a per-node UI which is accessible at https://<NodeIP>:442. Note that the node UI requires the addition of port 442 to the URL.

Management via API

Within NetApp HCI, both Element and VMware provide access to an API to accomplish everyday administrative tasks.

Element Storage

Element software allows you to use a set of objects, methods, and routines to manage Element storage. The Element API is based on the JSON-RPC protocol over HTTPS. You can monitor API operations in the Element UI by enabling the API Log; this allows you to see the methods that are being issued to the system. You can enable both requests and responses to see how the system replies to the methods that are issued.

Please see the NetApp Element 12.0 API Reference Guide for more details.

VMware

You can monitor API operations for VMware specific products; see VMware's API and SDK documentation.

Management Node (mNode)**

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

Note: The mNode enables Element Plug-in for vCenter Server (VCP) and Hybrid Cloud Control (HCC) features.

Login and Password Parameters

An effective security posture adheres to established organizational policies, guidelines, and any governance or standards that apply to the organization. Examples of these requirements include user-name lifetime, password-length requirements, character requirements, and the storage of such accounts. The NetApp HCI solution provides features and functions to address these security constructs.

SHA-512 Support

To enhance password security, Element and VMware supports the SHA-2 password hash function and defaults to using SHA-512 for hashing newly created or changed passwords. Operators and administrators can also expire or lock accounts as needed.

Preexisting Element 11.5 user accounts with unchanged passwords continue to use the MD5 hash function after the upgrade to Element 11.5 or later.

Note: NetApp strongly recommends that these user accounts migrate to the more secure SHA-512 solution by having users change their passwords.

Role-Based Access Control (RBAC)

You can maximize the security and manageability of your NetApp HCI environment by following best practices for roles and permissions.

Local Users

In greenfield deployments, the initial local cluster administrator accounts are created for Element and vCenter clusters when using the NetApp Deployment Engine (NDE). This account is used to conduct initial administrative tasks in Element and vCenter environments.

In brownfield deployments, NetApp HCI leverages existing RBAC implementations.

Lightweight Directory Application Protocol (LDAP/LDAPS)

Both Element and VMware supports the Lightweight Directory Application Protocol (LDAP/LDAPS) and Active Directory. With LDAP/Active Directory user accounts, administrators can create, modify, or delete custom access control roles, and they can specify account restrictions for specific users.

With RBAC, local users have access to only the systems and options that are required for their job roles and functions. The RBAC solution within VMware and Element limits users' administrative access to the level granted for their defined role, which allows administrators to manage local users by assigned roles.

Multi-factor authentication (MFA)

Multi-factor authentication (MFA) uses a third-party Identity Provider (IdP) via the Security Assertion Markup Language (SAML) to manage user sessions. MFA enables administrators to configure additional factors of authentication as required, such as password and text message, and password and email message.

Best Practices

- Configure one or more RBAC instances for added security for Element and VMware products.
- NetApp recommends the following password standards:
  - By default, you must include a mix of lowercase letters, uppercase letters, numbers, and special characters when creating a password.
  - By default, password length is more than 7 and less than 40 characters.
  - Passwords cannot contain a dictionary word or part of a dictionary word.
- For multiple users, only grant permissions on objects where they are needed and assign privileges only to users or groups that must have them.

For more information for individual RBAC solutions and implementation please see the following resources:

- Managing cluster administrator user accounts in the NetApp Element User Guide
- Enabling multi-factor authentication in the NetApp Element User Guide
- Configuring vCenter Single Sign-On Identity Sources in the VMware vSphere Product Documentation
- Best Practices for Roles and Permissions in VMware vSphere Product Documentation

The following table lists default users in greenfield deployments.

Local User	Brief Description
administrator	Top-level administrative account for element
administrator@vsphere.local	Top-level administrative account for vCenter

The following table lists element user types for cluster administrators.

Local User	Brief Description
Cluster Admin	Top-level administrative account
LDAP	Enables LDAP administrators to centrally manage the cluster
IDP	Enables MFA administrators to the centrally manage the cluster

This table lists element user permissions for cluster administrators.

Privileges	Brief Description
Reporting	Provide access to reporting for Element Cluster
Volumes	Provide access to Volume information for Element Cluster
Accounts	Provide access to Account information for Element Cluster
Nodes	Provide access to Nodes information for Element Cluster
Drives	Provide access to Drives information for Element Cluster
Administrator	Provides full access to Element Cluster

The following table lists default VMware local users and domains.

Local User	Brief Description
root	Local ESXi administrative account
{Local user}@vsphere.local	Local vCenter administrative account
vsphere.local	Local vCenter Single Sign-on Domain

System Auditing

Event Notification

Event notifications for both Element and vCenter are listed in vCenter. For issues that require manual intervention in Element, follow the steps to access reporting.

Event Notification in Element

You can review event logs for operations performed on the selected cluster along with cluster faults that might occur. Most errors are resolved automatically by the system. Other faults might require manual intervention.

To review event logs in Element, complete the following steps:

1. Select NetApp Element Management > Reporting. If two or more clusters are added, the cluster you intend to use for the task must be selected.

2. Click Event Log. The page displays a list of all events on the cluster.

3. Select an individual event that you want to review.

4. Select Details. The message displays the cluster event details.

Forwarding Syslog

Log and audit information is invaluable to an organization from a support and availability standpoint. In addition, the information and details contained in logs (syslog), audit reports, and outputs are generally of a sensitive nature. To maintain security controls and posture, it is imperative that organizations manage log and audit data in a secure manner.

Offloading of syslog information is necessary for limiting the scope or footprint of a breach to a single system or solution. Therefore, NetApp recommends securely offloading syslog information to a secure storage or retention location.

To do so, run the following API call:

```
https://mvip/json-
rpc/1.0?method=Set...remoteHosts=[{"host":"<IP_hostA>","port":10514},{"host":"<IP_hostB>","por
t":10515},...]
```

The logging server must monitor on TCP. SolidFire sends logs through TCP only, not UDP. Everything that is logged to /var/log/* on the storage nodes is sent to the syslog server and collected in each log file name.

Example: Every node's sf-master.info log files are gathered in one sf-master.info log file on the syslog server.

To forward vCenter server log files to a remote syslog Server, complete the following steps:

1. In the vCenter Server Management Interface, select Syslog.
2. In the Forwarding Configuration section, click Configure if you have not configured any remote syslog hosts. Click Edit if you already have configured hosts.
3. In the Create Forwarding Configuration pane, enter the server address of the destination host. The maximum number of supported destination hosts is three.
4. From the Protocol drop-down menu, select the protocol to use.

Menu Item	Description
TLS	Transport Layer Security
TCP	Transmission Control Protocol
RELP	Reliable Event Logging Protocol
UDP	User Datagram Protocol

5. In the Port text box, enter the port number to use for communication with the destination host.
6. In the Create Forwarding Configuration pane, click Add to enter another remote syslog server.
7. Click Save.
8. Verify that the remote syslog server is receiving messages.
9. In the Forwarding Configuration section, click Send Test Message.
10. Verify that the test message was received on the remote syslog server.

The new configuration settings are shown in the Forwarding Configuration section.

NetApp 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.

ActiveIQ can be access here.

SNMP Monitoring

Both Element and VMware supports alert notifications to be sent through email, SNMP traps, and Syslog. Alerts notify administrators about important events that occur on the storage array. Element supports SNMPv3c and version 3, which supports authentication and encryption.

Capabilities include the following:

- SNMP requestor
- Select which version of SNMP to use
- Identify the SNMP User-based Security Model (USM) user
- Configure traps to monitor

For more information on configuring SNMP, complete the following steps:

Confgure SNMP for Element.

Configure SNMP for ESXi

Configure SNMP Settings for vCenter Server

Note: For security reasons, NetApp recommends not configuring SNMP. Rather, you should configure secure Syslog instead.

Note: If a secure Syslog is unavailable, NetApp recommends configuring the SNMP community string to secure it. SNMP community string is like a user ID or password that allows access to a device's statistics.

Data Security and Integrity

Element clusters allow you to encrypt all data stored on the cluster. All drives in storage nodes capable of encryption use AES 256-bit encryption at the drive level. Each drive has its own encryption key, which is created when the drive is first initialized. When you enable the encryption feature, a cluster-wide password is created, and chunks of the password are then distributed to all nodes in the cluster. No single node stores the entire password. The password is then used to password-protect all access to the drives. The password is needed to unlock the drive, and it is not needed unless power is removed from the drive or the drive is locked.

Enabling the encryption at rest feature does not affect performance or efficiency on the cluster. Additionally, if an encryption-enabled drive or node is removed from the cluster with the Element API or Element UI, encryption at rest will be disabled on the drives. After the drive is removed, the drive can be secure erased by using the Secure erase drives API method. If a drive or node is forcibly removed from the cluster, the data remains protected by the cluster-wide password and the drive’s individual encryption keys.

With NetApp Element software, you can choose to enable Federal Information Processing Standards (FIPS) 140-2 operating mode on your cluster. Enabling this mode activates the NetApp Cryptographic Security Module (NCSM) and leverages FIPS 140-2 Level 1 certified encryption for all communication with HTTPS to the NetApp Element UI and API.

Enabling FIPS drives

Security is becoming increasingly critical for the deployment of solutions in many customer environments. Federal Information Processing Standards (FIPS) are standards for computer security and interoperability. FIPS 140-2 certified encryption for data at rest is a component of the overall security solution.

For more information, see Creating a cluster supporting FIPS drives and NetApp Element 12.0 API Reference Guide.

Enabling FIPS 140-2 for HTTPS

With NetApp Element software, you can enable Federal Information Processing Standards (FIPS) 140-2 operating mode on your cluster. Enabling this mode activates the NetApp Cryptographic Security Module (NCSM) and leverages FIPS 140-2 Level 1 certified encryption for all communication through HTTPS to the NetApp Element UI and API.

The following is an example of the API request to enable FIPS on Element:

```
{
"method": "EnableFeature",
"params": {
"feature" : "fips"
},
"id": 1
}
```

After this operating mode is enabled, all HTTPS communication uses the FIPS 140-2-approved ciphers.

For more information, see Enabling FIPS 140-2 for HTTPS on your cluster and NetApp Element 12.0 API Reference Guide.

SED and Key Management

External key management (EKM) provides secure Authentication Key (AK) management in conjunction with an off-cluster external key server (EKS). The EKS provides secure generation and storage of AKs.

The AKs are used to lock and unlock Self Encrypting Drives (SEDs) when Encryption At Rest (EAR) is enabled on the cluster. The cluster utilizes the Key Management Interoperability Protocol (KMIP), an OASIS defined standard protocol, to communicate with the EKS.

See Getting Started with External Key Management for the following subjects:

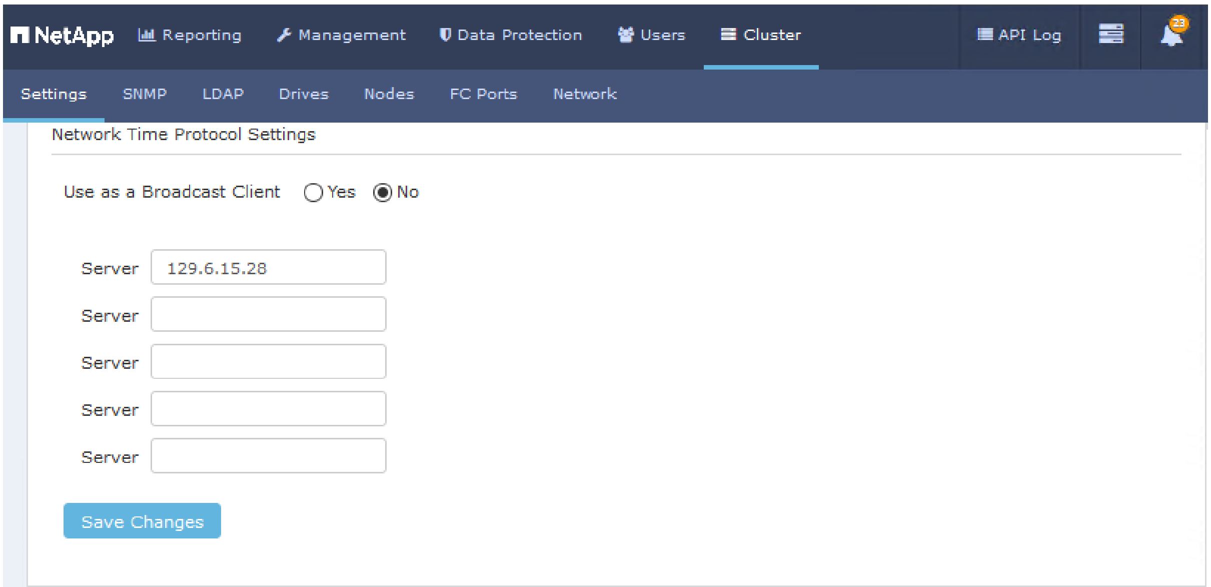
- Set up External key management via API
- Recover inaccessible or invalid Authentication Keys
- External Key Management API Commands.
- Keeping VMware vSphere up to date

  Need more explanation from prod team for this process.

Network Time Protocol

Element System Manager (Cluster> Settings > Network Time Protocol Settings) enables you to configure Network Time Protocol (NTP) servers to synchronize the cluster time with external NTP servers. NTP on HCI does not support secure NTP. Without the ability to cryptographically sign packets for authentication, an NTP server can be susceptible to man-in-the-middle attacks.

NetApp recommends using NTP servers that are internal to your network.



Network Time Protocol Settings

Use as a Broadcast Client ○ Yes ● No

Server 129.6.15.28

Server

Server

Server

Server

For details, see the NetApp Element 12.0 API Reference Guide in the ONTAP 9 Documentation Center.

Installing CA-Signed Digital Certificate

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

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

- **GetSSLCertificate.** You can use this method to retrieve information about the currently installed SSL certificate including all certificate details.
- **SetSSLCertificate.** You can use this 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.** This method removes the currently installed SSL certificate and private key. The cluster then generates a new self-signed certificate and private key.

For information about each method, see the NetApp Element Software API Reference Guide.

TLS and SSL

SSL ciphers are encryption algorithms used by hosts to establish a secure communication. There are standard ciphers that Element software supports and non-standard ones when FIPS 140-2 mode is enabled.

The following lists provide the standard Secure Socket Layer (SSL) ciphers supported by Element software and the SSL ciphers supported when FIPS 140-2 mode is enabled:

FIPS 140-2 disabled

- TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C

- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
- TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
- TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
- TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
- TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
- TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048) - A

FIPS 140-2 enabled

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
- TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
- TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
- TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A

Securing Protocols and Ports

Network ports used by NetApp HCI

In addition to performing on-box security operations and functions, the hardening of a solution must also include off-box security mechanisms. Using additional infrastructure devices, such as firewalls, intrusion prevention systems (IPSs), and other security devices, for filtering and limiting access to Element is an effective way to establish and maintain a stringent security posture.

The following table lists the common protocols and ports used in the Element solution. This information is a key component for filtering and limiting access to the environment and its resources.

Service	Port/Protocol	Description
SSH	22/TCP	Secure Shell login
SMTP	25/TCP	Simple Mail Transfer Protocol
HTTP	80/TCP	Administrative REST interface (redirects to 8443)
NTP	123/UDP	Network Time Protocol
SNMP	161/TCP/UDP	Simple Network Management Protocol
SNMP	162/UDP	Simple Network Management Protocol
LDAP	389/(UCP/TCP)	Local directory

HTTPS	443/TCP	Secure HTTP for administrative REST interface
Syslog	515/UDP	Syslog server
LDAPS	636/TCP	Secure LDAP
SYMbol	2463/TCP	Legacy Management Interface
iSCSI	3260/TCP	iSCSI target port
External Key Mgmt.	5696/TCP	External Key Management
HTTP	8080/TCP	Administrative REST interface (redirects to 8443)
HTTPS	8443/TCP	Administrative REST interface

Security Resources

For information regarding the reporting of vulnerabilities and incidents, NetApp security responses, and customer confidentiality, see the NetApp security portal.

Where to Find Additional Information

To learn more about the information described in this document, refer to the following documents and/or websites:

Security Based HCI Solutions

- NetApp HCI Solutions Catalog
  https://docs.netapp.com/us-en/hci-solutions/index.html
- NetApp HCI - NIST Security Controls for FISMA with HyTrust for Multitenant Infrastructure
  https://www.netapp.com/us/media/nva-1143.pdf
- NetApp HCI Verified Reference Architecture for PCI DSS 3.2.1
  https://www.netapp.com/us/media/wp-7327.pdf

Latest NetApp HCI Documentation

- NetApp HCI Documentation Center
  https://docs.netapp.com/hci/index.jsp
- SolidFire and Element 12.0 Documentation Center
  https://docs.netapp.com/sfe-120/index.jsp
- NetApp Element 12.0 User Guide
  https://docs.netapp.com/sfe-120/index.jsp?topic=%2Fcom.netapp.doc.sfe-ug%2Fhome.html&cp=4_0
- NetApp Element 12.0 Element Plug-in for vCenter Server 4.5 User Guide
  https://docs.netapp.com/sfe-120/index.jsp?topic=%2Fcom.netapp.doc.sfe-mg-vcp%2Fhome.html&cp=4_1
- NetApp Element 12.0 API Reference Guide
- https://docs.netapp.com/sfe-120/index.jsp?topic=%2Fcom.netapp.doc.sfe-api%2Fhome.html&cp=4_2
- NetApp HCI Management node (mNode) overview
  https://docs.netapp.com/us-en/hci/docs/task_mnode_work_overview.html

Element 11.3 NetApp HCI Documentation

- SolidFire and Element 11.3 Documentation Center
  https://docs.netapp.com/sfe-113/index.jsp?topic=%2Fcom.netapp.doc.sfe-ug%2Fhome.html&cp=4_0
- NetApp Element 11.3 User Guide

https://docs.netapp.com/sfe-113/index.jsp?topic=%2Fcom.netapp.doc.sfe-ug%2Fhome.html&cp=4_0

- NetApp Element 11.3 API Reference Guide

  https://docs.netapp.com/sfe-113/index.jsp?topic=%2Fcom.netapp.doc.sfe-api%2Fhome.html&cp=4_2
- https://docs.netapp.com/sfe-113/index.jsp?topic=%2Fcom.netapp.doc.sfe-mg-vcp%2Fhome.html&cp=4_1NetApp Element 11.3 Management Node User Guide for NetApp Element Software

  https://docs.netapp.com/sfe-113/index.jsp?topic=%2Fcom.netapp.doc.sfe-mg-mn%2Fhome.html&cp=4_3