NetApp HCI security

HCI

Michael Wallis, Ann-Marie Grissino
November 16, 2020

Table of Contents

NetApp HCI security

When you use NetApp HCI, your data is protected by industry-standard security protocols.

Encryption at Rest for storage nodes

NetApp HCI enables you to encrypt all data stored on the storage cluster.

All drives in storage nodes that are 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 storage-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. You need the password to unlock the drive, and since the drive is encrypting all data, your data is secure at all times.

When you enable Encryption at Rest, performance and efficiency of the storage cluster are unaffected. Additionally, if you remove an encryption-enabled drive or node from the storage cluster with the Element API or Element UI, Encryption at Rest is disabled on the drives and the drives are securely erased, protecting the data that was previously stored on those drives. After you remove the drive, you can securely erase the drive with the `SecureEraseDrives` API method. If you forcibly remove a drive or node from the storage cluster, the data remains protected by the cluster-wide password and the drive's individual encryption keys.

For information on enabling and disabling Encryption at Rest, see Enabling and disabling encryption for a cluster in the SolidFire and Element Documentation Center.

Software Encryption at Rest

Software Encryption at Rest enables all data written to the SSDs in a storage cluster to be encrypted. This provides a primary layer of encryption in SolidFire Enterprise SDS nodes that do not include Self-Encrypting Drives (SEDs).

External key management

You can configure Element software to use a third-party KMIP-compliant key management service (KMS) to manage storage cluster encryption keys. When you enable this feature, the storage cluster's cluster-wide drive access password encryption key is managed by a KMS that you specify.
Element can use the following key management services:

- Gemalto SafeNet KeySecure
- SafeNet AT KeySecure
- HyTrust KeyControl
- Vormetric Data Security Manager
- IBM Security Key Lifecycle Manager

For more information on configuring External Key Management, see Getting started with External Key Management in the SolidFire and Element Documentation Center.

Multi-factor authentication

Multi-factor authentication (MFA) enables you to require users to present multiple types of evidence to authenticate with the NetApp Element web UI or storage node UI upon login. You can configure Element to accept only multi-factor authentication for logins integrating with your existing user management system and identity provider.
You can configure Element to integrate with an existing SAML 2.0 identity provider which can enforce multiple authentication schemes, such as password and text message, password and email message, or other methods.

You can pair multi-factor authentication with common SAML 2.0 compatible identity providers (IdPs), such as Microsoft Active Directory Federation Services (ADFS) and Shibboleth.

To configure MFA, see Enabling multi-factor authentication in the SolidFire and Element Documentation Center.

FIPS 140-2 for HTTPS and data at rest encryption

NetApp SolidFire storage clusters and NetApp HCI systems support encryption that complies with the Federal Information Processing Standard (FIPS) 140-2 requirements for cryptographic modules. You can enable FIPS 140-2 compliance on your NetApp HCI or SolidFire cluster for both HTTPS communications and drive encryption.

When you enable FIPS 140-2 operating mode on your cluster, the cluster activates the NetApp Cryptographic Security Module (NCSM) and leverages FIPS 140-2 Level 1 certified encryption for all communication via HTTPS to the NetApp Element UI and API. You use the `EnableFeature` Element API with the `fips` parameter to enable FIPS 140-2 HTTPS encryption. On storage clusters with FIPS-compatible hardware, you can also enable FIPS drive encryption for data at rest using the `EnableFeature` Element API with the `FipsDrives` parameter.

For more information about preparing a new storage cluster for FIPS 140-2 encryption, see Creating a cluster supporting FIPS drives.

For more information about enabling FIPS 140-2 on an existing, prepared cluster, see The EnableFeature Element API.