Secure your data

ASA r2

NetApp
September 26, 2024

Table of Contents

Secure your data

Encrypt data at rest on ASA r2 storage systems

When you encrypt data at rest, it can't be read if a storage medium is repurposed, returned, misplaced, or stolen. You can use ONTAP System Manager to encrypt your data at the hardware and software level for dual-layer protection.

NetApp Storage Encryption (NSE) supports hardware encryption using self-encrypting drives (SEDs). SEDs encrypt data as it is written. Each SED contains a unique encryption key. Encrypted data stored on the SED can't be read without the SED's encryption key. Nodes attempting to read from an SED must be authenticated to access the SED's encryption key. Nodes are authenticated by obtaining an authentication key from a key manager, then presenting the authentication key to the SED. If the authentication key is valid, the SED will give the node its encryption key to access the data it contains.

Use the ASA r2 onboard key manager or an external key manager to serve authentication keys to your nodes.

In addition to NSE, you can also enable software encryption to add another layer of security to your data.

Steps

1. In System manager, select **Cluster > Settings**.
2. In the **Security** section, under **Encryption**, select **Configure**.
3. Configure the key manager.

Option	Steps
Configure the Onboard key Manager	a. Select **Onboard Key Manager** to add the key servers. b. Enter a passphrase.
Configure an external key manager	a. Select **External key manager** to add the key servers. b. Select + Add to add the key servers. c. Add the KMIP server CA certificates. d. Add the KMIP client certificates.

4. Select **Dual-layer encryption** to enable software encryption.
5. Select **Save**.

What's next?

Now that you have encrypted your data at rest, if you are using the NVMe/TCP protocol, you can encrypt all the data sent over the network between your NVMe/TCP host and your ASA r2 system.

Protect against ransomware attacks on ASA r2 storage systems

For enhanced protection against ransomware attacks, replicate snapshots to a remote cluster, then lock the destination snapshots to make them tamper-proof. Locked snapshots cannot be deleted accidentally or maliciously. You can use locked snapshots to recover data if a storage unit is ever compromised by a ransomware attack.

Initialize the Snaplock compliance clock

Before you can create tamper-proof snapshots, you must initialize the Snaplock compliance clock on your local and destination clusters.

Steps

1. Select **Cluster > Overview**.
2. In the **Nodes** section, select **Initialize SnapLock Compliance Clock**.
3. Select **Initialize**.
4. Verify that the compliance clock is initialized.
   a. Select **Cluster > Overview**.
   b. In the **Nodes** section, select ; then select **SnapLock Compliance Clock**.

What's next?

After you have initialized the Snaplock compliance clock on your local and destination clusters, you are ready to create a replication relationship with locked snapshots.

Secure NVMe connections on your ASA r2 storage systems

If you are using the NVMe protocol, you can configure in-band authentication to enhance your data security. In-band authentication allows secure bidirectional and unidirectional authentication between your NVMe hosts and your ASA r2 system. In-band authentication is available for all NVMe hosts. If you are using the NVMe/TCP protocol, you can further enhance your data security by configuring transport layer security (TLS) to encrypt all data sent over the network between your NVMe/TCP hosts and your ASA r2 system.

Steps

1. Select **Hosts**; then select **NVMe**.
2. Select + Add .
3. Enter the host name; then select the host operating system.
4. Enter a host description; then select the storage VM to connect to the host.
5. Select next to the host name.
6. Select **In-band authentication**.
7. If you are using the NVMe/TCP protocol, select **Require Transport Layer Security (TLS)**.
8. Select **Add**.

Result

The security of your data is enhanced with in-band authentication and/or TLS.

Copyright information

Trademark information