保护数据安全
ASA r2

NetApp
September 26, 2024

目录

保护数据安全

对ASA R2存储系统上的空闲数据进行加密

在对空闲数据进行加密时、如果存储介质被改作他用、退回、放置在不当位置或被盗、则无法读取这些数据。您可以使用ONTAP系统管理器在硬件和软件级别对数据进行加密、以实现双层保护。

NetApp存储加密(NSE)支持使用自加密驱动器(Self-Encryption Drive、SE)进行硬件加密。在写入数据时、SED会对数据进行加密。每个SED都包含一个唯一的加密密钥。如果没有SED的加密密钥、则无法读取SED上存储的加密数据。要访问SED的加密密钥、必须对尝试从SED读取的节点进行身份验证。通过从密钥管理器获取身份验证密钥、然后将身份验证密钥提供给SED、可以对节点进行身份验证。如果身份验证密钥有效、SED将向节点提供其加密密钥以访问其包含的数据。

使用ASA R2板载密钥管理器或外部密钥管理器为节点提供身份验证密钥。

除了NSE之外、您还可以启用软件加密、为数据添加另一层安全保护。

步骤

1. 在System Manager中，选择*Cluster > Settings*。
2. 在*安全性*部分的*加密*下，选择*配置*。
3. 配置密钥管理器。

选项	步骤
配置板载密钥管理器	a. 选择*板载密钥管理器*以添加密钥服务器。 b. 输入密码短语。
配置外部密钥管理器	a. 选择*外部密钥管理器*以添加密钥服务器。 b. 选择 + Add 以添加密钥服务器。 c. 添加KMIP服务器CA证书。 d. 添加KMIP客户端证书。

4. 选择*双层加密*以启用软件加密。
5. 选择 * 保存 * 。

下一步是什么?

现在、您已对空闲数据进行加密、如果您使用的是NVMe/TCP协议、则可以"对通过网络发送的所有数据进行加密"在NVMe/TCP主机和ASA R2系统之间进行加密。

防范ASA R2存储系统上的勒索软件攻击

为了增强对勒索软件攻击的防护、请将快照复制到远程集群、然后锁定目标快照以防止其

篡改。锁定的快照不会被意外或恶意删除。如果某个存储单元受到勒索软件攻击的威胁、您可以使用锁定的快照来恢复数据。

初始化SnapLock Compliance时钟

在创建防篡改快照之前、您必须初始化本地和目标集群上的SnapLock Compliance时钟。

步骤

1. 选择 * 集群 > 概述 * 。
2. 在*N节点*部分中，选择*初 始化SnapLock Compliance Clock*。
3. 选择*初始化*。
4. 验证Compliance时钟是否已初始化。
   a. 选择 * 集群 > 概述 * 。
   b. 在*节点*部分中，选择；然后选择* SnapLock Compliance Clock*。

下一步是什么?

在本地集群和目标集群上初始化SnapLock Compliance时钟后，即可开始"使用锁定的快照创建复制关系"。

ASA R2存储系统上的安全NVMe连接

如果您使用的是NVMe协议、则可以配置带内身份验证以增强数据安全性。带内身份验证允许在NVMe主机和ASA R2系统之间进行安全的双向和单向身份验证。所有NVMe主机均可使用带内身份验证。如果您使用的是NVMe/TCP协议、则可以通过配置传输层安全性(Transport Layer Security、TLS)来对NVMe/TCP主机和ASA R2系统之间通过网络发送的所有数据进行加密、从而进一步增强数据安全性。

步骤

1. 选择*hosts*；然后选择*NVMe*。
2. 选择。 + Add
3. 输入主机名、然后选择主机操作系统。
4. 输入主机说明、然后选择要连接到主机的Storage VM。
5. 选择 主机名旁边的。
6. 选择*带内身份验证*。
7. 如果使用的是NVMe/TCP协议，请选择*需要传输层安全(TL)*。
8. 选择 * 添加 * 。

结果

通过带内身份验证和(或) TLS增强数据的安全性。

版权信息

商标信息