



保护数据安全

ASA r2

NetApp
September 26, 2024

目录

保护数据安全	1
对ASA R2存储系统上的空闲数据进行加密	1
防范ASA R2存储系统上的勒索软件攻击	1
ASA R2存储系统上的安全NVMe连接	2

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	<ol style="list-style-type: none">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	<ol style="list-style-type: none">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*。

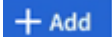

下一步是什么?

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。 
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

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。