Sécurisez vos données

ASA r2

NetApp
September 26, 2024

Sommaire

Sécurisez vos données 1
Chiffrement des données au repos sur les systèmes de stockage ASA r2 1
Protégez-vous contre les attaques par ransomware sur les systèmes de stockage ASA r2 2
Sécurisez les connexions NVMe sur vos systèmes de stockage ASA r2 2

Sécurisez vos données

Chiffrement des données au repos sur les systèmes de stockage ASA r2

Lorsque vous chiffrez les données au repos, elles ne peuvent pas être lues si un support de stockage est requalifié, perdu ou volé. Vous pouvez utiliser ONTAP System Manager pour chiffrer vos données au niveau matériel et logiciel afin de bénéficier d'une protection double couche.

NetApp Storage Encryption (NSE) prend en charge le chiffrement matériel à l'aide de disques à autochiffrement (SED). Les disques SED chiffrent les données au fur et à mesure de leur écriture. Chaque SED contient une clé de chiffrement unique. Les données chiffrées stockées sur le SED ne peuvent pas être lues sans la clé de chiffrement du SED. Les nœuds qui tentent de lire à partir d'un SED doivent être authentifiés pour accéder à la clé de cryptage du SED. Les nœuds sont authentifiés en obtenant une clé d'authentification auprès d'un gestionnaire de clés, puis en présentant la clé d'authentification au SED. Si la clé d'authentification est valide, le SED donnera au nœud sa clé de cryptage pour accéder aux données qu'il contient.

Utilisez le gestionnaire de clés intégré ASA r2 ou un gestionnaire de clés externe pour transmettre des clés d'authentification à vos nœuds.

En plus de NSE, vous pouvez également activer le chiffrement logiciel afin d'ajouter une couche supplémentaire de sécurité à vos données.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Dans la section **sécurité**, sous **cryptage**, sélectionnez **configurer**.
3. Configurez le gestionnaire de clés.

Option	Étapes
Configurez le gestionnaire de clés intégré	a. Sélectionnez **Onboard Key Manager** pour ajouter les serveurs de clés. b. Saisissez une phrase de passe.
Configurez un gestionnaire de clés externe	a. Sélectionnez **Gestionnaire de clés externe** pour ajouter les serveurs de clés. b. Sélectionnez + Add pour ajouter les serveurs clés. c. Ajoutez les certificats de l'autorité de certification du serveur KMIP. d. Ajoutez les certificats client KMIP.

4. Sélectionnez **chiffrement double couche** pour activer le chiffrement logiciel.
5. Sélectionnez **Enregistrer**.

Et la suite ?

Une fois que vous avez chiffré vos données au repos, si vous utilisez le protocole NVMe/TCP, vous pouvez le "chiffrez toutes les données envoyées sur le réseau" faire entre votre hôte NVMe/TCP et votre système ASA r2.

Protégez-vous contre les attaques par ransomware sur les systèmes de stockage ASA r2

Pour une protection renforcée contre les attaques par ransomware, répliquez les snapshots sur un cluster distant, puis verrouillez les snapshots de destination pour les protéger contre toute tentative d'altération. Les snapshots verrouillés ne peuvent pas être supprimés accidentellement ou de manière malveillante. Vous pouvez utiliser des snapshots verrouillés pour restaurer des données si une unité de stockage n'est jamais compromise par une attaque par ransomware.

Initialiser l'horloge SnapLock Compliance

Avant de pouvoir créer des instantanés inviolables, vous devez initialiser l'horloge SnapLock Compliance sur vos clusters locaux et de destination.

Étapes

1. Sélectionnez **Cluster > Présentation**.
2. Dans la section **nœuds**, sélectionnez **initialiser horloge SnapLock Compliance**.
3. Sélectionnez **initialiser**.
4. Vérifiez que l'horloge de conformité est initialisée.
   a. Sélectionnez **Cluster > Présentation**.
   b. Dans la section **nœuds**, sélectionnez ; puis **SnapLock Compliance horloge**.

Et la suite ?

Après avoir initialisé l'horloge SnapLock Compliance sur vos clusters locaux et de destination, vous êtes prêt à "créer une relation de réplication avec des snapshots verrouillés".

Sécurisez les connexions NVMe sur vos systèmes de stockage ASA r2

Si vous utilisez le protocole NVMe, vous pouvez configurer l'authentification intrabande pour renforcer la sécurité de vos données. L'authentification intrabande permet une authentification bidirectionnelle et unidirectionnelle sécurisée entre vos hôtes NVMe et votre système ASA r2. L'authentification intrabande est disponible pour tous les hôtes NVMe. Si vous utilisez le protocole NVMe/TCP, vous pouvez renforcer encore la sécurité de vos données en configurant transport Layer Security (TLS) pour chiffrer toutes les données envoyées sur le réseau entre vos hôtes NVMe/TCP et votre système ASA r2.

Étapes

1. Sélectionnez **hosts**, puis **NVMe**.

2. Sélectionnez + Add .
3. Entrez le nom d'hôte, puis sélectionnez le système d'exploitation hôte.
4. Entrez une description d'hôte, puis sélectionnez la VM de stockage à connecter à l'hôte.
5. Sélectionnez ⌄ en regard du nom d'hôte.
6. Sélectionnez **authentification intrabande**.
7. Si vous utilisez le protocole NVMe/TCP, sélectionnez **nécessite TLS (transport Layer Security)**.
8. Sélectionnez **Ajouter**.

Résultat

La sécurité de vos données est renforcée par l'authentification intrabande et/ou TLS.

Informations sur le copyright

Informations sur les marques commerciales