



Metti al sicuro i tuoi dati

ASA r2

NetApp
September 26, 2024

Sommario

- Metti al sicuro i tuoi dati 1
 - Esegui la crittografia dei dati inutilizzati nei sistemi di storage ASA R2 1
 - Proteggiti dagli attacchi ransomware sui sistemi storage ASA R2 2
 - Connessioni NVMe sicure sui tuoi sistemi storage ASA R2 2

Metti al sicuro i tuoi dati

Esegui la crittografia dei dati inutilizzati nei sistemi di storage ASA R2

Quando si crittografano i dati a riposo, non è possibile leggerli se un supporto storage viene riutilizzato, restituito, smarrito o rubato. Puoi utilizzare Gestione sistema di ONTAP per crittografare i dati a livello hardware e software per una protezione a doppio livello.

NetApp Storage Encryption (NSE) supporta la crittografia hardware utilizzando dischi con crittografia automatica (SED). I SEDS crittografano i dati durante la scrittura. Ogni SED contiene una chiave di crittografia univoca. I dati crittografati memorizzati sul SED non possono essere letti senza la chiave di crittografia del SED. I nodi che tentano di leggere da un SED devono essere autenticati per accedere alla chiave di crittografia del SED. I nodi vengono autenticati ottenendo una chiave di autenticazione da un gestore di chiavi, quindi presentando la chiave di autenticazione al SED. Se la chiave di autenticazione è valida, il SED fornirà al nodo la propria chiave di crittografia per accedere ai dati in esso contenuti.

Utilizza il gestore delle chiavi integrato in ASA R2 o un gestore delle chiavi esterno per fornire le chiavi di autenticazione ai tuoi nodi.

Oltre a NSE, puoi anche abilitare la crittografia software per aggiungere un altro livello di sicurezza ai dati.

Fasi

1. In Gestione di sistema, selezionare **Cluster > Impostazioni**.
2. Nella sezione **protezione**, in **crittografia**, selezionare **Configura**.
3. Configurare il gestore delle chiavi.

| Opzione | Fasi |
|--|---|
| Configurare il gestore chiavi integrato | <ol style="list-style-type: none">a. Selezionare Onboard Key Manager per aggiungere i server delle chiavi.b. Inserire una passphrase. |
| Configurare un gestore di chiavi esterno | <ol style="list-style-type: none">a. Selezionare Gestore chiavi esterno per aggiungere i server chiavi.b. Selezionare + Add per aggiungere i server chiavi.c. Aggiungere i certificati CA del server KMIP.d. Aggiungere i certificati client KMIP. |

4. Selezionare **crittografia a doppio livello** per abilitare la crittografia software.
5. Selezionare **Salva**.

Quali sono le prossime novità?

Ora che hai crittografato i tuoi dati a riposo, se stai utilizzando il protocollo NVMe/TCP, potrai ["crittografare tutti i dati inviati in rete"](#) collegare l'host NVMe/TCP e il sistema ASA R2.

Proteggiti dagli attacchi ransomware sui sistemi storage ASA R2

Per una protezione avanzata contro gli attacchi ransomware, replica le snapshot su un cluster remoto, quindi blocca le snapshot di destinazione per renderle a prova di manomissione. Gli snapshot bloccati non possono essere eliminati accidentalmente o in modo pericoloso. Puoi utilizzare snapshot bloccate per ripristinare i dati, se un'unità di storage viene mai compromessa da un attacco ransomware.

Inizializzare l'orologio SnapLock Compliance

Prima di poter creare snapshot a prova di manomissione, è necessario inizializzare il clock SnapLock Compliance sui cluster locali e di destinazione.

Fasi

1. Selezionare **Cluster > Overview** (Cluster > Panoramica).
2. Nella sezione **nod**i, selezionare **Inizializza orologio SnapLock Compliance**.
3. Selezionare **Inizializza**.
4. Verificare che l'orologio di conformità sia inizializzato.
 - a. Selezionare **Cluster > Overview** (Cluster > Panoramica).
 - b. Nella sezione **nod**i, selezionare ; quindi selezionare **SnapLock Compliance Clock**.

Cosa succederà?

Dopo aver inizializzato l'orologio SnapLock Compliance sui cluster locali e di destinazione, si è pronti per ["creare una relazione di replica con gli snapshot bloccati"](#).

Connessioni NVMe sicure sui tuoi sistemi storage ASA R2

Se stai utilizzando il protocollo NVMe, puoi configurare l'autenticazione in-band per migliorare la sicurezza dei tuoi dati. L'autenticazione in-band consente un'autenticazione sicura bidirezionale e unidirezionale tra gli host NVMe e il sistema ASA R2.

L'autenticazione in banda è disponibile per tutti gli host NVMe. Se stai utilizzando il protocollo NVMe/TCP, puoi migliorare ulteriormente la sicurezza dei dati configurando TLS (Transport Layer Security) in modo da crittografare tutti i dati inviati in rete tra gli host NVMe/TCP e il sistema ASA R2.

Fasi

1. Selezionare **hosts**, quindi selezionare **NVMe**.
2. Selezionare .
3. Immettere il nome host, quindi selezionare il sistema operativo host.
4. Immettere una descrizione dell'host, quindi selezionare la VM di storage da connettere all'host.
5. Selezionare  accanto al nome host.
6. Selezionare **autenticazione in banda**.
7. Se si utilizza il protocollo NVMe/TCP, selezionare **Richiedi TLS (Transport Layer Security)**.

8. Selezionare **Aggiungi**.

Risultato

La sicurezza dei dati è migliorata con l'autenticazione in banda e/o TLS.

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.