Datensicherung

ASA r2

NetApp
September 26, 2024

Inhalt

Datensicherung

Verschlüsselung von Daten im Ruhezustand auf ASA r2 Storage-Systemen

Wenn Daten im Ruhezustand verschlüsselt werden, sind sie auch dann nicht lesbar, wenn ein Storage-Medium einem anderen Zweck zugewiesen, zurückgegeben, verlegt oder gestohlen wird. Sie können ONTAP System Manager zur Verschlüsselung Ihrer Daten auf Hardware- und Softwareebene für einen Dual-Layer-Schutz verwenden.

NetApp Storage Encryption (NSE) unterstützt Hardwareverschlüsselung über Self-Encrypting Drives (SEDs). SEDs verschlüsseln Daten beim Schreiben. Jede SED enthält einen eindeutigen Verschlüsselungsschlüssel. Verschlüsselte Daten, die auf der SED gespeichert sind, können ohne den SED-Verschlüsselungsschlüssel nicht gelesen werden. Knoten, die versuchen, von einer SED zu lesen, müssen authentifiziert werden, um auf den Verschlüsselungsschlüssel der SED zuzugreifen. Knoten werden authentifiziert, indem ein Authentifizierungsschlüssel von einem Schlüsselmanager abgerufen und dann der SED den Authentifizierungsschlüssel vorgelegt wird. Wenn der Authentifizierungsschlüssel gültig ist, gibt die SED dem Knoten seinen Verschlüsselungsschlüssel für den Zugriff auf die darin enthaltenen Daten.

Verwenden Sie den integrierten Schlüsselmanager von ASA r2 oder einen externen Schlüsselmanager, um Ihren Nodes Authentifizierungsschlüssel bereitzustellen.

Neben NSE können Sie auch Softwareverschlüsselung aktivieren, um Ihre Daten um eine weitere Sicherheitsebene zu erweitern.

Schritte

1. Wählen Sie im System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie im Abschnitt **Sicherheit** unter **Verschlüsselung Konfigurieren** aus.
3. Konfigurieren Sie den Schlüsselmanager.

Option	Schritte
Konfigurieren Sie den Onboard Key Manager	a. Wählen Sie **Onboard Key Manager**, um die Schlüsselserver hinzuzufügen. b. Geben Sie eine Passphrase ein.
Konfigurieren Sie einen externen Schlüsselmanager	a. Wählen Sie **External Key Manager**, um die Schlüsselserver hinzuzufügen. b. Wählen Sie + Add diese Option aus, um die Schlüsselserver hinzuzufügen. c. Fügen Sie die CA-Zertifikate des KMIP-Servers hinzu. d. Fügen Sie die KMIP-Client-Zertifikate hinzu.

4. Wählen Sie **Dual-Layer-Verschlüsselung**, um die Softwareverschlüsselung zu aktivieren.
5. Wählen Sie **Speichern**.

Was kommt als Nächstes?

Nachdem Sie nun Ihre Daten im Ruhezustand verschlüsselt haben, können Sie jetzt mit dem "Verschlüsseln Sie alle über das Netzwerk gesendeten Daten"NVMe-/TCP-Protokoll zwischen Ihrem NVMe-/TCP-Host und Ihrem ASA r2-System wechseln.

Schutz vor Ransomware-Angriffen auf ASA r2 Storage-Systeme

Um besser gegen Ransomware-Angriffe zu schützen, replizieren Sie Snapshots in ein Remote-Cluster und sperren Sie dann die Ziel-Snapshots, damit sie manipulationssicher sind. Gesperrte Snapshots können nicht versehentlich oder böswillig gelöscht werden. Sie können gesperrte Snapshots verwenden, um Daten wiederherzustellen, wenn ein Storage-Gerät jemals durch einen Ransomware-Angriff kompromittiert wurde.

Initialisieren Sie die SnapLock Compliance-Uhr

Bevor Sie manipulationssichere Snapshots erstellen können, müssen Sie die SnapLock Compliance Uhr auf Ihren lokalen und Ziel-Clustern initialisieren.

Schritte

1. Wählen Sie **Cluster > Übersicht**.
2. Wählen Sie im Abschnitt **Knoten** die Option **SnapLock Compliance-Uhr initialisieren** aus.
3. Wählen Sie **Initialisieren**.
4. Vergewissern Sie sich, dass die Compliance-Uhr initialisiert ist.
   a. Wählen Sie **Cluster > Übersicht**.
   b. Wählen Sie im Abschnitt **Knoten** die Option ; und wählen Sie dann **SnapLock Compliance Uhr**.

Was kommt als Nächstes?

Nachdem Sie die SnapLock Compliance-Uhr auf Ihren lokalen und Ziel-Clustern initialisiert haben, sind Sie bereit zu "Erstellen Sie eine Replikationsbeziehung mit gesperrten Snapshots".

Sichere NVMe-Verbindungen auf Ihren ASA r2 Storage-Systemen

Bei Verwendung des NVMe-Protokolls können Sie die in-Band-Authentifizierung konfigurieren, um die Datensicherheit zu erhöhen. Die in-Band-Authentifizierung ermöglicht eine sichere bidirektionale und unidirektionale Authentifizierung zwischen den NVMe Hosts und dem ASA r2 System. Die in-Band-Authentifizierung ist für alle NVMe-Hosts verfügbar. Bei Verwendung des NVMe/TCP-Protokolls können Sie die Datensicherheit weiter erhöhen, indem Sie TLS (Transport Layer Security) für die Verschlüsselung aller Daten konfigurieren, die zwischen Ihren NVMe/TCP-Hosts und Ihrem ASA r2-System über das Netzwerk übertragen werden.

Schritte

1. Wählen Sie **Hosts** aus, und wählen Sie dann **NVMe** aus.

2. Wählen Sie + Add .
3. Geben Sie den Hostnamen ein, und wählen Sie dann das Host-Betriebssystem aus.
4. Geben Sie eine Hostbeschreibung ein, und wählen Sie dann die Speicher-VM aus, die mit dem Host verbunden werden soll.
5. Wählen Sie ⌄ neben dem Hostnamen aus.
6. Wählen Sie **bandinterne Authentifizierung** aus.
7. Wenn Sie das NVMe/TCP-Protokoll verwenden, wählen Sie **benötigt Transport Layer Security (TLS)** aus.
8. Wählen Sie **Hinzufügen**.

Ergebnis

Die Sicherheit Ihrer Daten wird durch die in-Band-Authentifizierung und/oder TLS erhöht.