Sicherheit und Datenverschlüsselung

Cloud Volumes ONTAP

NetApp
December 05, 2022

Inhaltsverzeichnis

Sicherheit und Datenverschlüsselung

Verschlüsseln von Volumes mit NetApp Verschlüsselungslösungen

Cloud Volumes ONTAP unterstützt NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE). NVE und NAE sind softwarebasierte Lösungen, die die Verschlüsselung von Daten im Ruhezustand nach FIPS 140 ermöglichen. "Weitere Informationen zu diesen Verschlüsselungslösungen".

Sowohl NVE als auch NAE werden von einem externen Schlüsselmanager unterstützt.

Neue Aggregate haben standardmäßig NAE aktiviert, nachdem Sie einen externen Schlüsselmanager eingerichtet haben. Für neue Volumes, die nicht Teil eines NAE-Aggregats sind, ist NVE standardmäßig aktiviert (bei vorhandenen Aggregaten, die vor dem Einrichten eines externen Schlüsselmanagers erstellt wurden).

Cloud Volumes ONTAP unterstützt kein Onboard-Verschlüsselungsmanagement.

Ihr Cloud Volumes ONTAP System sollte beim NetApp Support registriert sein. Auf jedem Cloud Volumes ONTAP System, das beim NetApp Support registriert ist, wird automatisch eine Lizenz für NetApp Volume Encryption installiert.

- "Hinzufügen von Konten für die NetApp Support Site zu BlueXP"
- "Registrieren von Pay-as-you-go-Systemen"

BlueXP installiert die NVE-Lizenz nicht auf Systemen, die sich in der Region China befinden.

Schritte

1. Überprüfen Sie die Liste der unterstützten Schlüsselmanager im "NetApp Interoperabilitäts-Matrix-Tool".

   Suchen Sie nach der **Key Manager**-Lösung.

2. "Stellen Sie eine Verbindung zur Cloud Volumes ONTAP-CLI her".
3. Externes Verschlüsselungsmanagement konfigurieren.
   - Google Cloud: "Google Cloud Key Management Service"

Verwalten Sie Schlüssel mit Google Cloud Key Management Service

Verwenden Sie können "Der Verschlüsselungsmanagement-Service (Cloud KMS) der Google Cloud-Plattform" Zum Schutz Ihrer ONTAP Verschlüsselungen in einer vom Google Cloud-Plattform bereitgestellten Applikation.

Das Verschlüsselungsmanagement mit Cloud KMS kann über die CLI oder die ONTAP REST-API aktiviert werden.

Beachten Sie bei der Verwendung von Cloud KMS, dass standardmäßig eine LIF der Daten-SVMs zur Kommunikation mit dem Endpunkt des Cloud-Verschlüsselungsmanagement verwendet wird. Zur

Kommunikation mit den Authentifizierungsservices des Cloud-Providers wird ein Node-Managementnetzwerk verwendet (oauth2.googleapis.com). Wenn das Cluster-Netzwerk nicht korrekt konfiguriert ist, nutzt das Cluster den Verschlüsselungsmanagementservice nicht ordnungsgemäß.

Voraussetzungen

- Cloud Volumes ONTAP muss Version 9.10.1 oder höher ausführen
- Volume Encryption (VE)-Lizenz installiert
- Multi-Tenant Encryption Key Management-Lizenz (MTEKM) installiert
- Sie müssen ein Cluster- oder SVM-Administrator sein
- Ein aktives Google Cloud Platform Abonnement

Einschränkungen

- Cloud KMS kann nur auf einer Daten-SVM konfiguriert werden

Konfiguration

Google Cloud

1. In Ihrer Google Cloud-Umgebung "Erstellen Sie einen symmetrischen GCP-Schlüsselring und -Schlüssel".
2. Erstellen Sie eine benutzerdefinierte Rolle für Ihr Cloud Volumes ONTAP-Servicekonto.

```
gcloud iam roles create kmsCustomRole
    --project=<project_id>
    --title=<kms_custom_role_name>
    --description=<custom_role_description>

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourcemanager.projects.get
    --stage=GA
```

3. Weisen Sie den Cloud-KMS-Schlüssel und das Cloud Volumes ONTAP-Servicekonto die benutzerdefinierte Rolle zu:
`gcloud kms keys add-iam-policy-binding` *`key_name`* `--keyring` *`key_ring_name`* `--location` *`key_location`* `--member serviceAccount:_service_account_Name_ --role projects/`*`customer_project_id`*`/roles/kmsCustomRole`
4. Service-Konto-JSON-Schlüssel herunterladen:
`gcloud iam service-accounts keys create key-file --iam-account=`*`sa-name`*`@`*`project-id`*`.iam.gserviceaccount.com`

Cloud Volumes ONTAP

1. Stellen Sie eine Verbindung zur Cluster-Management-LIF mit dem bevorzugten SSH-Client her.
2. Wechseln zur erweiterten Berechtigungsebene:
`set -privilege advanced`
3. DNS für die Daten-SVM erstellen.
`dns create -domains c.<`*`project`*`>.internal -name-servers` *`server_address`* `-vserver`

SVM_name

4. CMEK-Eintrag erstellen:
`security key-manager external gcp enable -vserver SVM_name -project-id project -key-ring-name key_ring_name -key-ring-location key_ring_location -key-name key_name`
5. Geben Sie bei der entsprechenden Aufforderung den JSON-Schlüssel Ihres GCP-Kontos ein.
6. Bestätigen Sie, dass der aktivierte Prozess erfolgreich war:
`security key-manager external gcp check -vserver svm_name`
7. OPTIONAL: Erstellen Sie ein Volume zum Testen der Verschlüsselung `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

Fehlerbehebung

Wenn Sie Fehler beheben müssen, können Sie die RAW REST API-Logs in den letzten beiden Schritten oben:

1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Besserer Schutz gegen Ransomware

Ransomware-Angriffe können das Unternehmen Zeit, Ressourcen und Image-Schäden kosten. BlueXP ermöglicht Ihnen die Implementierung der NetApp Lösung für Ransomware, die mit effektiven Tools für Transparenz, Erkennung und Problembehebung ausgestattet ist.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Symbol **Ransomware**.

2. Implementierung der NetApp Lösung für Ransomware:

   a. Klicken Sie auf **Snapshot-Richtlinie aktivieren**, wenn Volumes ohne Snapshot-Richtlinie aktiviert sind.

      Die NetApp Snapshot-Technologie bietet die branchenweit beste Lösung zur Behebung von Ransomware. Der Schlüssel zu einer erfolgreichen Recovery liegt im Restore aus einem nicht

infizierten Backup. Snapshot Kopien sind schreibgeschützt, der Ransomware-Beschädigungen verhindert. Sie können außerdem die Granularität nutzen, um Images einer einzelnen Dateikopie oder einer kompletten Disaster-Recovery-Lösung zu erstellen.

b. Klicken Sie auf **FPolicy** aktivieren, um die FPolicy Lösung von ONTAP zu aktivieren, die Dateivorgänge auf Basis der Dateierweiterung blockieren kann.

   Diese präventive Lösung verbessert den Schutz vor Ransomware-Angriffen, indem sie gängige Ransomware-Dateitypen blockiert.

   Die standardmäßige FPolicy Scope blockiert Dateien, die die folgenden Erweiterungen haben:

   Micro, verschlüsselt, gesperrt, Crypto, Crypt, Crinf, r5a, XRNT, XTBL, R16M01D05, Pzdc, gut, LOL!, OMG!, RDM, RK, verschlüsseltedRS, Crjoker, entschlüsselt, LeChiffre

BlueXP erstellt diesen Bereich, wenn Sie FPolicy auf Cloud Volumes ONTAP aktivieren. Die Liste basiert auf gängigen Ransomware-Dateitypen. Sie können die blockierten Dateierweiterungen mithilfe der Befehle *vserver fpolicy Scope* von der Cloud Volumes ONTAP CLI anpassen.