Sicherheit und Datenverschlüsselung

Cloud Volumes ONTAP

NetApp
December 09, 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.

Was Sie benötigen

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.
   - Azure: "Azure Key Vault (AKV)"

Verschlüsselungsmanagement mit Azure Key Vault

Verwenden Sie können "Azure Key Vault (AKV)" Um Ihre ONTAP Verschlüsselungen in einer von Azure implementierten Applikation zu schützen.

AKV kann zum Schutz verwendet werden "NetApp Volume Encryption (NVE)-Schlüssel" Nur für Data SVMs.

Die Schlüsselverwaltung mit AKV kann über die CLI oder die ONTAP REST API aktiviert werden.

Bei Verwendung von AKV ist zu beachten, dass standardmäßig eine LIF der Daten-SVM zur Kommunikation mit dem Endpunkt des Cloud-Verschlüsselungsmanagement verwendet wird. Zur Kommunikation mit den

Authentifizierungsservices des Cloud-Providers wird ein Node-Managementnetzwerk verwendet (login.microsoftonline.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 ist installiert. (NetApp Volume Encryption-Lizenz wird automatisch auf jedem Cloud Volumes ONTAP System installiert, das beim NetApp Support registriert ist).
- Multi-Tenant Encryption Key Management-Lizenz (MTEKM) installiert
- Sie müssen ein Cluster- oder SVM-Administrator sein
- Ein Active Azure Abonnement

Einschränkungen

- AKV kann nur auf einer Daten-SVM konfiguriert werden

Konfigurationsprozess

In den beschriebenen Schritten wird erfasst, wie Sie Ihre Cloud Volumes ONTAP Konfiguration bei Azure registrieren sowie wie ein Azure SchlüsselVault und -Schlüssel erstellt werden. Wenn Sie diese Schritte bereits ausgeführt haben, stellen Sie sicher, dass Sie über die richtigen Konfigurationseinstellungen verfügen, insbesondere in Erstellen Sie einen Azure Key Vault, Und dann weiter zu Cloud Volumes ONTAP-Konfiguration.

- Azure Application Registration
- Azure-Client Secret erstellen
- Erstellen Sie einen Azure Key Vault
- Erstellen eines Verschlüsselungsschlüssels
- Azure Active Directory Endpunkt erstellen (nur HA)
- Cloud Volumes ONTAP-Konfiguration

Azure Application Registration

1. Zunächst müssen Sie Ihre Applikation im Azure Abonnement registrieren, das Cloud Volumes ONTAP für den Zugriff auf Azure SchlüsselVault verwenden soll. Wählen Sie im Azure-Portal die Option **App-Registrierungen** aus.
2. Wählen Sie **Neu registrieren**.
3. Geben Sie einen Namen für Ihre Anwendung ein, und wählen Sie einen unterstützten Anwendungstyp aus. Der standardmäßige einzelne Mandant ist für die Verwendung von Azure Key Vault ausreichend. Wählen Sie **Register**.
4. Wählen Sie im Fenster Azure Overview die Anwendung aus, die Sie registriert haben. Kopieren Sie die **Anwendung (Client) ID** und die **Verzeichnis-ID** an einen sicheren Ort. Diese werden später bei der Registrierung benötigt.

Azure-Client Secret erstellen

1. Wählen Sie im Azure-Portal für Ihre Cloud Volumes ONTAP-Anwendung den Fensterbereich **Certificates & Secrets** aus.
2. Wählen Sie **Neues Kundengeheimnis** Geben Sie einen aussagekräftigen Namen für Ihr Kundengeheimnis ein. NetApp empfiehlt einen 24-monatigen Ablaufdatum, allerdings müssen Ihre spezifischen Cloud Governance-Richtlinien möglicherweise eine andere Einstellung erfordern.

3. Wählen Sie **Hinzufügen**, um den Client geheim zu speichern. Kopieren Sie sofort den **Wert** des Geheimnisses und speichern Sie ihn für zukünftige Konfigurationen sicher. Der geheime Wert wird nicht angezeigt, wenn Sie von der Seite wegnavigieren.

Erstellen Sie einen Azure Key Vault

1. Wenn Sie bereits über einen Azure Schlüsselault verfügen, können Sie ihn mit Ihrer Cloud Volumes ONTAP Konfiguration verbinden. Die Zugriffsrichtlinien müssen jedoch an die Einstellungen in diesem Prozess angepasst werden.
2. Navigieren Sie im Azure-Portal zum Abschnitt **Key Vaults**.
3. Wählen Sie **Erstellen**. Geben Sie die erforderlichen Informationen einschließlich Ressourcengruppe, Region und Preisebene ein, und wählen Sie die Tage aus, um gelöschte Vaults zu behalten, und ob der Schutz zum Löschen aktiviert ist oder nicht. Für diese Konfiguration sind Standards ausreichend. Ihre spezifischen Cloud Governance-Richtlinien können jedoch unterschiedliche Einstellungen erfordern.
4. Wählen Sie **Weiter**, um eine Zugriffsrichtlinie auszuwählen.
5. Wählen Sie **Azure Disk Encryption** für die Option Volume Encryption und **Vault Access Policy** für das Berechtigungsmodell.
6. Wählen Sie **Zugangsrichtlinie Hinzufügen**.
7. Wählen Sie das Caret neben dem Feld **Configure from Template (optional)** aus. Wählen Sie dann **Schlüssel, Geheimnis und Zertifizierungsmanagement.**
8. Wählen Sie die einzelnen Dropdown-Menüs für Berechtigungen (Schlüssel, Geheimnis, Zertifikat) und anschließend **Wählen Sie alle** oben in der Menüliste aus, um alle verfügbaren Berechtigungen auszuwählen. Sie sollten Folgendes haben:
   - **Hauptberechtigungen**: 19 ausgewählt
   - **Geheimberechtigungen**: 8 ausgewählt
   - **Zertifikatberechtigungen**: 16 ausgewählt
9. Wählen Sie **Hinzufügen**, um die Zugriffsrichtlinie zu erstellen.
10. Wählen Sie **Weiter**, um zu **Networking**-Optionen zu gelangen.
11. Wählen Sie die geeignete Netzwerkzugangsmethode oder wählen Sie **Alle Netzwerke** und **Überprüfen + Erstellen**, um den SchlüsselTresor zu erstellen. (Netzwerkzugriffsmethode kann von einer Governance-Richtlinie oder einem Sicherheitsteam Ihres Unternehmens für Cloud-Sicherheit vorgeschrieben werden.)
12. Notieren Sie den Key Vault URI: Navigieren Sie im von Ihnen erstellten Schlüsselspeicher zum Menü Übersicht und kopieren Sie den **Vault URI** aus der rechten Spalte. Sie benötigen dies für einen späteren Schritt.

Erstellen eines Verschlüsselungsschlüssels

1. Navigieren Sie im Menü für den für Cloud Volumes ONTAP erstellten Schlüsseldefault zur Option **Schlüssel**.
2. Wählen Sie **Erzeugen/Importieren**, um einen neuen Schlüssel zu erstellen.
3. Lassen Sie die Standardoption auf **Erzeugen** gesetzt.
4. Geben Sie die folgenden Informationen an:
   - Name des Verschlüsselungsschlüssels
   - Schlüsseltyp: RSA
   - RSA-Schlüsselgröße: 2048
   - Aktiviert: Ja

5. Wählen Sie **Erstellen**, um den Verschlüsselungsschlüssel zu erstellen.
6. Kehren Sie zum Menü **Tasten** zurück und wählen Sie die Taste aus, die Sie gerade erstellt haben.
7. Wählen Sie die Schlüssel-ID unter **Aktuelle Version** aus, um die Schlüsseleigenschaften anzuzeigen.
8. Suchen Sie das Feld **Key Identifier**. Kopieren Sie den URI nach oben, jedoch nicht mit dem hexadezimalen String.

Azure Active Directory Endpunkt erstellen (nur HA)

1. Dieser Prozess ist nur erforderlich, wenn Sie Azure Key Vault für eine HA Cloud Volumes ONTAP Arbeitsumgebung konfigurieren.
2. Navigieren Sie im Azure-Portal zu **Virtual Networks**.
3. Wählen Sie das virtuelle Netzwerk aus, in dem Sie die Cloud Volumes ONTAP-Arbeitsumgebung bereitgestellt haben, und wählen Sie das Menü **Subnetze** auf der linken Seite aus.
4. Wählen Sie in der Liste den Subnetznamen für Ihre Cloud Volumes ONTAP-Bereitstellung aus.
5. Navigieren Sie zur Überschrift **Service-Endpunkte**. Wählen Sie im Dropdown-Menü in der Liste die Option **Microsoft.AzureActiveDirectory** aus.
6. Wählen Sie **Speichern**, um Ihre Einstellungen zu erfassen.

Cloud Volumes ONTAP-Konfiguration

1. Stellen Sie eine Verbindung zur Cluster-Management-LIF mit dem bevorzugten SSH-Client her.
2. Geben Sie in ONTAP den erweiterten Berechtigungsmodus ein:
   `set advanced -con off`
3. Identifizieren Sie die gewünschte Daten-SVM und überprüfen Sie deren DNS-Konfiguration:
   `vserver services name-service dns show`
   a. Wenn ein DNS-Eintrag für die gewünschte Daten-SVM existiert und ein Eintrag für den Azure DNS enthält, ist keine Aktion erforderlich. Ist dies nicht der Fall, fügen Sie einen DNS-Servereintrag für die Daten-SVM hinzu, der auf den Azure DNS, den privaten DNS oder den lokalen Server verweist. Dies sollte der Eintrag für die Cluster Admin SVM entsprechen:
      `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`
   b. Vergewissern Sie sich, dass der DNS-Service für die Daten-SVM erstellt wurde:
      `vserver services name-service dns show`
4. Aktivieren Sie Azure Key Vault mithilfe der Client-ID und der Mandanten-ID, die nach der Registrierung der Applikation gespeichert wurden:
   `security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name Azure_key_name -key-id Azure_key_ID`
5. Überprüfen Sie die Schlüsselmanager-Konfiguration:
   `security key-manager external azure show`
6. Überprüfen Sie den Status des Schlüsselmanagers:
   `security key-manager external azure check`Die Ausgabe sieht wie folgt aus:

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
    Status: OK

Category: ekmip_server
    Status: OK

Category: kms_wrapped_key_status
    Status: UNKNOWN
    Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

Wenn der `service_reachability` Status ist nicht `OK`, Die SVM kann den Azure Key Vault Service nicht mit allen erforderlichen Konnektivitäts- und Berechtigungen erreichen. Der `kms_wrapped_key_status` Wird berichten `UNKNOWN` Bei der Erstkonfiguration. Sein Status ändert sich in `OK` Nach der Verschlüsselung des ersten Volume.

7. OPTIONAL: Erstellen Sie ein Test-Volume, um die Funktionalität von NVE zu überprüfen.

   `vol create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggr`* `-size` *`size`* `-state online -policy default`

   Bei korrekter Konfiguration erstellt Cloud Volumes ONTAP automatisch das Volume und aktiviert die Volume-Verschlüsselung.

8. Bestätigen Sie, dass das Volume ordnungsgemäß erstellt und verschlüsselt wurde. Wenn das der Fall ist, wird der angezeigt `-is-encrypted` Der Parameter wird als angezeigt `true`.
   `vol show -vserver` *`SVM_name`* `-fields is-encrypted`

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.

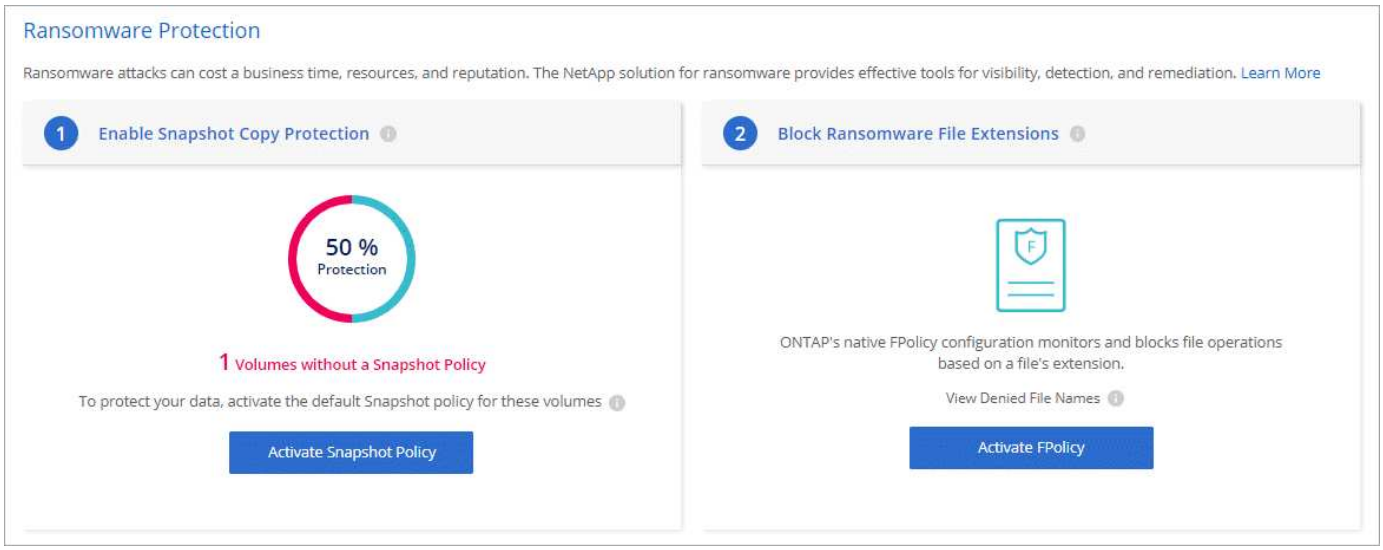
   b. Klicken Sie auf **FPolicy** aktivieren, um die FPolicy Lösung von ONTAP zu aktivieren, die Dateivorgänge auf Basis der Dateierweiterung blockieren kann.

      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.


Ransomware Protection
Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. Learn More
1
Enable Snapshot Copy Protection
50 %
Protection
1 Volumes without a Snapshot Policy
To protect your data, activate the default Snapshot policy for these volumes
Activate Snapshot Policy
2
Block Ransomware File Extensions
ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.
View Denied File Names
Activate FPolicy