



# **Sicherheit und Datenverschlüsselung**

## **Cloud Volumes ONTAP**

NetApp  
April 23, 2024

# Inhalt

- Sicherheit und Datenverschlüsselung ..... 1
  - Verschlüsseln von Volumes mit NetApp Verschlüsselungslösungen ..... 1
  - Schlüsselmanagement mit AWS Key Management Service ..... 1
  - Verschlüsselungsmanagement mit Azure Key Vault ..... 2
  - Verwalten Sie Schlüssel mit Google Cloud Key Management Service ..... 10
  - Besserer Schutz gegen Ransomware ..... 12

# 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.

## Schlüsselmanagement mit AWS Key Management Service

Verwenden Sie können ["AWS Key Management Service \(KMS\)"](#) Zum Schutz Ihrer ONTAP Verschlüsselungen in einer über AWS bereitgestellten Applikation.

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

Bei Verwendung des KMS ist zu beachten, dass standardmäßig die LIF einer Daten-SVM verwendet wird, um mit dem Endpunkt des Cloud-Schlüsselmanagements zu kommunizieren. Ein Node-Managementnetzwerk wird zur Kommunikation mit den Authentifizierungsdiensten von AWS verwendet. Wenn das Cluster-Netzwerk nicht korrekt konfiguriert ist, nutzt das Cluster den Verschlüsselungsmanagementservice nicht ordnungsgemäß.

### Bevor Sie beginnen

- Cloud Volumes ONTAP muss Version 9.12.0 oder höher ausführen
- Sie müssen die Volume Encryption (VE)-Lizenz und installiert haben
- Sie müssen die MTEKM-Lizenz (Multi-Tenant Encryption Key Management) installiert haben.
- Sie müssen ein Cluster- oder SVM-Administrator sein
- Sie müssen über ein aktives AWS-Abonnement verfügen



Schlüssel können nur für eine Daten-SVM konfiguriert werden.

## Konfiguration

### AWS

1. Sie müssen einen erstellen ["Gewähren"](#) Für den AWS-KMS-Schlüssel, der von der IAM-Rolle zum Managen der Verschlüsselung verwendet wird. Die IAM-Rolle muss eine Richtlinie enthalten, die die folgenden Operationen zulässt:
  - DescribeKey
  - Encrypt
  - DecryptInformationen zum Erstellen einer Erteilung finden Sie unter ["AWS-Dokumentation"](#).
2. ["Fügen Sie der entsprechenden IAM-Rolle eine Richtlinie hinzu."](#) Die Politik sollte die unterstützen

DescribeKey, Encrypt, und Decrypt Betrieb:

## Cloud Volumes ONTAP

1. Wechseln Sie zu Ihrer Cloud Volumes ONTAP Umgebung.
2. Wechseln zur erweiterten Berechtigungsebene:  
`set -privilege advanced`
3. Aktivieren Sie den AWS Schlüsselmanager:  
`security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. Geben Sie den geheimen Schlüssel ein, wenn Sie dazu aufgefordert werden.
5. Überprüfen Sie, ob der AWS-KMS ordnungsgemäß konfiguriert wurde:  
`security key-manager external aws show -vserver svm_name`

## 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.

### Bevor Sie beginnen

- 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).
- Sie benötigen eine Multi-Tenant Encryption Key Management (MT\_EK\_MGMT)-Lizenz
- Sie müssen ein Cluster- oder SVM-Administrator sein
- Ein Active Azure Abonnement

### Einschränkungen

- AKV kann nur auf einer Daten-SVM konfiguriert werden
- NAE kann nicht mit AKV verwendet werden. NAE erfordert einen extern unterstützten KMIP-Server.

## 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 Azure Key Vault-App-Registrierung den Fensterbereich **Zertifikate & Geheimnisse** aus.
2. Wählen Sie **Neuer Client Secret**. Geben Sie einen aussagekräftigen Namen für Ihr Kundegeheimnis ein. NetApp empfiehlt einen 24-monatigen Verfallszeitraum. Ihre spezifischen Cloud Governance-Richtlinien erfordern jedoch unter Umständen eine andere Einstellung.
3. Klicken Sie auf **Hinzufügen**, um das Clientgeheimnis zu erstellen. Kopieren Sie die in der Spalte **Wert** aufgeführte geheime Zeichenfolge und speichern Sie sie an einem sicheren Ort zur späteren Verwendung in [Cloud Volumes ONTAP-Konfiguration](#). Der geheime Wert wird nach der Navigation von der Seite nicht erneut angezeigt.

### Erstellen Sie einen Azure Key Vault

1. Falls Sie bereits über einen Azure Schlüsselvault 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. Klicken Sie auf **+Erstellen** und geben Sie die erforderlichen Informationen einschließlich Ressourcengruppe, Region und Preisebene ein. Geben Sie außerdem die Anzahl der Tage ein, um gelöschte Vaults zu behalten, und wählen Sie **Spülschutz aktivieren** auf dem Schlüsselgewölbe aus.
4. Wählen Sie **Weiter**, um eine Zugriffsrichtlinie auszuwählen.
5. Wählen Sie die folgenden Optionen aus:
  - a. Wählen Sie unter **Zugriffskonfiguration** die Zugriffspolitik **Vault** aus.
  - b. Wählen Sie unter **Resource Access** **Azure Disk Encryption für Volume Encryption** aus.
6. Wählen Sie **+Create**, um eine Zugriffsrichtlinie hinzuzufügen.
7. Klicken Sie unter **Konfigurieren aus einer Vorlage** auf das Dropdown-Menü und wählen Sie dann die Vorlage **Schlüssel, Schlüssel und Zertifikatmanagement** aus.

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:** 20 ausgewählt
  - **Geheimberechtigungen:** 8 ausgewählt
  - **Zertifikatberechtigungen:** 16 ausgewählt

# Create an access policy



- 1 Permissions 2 Principal 3 Application (optional) 4 Review + create

Configure from a template

Key, Secret, & Certificate Management

## Key permissions

### Key Management Operations

- ☒ Select all
- ☒ Get
- ☒ List
- ☒ Update
- ☒ Create
- ☒ Import
- ☒ Delete
- ☒ Recover
- ☒ Backup
- ☒ Restore

### Cryptographic Operations

- ☒ Select all
- ☒ Decrypt
- ☒ Encrypt
- ☒ Unwrap Key
- ☒ Wrap Key
- ☒ Verify
- ☒ Sign

### Privileged Key Operations

- ☒ Select all
- ☒ Purge
- ☒ Release

### Rotation Policy Operations

- ☒ Select all
- ☒ Rotate
- ☒ Get Rotation Policy
- ☒ Set Rotation Policy

## Secret permissions

### Secret Management Operations

- ☒ Select all
- ☒ Get
- ☒ List
- ☒ Set
- ☒ Delete
- ☒ Recover
- ☒ Backup
- ☒ Restore

### Privileged Secret Operations

- ☒ Select all
- ☒ Purge

## Certificate permissions

### Certificate Management Operations

- ☒ Select all
- ☒ Get
- ☒ List
- ☒ Update
- ☒ Create
- ☒ Import
- ☒ Delete
- ☒ Recover
- ☒ Backup
- ☒ Restore
- ☒ Manage Contacts
- ☒ Manage Certificate Authorities
- ☒ Get Certificate Authorities
- ☒ List Certificate Authorities
- ☒ Set Certificate Authorities
- ☒ Delete Certificate Authorities

### Privileged Certificate Operations

- ☒ Select all
- ☒ Purge

Previous

Next

9. Klicken Sie auf **Weiter**, um die in erstellte Anwendung **Principal** Azure auszuwählen [Azure Application Registration](#). Wählen Sie **Weiter**.



Pro Richtlinie kann nur ein Principal zugewiesen werden.

## Create an access policy

Permissions **Principal** Application (optional) Review + create

Only 1 principal can be assigned per access policy.  
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

**Selected item**  
No item selected

Previous **Next**

10. Klicken Sie zweimal auf **Weiter**, bis Sie bei **Review und create** angekommen sind. Klicken Sie dann auf **Erstellen**.
11. Wählen Sie **Weiter**, um zu **Networking**-Optionen zu gelangen.
12. 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.)
13. 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 brauchen 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 Folgendes aus:

- **Microsoft.AzureActiveDirectory**
- **Microsoft.KeyVault**
- **Microsoft.Storage** (optional)

### SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

3 selected

Service	Status	
Microsoft.Storage	Succeeded	
Microsoft.AzureActiveDirectory	Succeeded	
Microsoft.KeyVault	Succeeded	

Service endpoint policies

0 selected

### SUBNET DELEGATION

Delegate subnet to a service ⓘ

None

### NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. [Learn more](#)

Private endpoint network policy

Disabled

Save

Cancel

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 key_vault_URI -key-id  
full_key_URI
```



Der `_full_key_URI` Wert muss den verwenden `<https:// <key vault host name>/keys/<key label>` Formatieren.

5. Nach der erfolgreichen Aktivierung von Azure Key Vault geben Sie den ein `client secret value` Wenn Sie dazu aufgefordert werden.

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: ekvip_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. Stellen Sie sicher, dass Ihre Azure Netzwerkrichtlinien und Ihr Routing Ihr privates vnet nicht an den öffentlichen Endpunkt von Azure

KeyVault blockieren. Falls dies der Fall ist, sollten sie einen Azure Private Endpunkt zum Zugriff auf den Schlüsselvaults innerhalb der vnet-Umgebung verwenden. Möglicherweise müssen Sie auch einen statischen Hosteintrag auf Ihrer SVM hinzufügen, um die private IP-Adresse für Ihren Endpunkt zu lösen.

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
```

## 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.

Bei der Verwendung von Cloud KMS ist zu beachten, dass standardmäßig die LIF einer Daten-SVM verwendet wird, um mit dem Endpunkt des Cloud-Schlüsselmanagements zu kommunizieren. 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.

### Bevor Sie beginnen

- Cloud Volumes ONTAP muss Version 9.10.1 oder höher ausführen
- Volume Encryption (VE)-Lizenz installiert
- Mandantenfähige MTEKM-Lizenz (Encryption Key Management) ist ab Cloud Volumes ONTAP 9.12.1 GA 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. Mit BlueXP können Sie zwei NetApp Lösungen für Ransomware implementieren: Schutz vor gängigen Ransomware-Dateierweiterungen und Autonomer Ransomware-Schutz (ARP). Diese Lösungen bieten effektive Tools für Transparenz, Erkennung und Behebung von Problemen.

## Schutz vor gängigen Ransomware-Dateiendungen

Die in BlueXP verfügbare Einstellung für den Schutz vor Ransomware ermöglicht Ihnen die Nutzung der ONTAP FPolicy Funktion zum Schutz vor gängigen Dateierweiterungen für Ransomware-Angriffe.

### Schritte

1. Doppelklicken Sie auf der Seite Bildschirm auf den Namen des Systems, das Sie für den Ransomware-Schutz konfigurieren.
2. Klicken Sie auf der Registerkarte Übersicht auf das Bedienfeld Funktionen und dann auf das Bleistiftsymbol neben **Ransomware-Schutz**.
3. 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

## Autonomer Schutz Durch Ransomware

Cloud Volumes ONTAP unterstützt die ARP-Funktion (Autonomous Ransomware Protection), die Workload-Analysen durchführt, um abnormale Aktivitäten, die auf einen Ransomware-Angriff hinweisen, proaktiv zu erkennen und zu warnen.

Trennen Sie sich von den Schutzmaßnahmen für die Dateierweiterung, die im bereitgestellt werden ["ransomware-Schutz-Einstellung"](#). Die ARP-Funktion verwendet Workload-Analyse, um den Benutzer auf mögliche Angriffe auf der Grundlage erkennt "abnorme Aktivität" zu warnen. Die Ransomware-Schutzeinstellung und die ARP-Funktion können in Verbindung für einen umfassenden Schutz vor Ransomware verwendet werden.

Die ARP-Funktion ist nur zur Verwendung mit BYOL-Lizenzen (Laufzeit von 1 bis 36 Monaten) sowohl für Node-basierte als auch für kapazitätsbasierte Lizenzmodell verfügbar. Wenden Sie sich an Ihren NetApp Vertriebsmitarbeiter, um eine neue, separate Add-on-Lizenz zur Verwendung mit der ARP-Funktion in Cloud Volumes ONTAP zu erwerben.

Die ARP Lizenz gilt als „fließende“ Lizenz, was bedeutet, dass sie nicht an eine einzelne Cloud Volumes ONTAP Instanz gebunden ist und auf mehrere Cloud Volumes ONTAP Umgebungen angewendet werden kann.



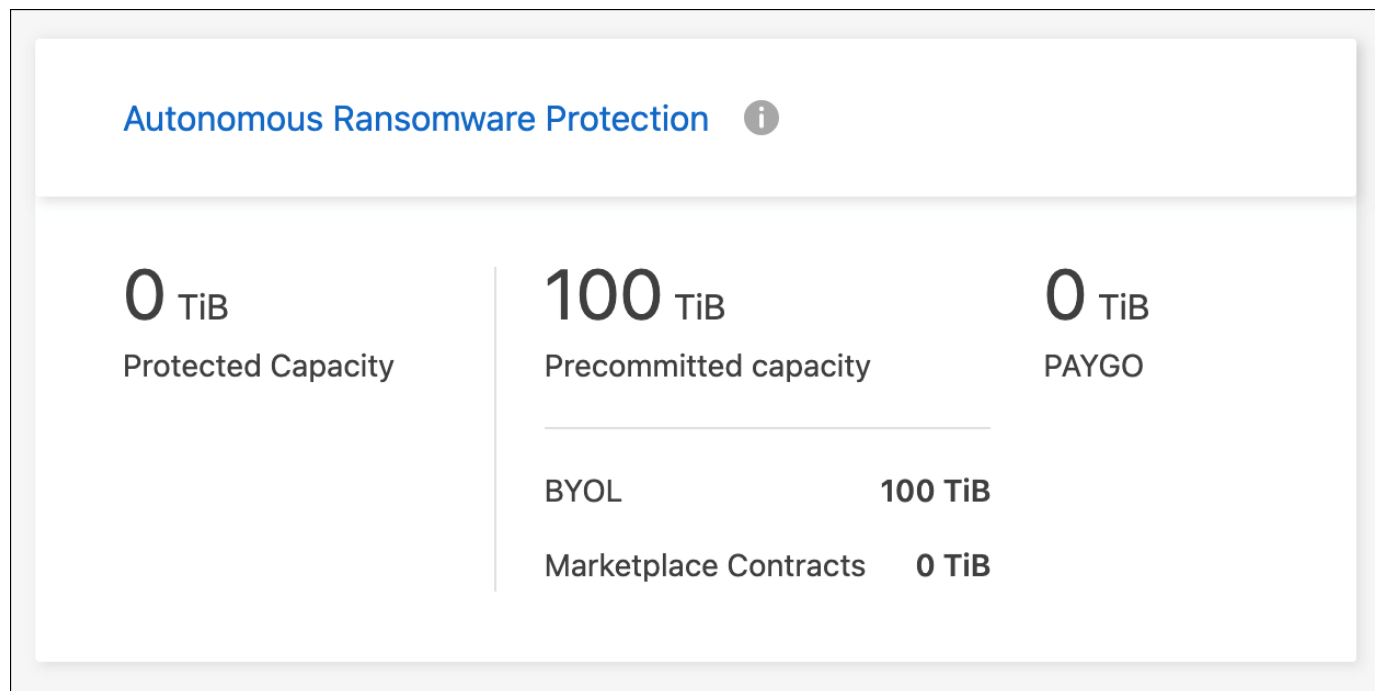
Die Verwendung der ARP-Funktion mit Node-basierten Cloud Volumes ONTAP-Lizenzen ist derzeit nicht in Digital Wallet enthalten. Die Möglichkeit, die Node-basierte ARP-Nutzung anzuzeigen, wird in einer zukünftigen Version unter Digital Wallet verfügbar sein.

Beim Kauf einer Add-on-Lizenz und beim Hinzufügen zur Digital Wallet können Sie ARP mit Cloud Volumes ONTAP auf Volume-Basis aktivieren. Die Abrechnung für ARP erfolgt auf Volume-Ebene entsprechend der insgesamt bereitgestellten Kapazität von Volumes mit aktivierter ARP-Funktion. Die minimale Lizenzkapazität beträgt 1 TB. Es gibt jedoch keine Mindestkapazitätsgebühren für die ARP-Funktion.

ARP-aktivierte Volumes haben einen bestimmten Status als „Lernmodus“ oder „aktiv“. Jede Lautstärke mit dem ARP-Status „deaktiviert“ ist vom Laden ausgeschlossen. Bei einer Cloud Volumes ONTAP-Umgebung mit 30 tib bereitgestellter Kapazität kann beispielsweise nur eine Teilmenge von 15 tib Volumes mit aktivierter ARP-Funktion gewählt werden.

Die Konfiguration von ARP für Volumes wird über ONTAP System Manager und ONTAP CLI durchgeführt.

Weitere Informationen zur Aktivierung von ARP mit ONTAP System Manager und CLI finden Sie unter ["Autonomer Schutz Vor Ransomware"](#).



Ohne Lizenz ist kein Support für die Nutzung lizenzierter Funktionen verfügbar.



## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.