セキュリティとデータ暗号化
Cloud Volumes ONTAP

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/storage-management-cloud-volumes-ontap/task-encrypting-volumes.html on February 13, 2026. Always check docs.netapp.com for the latest.

目次

セキュリティとデータ暗号化

NetApp暗号化ソリューションを使用してCloud Volumes ONTAP上のボリュームを暗号化する

Cloud Volumes ONTAP は、 NetApp Volume Encryption (NVE) とNetApp Aggregate Encryption (NAE) をサポートしています。 NVE と NAE は、ボリュームの FIPS 140-2 準拠の保存データ暗号化を可能にするソフトウェア ベースのソリューションです。"これらの暗号化ソリューションについて詳しく見る" 。

NVE と NAE はどちらも外部キー マネージャーでサポートされます。

] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[] ifdef::aws[] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[

AWS Key Management Service を使用してCloud Volumes ONTAP暗号化キーを管理する

使用できます"AWS のキー管理サービス (KMS)"AWS にデプロイされたアプリケーションでONTAP暗号化キーを保護します。

AWS KMS を使用したキー管理は、CLI またはONTAP REST API を使用して有効にできます。

KMS を使用する場合、クラウド キー管理エンドポイントとの通信にはデフォルトでデータ SVM の LIF が使用されることに注意してください。ノード管理ネットワークは、AWS の認証サービスとの通信に使用されます。クラスタ ネットワークが正しく設定されていないと、クラスタはキー管理サービスを適切に利用できません。

開始する前に

- Cloud Volumes ONTAP はバージョン 9.12.0 以降を実行している必要があります
- ボリューム暗号化（VE）ライセンスをインストールし、
- マルチテナント暗号化キー管理 (MTEKM) ライセンスがインストールされている必要があります。
- クラスタ管理者またはSVM管理者である必要があります。
- 有効なAWSサブスクリプションが必要です

データ SVM のキーのみを設定できます。

構成

AWS

1. 作成する必要があります"付与"暗号化を管理する IAM ロールによって使用される AWS KMS キー用。IAM ロールには、次の処理を許可するポリシーが含まれている必要があります。
    - `DescribeKey`

- Encrypt
- `Decrypt`助成金を作成するには、"AWSのドキュメント" 。

2. "適切な IAM ロールにポリシーを追加します。"この政策は、 DescribeKey 、 Encrypt 、 そして `Decrypt`操作。

Cloud Volumes ONTAP

1. Cloud Volumes ONTAP環境に切り替えます。
2. 高度な権限レベルに切り替えます:
   `set -privilege advanced`
3. AWS キーマネージャーを有効にします。
   `security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. プロンプトが表示されたら、シークレット キーを入力します。
5. AWS KMS が正しく設定されていることを確認します。
   `security key-manager external aws show -vserver svm_name`

Azure Key Vault を使用してCloud Volumes ONTAP暗号化キーを管理する

Azure Key Vault (AKV) を使用して、Azure にデプロイされたアプリケーション内のONTAP暗号化キーを保護できます。参照"Microsoftのドキュメント"。

AKV は、データ SVM のNetApp Volume Encryption (NVE) キーを保護するためにのみ使用できます。詳細については、 "ONTAPのドキュメント" 。

AKV によるキー管理は、CLI またはONTAP REST API を使用して有効にできます。

AKV を使用する場合、クラウド キー管理エンドポイントとの通信にはデフォルトでデータ SVM LIF が使用されることに注意してください。ノード管理ネットワークは、クラウド プロバイダーの認証サービス (login.microsoftonline.com) との通信に使用されます。クラスタ ネットワークが正しく設定されていないと、クラスタはキー管理サービスを適切に利用できません。

開始する前に

- Cloud Volumes ONTAP はバージョン 9.10.1 以降を実行している必要があります
- ボリューム暗号化 (VE) ライセンスがインストールされている (NetAppボリューム暗号化ライセンスは、NetAppサポートに登録されている各Cloud Volumes ONTAPシステムに自動的にインストールされます)
- マルチテナント暗号化キー管理（MT_EK_MGMT）ライセンスが必要です
- クラスタ管理者またはSVM管理者である必要があります。
- アクティブなAzureサブスクリプション

制限事項

- AKVはデータSVMでのみ構成できます
- NAE は AKV では使用できません。 NAE には外部でサポートされている KMIP サーバーが必要です。

- Cloud Volumes ONTAPノードは、アクセス可能性とキーの可用性を確認するために 15 分ごとに AKV をポーリングします。このポーリング期間は構成不可能であり、ポーリング試行が 4 回連続して失敗すると(合計 1 時間)、ボリュームはオフラインになります。

構成プロセス

概要を説明する手順では、 Cloud Volumes ONTAP構成を Azure に登録する方法と、Azure Key Vault とキーを作成する方法について説明します。これらの手順をすでに完了している場合は、特に以下の設定が正しいことを確認してください。Azure Key Vault を作成する 、次に進みましょうCloud Volumes ONTAP構成。

- Azure アプリケーション登録
- Azureクライアントシークレットを作成する
- Azure Key Vault を作成する
- 暗号化キーを作成する
- Azure Active Directory エンドポイントを作成する (HA のみ)
- Cloud Volumes ONTAP構成

Azure アプリケーション登録

1. まず、 Cloud Volumes ONTAP がAzure Key Vault にアクセスするために使用する Azure サブスクリプションにアプリケーションを登録する必要があります。 Azure ポータル内で、アプリの登録 を選択します。
2. 新規登録を選択します。
3. アプリケーションの名前を指定し、サポートされているアプリケーションの種類を選択します。 Azure Key Vault の使用には、デフォルトの単一テナントで十分です。 登録を選択します。
4. Azure の概要ウィンドウで、登録したアプリケーションを選択します。 アプリケーション **(**クライアント**) ID** と ディレクトリ **(**テナント**) ID** を安全な場所にコピーします。これらは、登録プロセスの後半で必要になります。

Azureクライアントシークレットを作成する

1. Azure Key Vault アプリ登録用の Azure portal で、**[**証明書とシークレット**]** ペインを選択します。
2. 新しいクライアント シークレット を選択します。クライアント シークレットに意味のある名前を入力します。 NetApp24 か月の有効期限を推奨していますが、特定のクラウド ガバナンス ポリシーによっては異なる設定が必要になる場合があります。
3. 追加 をクリックしてクライアント シークレットを作成します。 値列にリストされている秘密の文字列をコピーし、後で使用するために安全な場所に保存します。Cloud Volumes ONTAP構成 。ページから移動すると、秘密の値は再び表示されなくなります。

Azure Key Vault を作成する

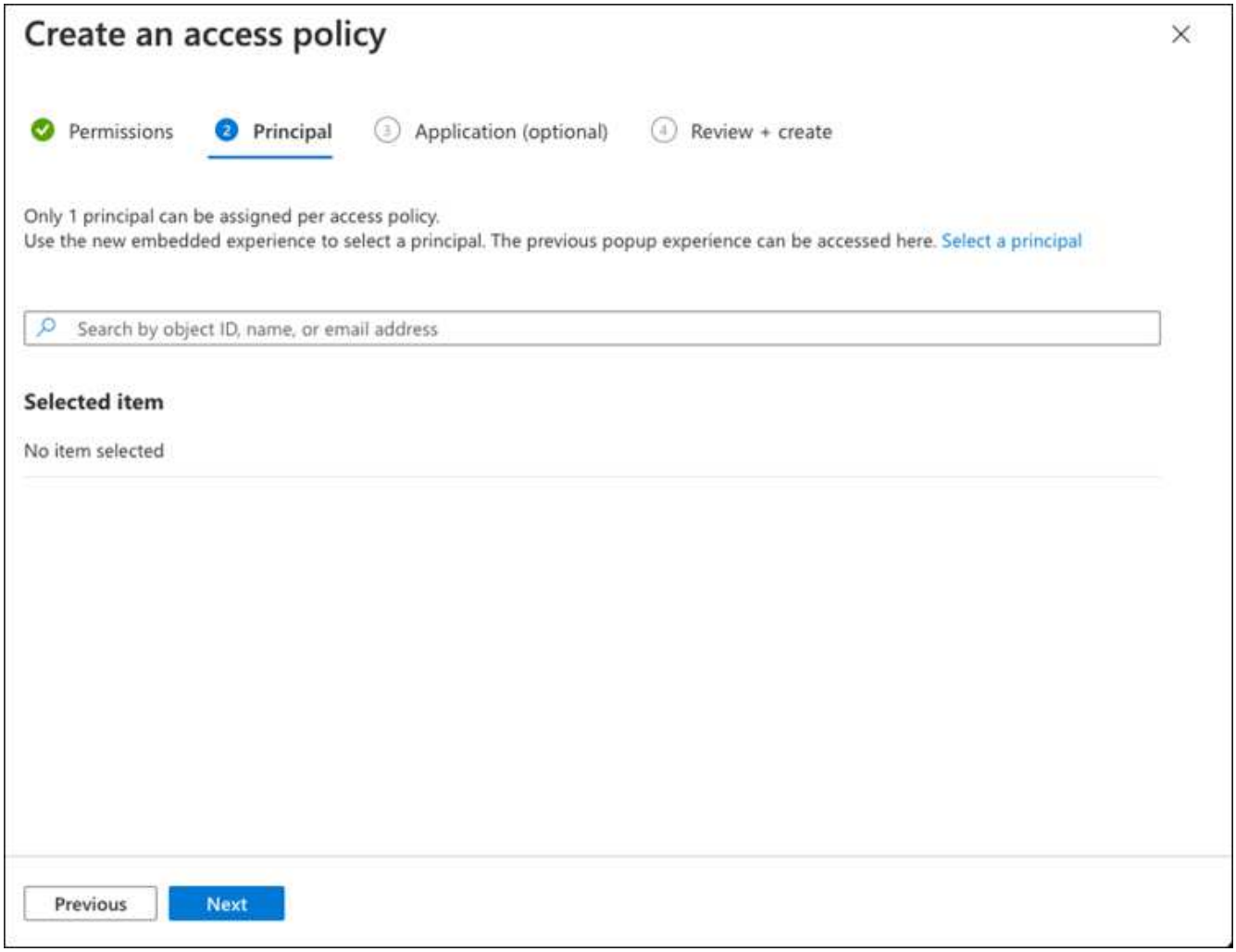
1. 既存の Azure Key Vault がある場合は、それをCloud Volumes ONTAP構成に接続できます。ただし、このプロセスではアクセス ポリシーを設定に合わせて調整する必要があります。
2. Azure ポータルで、**Key Vaults** セクションに移動します。
3. [**+** 作成] をクリックし、リソース グループ、リージョン、価格レベルなどの必要な情報を入力します。さらに、削除されたコンテナーを保持する日数を入力し、キー コンテナーで [消去保護を有効にする] を選択します。
4. アクセス ポリシーを選択するには、[次へ] を選択します。

5. 次のオプションを選択します。
   a. アクセス構成 で、**Vault** アクセス ポリシー を選択します。
   b. リソース アクセス で、ボリューム暗号化用の **Azure Disk Encryption** を選択します。
6. アクセス ポリシーを追加するには、[**+** 作成] を選択します。
7. テンプレートから構成 の下で、ドロップダウン メニューをクリックし、キー、シークレット、および証明書の管理 テンプレートを選択します。
8. 各ドロップダウン権限メニュー (キー、シークレット、証明書) を選択し、メニュー リストの上部にある [すべて選択] をクリックして、使用可能なすべての権限を選択します。次のものが必要です:
   - キー権限: 20個選択済み
   - 秘密の権限: 8 個選択済み
   - 証明書の権限: 16 個選択済み


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. 次へ をクリックして、プリンシパル Azure登録アプリケーションを選択します。Azure アプリケーション登録 。次へを選択します。

   ポリシーごとに割り当てることができるプリンシパルは 1 つだけです。



10. **[確認と作成]** に到達するまで **[次へ]** を 2 回クリックします。次に、[作成] をクリックします。
11. 次へ を選択して、ネットワーク オプションに進みます。
12. 適切なネットワーク アクセス方法を選択するか、すべてのネットワーク と 確認 **+** 作成 を選択してキーコンテナーを作成します。 (ネットワーク アクセス方法は、ガバナンス ポリシーまたは企業のクラウドセキュリティ チームによって規定される場合があります。)
13. Key Vault URI を記録します。作成した Key Vault で、[概要] メニューに移動し、右側の列から **Vault URI** をコピーします。これは後のステップで必要になります。

暗号化キーを作成する

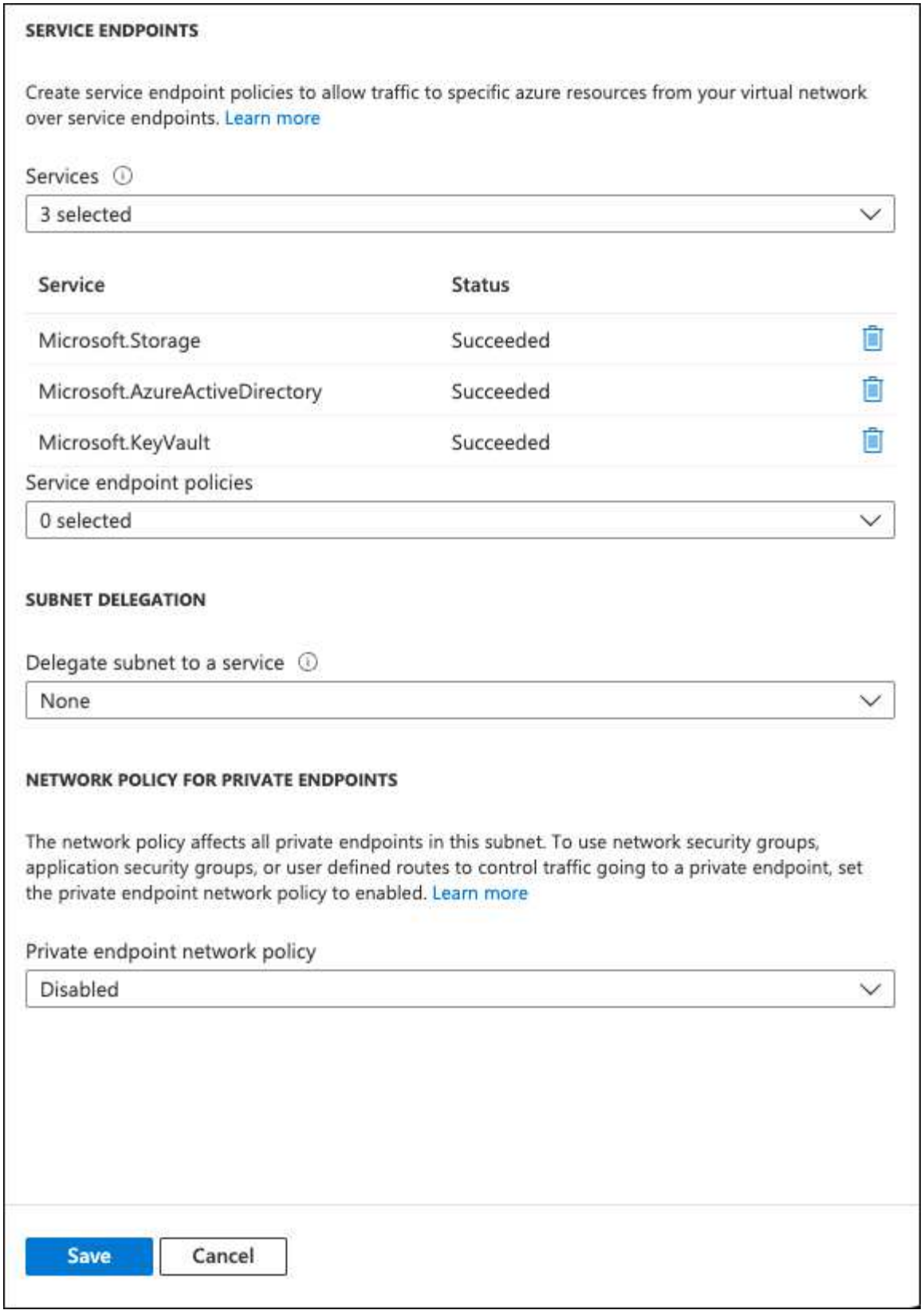
1. Cloud Volumes ONTAP用に作成した Key Vault のメニューで、[**Keys**] オプションに移動します。
2. 新しいキーを作成するには、[生成/インポート] を選択します。
3. デフォルト オプションは [生成] に設定したままにします。
4. 次の情報を入力します。

- 暗号化キー名
- キータイプ: RSA
- RSA鍵サイズ: 2048
- 有効: はい

5. 暗号化キーを作成するには、[作成] を選択します。
6. キー メニューに戻り、作成したキーを選択します。
7. キーのプロパティを表示するには、[現在のバージョン] の下のキー ID を選択します。
8. キー識別子 フィールドを見つけます。 URI を 16 進文字列までコピーします (16 進文字列は含まれません)。

Azure Active Directory エンドポイントを作成する **(HA** のみ**)**

1. このプロセスは、HA Cloud Volumes ONTAPシステム用に Azure Key Vault を構成する場合にのみ必要です。
2. Azure ポータルで、仮想ネットワーク に移動します。
3. Cloud Volumes ONTAPシステムを導入した仮想ネットワークを選択し、ページの左側にある [サブネット] メニューを選択します。
4. リストからCloud Volumes ONTAPデプロイメントのサブネット名を選択します。
5. サービス エンドポイント の見出しに移動します。ドロップダウン メニューで、以下を選択します。
   - **Microsoft.AzureActiveDirectory**
   - **Microsoft.KeyVault**
   - **Microsoft.Storage** (オプション)



6. 設定を保存するには、[保存] を選択します。

Cloud Volumes ONTAP構成

1. 好みの SSH クライアントを使用してクラスタ管理 LIF に接続します。
2. ONTAPで高度な権限モードに入ります。

```
set advanced -con off
```

3. 必要なデータ SVM を識別し、その DNS 構成を確認します。
`vserver services name-service dns show`

   a. 目的のデータ SVM の DNS エントリが存在し、それに Azure DNS のエントリが含まれている場合は、アクションは必要ありません。そうでない場合は、Azure DNS、プライベート DNS、またはオンプレミス サーバーを指すデータ SVM の DNS サーバー エントリを追加します。これは、クラスタ管理 SVM のエントリと一致する必要があります。
   `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`

   b. データ SVM に対して DNS サービスが作成されたことを確認します。
   `vserver services name-service dns show`

4. アプリケーションの登録後に保存されたクライアント ID とテナント ID を使用して Azure Key Vault を有効にします。
`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`

   その `_full_key_URI`価値を活用する必要がある `<https:// <key vault host name>/keys/<key label>`形式。

5. Azure Key Vaultの有効化に成功したら、 `client secret value`プロンプトが表示されたら。

6. キー マネージャーのステータスを確認します。
`security key-manager external azure check`出力は次のようになります。

```
::*> 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.
```

もし `service_reachability`ステータスは `OK`SVM は、必要なすべての接続とアクセス許可を備えて Azure Key Vault サービスにアクセスできません。 Azure ネットワーク ポリシーとルーティングによって、プライベート vNet が Azure Key Vault パブリック エンドポイントに到達するのがブロックされないようにしてください。そうなる場合は、Azure プライベート エンドポイントを使用して、vNet 内から

Key Vault にアクセスすることを検討してください。エンドポイントのプライベート IP アドレスを解決するには、SVM に静的ホスト エントリを追加する必要もあります。

その `kms_wrapped_key_status`報告します `UNKNOWN`初期設定時。ステータスは次のように変わります `OK`最初のボリュームが暗号化された後。

7. オプション: NVE の機能を検証するためのテスト ボリュームを作成します。

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

   正しく設定されていれば、 Cloud Volumes ONTAP は自動的にボリュームを作成し、ボリュームの暗号化を有効にします。

8. ボリュームが正しく作成され、暗号化されていることを確認します。もしそうなら、 `-is-encrypted` パラメータは次のように表示されます `true`。
   ```
   vol show -vserver SVM_name -fields is-encrypted
   ```

9. オプション: Azure Key Vault 認証証明書の資格情報を更新する場合は、次のコマンドを使用します。
   ```
   security key-manager external azure update-credentials -vserver v1
   -authentication-method certificate
   ```

関連リンク

- "Azureで顧客管理キーを使用するようにCloud Volumes ONTAPを設定する"
- "Microsoft Azure ドキュメント: Azure Key Vault について"
- "ONTAPコマンドリファレンスガイド"

Google Cloud KMS でCloud Volumes ONTAP の暗号化キーを管理する

使用できます"Google Cloud Platform の鍵管理サービス (Cloud KMS)"Google Cloud Platform にデプロイされたアプリケーションでCloud Volumes ONTAP暗号化キーを保護します。

Cloud KMS によるキー管理は、 ONTAP CLI またはONTAP REST API を使用して有効にできます。

Cloud KMS を使用する場合、デフォルトではデータ SVM の LIF を使用してクラウド キー管理エンドポイントと通信することに注意してください。ノード管理ネットワークは、クラウド プロバイダーの認証サービス (oauth2.googleapis.com) との通信に使用されます。クラスタ ネットワークが正しく設定されていないと、クラスタはキー管理サービスを適切に利用できません。

開始する前に

- システムではCloud Volumes ONTAP 9.10.1以降が実行されている必要があります
- データ SVM を使用する必要があります。 Cloud KMS はデータ SVM でのみ構成できます。
- クラスタ管理者またはSVM管理者である必要があります。
- ボリューム暗号化（VE）ライセンスをSVMにインストールする必要があります
- Cloud Volumes ONTAP 9.12.1 GA以降では、マルチテナント暗号化キー管理（MTEKM）ライセンスもイ

ンストールする必要があります。

- 有効な Google Cloud Platform サブスクリプションが必要です

構成

Google Cloud

1. Google Cloud環境では、"対称GCPキーリングとキーを作成する" 。
2. Cloud KMS キーとCloud Volumes ONTAPサービス アカウントにカスタム ロールを割り当てます。
   a. カスタム ロールを作成します。

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

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersio
ns.list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVer
sions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,clou
dkms.locations.get,cloudkms.locations.list,resourcemanager.projects.g
et
    --stage=GA
```

   b. 作成したカスタム ロールを割り当てます。
   `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`

> Cloud Volumes ONTAP 9.13.0 以降を使用している場合は、カスタム ロールを作成する必要はありません。定義済みの[cloudkms.cryptoKeyEncrypterDecrypter^] の役割。

3. サービス アカウントの JSON キーをダウンロードします:
   `gcloud iam service-accounts keys create key-file --iam-account=`*`sa-name`*`@`*`project-id`*`.iam.gserviceaccount.com`

Cloud Volumes ONTAP

1. 好みの SSH クライアントを使用してクラスタ管理 LIF に接続します。
2. 高度な権限レベルに切り替えます:
   `set -privilege advanced`
3. データ SVM の DNS を作成します。
   `dns create -domains c.<`*`project`*`>.internal -name-servers` *`server_address`* `-vserver` *`SVM_name`*
4. CMEK エントリを作成します。
   `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. プロンプトが表示されたら、GCP アカウントのサービス アカウント JSON キーを入力します。
6. 有効化されたプロセスが成功したことを確認します。
`security key-manager external gcp check -vserver *svm_name*`
7. オプション: 暗号化をテストするためのボリュームを作成する `vol create *volume_name* -aggregate *aggregate* -vserver *vserver_name* -size 10G`

トラブルシューティング

トラブルシューティングが必要な場合は、上記の最後の 2 つの手順で生の REST API ログを tail できます。

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

Cloud Volumes ONTAPでNetAppランサムウェア保護ソリューションを有効にする

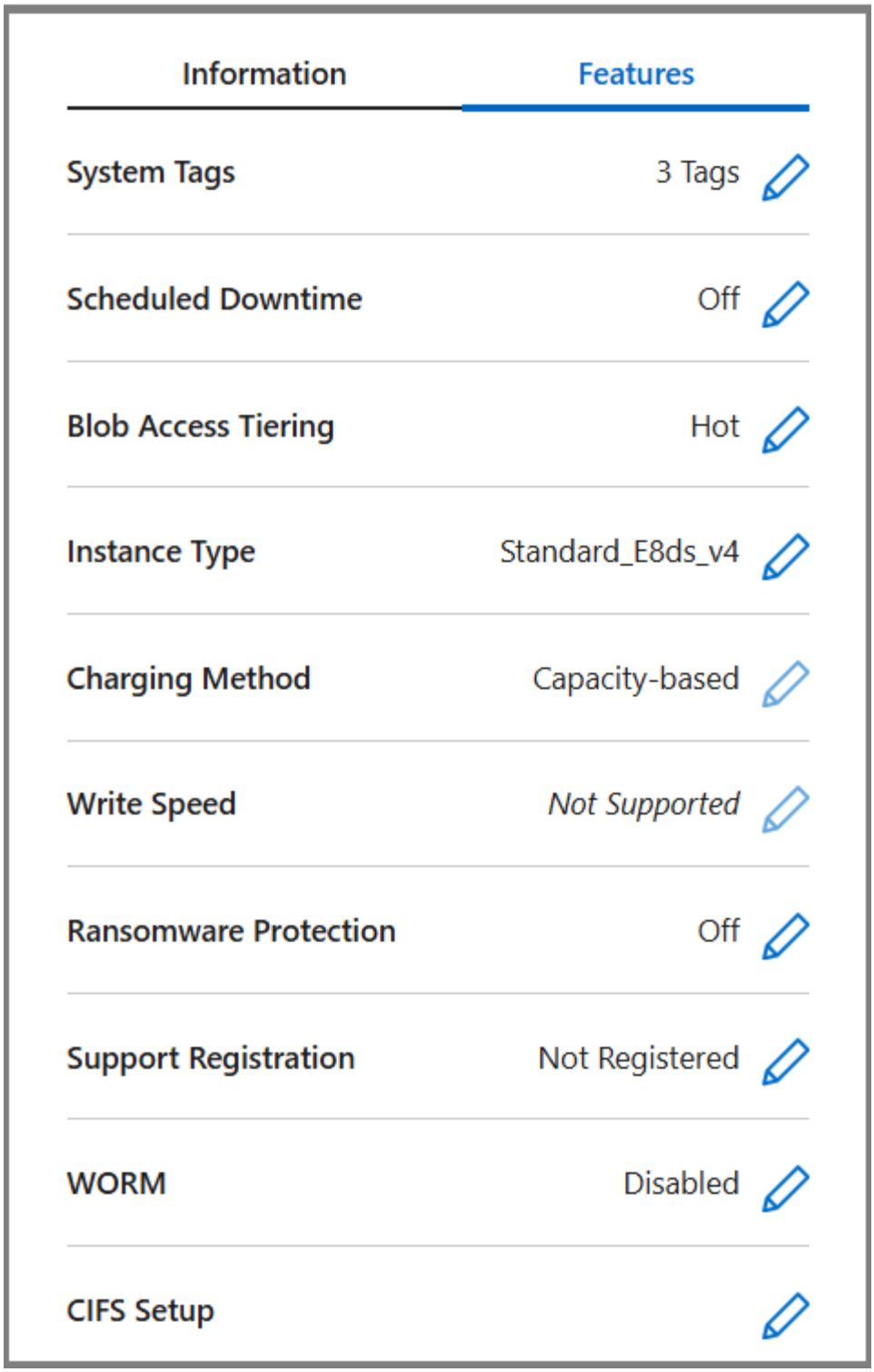
ランサムウェア攻撃は、企業の時間、リソース、評判に損害を与える可能性があります。 NetApp Consoleを使用すると、一般的なランサムウェア ファイル拡張子からの保護と自律ランサムウェア保護 (ARP) という 2 つのランサムウェア対策NetAppソリューションを実装できます。これらのソリューションは、可視性、検出、修復のための効果的なツールを提供します。

一般的なランサムウェアのファイル拡張子からの保護

コンソールで利用可能なランサムウェア保護設定を使用すると、 ONTAP FPolicy 機能を利用して、一般的なランサムウェアのファイル拡張子タイプから保護することができます。

手順

1. *システム*ページで、ランサムウェア保護を使用するように構成したCloud Volumes ONTAPシステムの名前をダブルクリックします。
2. [概要] タブで [機能] パネルをクリックし、[ランサムウェア保護] の横にある鉛筆アイコンをクリックします。



3. ランサムウェアに対するNetAppソリューションを実装します。

   a. スナップショット ポリシーが有効になっていないボリュームがある場合は、[スナップショット ポリシーのアクティブ化] をクリックします。

      NetApp Snapshot テクノロジーは、ランサムウェア修復のための業界最高のソリューションを提供します。復旧を成功させる鍵は、感染していないバックアップから復元することです。スナップショット コピーは読み取り専用であるため、ランサムウェアによる破損を防ぎます。また、単一のファイルコピーまたは完全な災害復旧ソリューションのイメージを作成するための細分性も提供できます。

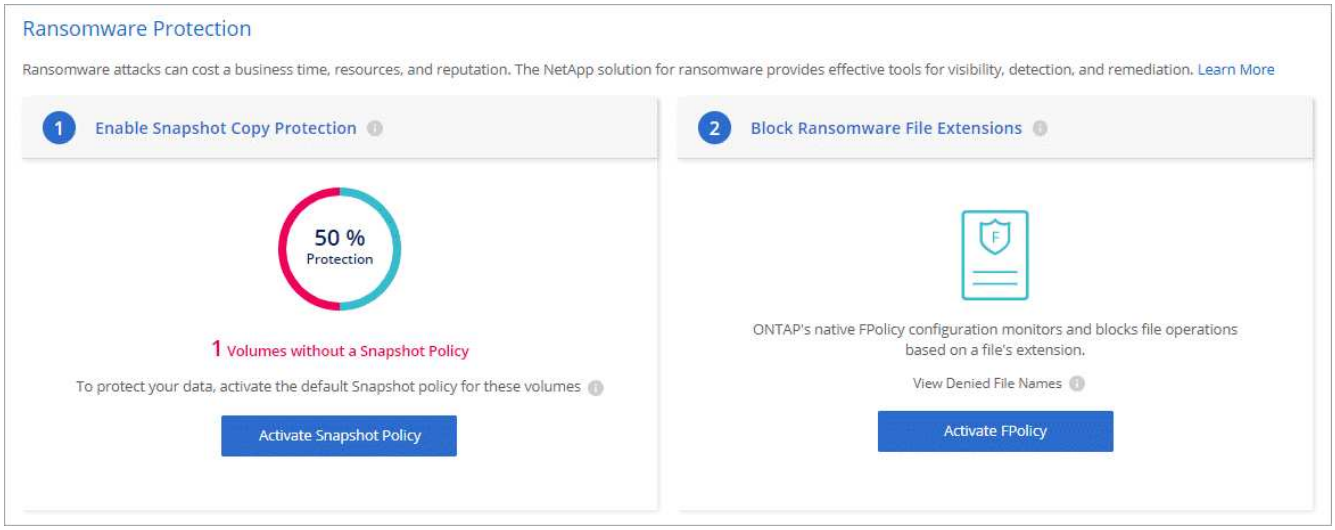
b. **FPolicy** のアクティブ化 をクリックして、ファイルの拡張子に基づいてファイル操作をブロックできる ONTAP の FPolicy ソリューションを有効にします。

この予防ソリューションは、一般的なランサムウェア ファイルの種類をブロックすることで、ランサムウェア攻撃からの保護を強化します。

デフォルトの FPolicy スコープは、次の拡張子を持つファイルをブロックします。

micro、暗号化、ロック、暗号、crypt、crinf、r5a、XRNT、XTBL、R16M01D05、pzdc、良い、LOL!、OMG!、RDM、RRK、encryptedRS、crjoker、EnCiPhErEd、LeChiffre

このスコープは、Cloud Volumes ONTAPで FPolicy をアクティブ化すると作成されます。リストは、一般的なランサムウェアのファイルタイプに基づいています。 Cloud Volumes ONTAP CLI の *vserver fpolicy policy scope* コマンドを使用して、ブロックされるファイル拡張子をカスタマイズできます。



自律型ランサムウェア対策

Cloud Volumes ONTAP は、ワークロードを分析して、ランサムウェア攻撃の兆候となる可能性のある異常なアクティビティをプロアクティブに検出し、警告する Autonomous Ransomware Protection (ARP) 機能をサポートしています。

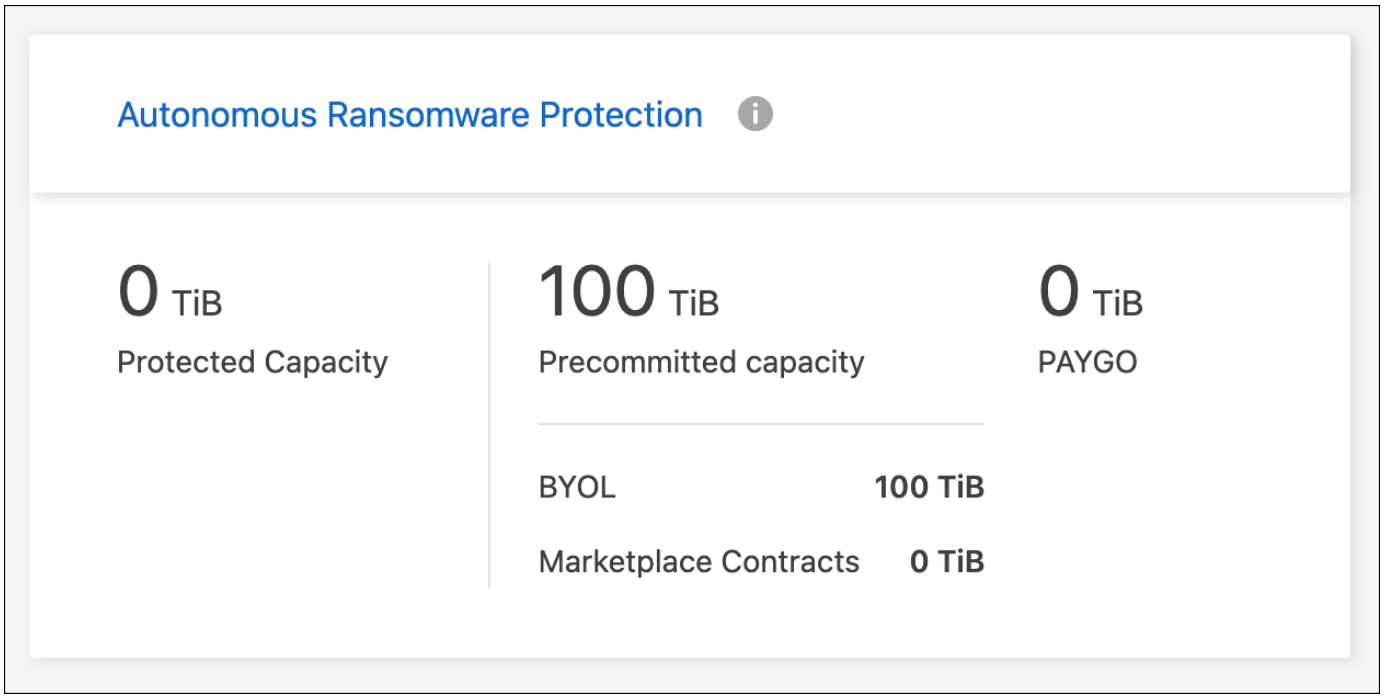
提供されるファイル拡張子保護とは別に、 "ランサムウェア保護設定" ARP 機能はワークロード分析を使用して、検出された「異常なアクティビティ」に基づいて潜在的な攻撃をユーザーに警告します。ランサムウェア保護設定と ARP 機能の両方を組み合わせて使用することで、包括的なランサムウェア保護を実現できます。

ARP 機能は、BYOL (個人ライセンス使用) およびマーケットプレイス サブスクリプションで追加料金なしでご利用いただけます。

ARP 対応ボリュームには、「学習モード」または「アクティブ」という指定状態があります。

ボリュームの ARP の設定は、 ONTAP System Manager およびONTAP CLI を通じて実行されます。

ONTAP System ManagerおよびONTAP CLIでARPを有効にする方法の詳細については、 "ONTAPドキュメント: 自律型ランサムウェア保護の有効化" 。



Cloud Volumes ONTAPで WORM ファイルの改ざん防止スナップショット コピーを作成します

Cloud Volumes ONTAPシステムで、一度だけ書き込み、何度も読み取る (WORM) ファイルの改ざん防止スナップショット コピーを作成し、特定の保持期間にわたってスナップショットを変更されていない形式で保持することができます。この機能はSnapLockテクノロジーを活用しており、データ保護とコンプライアンスをさらに強化します。

開始する前に

スナップショット コピーの作成に使用するボリュームがSnapLockボリュームであることを確認します。ボリューム上でSnapLock保護を有効にする方法については、 "ONTAPドキュメント: SnapLockの設定" 。

手順

1. SnapLockボリュームからスナップショット コピーを作成します。 CLIまたはSystem Managerを使用してスナップショットコピーを作成する方法については、 "ONTAPドキュメント: ローカルスナップショットコピーの管理の概要" 。

   スナップショット コピーはボリュームの WORM プロパティを継承し、改ざん防止になります。基盤となるSnapLockテクノロジにより、指定された保持期間が経過するまで、スナップショットは編集や削除から保護されます。

2. これらのスナップショットを編集する必要がある場合は、保持期間を変更できます。詳細については、 "ONTAPドキュメント: 保持期間を設定する" 。

   スナップショット コピーは特定の保持期間保護されていますが、 Cloud Volumes ONTAPの WORM ストレージは「信頼できるストレージ管理者」モデルで動作するため、クラスター管理者はソース ボリュームを削除できます。さらに、信頼できるクラウド管理者は、クラウド ストレージ リソースを操作して WORM データを削除できます。

関連リンク

- WORMの詳細については、以下を参照してください。"Cloud Volumes ONTAPの WORM ストレージについて学ぶ" 。
- SnapLockボリュームの充電については、以下を参照してください。"Cloud Volumes ONTAPのライセンスと課金" 。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。