セキュリティとデータ暗号化
Cloud Volumes ONTAP

NetApp
July 11, 2022

目次

セキュリティとデータ暗号化

ネットアップの暗号化ソリューションによるボリュームの暗号化

Cloud Volumes ONTAP は、 NetApp Volume Encryption （ NVE ）および NetApp Aggregate Encryption （ NAE ）をサポートしています。NVEとNAEは、FIPS 140-2に準拠したボリュームの保管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の詳細については、こちらをご覧ください"。

NVE と NAE はどちらも外部キー管理機能でサポートされています。

外部キー管理ツールを設定すると、新しいアグリゲートで NAE がデフォルトで有効になります。NAE アグリゲートに含まれない新しいボリュームでは、 NVE がデフォルトで有効になります（たとえば、外部キー管理ツールを設定する前に作成された既存のアグリゲートがある場合）。

Cloud Volumes ONTAP はオンボードキー管理をサポートしていません。

Cloud Volumes ONTAP システムがネットアップサポートに登録されている必要があります。ネットアップサポートに登録されている各 Cloud Volumes ONTAP システムには、 NetApp Volume Encryption ライセンスが自動的にインストールされます。

- "Cloud Manager へのネットアップサポートサイトのアカウントの追加"
- "従量課金制システムの登録"

Cloud Manager は、中国地域のシステムに NVE ライセンスをインストールしません。

手順

1. でサポートされているキー管理ツールのリストを確認します "NetApp Interoperability Matrix Tool で確認できます"。

   Key Managers * ソリューションを検索します。

2. "Cloud Volumes ONTAP CLI に接続します"。
3. 外部キー管理を設定
   - AWS "手順については、 ONTAP のドキュメントを参照してください"
     - Azure "Azure キーボールト（ AKV ）"
     - Google Cloud "Google Cloud Key Management Serviceの略"

Azure Key Vaultを使用してキーを管理します

を使用できます "Azure キーボールト（ AKV ）" Azureで導入されたアプリケーションでONTAP 暗号化キーを保護するため。

AKVは保護に使用できます "NetApp Volume Encryption （ NVE ）キー" データSVMの場合のみ。

AKV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。

AKVを使用する場合、デフォルトではクラウドキー管理エンドポイントとの通信にデータ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、クラスタでキー管理サービスが適切に利用されません。

前提条件

- Cloud Volumes ONTAP でバージョン9.10.1以降が実行されている必要があります
- Volume Encryption（VE）ライセンスがインストールされている（ネットアップサポートに登録されている各Cloud Volumes ONTAP システムにNetApp Volume Encryptionライセンスが自動的にインストールされる）
- Multi-tenant Encryption Key Management （ MTEKM ）ライセンスがインストールされています
- クラスタ管理者またはSVMの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

- AKVはデータSVM上でのみ設定できます

設定プロセス

AzureにCloud Volumes ONTAP 構成を登録する方法と、Azure Key Vaultとキーを作成する方法を概説しています。これらの手順をすでに完了している場合は、特に、で正しい設定を行っていることを確認してください Azureキーバックアップを作成しますをクリックし、に進みます 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キーバックアップを作成します
- 暗号化キーを作成します
- Azure Active Directoryエンドポイントの作成（HAのみ）
- Cloud Volumes ONTAP 構成

Azureアプリケーション登録

1. Cloud Volumes ONTAP からAzure Key Vaultへのアクセスに使用するAzureサブスクリプションにアプリケーションを登録しておく必要があります。Azureポータルで、アプリケーション登録を選択します。
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タイプを選択します。デフォルトの単一テナントでAzure Key Vaultの使用量が十分に設定されていること。[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**およびディレクトリ（テナント）**ID**を安全な場所にコピーします。これらの情報は、後で登録プロセスで必要になります。

Azureクライアントシークレットを作成する

1. Cloud Volumes ONTAP アプリケーション用のAzureポータルで、[** Ceritificates & secrets]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クライアントシークレットに意味のある名前を入力してください。ネットアップでは24カ月の有効期限を推奨していますが、クラウドガバナンスポリシーによっては、別の設定が必要になる場合があります。
3. クライアントシークレットを保存するには、[追加]を選択します。シークレットの値**をすぐにコピーして、将来の設定のために安全な場所に保管してください。ページから移動してもシークレット値は表示されません。

Azureキーバックアップを作成します

1. 既存のAzure Key Vaultを使用している場合は、Cloud Volumes ONTAP 構成に接続できますが、アクセスポリシーをこのプロセスの設定に合わせる必要があります。
2. Azureポータルで、[** Key Vaults（キーボルト）]セクションに移動します。
3. [作成]を選択します。リソースグループ、地域、価格階層などの必要な情報を入力し、削除されたボールトを保持する日数と、パージ保護が有効かどうかを選択します。この構成ではデフォルトで十分ですが、クラウドガバナンスポリシーごとに異なる設定が必要になる場合があります。
4. アクセスポリシーを選択するには、 **Next**を選択してください。
5. ボリューム暗号化オプションとして[**Azure Disk Encryption]**を選択し、権限モデルとして**[**Vault access policy]を選択します。
6. ［アクセスポリシーの追加］を選択します。
7. [テンプレートから構成する（オプション）]フィールドの横にあるキャレットを選択します。次に、[**Key]**、**[Secret]**、**[Certification Management]**を選択します。
8. 各ドロップダウンメニュー(キー、シークレット、証明書)を選択し、メニューリストの一番上にある**[All]**を選択して、使用可能なすべてのアクセス許可を選択します。次の作業を完了しておきます
   - キー権限:19が選択されています
   - シークレット権限:8が選択されています
   - 証明書のアクセス許可:16が選択されています
9. アクセスポリシーを作成するには、[**追加]を選択します。
10. **Next**を選択して、**Networking**オプションに進みます。
11. 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およびレビュー**+**作成を選択して、キーボールトを作成します。（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ている場合があります）。
12. キーボールトURIを記録します。作成したキーボールトで、概要メニューに移動し、右側のカラムから**Vault URI** をコピーします。これは、あとの手順で必要になります。

暗号化キーを作成します

1. Cloud Volumes ONTAP 用に作成したキー・ボールトのメニューで、[**Keys**（キー**）]オプションに移動します。
2. [生成/インポート]を選択して、新しいキーを作成します。
3. デフォルトのオプションは **Generate** のままにしておきます。
4. 次の情報を入力します。

- 暗号化キー名
- キータイプ：rsa
- RSAキーのサイズ：2048
- Enabled：はい

5. [**Create]を選択して、暗号キーを作成します。
6. [**Keys**（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、[**Current version**（現在のバージョン**）]でキーIDを選択します。
8. [**Key Identifier**（キー識別子**）]フィールドを探します。URIを16進数の文字列以外の値にコピーします。

Azure Active Directoryエンドポイントの作成（**HA**のみ）

1. このプロセスは、HA Cloud Volumes ONTAP 作業環境用にAzure Key Vaultを設定する場合にのみ必要です。
2. Azureポータルで、**Virtual Networks**に移動します。
3. Cloud Volumes ONTAP 作業環境を展開した仮想ネットワークを選択し、ページの左側にある **Subnets** メニューを選択します。
4. Cloud Volumes ONTAP 環境のサブネット名をリストから選択します。
5. [サービスエンドポイント]見出しに移動します。ドロップダウンメニューで、リストから**Microsoft.AzureActiveDirectory** を選択します。
6. 保存を選択して、設定を取得します。

Cloud Volumes ONTAP 構成

1. 優先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advanced権限モードに切り替えます。「set advanced-con off`」
3. 目的のデータSVMを特定し、そのDNS設定を確認します。「vserver services name-service dns show
   a. 目的のデータSVMのDNSエントリが存在し、そのエントリにAzure DNSのエントリが含まれている場合は、対処は必要ありません。表示されない場合は、Azure DNS、プライベートDNS、またはオンプレミスサーバを指すデータSVMのDNSサーバエントリを追加します。これは、クラスタ管理SVMのエントリと一致している必要があります。vserver services name-service dns create -vserver _svm_name -domains_domain_name-servers _ip_address _'
   b. データSVM用に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_caz_client_client_ID_tenant_ID_name_azure-name_aze_key_name_-key_key_id_azure_key_id_id_`
5. キー管理ツールの構成を確認します。「security key-manager external Azure show
6. キー管理ツール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.
```

「SERVICE_Reachability」ステータスが「OK」でない場合、SVMは必要なすべての接続および権限を使用してAzure Key Vaultサービスに到達できません。初期構成で'kms _ wrapped _key_status'は'unknown'を報告します最初のボリュームが暗号化されると'ステータスはOKに変わります

7. オプション：NVEの機能を検証するテストボリュームを作成する

   vol create -vserver_svm_name_-volume_name_-aggregate _aggr_size_state online -policy default'

   正しく設定されていれば、Cloud Volumes ONTAP でボリュームが自動的に作成され、ボリューム暗号化が有効になります。

8. ボリュームが正しく作成および暗号化されたことを確認します。その場合、「-is-encrypted」パラメータは「true」と表示されます。vol show -vserver_svm_name_-fields is-cencryptedです

GoogleのCloud Key Management Serviceを使用してキーを管理します

を使用できます "Google Cloud Platform のキー管理サービス（ Cloud KMS ）" Google Cloud Platform導入アプリケーションでONTAP 暗号化キーを保護します。

Cloud KMSを使用したキー管理は、CLIまたはONTAP REST APIを使用して有効にすることができます。

Cloud KMSを使用する際は、デフォルトでデータSVM LIFがクラウドキー管理エンドポイントとの通信に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、クラスタでキー管理サービスが適切に利用されません。

前提条件

- Cloud Volumes ONTAP でバージョン9.10.1以降が実行されている必要があります

- Volume Encryption （ VE ）ライセンスがインストールされている
- Multi-tenant Encryption Key Management （ MTEKM ）ライセンスがインストールされています
- クラスタ管理者またはSVMの管理者である必要があります
- アクティブなGoogle Cloud Platformサブスクリプション

制限

- クラウドKMSはデータSVMでのみ設定できます

設定

Google Cloud

1. Google Cloud環境では、 "対称GCPキーリングとキーを作成します"。
2. Cloud Volumes ONTAP サービスアカウント用の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.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. カスタムロールをCloud KMSキーとCloud Volumes ONTAP サービスアカウントに割り当てます。「gcloud kms keys add -iam-policy binding_key_name_-- keyring_key_ring_name — location_key_location_- member serviceAccount ：_service_account_Name — role project_id_id_roles/custommskmsk`key
4. 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. 優先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. advanced権限レベルに切り替えます:'set -privilege advanced
3. データSVM用のDNSを作成’dns create -domains C.<プロジェクト>.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JSONキーを入力します。
6. 有効な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「vol create _volume_name」をテストするボリュームを作成します。-aggregate -aggregate_aggregate_aggregate—vserver vserver_name _size 10Gです

トラブルシューティングを行う

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REST APIのrawログをテールできます。

1. 「set d`」
2. 「systemshell -node _node」コマンドtail -f /mroot/etc/log/mlog/kmip2_client.log

ランサムウェアからの保護を強化

ランサムウェア攻撃は、ビジネス時間、リソース、評判を低下させる可能性があります。Cloud Manager では、ランサムウェアに対応したネットアップソリューションを実装できます。これにより、可視化、検出、修復のための効果的なツールが提供されます。

この機能を使用すると、ランサムウェアに対する保護を強化し、とは別のユースケースに対処できます "ONTAP ランサムウェア対策機能" 有効にするには、System ManagerまたはONTAP CLIを使用します。

手順

1. 作業環境で、「 * ランサムウェア * 」アイコンをクリックします。

2. ネットアップのランサムウェア向けソリューションを導入する：

   a. Snapshot 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、 * Snapshot ポリシーのアクティブ化 * をクリックします。

      NetApp Snapshot テクノロジは、ランサムウェアの修復に業界最高のソリューションを提供します。リカバリを成功させるには、感染していないバックアップからリストアすることが重要です。Snapshot コピーは読み取り専用であり、ランサムウェアによる破損を防止します。単一のファイルコピーまたは完全なディザスタリカバリソリューションのイメージを作成する際の単位を提供することもできます。

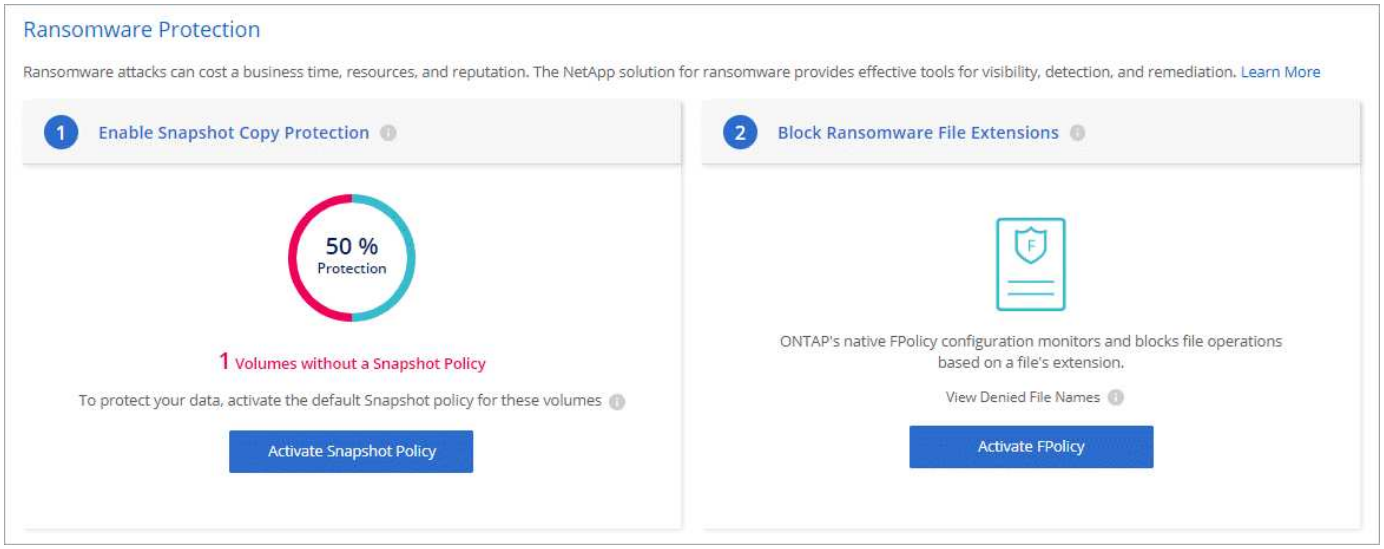
   b. FPolicy のアクティブ化 * をクリックして ONTAP の FPolicy ソリューションを有効にします。これにより、ファイルの拡張子に基づいてファイル操作をブロックできます。

この予防ソリューションは、ランサムウェア攻撃からの保護を強化する一般的なランサムウェアファイルタイプをブロックします。

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。

マイクロ、暗号化、ロック、暗号化、暗号化、暗号化 crinf 、 r5a 、 XRNT 、 XTBL 、 R16M01D05 、 pzdc 、 good 、 LOL! 、 OMG! 、 RDM 、 RRK 、 encryptedRS 、 crjoker 、 enciphered 、 LeChiffre

Cloud Manager では、 Cloud Volumes ONTAP で FPolicy をアクティブ化するときにこのスコープを作成します。このリストは、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。ブロックされるファイル拡張子をカスタマイズするには、 Cloud Volumes ONTAP CLI から _ vserver fpolicy policy scope_コマンド を使用します。



著作権情報

商標情報