セキュリティとデータ暗号化
Cloud Volumes ONTAP

NetApp
June 01, 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

   "手順については、 ONTAP のドキュメントを参照してください"。

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。

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。

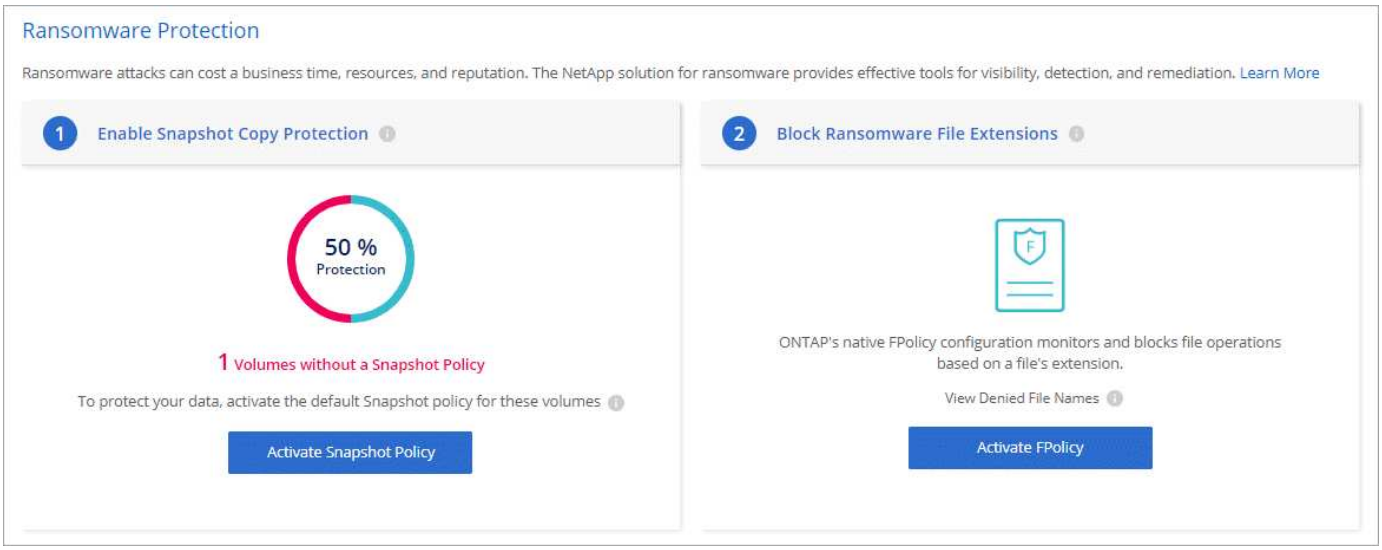
   b. FPolicy のアクティブ化 * をクリックして ONTAP の FPolicy ソリューションを有効にします。これにより、ファイルの拡張子に基づいてファイル操作をブロックできます。

      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。



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 と Cloud KMS を使用して保護することができます "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
- Cloud Volumes ONTAP クラスタのノードでNVEがサポート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Azureサブスクリプション

制限

- AKVはNSEキーおよびNAEキーでは使用できません
- AKVはMetroCluster 構成では使用できません。
- AKVはデータSVM上でのみ設定できます

設定プロセス

ONTAP の設定

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：テストボリュームを作成してAKVの機能を確認します。vol create -vserver_svm_name_ -volume_name_-aggregate_aggr_size_size__ state online -policy default '正しく設定されていると、ONTAP によってボリュームが自動的に作成され、ボリュームの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。

キー管理Cloud KMS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 Volumes ONTAP 用にCloud KMSを設定するには、まず必要があります

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 クラスタのノードでNVEがサポート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

制限

- 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
- クラウドKMSはNSEとNAEには利用できません。
- MetroCluster 構成では、クラウドKMSは利用できません。
- クラウドKMSはデータSVMでのみ設定できます
- アクティブなGoogle Cloud Platformサブスクリプション

—有効にします

1. Google Cloud環境の場合：
   a. 対称GCPキーリングとキーを作成します。
   b. 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=*tks_custom_role_name* --description=ks.cryptoKeyVersionsGet、kms.cryptoKeyVersions.get、kms.cryptoKeyVersions.list 、cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.locations.get,cloudkms.locations.list,resourcemanager.projects.get -stage /ga/ga/ga/ga?-stage
   c. 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_projects/customers_projects_projects_security_security_security_security_security_roles/<_project.<_security_security_account>
   d. 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
2. Cloud Volumes ONTAP 環境に切り替えます。

a. advanced権限レベルに切り替えます:'set -privilege advanced

b. データSVM用のDNSを作成DNS create -domains c.*[project]*.internal -name-servers_server_address_ -vserver_svm_name_`

c. 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_`

d. 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。

e. 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 _」

f. オプション：暗号化「vol create *volume_name*>-aggregate *vserver_name*-size 10G」をテストするボリュームを作成します

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

著作権情報

商標情報