セキュリティとデータ暗号化

Cloud Volumes ONTAP

NetApp
April 23, 2024

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。

AWS Key Management Serviceを使用してキーを管理します

を使用できます "AWS Key Management Service（KMS）" AWSに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。

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を使用する場合は、デフォルトではデータSVMの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、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、クラスタでキー管理サービスが適切に利用されません。

作業を開始する前に

- Cloud Volumes ONTAPでバージョン9.12.0以降が実行されている必要があります
- Volume Encryption（VE）ライセンスとをインストールしておく必要があります
- Multi-tenant Encryption Key Management（MTEKM）ライセンスをインストールしておく必要があります。
- 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
- 有効なAWSサブスクリプションが必要です

> 設定できるのはデータSVMのキーだけです。

設定

AWS

1. を作成する必要があります "グラント" 暗号化を管理するIAMロールで使用される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`

認可を作成するには、を参照してください "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。" ポリシーでがサポートされている必要があります `DescribeKey`、 `Encrypt`および `Decrypt` 操作：

Cloud Volumes ONTAP

1. Cloud Volumes ONTAP環境に切り替えます。
2. advanced権限レベルに切り替えます:'set -privilege advanced
3. AWSキー管理ツールを有効にします。
   `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が正しく設定されたことを確認します。
   `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。

作業を開始する前に

- 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）
- 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
- NAEはAKVでは使用できません。NAEには、外部でサポートされるKMIPサーバが必要です。

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. Azure Key Vaultアプリケーション登録用のAzureポータルで、[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わかりやすい名前を入力します。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作成するには、[追加**]**をクリックします。value**カラムに表示されているシークレット文字列をコピーし、後でで使用できるように安全な場所に保存します Cloud Volumes ONTAP 構成。シークレット値は、ページから移動したあとに再び表示されません。

Azureキーバックアップを作成します

1. 既存のAzure Key Vaultがある場合はCloud Volumes ONTAP 構成に接続できますが、このプロセスの設定にアクセスポリシーを適用する必要があります。
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. **[+Create]**をクリックして、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ます。また、削除したボールトを保持する日数を入力し、キーボールトでパージ保護を有効にする**を選択します。
4. アクセスポリシーを選択するには、 **Next**を選択してください。
5. 次のオプションを選択します。
   a. [アクセス構成]で、[ボールトアクセスポリシー]を選択します。
   b. [リソースアクセス]で、[**Azure Disk Encryption for Volume Encryption**]を選択します。
6. アクセスポリシーを追加するには、**+Create**を選択します。
7. [テンプレートから構成する]の下の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**]**、**[**証明書管理]テンプレートを選択します。

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:20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

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

- [x] Select all
- [x] Get
- [x] List
- [x] Update
- [x] Create
- [x] Import
- [x] Delete
- [x] Recover
- [x] Backup
- [x] Restore

Cryptographic Operations

- [x] Select all
- [x] Decrypt
- [x] Encrypt
- [x] Unwrap Key
- [x] Wrap Key
- [x] Verify
- [x] Sign

Privileged Key Operations

- [x] Select all
- [x] Purge
- [x] Release

Rotation Policy Operations

- [x] Select all
- [x] Rotate
- [x] Get Rotation Policy
- [x] Set Rotation Policy

Secret permissions

Secret Management Operations

- [x] Select all
- [x] Get
- [x] List
- [x] Set
- [x] Delete
- [x] Recover
- [x] Backup
- [x] Restore

Privileged Secret Operations

- [x] Select all
- [x] Purge

Certificate permissions

Certificate Management Operations

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

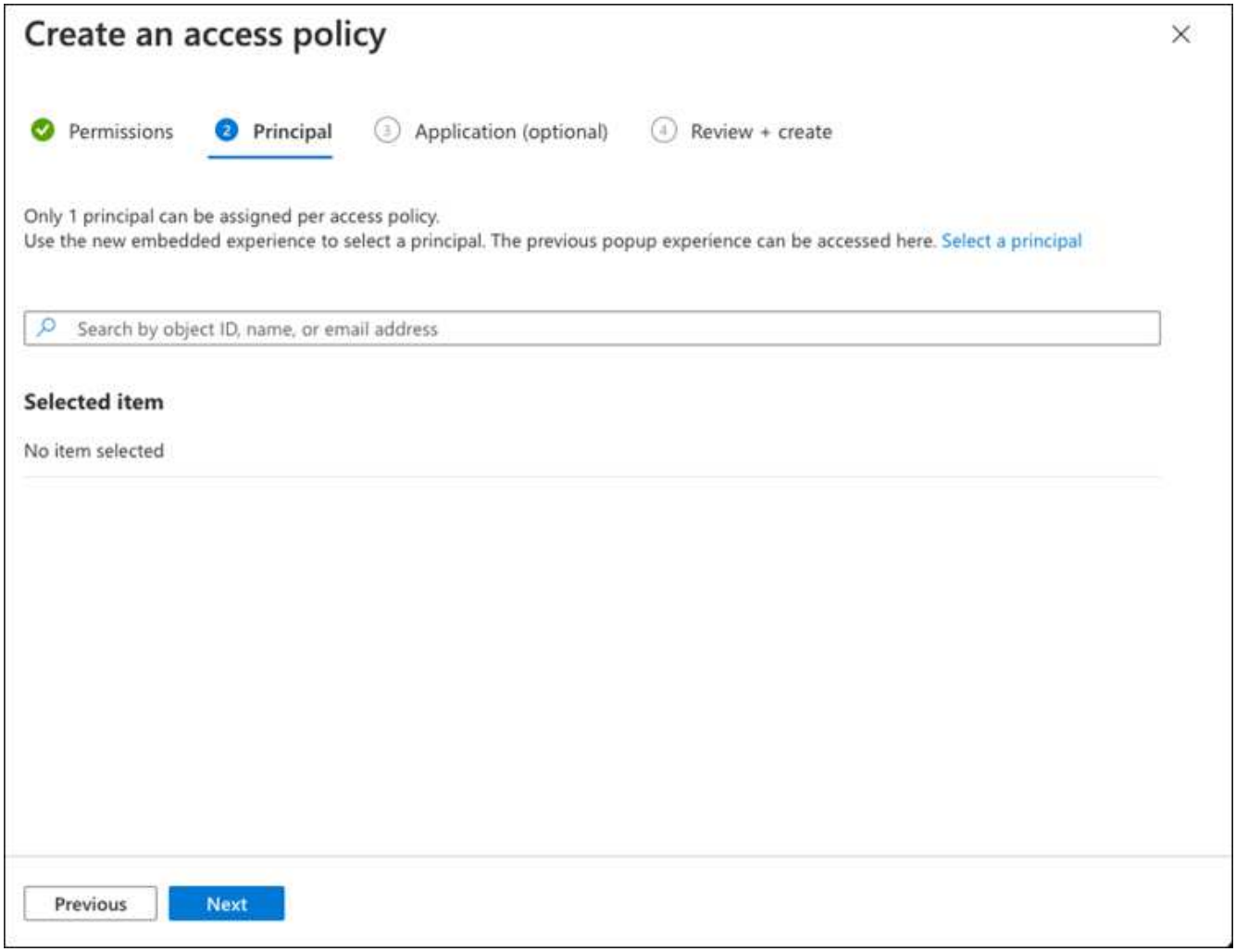
Privileged Certificate Operations

- [x] Select all
- [x] Purge

Previous Next

9. **Next**をクリックして、で作成した**Principal** 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。 **Next** を選択します。

> 1つのポリシー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. 「次へ」を2回クリックして「レビュー」および「作成」に到着します。次に、[作成]をクリックします。
11. **Next**を選択して、**Networking**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）。
13. 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。これはあとで実行する必要があります。

暗号化キーを作成します

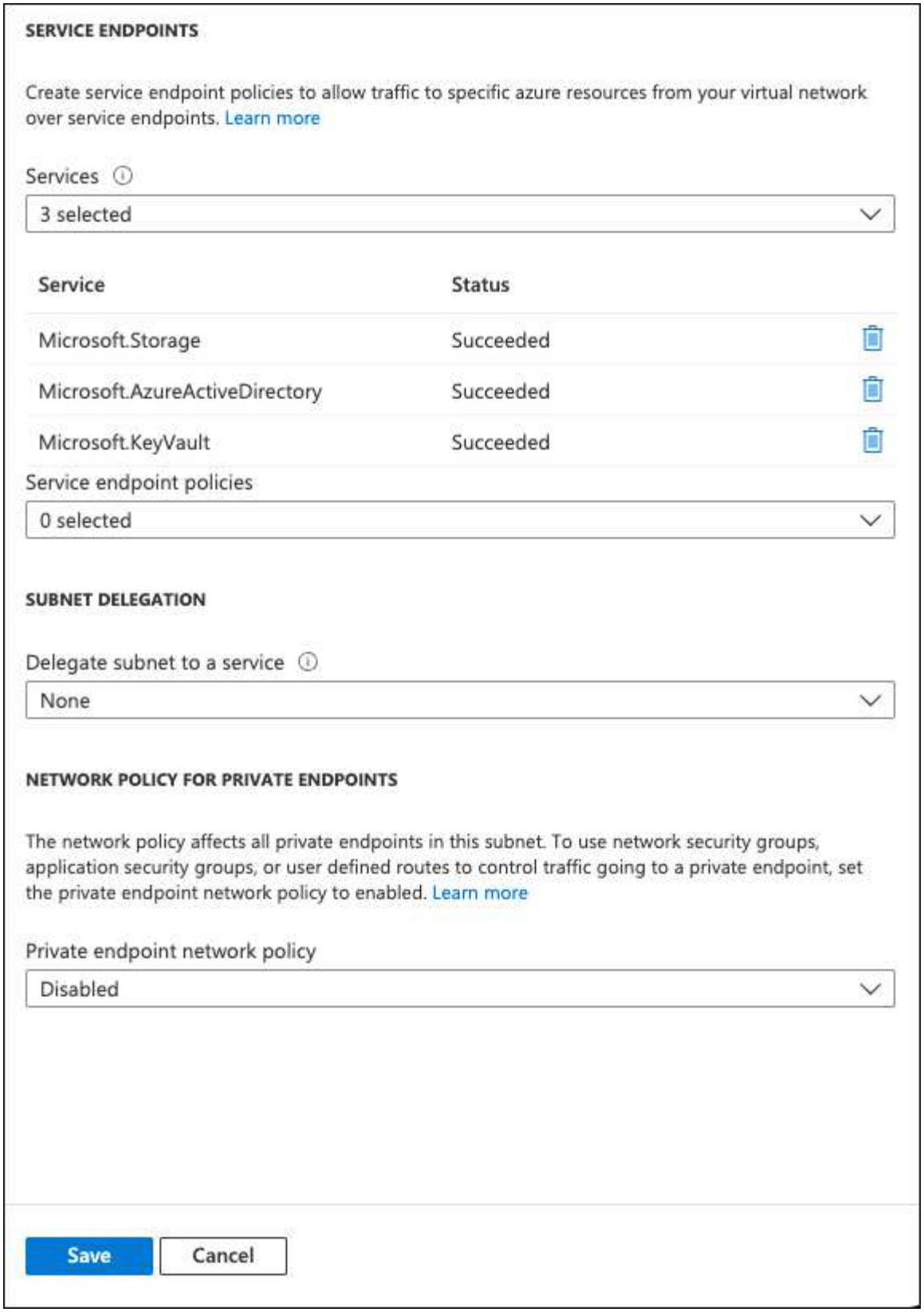
1. Cloud Volumes ONTAP 用に作成したキー・ボールトのメニューで、[**Keys**（キー**）]オプションに移動します。
2. [生成/インポート]を選択して、新しいキーを作成します。
3. デフォルトのオプションは **Generate** のままにしておきます。
4. 次の情報を入力します。

- 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、次のいずれかを選択します。
   - **Microsoft.AzureActiveDirectory**
   - **Microsoft.KeyVault**
   - **Microsoft.Storage**（オプション）



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 *Azure_client_ID* -tenant-id *Azure_tenant_ID* -name *key_vault_URI* -key-id *full_key_URI*

   > 。 _full_key_URI 値は、 <https:// <key vault host name>/keys/<key label> の形式で入力し

5. Azure Key Vaultが有効になったら、 client secret value プロンプトが表示されたら、
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.
```

状況に応じて service_reachability ステータスがではありません `OK`では、必要なすべての接続と権限を使用してSVMがAzure Key Vaultサービスにアクセスすることはできません。Azureの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 KeyVaultパブリックエンドポイントに到達できないようにしてください。その場合は、Azureプライベートエンドポイントを使用してVNet内からキーヴォールト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ために、SVMに静的ホストエントリを追加する必要がある場合もあります。

。 `kms_wrapped_key_status` が報告します `UNKNOWN` 初期設定時。ステータスがに変わります `OK` 最初のボリュームが暗号化されたあと。

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を使用する場合は、デフォルトではデータSVMの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。

作業を開始する前に

- 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
- Cloud Volumes ONTAP 9.12.1 GA以降、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。BlueXPでは、ランサムウェア向けの2つのNetAppソリューションを実装できます。一般的なランサムウェアファイル拡張子からの保護と、自律型ランサムウェア対策

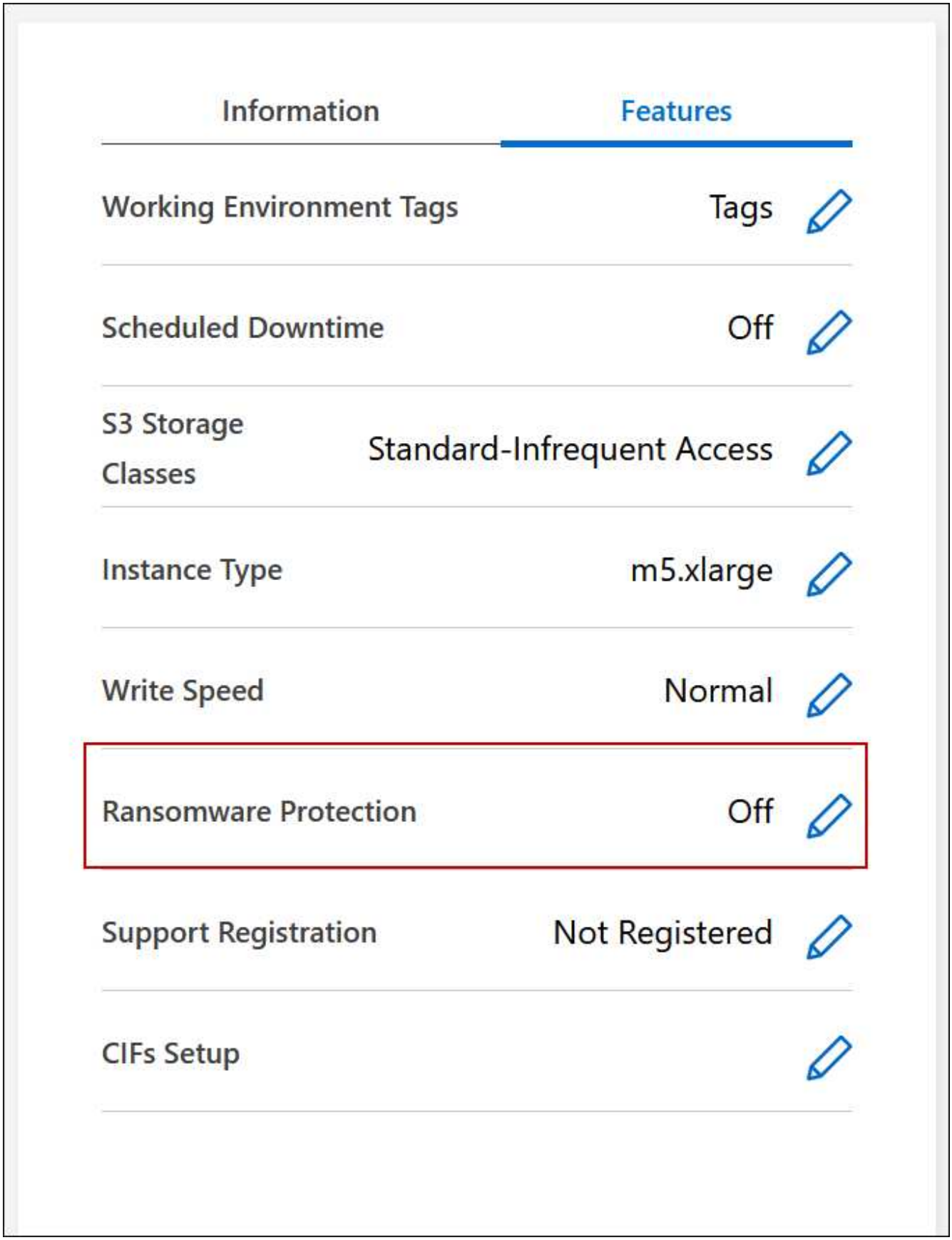
（ARP）です。これらのソリューションは、可視化、検出、修復のための効果的なツールを提供します。

一般的なランサムウェアのファイル拡張子から保護

BlueXPで利用可能なランサムウェア対策設定を使用すると、ONTAP FPolicy機能を利用して、一般的なランサムウェアファイル拡張子タイプから保護できます。

手順

1. [Canvas]ページで、ランサムウェア対策に設定したシステムの名前をダブルクリックします。
2. [Overview]タブで、[Features]パネルをクリックし、*[Ransomware Protection]*の横にある鉛筆アイコンをクリックします。



3. 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。

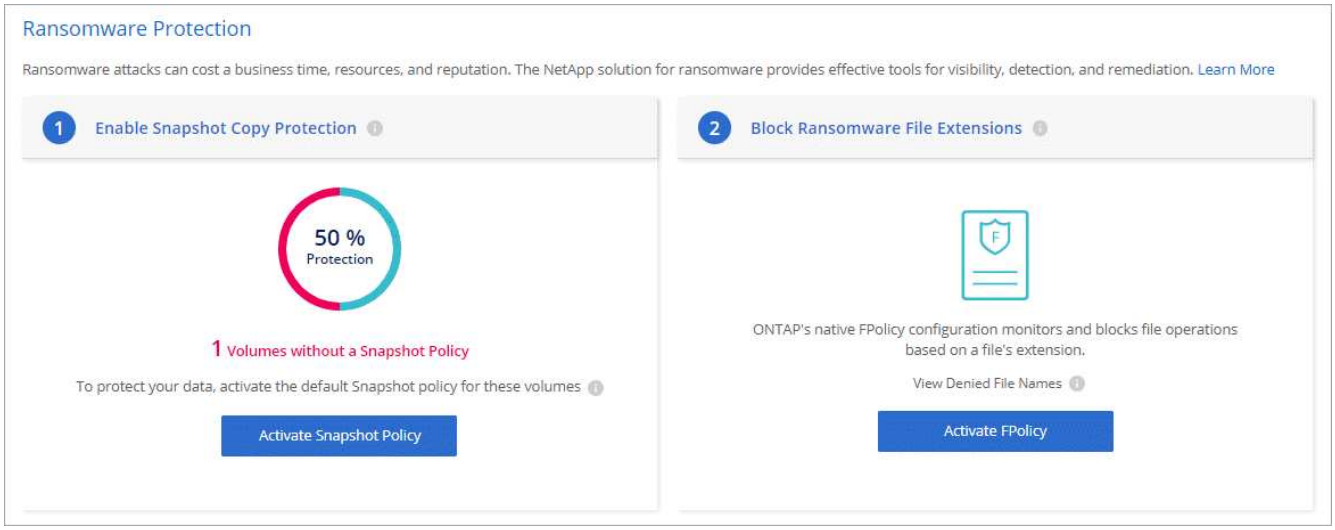
b. FPolicy のアクティブ化 * をクリックして ONTAP の FPolicy ソリューションを有効にします。これにより、ファイルの拡張子に基づいてファイル操作をブロックできます。

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 Volumes ONTAP でFPolicyをアクティブ化すると、このスコープが作成されます。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。



自律的なランサムウェア防御

Cloud Volumes ONTAPは、Autonomous Ransomware Protection（ARP）機能をサポートしています。この機能は、ワークロードを分析し、ランサムウェア攻撃の可能性がある異常なアクティビティをプロアクティブに検出して警告します。

で提供されるファイル拡張子保護とは別に、 "ランサムウェア対策設定"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についてユーザに警告します。ランサムウェア対策設定とARP機能の両方を組み合わせて、包括的なランサムウェア対策を行うことができます。

ARP機能は、ノードベースと容量ベースの両方のライセンスモデルで、BYOLライセンスでのみ使用できます

（1~36カ月）。Cloud Volumes ONTAPのARP機能で使用する新しいアドオンライセンスを別途購入するには、NetAppの営業担当者にお問い合わせください。

ARPライセンスは「フローティング」ライセンスと見なされます。つまり、単一のCloud Volumes ONTAPインスタンスにバインドされず、複数のCloud Volumes ONTAP環境に適用できます。

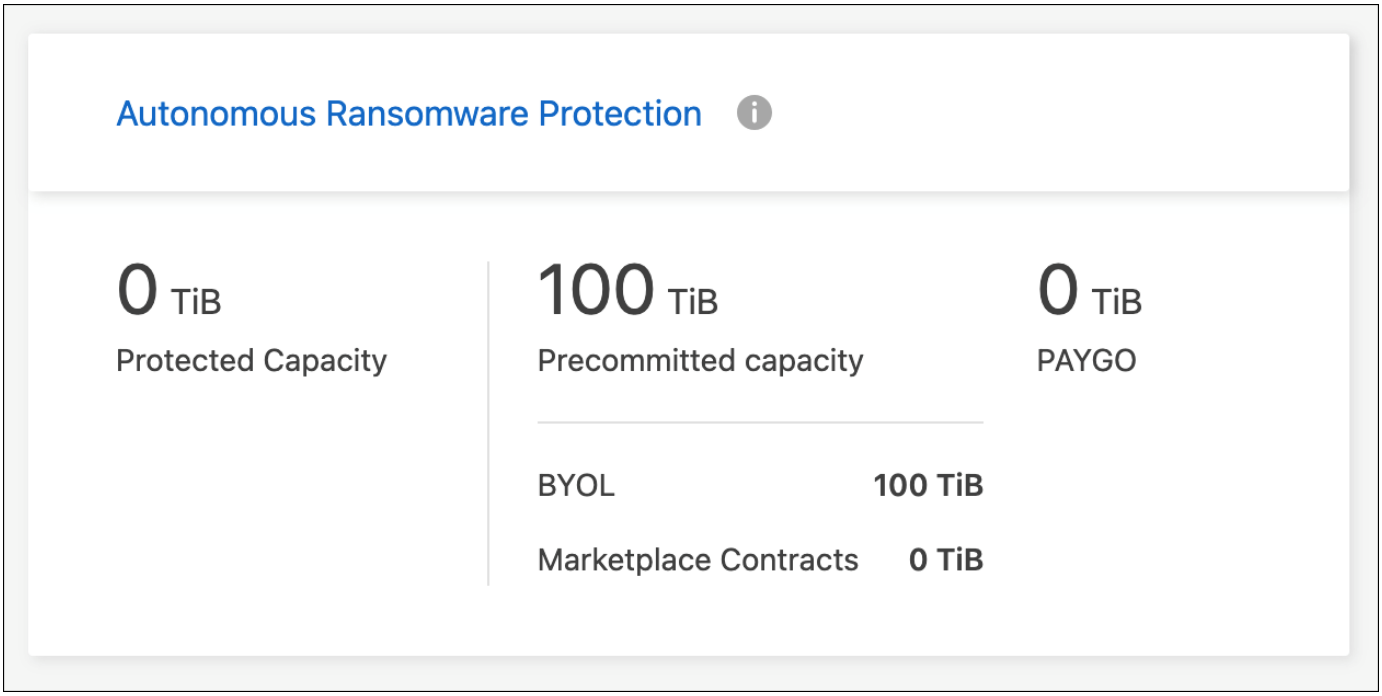
> ノードベースのCloud Volumes ONTAPライセンスでのARP機能の使用は、現在Digital Walletには反映されていません。ノードベースのARP使用状況を表示する機能は、今後のリリースでDigital Walletで利用できるようになる予定です。

アドオンライセンスを購入してデジタルウォレットに追加すると、Cloud Volumes ONTAPを使用してボリューム単位でARPを有効にできます。ARPの課金は、ARP機能が有効になっているボリュームのプロビジョニング済み容量の合計に基づいて、ボリュームレベルで計測されます。最小ライセンス容量は1TBです。ただし、ARP機能の最小容量課金はありません。

ARPが有効なボリュームの状態は「ラーニングモード」または「アクティブ」になります。ARP状態が「Disabled」のボリュームは課金対象から除外されます。たとえば、30TiBの容量がプロビジョニングされたCloud Volumes ONTAP環境では、ARPが有効な15TiBのボリュームの一部のみを含めることができます。

ボリュームのARPの設定は、ONTAP System ManagerとONTAP CLIを使用して実行します。

ONTAP System ManagerおよびCLIでARPを有効にする方法の詳細については、を参照してください "自動ランサムウェア対策を有効化"。



> ライセンスがないと、ライセンスされた機能の使用はサポートされません。