Security and data encryption

Cloud Volumes ONTAP

NetApp
June 01, 2022

Table of Contents

Security and data encryption

Encrypting volumes with NetApp encryption solutions

Cloud Volumes ONTAP supports NetApp Volume Encryption (NVE) and NetApp Aggregate Encryption (NAE). NVE and NAE are software-based solutions that enable (FIPS) 140-2–compliant data-at-rest encryption of volumes. Learn more about these encryption solutions.

Both NVE and NAE are supported with an external key manager.

If you use NVE, you have the option to use your cloud provider’s key vault to protect ONTAP encryption keys:

- Azure Key Vault (AKV)
- Google Cloud Key Management Service

New aggregates will have NAE enabled by default after you set up an external key manager. New volumes that aren’t part of an NAE aggregate will have NVE enabled by default (for example, if you have existing aggregates that were created before setting up an external key manager).

Cloud Volumes ONTAP doesn’t support onboard key management.

What you’ll need

Your Cloud Volumes ONTAP system should be registered with NetApp support. A NetApp Volume Encryption license is automatically installed on each Cloud Volumes ONTAP system that is registered with NetApp Support.

- Adding NetApp Support Site accounts to Cloud Manager
- Registering pay-as-you-go systems

> Cloud Manager doesn’t install the NVE license on systems that reside in the China region.

Steps

1. Review the list of supported key managers in the NetApp Interoperability Matrix Tool.

   > Search for the **Key Managers** solution.

2. Connect to the Cloud Volumes ONTAP CLI.
3. Configure external key management.

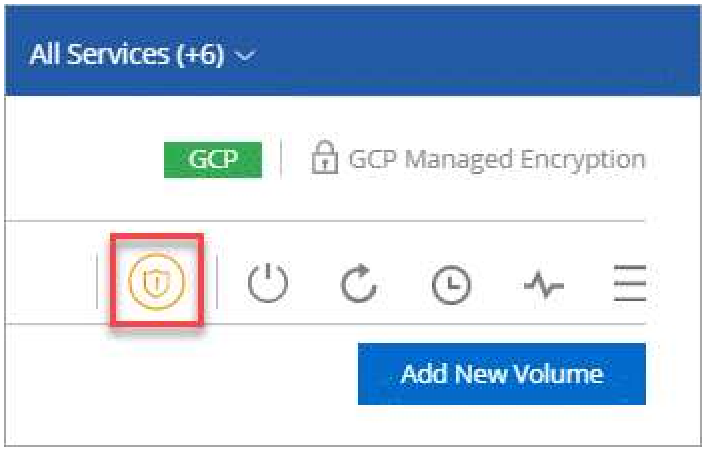
   Go to the ONTAP documentation for instructions.

Improving protection against ransomware

Ransomware attacks can cost a business time, resources, and reputation. Cloud Manager enables you to implement the NetApp solution for ransomware, which provides effective tools for visibility, detection, and remediation.

Steps

1. From the working environment, click the **Ransomware** icon.



2. Implement the NetApp solution for ransomware:

   a. Click **Activate Snapshot Policy**, if you have volumes that do not have a Snapshot policy enabled.

   NetApp Snapshot technology provides the industry’s best solution for ransomware remediation. The key to a successful recovery is restoring from uninfected backups. Snapshot copies are read-only, which prevents ransomware corruption. They can also provide the granularity to create images of a single file copy or a complete disaster recovery solution.

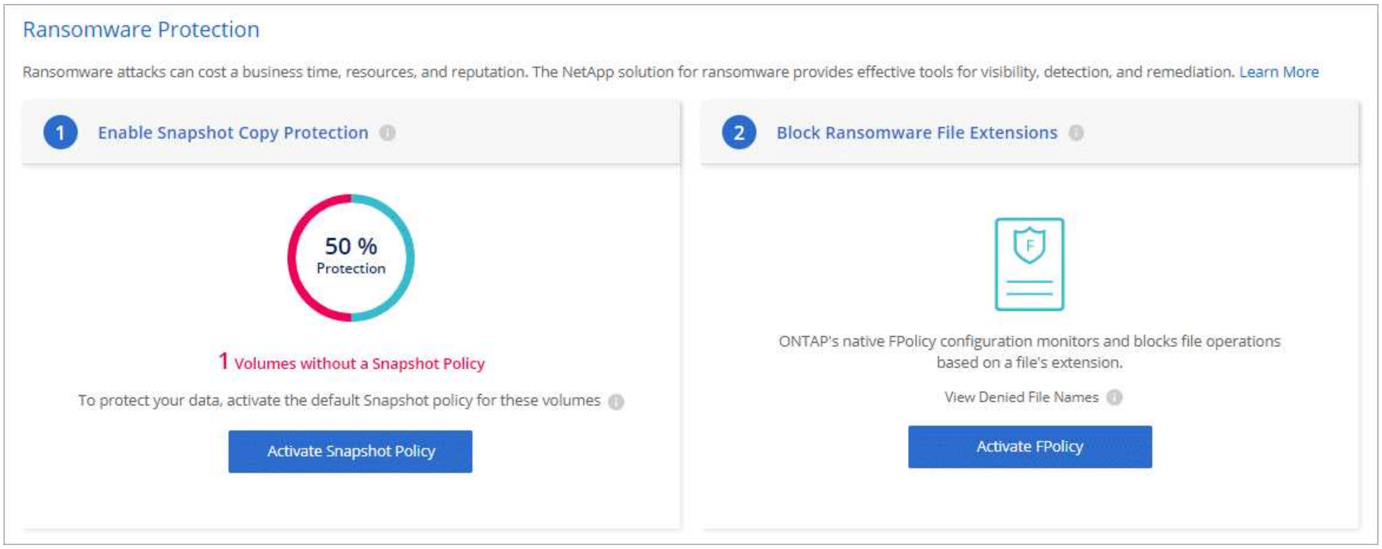
   b. Click **Activate FPolicy** to enable ONTAP’s FPolicy solution, which can block file operations based on a file’s extension.

   This preventative solution improves protection from ransomware attacks by blocking common ransomware file types.

   The default FPolicy scope blocks files that have the following extensions:

   micro, encrypted, locked, crypto, crypt, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, good, LOL!, OMG!, RDM, RRK, encryptedRS, crjoker, EnCiPhErEd, LeChiffre

   Cloud Manager creates this scope when you activate FPolicy on Cloud Volumes ONTAP. The list is based on common ransomware file types. You can customize the blocked file extensions by using the *vserver fpolicy policy scope* commands from the Cloud Volumes ONTAP CLI.



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

To protect your data, activate the default Snapshot policy for these volumes

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

Manage keys with Azure Key Vault

You can use Azure Key Vault (AKV) to protect your ONTAP encryption keys in an Azure-deployed application.

AKV and Cloud KMS can be used to protect NetApp Volume Encryption (NVE) keys only for data SVMs.

Key management with AKV can be enabled with the CLI or the ONTAP REST API.

When using AKV, be aware that by default a data SVM LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider’s authentication services (login.microsoftonline.com). If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

Prerequisites

- Cloud Volumes ONTAP must be running version 9.10.1 or later
- The Cloud Volumes ONTAP cluster’s nodes must support NVE
- Volume Encryption (VE) license installed
- Multi-tenant Encryption Key Management (MTEKM) license installed
- You must be a cluster or SVM administrator
- An Active Azure subscription

Limitations

- AKV is not available for NSE and NAE keys
- AKV is not available for MetroCluster configurations.
- AKV can only be configured on a data SVM

Configuration process

ONTAP configuration

1. Connect to the cluster management LIF with your preferred SSH client.
2. Enter the advanced privilege mode in ONTAP:
```
set advanced -con off`
```

3. Identify the desired data SVM and verify its DNS configuration:
   ```
   vserver services name-service dns show
   ```
   a. If a DNS entry for the desired data SVM exists and it contains an entry for the Azure DNS, then no action is required. If it does not, add a DNS server entry for the data SVM that points to the Azure DNS, private DNS, or on-premise server. This should match the entry for the cluster admin SVM:
      ```
      vserver services name-service dns create -vserver SVM_name -domains domain
      -name-servers IP_address
      ```
   b. Verify the DNS service has been created for the data SVM:
      ```
      vserver services name-service dns show
      ```
4. Enable Azure Key Vault using the client ID and tenant ID saved after the application registration:
   ```
   security key-manager external azure enable -vserver SVM_name -client-id
   Azure_client_ID -tenant-id Azure_tenant_ID -name Azure_key_name -key-id
   Azure_key_ID
   ```
5. Verify the key manager configuration:
   ```
   security key-manager external azure show
   ```
6. Check the status of the key manager:
   ```
   security key-manager external azure check
   ```
   The output will look like:
   ```
   ::*> 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.
   ```
   If the `service_reachability` status is not `OK`, the SVM cannot reach the Azure Key Vault service with all the required connectivity and permissions.
   The `kms_wrapped_key_status` will report `UNKNOWN` at initial configuration. Its status will change to `OK` after the first volume is encrypted.
7. OPTIONAL: Create a test volume to verify the functionality of AKV.
   ```
   vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
   -state online -policy default
   ```
   If configured correctly, ONTAP will automatically create the volume and enable volume encryption.

8. Confirm the volume was created and encrypted correctly. If it is, the `-is-encrypted` parameter will display as `true`.
   ```
   vol show -vserver SVM_name -fields is-encrypted
   ```

Manage keys with Google's Cloud Key Management Service

You can use Google Cloud Platform's Key Management Service (Cloud KMS) to protect your ONTAP encryption keys in a Google Cloud Platform-deployed application.

Key management Cloud KMS can be enabled with the CLI or the ONTAP REST API. To configure Cloud KMS for Cloud Volumes ONTAP, you must first

When using Cloud KMS, be aware that by default a data SVMs LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider's authentication services (oauth2.googleapis.com). If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

Prerequisites

- The Cloud Volumes ONTAP cluster's nodes must support NVE
- Volume Encryption (VE) license installed
- Multi-tenant Encryption Key Management (MTEKM) license installed
- You must be a cluster or SVM administrator

Limitations

- Cloud Volumes ONTAP must be running version 9.10.1 or later
- Cloud KMS is not available for NSE and NAE.
- Cloud KMS is not available for MetroCluster configurations.
- Cloud KMS can only be configured on a data SVM
- An active Google Cloud Platform subscription

Enable

1. In your Google Cloud environment:
   a. Create a symmetric GCP key ring and key:
   b. Create a custom role for your Cloud Volumes ONTAP service account:
      ```
      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.useToEnc
      rypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.locations.get,cl
      oudkms.locations.list,resourcemanager.projects.get
      --stage=GA //does it have to be GA?
      ```
   c. Assign the custom role to the Cloud KMS key and Cloud Volumes ONTAP service account:
      ```
      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
```

d. Download service account JSON key:

```
gcloud iam service-accounts keys create key-file --iam-account=sa-name
@project-id.iam.gserviceaccount.com
```

2. Switch to your Cloud Volumes ONTAP environment:

a. Switch to the advanced privilege level:

```
set -privilege advanced
```

b. Create a DNS for the data SVM.

```
dns create -domains c.[project].internal -name-servers server_address
-vserver SVM_name
```

c. Create CMEK entry:

```
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. When prompted, enter the service account JSON key from your GCP account.

e. Confirm the enabled process succeeded:

```
security key-manager external gcp check -vserver svm_name
```

f. OPTIONAL: Create a volume to test encryption `vol create volume_name> -aggregate aggregate -vserver vserver_name -size 10G`

Troubleshoot

If you need to troubleshoot, you can tail the raw REST API logs in the final two steps above:

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

Copyright Information

Trademark Information