Security and data encryption

Cloud Volumes ONTAP

NetApp
March 20, 2023

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 BlueXP
- Registering pay-as-you-go systems

> ⓘ   BlueXP 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.
   - AWS: Go to the ONTAP documentation for instructions
   - Azure: Azure Key Vault (AKV)
   - Google Cloud: Google Cloud Key Management Service

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 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
- Volume Encryption (VE) license installed (NetApp Volume Encryption license is automatically installed on each Cloud Volumes ONTAP system that is registered with NetApp Support)
- You must have a Multi-tenant Encryption Key Management (MT_EK_MGMT) license
- You must be a cluster or SVM administrator
- An Active Azure subscription

Limitations

- AKV can only be configured on a data SVM

Configuration process

The outlined steps capture how to register your Cloud Volumes ONTAP configuration with Azure and how to create an Azure Key Vault and keys. If you have already completed these steps, ensure you have the correct configuration settings, particularly in Create an Azure Key Vault, and then proceed to Cloud Volumes ONTAP configuration.

- Azure Application Registration
- Create Azure client secret
- Create an Azure Key Vault
- Create encryption key
- Create an Azure Active Directory Endpoint (HA only)
- Cloud Volumes ONTAP configuration

Azure Application Registration

1. You must first register your application in the Azure subscription that you want the Cloud Volumes ONTAP to use for access the Azure Key Vault. Within the Azure portal, select **App registrations**.
2. Select **New registration**.
3. Provide a name for your application and select a supported application type. The default single tenant suffices for Azure Key Vault usage. Select **Register**.
4. In the Azure Overview window, select the application you have registered. Copy the **application (client) ID** and the **directory (tenant) ID** to a secure location. They will be required later in the registration process.

Create Azure client secret

1. In the Azure portal for your Azure Key Vault app registration, select the **Certificates & secrets** pane.
2. Select **New client secret**. Enter a meaningful name for your client secret. NetApp recommends a 24-month expiration period; however, your specific cloud governance policies may require a different setting.
3. Click **Add** to create the client secret. Copy the secret string listed in the **Value** column and store it in a secure location for use later in Cloud Volumes ONTAP configuration. The secret value will not be displayed

again after you navigate away from the page.

Create an Azure Key Vault

1. If you have an existing Azure Key Vault, you can connect it to your Cloud Volumes ONTAP configuration; however, you must adapt the access policies to the settings in this process.

2. In the Azure portal, navigate to the **Key Vaults** section.

3. Click **+Create** and enter the required information including resource group, region, and pricing tier. In addition, enter the number of days to retain deleted vaults and select **Enable purge protection** on the key vault.

4. Select **Next** to choose an access policy.

5. Select the following options:

   a. Under **Access configuration**, select the **Vault access policy**.

   b. Under **Resource access**, select **Azure Disk Encryption for volume encryption**.

6. Select **+Create** to add an access policy.

7. Under **Configure from a template**, click the drop-down menu and then select the **Key, Secret, and Certificate Management** template.

8. Choose each of the drop-down permissions menus (key, secret, certificate) and then **Select all** at the top of the menu list to select all the permissions available. You should have:

   ◦ **Key permissions**: 20 selected

   ◦ **Secret permissions**: 8 selected

   ◦ **Certificate permissions**: 16 selected

Create an access policy   ✕

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. Click **Next** to select the **Principal** Azure registered application you created in Azure Application Registration. Select **Next**.

> ⓘ   Only one principal can be assigned per policy.

Create an access policy   ✕

✓ Permissions   ② **Principal**   ③ Application (optional)   ④ Review + create

Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. Select a principal

🔍 Search by object ID, name, or email address

Selected item

No item selected

[Previous]   [**Next**]

10. Click **Next** two times until you arrive at **Review and create**. Then, click **Create**.

11. Select **Next** to advance to **Networking** options.

12. Choose the appropriate network access method or select **All networks** and **Review + Create** to create the key vault. (Network access method may be prescribed by a governance policy or your corporate cloud security team.)

13. Record the Key Vault URI: In the key vault you created, navigate to the Overview menu and copy the **Vault URI** from the right-hand column. You need this for a later step.

Create encryption key

1. In the menu for the Key Vault you have created for Cloud Volumes ONTAP, navigate to the **Keys** option.

2. Select **Generate/import** to create a new key.

3. Leave the default option set to **Generate**.

4. Provide the following information:
   ◦ Encryption key name

- Key type: RSA
- RSA key size: 2048
- Enabled: Yes

5. Select **Create** to create the encryption key.

6. Return to the **Keys** menu and select the key you just created.

7. Select the key ID under **Current version** to view the key properties.

8. Locate the **Key Identifier** field. Copy the URI up to but not including the hexadecimal string.

Create an Azure Active Directory Endpoint (HA only)

1. This process is only required if you are configuring Azure Key Vault for an HA Cloud Volumes ONTAP Working Environment.

2. In the Azure portal navigate to **Virtual Networks**.

3. Select the Virtual Network where you deployed the Cloud Volumes ONTAP working environment and select the **Subnets** menu on the left side of the page.

4. Select the subnet name for you Cloud Volumes ONTAP deployment from the list.

5. Navigate to the **Service Endpoints** heading. In the drop-down menu, select the following:

- **Microsoft.AzureActiveDirectory**
- **Microsoft.KeyVault**
- **Microsoft.Storage** (optional)

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more

Services ⓘ

3 selected	⌄

Service	Status	
Microsoft.Storage	Succeeded	🗑
Microsoft.AzureActiveDirectory	Succeeded	🗑
Microsoft.KeyVault	Succeeded	🗑

Service endpoint policies

0 selected	⌄

SUBNET DELEGATION

Delegate subnet to a service ⓘ

None	⌄

NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. Learn more

Private endpoint network policy

Disabled	⌄

Save   Cancel

6. Select **Save** to capture your settings.

Cloud Volumes 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_vault_name -key-id
   Azure_key_ID
   ```

5. 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. Ensure that your Azure network policies and routing don't block your private vNet from reaching the Azure KeyVault Public endpoint. If they do, consider using an Azure Private endpoint to access the Key vault from within the vNet. You may also need to add a static hosts entry on your SVM to resolve the private IP address for your endpoint.

   The `kms_wrapped_key_status` will report `UNKNOWN` at initial configuration. Its status will change to `OK` after the first volume is encrypted.

6. OPTIONAL: Create a test volume to verify the functionality of NVE.

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

If configured correctly, Cloud Volumes ONTAP will automatically create the volume and enable volume encryption.

7. 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 with Cloud KMS can be enabled with the CLI or the ONTAP REST API.

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

- Cloud Volumes ONTAP must be running version 9.10.1 or later
- Volume Encryption (VE) license installed
- Multi-tenant Encryption Key Management (MTEKM) license installed, starting with Cloud Volumes ONTAP 9.12.1 GA.
- You must be a cluster or SVM administrator
- An active Google Cloud Platform subscription

Limitations

- Cloud KMS can only be configured on a data SVM

Configuration

Google Cloud

1. In your Google Cloud environment, create a symmetric GCP key ring and key.
2. 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.
    useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
    tions.get,cloudkms.locations.list,resourcemanager.projects.get
    --stage=GA
```

3. 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
   ```

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

Cloud Volumes ONTAP

1. Connect to the cluster management LIF with your preferred SSH client.

2. Switch to the advanced privilege level:
   ```
   set -privilege advanced
   ```

3. Create a DNS for the data SVM.
   ```
   dns create -domains c.<project>.internal -name-servers server_address -vserver
   SVM_name
   ```

4. 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
   ```

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

6. Confirm the enabled process succeeded:
   ```
   security key-manager external gcp check -vserver svm_name
   ```

7. 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:

1. `set d`

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

Improving protection against ransomware

Ransomware attacks can cost a business time, resources, and reputation. BlueXP 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

   > 💡 BlueXP 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 Protection

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

1 Enable Snapshot Copy Protection ⓘ

2 Block Ransomware File Extensions ⓘ

50 %
Protection

1 Volumes without a Snapshot Policy

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

Activate Snapshot Policy

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

View Denied File Names ⓘ

Activate FPolicy