Set up Cloud Volumes ONTAP to use a customer-managed key in Azure

Cloud Manager

Ben Cammett
September 02, 2021

Table of Contents

Set up Cloud Volumes ONTAP to use a customer-managed key in Azure 1
Data encryption overview 1
Create a key vault and generate a key 1
Create a working environment that uses the encryption key 2

Set up Cloud Volumes ONTAP to use a customer-managed key in Azure

Data is automatically encrypted on Cloud Volumes ONTAP in Azure using Azure Storage Service Encryption with a Microsoft-managed key. But you can use your own encryption key instead by following the steps on this page.

Data encryption overview

Cloud Volumes ONTAP data is automatically encrypted in Azure using Azure Storage Service Encryption. The default implementation uses a Microsoft-managed key. No setup is required.

If you want to use a customer-managed key with Cloud Volumes ONTAP, then you need to complete the following steps:

1. From Azure, create a key vault and then generate a key in that vault
2. From Cloud Manager, use the API to create a Cloud Volumes ONTAP working environment that uses the key

Key rotation

If you create a new version of your key, Cloud Volumes ONTAP automatically uses the latest key version.

How data is encrypted

After you create a Cloud Volumes ONTAP working environment that is configured to use a customer-managed key, Cloud Volumes ONTAP data is encrypted as follows.

HA pairs

- All Azure storage accounts for Cloud Volumes ONTAP are encrypted using a customer-managed key.
- Any new storage accounts (for example, when you add disks or aggregates) also use the same key.

Single node

- All Azure storage accounts for Cloud Volumes ONTAP are encrypted using a customer-managed key.
- For root, boot, and data disks, Cloud Manager uses a disk encryption set, which enables management of encryption keys with managed disks.
- Any new data disks also use the same disk encryption set.
- NVRAM and the core disk are encrypted using a Microsoft-managed key, instead of the customer-managed key.

Create a key vault and generate a key

The key vault must reside in the same Azure subscription and region in which you plan to create the Cloud Volumes ONTAP system.

Steps

1. Create a key vault in your Azure subscription.

Note the following requirements for the key vault:

- The key vault must reside in the same region as the Cloud Volumes ONTAP system.
- The following options should be enabled:
  - **Soft-delete** (this option is enabled by default, but must *not* be disabled)
  - **Purge protection**
  - **Azure Disk Encryption for volume encryption** (for single node Cloud Volumes ONTAP systems only)

2. Generate a key in the key vault.

   Note the following requirements for the key:

   - The key type must be **RSA**.
   - The recommended RSA key size is **2048**, but other sizes are supported.

Create a working environment that uses the encryption key

After you create the key vault and generate an encryption key, you can create a new Cloud Volumes ONTAP system that is configured to use the key. These steps are supported by using the Cloud Manager API.

Required permissions

If you want to use a customer-managed key with a single node Cloud Volumes ONTAP system, ensure that the Cloud Manager Connector has the following permissions:

```
"Microsoft.Compute/diskEncryptionSets/read"
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write"
```

You can find the latest list of permissions on the Cloud Manager policies page.

These permissions aren't required for HA pairs.

Steps

1. Obtain the list of key vaults in your Azure subscription by using the following Cloud Manager API call.

   For an HA pair: `GET /azure/ha/metadata/vaults`

   For single node: `GET /azure/vsa/metadata/vaults`

   Make note of the **name** and **resourceGroup**. You'll need to specify those values in the next step.

   Learn more about this API call.

2. Obtain the list of keys within the vault by using the following Cloud Manager API call.

For an HA pair: `GET /azure/ha/metadata/keys-vault`

For single node: `GET /azure/vsa/metadata/keys-vault`

Make note of the **keyName**. You'll need to specify that value (along with the vault name) in the next step.

Learn more about this API call.

3. Create a Cloud Volumes ONTAP system by using the following Cloud Manager API call.
   a. For an HA pair:

      `POST /azure/ha/working-environments`

      The request body must include the following fields:

      ```
      "azureEncryptionParameters": {
             "key": "keyName",
             "vaultName": "vaultName"
      }
      ```

      Learn more about this API call.

   b. For a single node system:

      `POST /azure/vsa/working-environments`

      The request body must include the following fields:

      ```
      "azureEncryptionParameters": {
             "key": "keyName",
             "vaultName": "vaultName"
      }
      ```

      Learn more about this API call.

Result

You have a new Cloud Volumes ONTAP system that is configured to use your customer-managed key for data encryption.