Default configuration for Cloud Volumes ONTAP

Cloud Manager

Ben Cammett
October 21, 2020

Table of Contents

Default configuration for Cloud Volumes ONTAP

Understanding how Cloud Volumes ONTAP is configured by default can help you set up and administer your systems, especially if you are familiar with ONTAP because the default setup for Cloud Volumes ONTAP is different than ONTAP.

Defaults

- Cloud Volumes ONTAP is available as a single-node system in AWS, Azure, and GCP, and as an HA pair in AWS and Azure.
- Cloud Manager creates one data-serving storage VM when it deploys Cloud Volumes ONTAP. Some configurations support additional storage VMs. Learn more about managing storage VMs.
- Cloud Manager automatically installs the following ONTAP feature licenses on Cloud Volumes ONTAP:
  - CIFS
  - FlexCache
  - FlexClone
  - iSCSI
  - NetApp Volume Encryption (only for BYOL or registered PAYGO systems)
  - NFS
  - SnapMirror
  - SnapRestore
  - SnapVault
- Several network interfaces are created by default:
  - A cluster management LIF
  - An intercluster LIF
  - An SVM management LIF on HA systems in Azure, single node systems in AWS, and optionally on HA systems in multiple AWS Availability Zones
  - A node management LIF
  - An iSCSI data LIF
  - A CIFS and NFS data LIF

LIF failover is disabled by default for Cloud Volumes ONTAP due to EC2 requirements. Migrating a LIF to a different port breaks the external mapping between IP addresses and network interfaces on the instance, making the LIF inaccessible.

- Cloud Volumes ONTAP sends configuration backups to the Connector using HTTPS.

  The backups are accessible from https://ipaddress/occm/offboxconfig/ where *ipaddress* is the IP address of the Connector host.

- Cloud Manager sets a few volume attributes differently than other management tools (System Manager or the CLI, for example).

  The following table lists the volume attributes that Cloud Manager sets differently from the defaults:

Attribute	Value set by Cloud Manager
Autosize mode	grow
Maximum autosize	1,000 percent The Account Admin can modify this value from the Settings page.
Security style	NTFS for CIFS volumes UNIX for NFS volumes
Space guarantee style	none
UNIX permissions (NFS only)	777

  See the *volume create* man page for information about these attributes.

Boot and root data for Cloud Volumes ONTAP

In addition to the storage for user data, Cloud Manager also purchases cloud storage for boot and root data on each Cloud Volumes ONTAP system.

AWS

- Two disks per node for boot and root data:

    - 9.7: 160 GB io1 disk for boot data and a 220 GB gp2 disk for root data
    - 9.6: 93 GB io1 disk for boot data and a 140 GB gp2 disk for root data
    - 9.5: 45 GB io1 disk for boot data and a 140 GB gp2 disk for root data
- One EBS snapshot for each boot disk and root disk
- For HA pairs, one EBS volume for the Mediator instance, which is approximately 8 GB

Azure (single node)

- Three Premium SSD disks:
    - One 10 GB disk for boot data
    - One 140 GB disk for root data
    - One 128 GB disk for NVRAM

      If the virtual machine that you chose for Cloud Volumes ONTAP supports Ultra SSDs, then the system uses an Ultra SSD for NVRAM, rather than a Premium SSD.
- One 1024 GB Standard HDD disk for saving cores
- One Azure snapshot for each boot disk and root disk

Azure (HA pairs)

- Two 10 GB Premium SSD disks for the boot volume (one per node)
- Two 140 GB Premium Storage page blobs for the root volume (one per node)
- Two 1024 GB Standard HDD disks for saving cores (one per node)
- Two 128 GB Premium SSD disks for NVRAM (one per node)
- One Azure snapshot for each boot disk and root disk

GCP

- One 10 GB Standard persistent disk for boot data
- One 64 GB Standard persistent disk for root data
- One 500 GB Standard persistent disk for NVRAM
- One 216 GB Standard persistent disk for saving cores
- One GCP snapshot each for the boot disk and root disk

Where the disks reside

Cloud Manager lays out the storage as follows:

- Boot data resides on a disk attached to the instance or virtual machine.

This disk, which contains the boot image, is not available to Cloud Volumes ONTAP.

- Root data, which contains the system configuration and logs, resides in aggr0.
- The storage virtual machine (SVM) root volume resides in aggr1.
- Data volumes also reside in aggr1.

Encryption

Boot and root disks are always encrypted in Azure and Google Cloud Platform because encryption is enabled by default in those cloud providers.

When you enable data encryption in AWS using the Key Management Service (KMS), the boot and root disks for Cloud Volumes ONTAP are encrypted, as well. This includes the boot disk for the mediator instance in an HA pair. The disks are encrypted using the CMK that you select when you create the working environment.