Data protection and the cloud

ONTAP 9

NetApp
August 25, 2022

Table of Contents

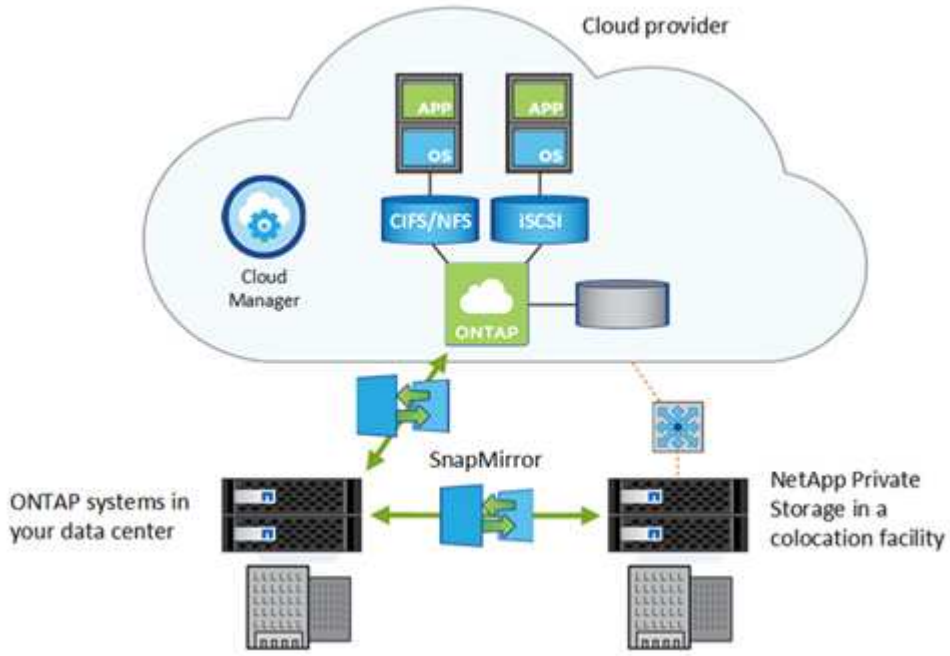
Data protection and the cloud

Data protection and the cloud overview

Data protection is often the first thing customers try when they begin their cloud journey. Protection can be as simple as asynchronous replication of key data or as complex as a complete hot-backup site. Data protection is based primarily on the familiar NetApp SnapMirror technology.

Data replication

SnapMirror technology keeps your data synchronized between on-premises and cloud installations by using ONTAP Snapshot copies. SnapMirror performs block-level incremental data transfers to ensure that only the data that has changed is sent to your destination replica.



Similarly, you can use a SnapMirror vault relationship to create a data archive for the local Snapshot copies created on a Cloud Volumes ONTAP system.

NetApp Cloud Backup delivers seamless and cost-effective backup and restore capabilities for protecting and archiving data to object storage in the cloud. Cloud Backup is available for both cloud-based data and for on-premises data.

Related information

Setting up a disaster recovery in the cloud with Cloud Volumes ONTAP

Efficient Data Replication Using Cloud Volumes ONTAP and SnapMirror

ONTAP Data Protection with the CLI

NetApp Cloud Backup

High availability

In an on-premises data center, physical nodes are configured in high-availability (HA) pairs for fault tolerance and nondisruptive operations. If a node fails or if you need to bring a node down for routine maintenance, its partner takes over its storage and continues to serve data from it.

In a cloud environment, you can create an HA pair of Cloud Volumes ONTAP instances for the same fault tolerance and non-disruptive operations as an on-premises HA pair. These recovery objectives are available with cloud HA pairs:

- The recovery point objective (RPO) is 0 seconds. Your data is transactionally consistent with no data loss.
- The recovery time objective (RTO) is 60 seconds. In the event of an outage, data should be available in 60 seconds or less.

Each cloud provider offers its own HA architecture and configuration options. For Cloud Volumes Service, high availability is guaranteed in the service level agreement.

Related information

High-availability pairs in AWS

High-availability pairs in Azure

Encryption of data at rest

ONTAP uses the same encryption technology to secure data in the cloud that you use to secure your on-premises data.

Cloud Volumes ONTAP supports NetApp Volume Encryption (NVE) and NetApp Aggregate Encryption (NAE) with an external key manager.

Cloud Volumes ONTAP also supports the following encryption technologies:

- AWS Key Management Service
- Azure Storage Service Encryption
- Google Cloud Platform default encryption

Data is always encrypted at rest when using Azure NetApp Files and NetApp Cloud Volumes Service for Google Cloud.

Related information

Encryption of data at rest in Cloud Volumes ONTAP

NetApp Volume Encryption and NetApp Aggregate Encryption

Encrypting volumes in Cloud Volumes ONTAP with NetApp encryption solutions

Antivirus protection

You likely use the integrated antivirus functionality on-premises to protect data from being compromised by viruses or other malicious code. This same antivirus protection is available in the cloud when you use Cloud Volumes ONTAP.

The ONTAP Antivirus Connector, installed on a local server, handles communication between the storage system and the antivirus software. For Cloud Volumes ONTAP, you install the Antivirus Connector on a virtual machine in the same cloud as ONTAP.

Related information

Antivirus configuration