Multi-Tier Cloud Replication with NetBackup and Veritas Alta

Contents

Introduction

Veritas Technologies is a leader in developing data resiliency solutions that focus on the protection and management of organizations' digital assets. Veritas Alta™ Data Protection for NetBackup Cloud Workloads (formerly known as NetBackup Enterprise for Cloud) is a key part of NetBackup, and together they are designed to protect data centers, hybrid-cloud, and multi-cloud environments.

Protecting data is an integral part of keeping an organization's intellectual property safe from human error, hardware failure, malware (including ransomware), espionage, and natural disasters. Data in the cloud is no exception, and companies must put proper backup and recovery procedures in place to avoid the same risks faced by on-premises data.

This technical brief outlines NetBackup and Veritas Alta Data Protection's multi-tier backup, recovery, and replication capabilities. It describes the components of this solution along with sizing guidance and some best practices. Although this document provides some deployment examples, please refer to the online NetBackup documentation and/or cloud provider documentation for full details on installation, configuration, and administration.

Architecture

Once you've created or saved data to the cloud, then how do you protect it? Administrators should be able to set up a storage lifecycle policy (SLP) that includes a snapshot and make a backup copy in a NetBackup storage-optimized format that is sent to any supported storage tier of the same cloud for a period defined by your SLP. Administrators should also be able to move backups to less-costly storage tiers for extended retention in compliance use cases.

With the power of NetBackup, Azure, Azure Stack, and Amazon Web Services (AWS) administrators can use multi-tier replication to ensure data is not only protected, but stored in any location they choose—including lower-cost storage options, either on-premises or in the cloud—and in a deduplicated format to minimize storage costs (see Figure 1).
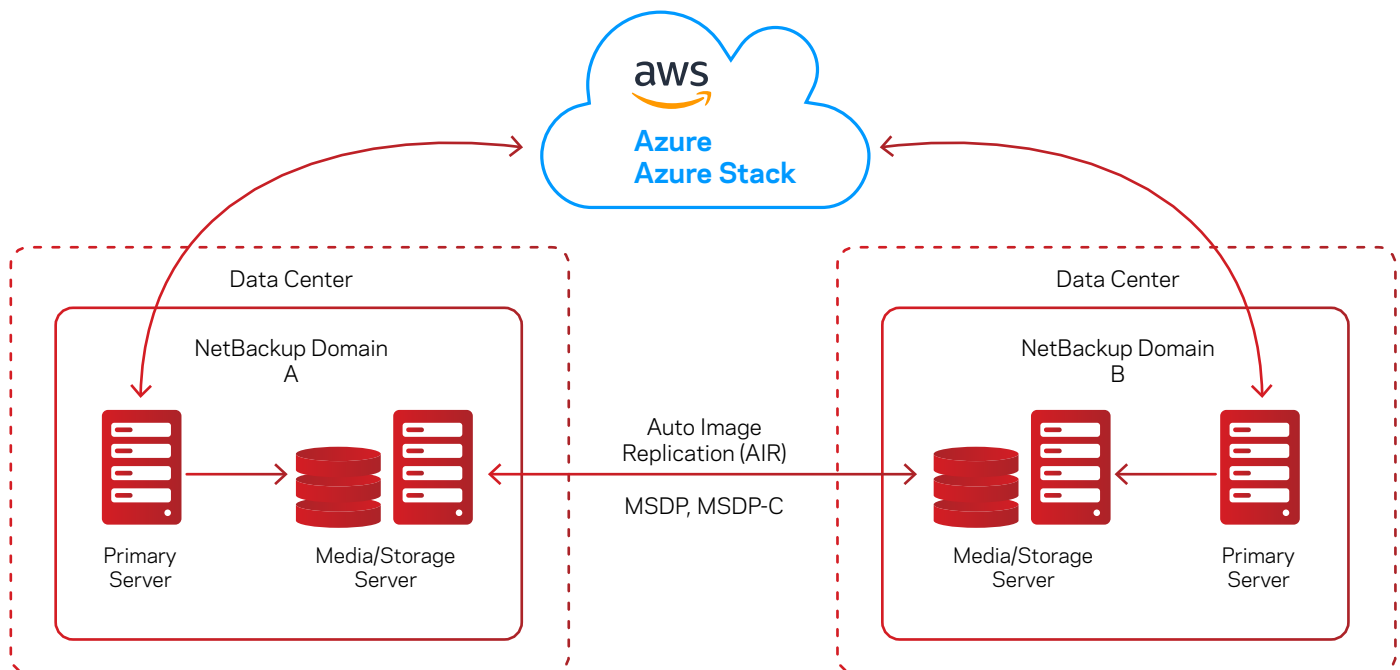

Figure 1. An overview of creating multi-tier backup copies and replication using NetBackup AIR technology.

How it Works

The process begins by creating a protection plan within the NetBackup web UI and choosing the cloud provider that currently houses the data you wish to back up to multiple locations and replicate (see Figure 2).
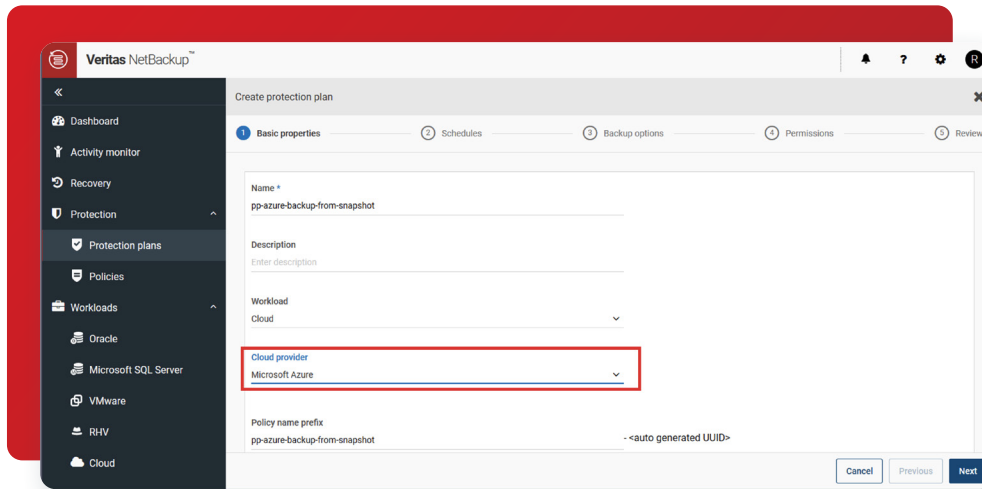

Figure 2. Creating a backup plan and selecting the cloud vendor in the NetBackup web UI.

When adding the backup schedule, a familiar page will appear that contains the new capabilities. The backup administrator has many options, but to create multiple copies and replication, the admin must choose either "Keep snapshot along with backup" or "Keep backup only" because snapshots are created by the cloud vendor and not by Veritas Alta Data Protection for NetBackup Cloud Workloads.

After choosing the snapshot and backup option, the administrator can choose to "Replicate this backup" and/or "Duplicate a copy immediately to long-term retention," with the ability to specify for how long (see Figure 3). Currently the admin can use only full backups and MSDP and MSDP-C storage units.
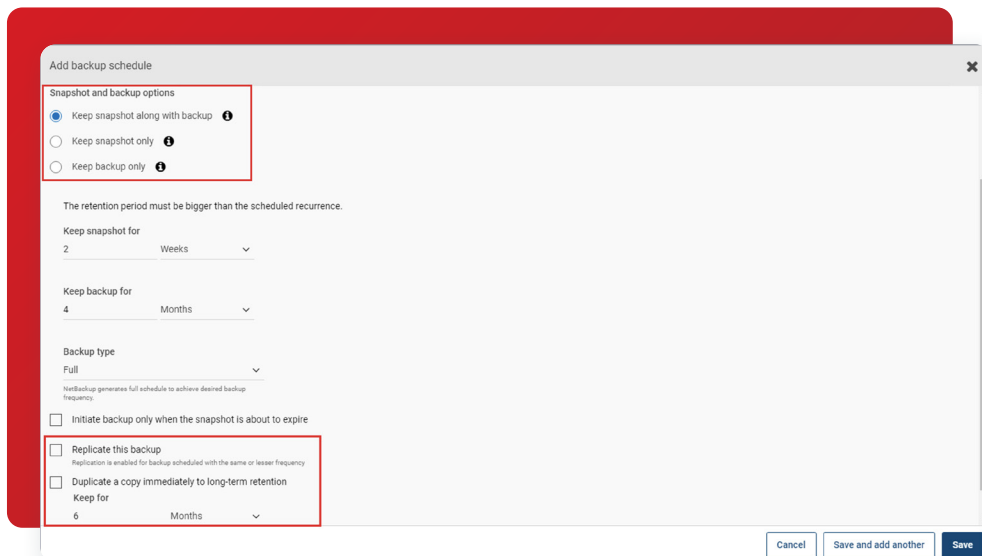

Figure 3. Selecting the backup and snapshot schedule in the NetBackup web UI.

Continuing with the configuration, the backup administrator will be presented with the screen shown in Figure 4 that displays both the backup storage as well as the long-term retention storage locations. The admin can edit and change these choices at any time for ease of use and flexibility.
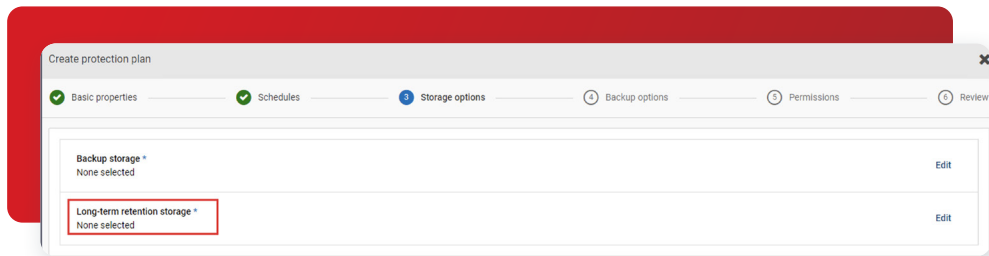

Figure 4. Selecting long-term retention (LTR) storage in the NetBackup web UI.

If the admin chose replication, another screen will appear that displays the replication target (see Figure 5).
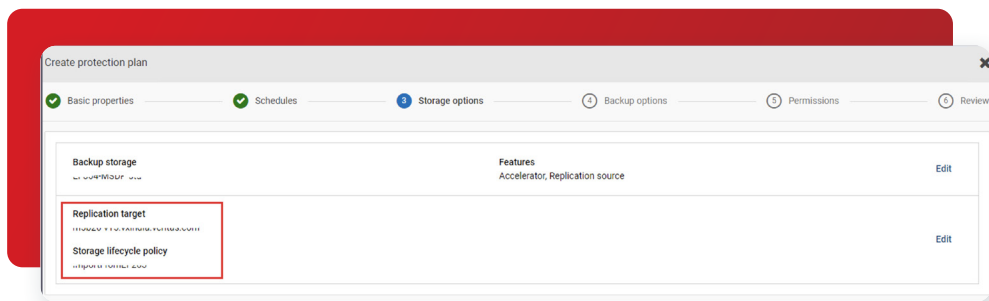

Figure 5. Creating a replication target in the NetBackup web UI.

Veritas knows how important your data is to your organization, but we also realize that storing data in its native format can be prohibitively costly. Veritas Alta Data Protection for NetBackup Cloud Workloads supports duplication and replication from a backup copy for Azure Cloud, Azure Stack, and AWS workloads. Users of Azure Cloud and Azure Stack workloads will see three copies—the snapshot copy, the backup copy, and another backup copy that is essentially the duplicate copy used for long-term retention.

Restoring Data

Now that your data is safe, how do you restore? The NetBackup web UI provides many helpful options to restore your data (see Figure 6).
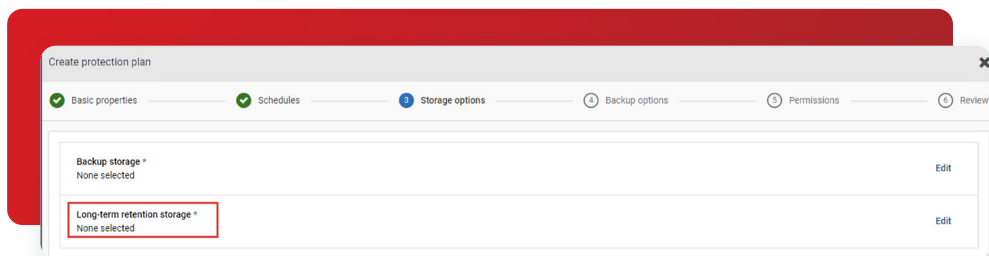

Figure 6. The cloud restore options available in the NetBackup web UI.

1. You can restore the backup image from one Azure Cloud/Azure Stack/AWS region to another Azure Cloud/Azure Stack/AWS region. You can change the region by selecting a different tenant or account in the NetBackup Snapshot Manager configuration and selecting one of the associated regions of that configuration.

2. You can restore the backup image to another subscription present within the configuration. When you click the subscription drop-down, it shows the list of subscriptions associated to the configuration. You should have role-based access control (RBAC) to the subscription. If a subscription is changed, the resource group of the virtual machine (VM) and its disks are cleared because they might be invalid once the subscription of the VM is changed. You need to select resource group of the VM. By design, once you've selected the resource group of the VM, the resource group of individual disks defaults to the resource group of the VM. You need to click the edit option of each disk and change the resource group of each disk if you want it to be different than that of the VM.

3. You can change the resource group of the VM or the resource group of individual disks for backup images like snapshot images.

4. You can change the network configuration of the VM. If you change the subscription of the VM, then the existing network configuration that belongs to a different subscription is invalidated and is cleared from the UI. You need to click on the search button to select the virtual network/subnet. The list shows the virtual network/subnet present in the selected subscription ID. The resource group name of the virtual network/subnet is shown in the display name, so it is easier for you to select a network. The list pop-up also has a search option that helps you search on the names of the networks.

5. You can restore the VM either in a powered-on state or a powered-off state.

6. By default, tags associated with a VM and its disks are restored during the restore operation. You have an option to not restore tags during the restore operation, which is useful for restores in test environments.

Summary

Where we compute and store our data is changing, and Veritas Alta Data Protection for NetBackup Cloud Workloads has the features to help keep your data safe and protected. With multi-tier backup and replication, your data can thrive in the cloud without compromises or risk of data loss. By incorporating innovative tools, Veritas makes protecting your data easier and lowers long-term storage costs as well.

For more information on Veritas Alta Data Protection for NetBackup Cloud Workloads, visit http://www.veritas.com/netbackup.

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS™

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact
information visit:
veritas.com/company/contact