VERITAS

Business Continuity and Disaster Recovery in Veritas NetBackup™ SaaS Protection

Ensuring the availability of SaaS application backup data.

White Paper | May 2022

Contents

Introduction

Enterprise IT leaders are looking to invest in technologies that help them recover data from modern threats, such as ransomware and rogue administrators, and accidental deletion. These IT leaders are looking to achieve a low recovery point objective (RPO), to minimize the amount of data lost, and a low recovery time objective (RTO), to minimize the time they are without access to their data.

To meet these requirements and protect their SaaS application data, more enterprises are selecting NetBackup SaaS Protection for backup and recovery, as well as ransomware resiliency.

Because no one schedules cyber attacks or accidental deletions, enterprises need a highly-available backup and recovery solution that has its own data protection. This document provides an overview of the technologies Veritas uses to ensure NetBackup SaaS Protection can give enterprises the SaaS application data they need, when they need it, even in the event of cloud infrastructure failures.

Critical Elements of the NetBackup SaaS Protection Architecture

The four architectural components that must be running properly for NetBackup SaaS Protection to make SaaS application data available for restores are described below:

1. Azure Blob Storage account(s):
   All content, access control lists, folder structures, and permissions can be solely recovered from blob storage. A customer's NetBackup SaaS Protection tenant can have one or multiple Azure Blob Storage accounts. Each account contains the objects that were backed up, as well as all item-level metadata.
2. Azure SQL database instances:
   Each Azure Blob Storage account in a customer's NetBackup SaaS Protection tenant will have an associated Azure SQL instance which contains auditing data, policies, statistics, permissions, and some item-level metadata.
3. Azure Active Directory (AD):
   Azure AD is a continuously-available data service. It is backed up and geo-replicated with multiple geographically-dispersed read-only copies.
4. Azure App Service:
   The Azure App Service manages all access and runs various jobs to update statistics, track activity, execute policies, etc. While the Azure App Service itself stores no data, it is required for access to data and for writing new data.

Technologies Used to Ensure NetBackup SaaS Protection Availability

Veritas employs multiple technologies to ensure that all critical elements of a customer's tenant are running and accessible. Different technology combinations can be used for the critical elements of the NetBackup SaaS Protection architecture to meet the specific high-availability requirements of the customer.

Availability of Azure Blob Storage accounts

A customer's Azure Blob Storage accounts are always replicated, providing a minimum of three copies of the data to ensure its durability and high-availability. This is accomplished by means of the Azure Locally-Redundant Storage (LRS) feature of Azure. These replicas are stored in the same physical data center. Replication is synchronous, meaning the data transfer to a remote copy within the same data center is immediate. There are no Azure data egress charges for these replicas.

While Azure Block Storage offers no native backup option, NetBackup SaaS Protection tenants offer an option, called Blob Storage Backup, for customers wanting a higher level of high-availability. When this option is enabled, NetBackup SaaS Protection will back up any new objects in the associated Azure Blob Storage accounts every 15 minutes. The data in these accounts is backed up to a secondary, customer-owned Azure Blob Storage account, in a different geographical region. By default, the backups are sent to the low-cost archive tier in the secondary account.

In a failover event, this secondary storage account can be used immediately for writes, giving NetBackup SaaS Protection a fully-functional high-availability solution in the event of a regional outage.

Availability of Azure SQL database instances

Like Blob Storage, Azure SQL databases have options for replication using Azure SQL Geo-Replication. Geo-replication of Azure SQL instances is a valuable feature for customers who want the shortest recovery times. This lower RTO is provided through the use of a warm standby copy of the database instance in a secondary region.

For greater data protection, Azure SQL instances can have point-in-time backups, as well as long-term retention (LTR) of full backups of the database instances. Geo-replicated copies of databases provide an RPO of less than 5 seconds and an RTO of less than 30 seconds. LTR copies of databases provide an additional recovery option that can be used as a last resort, with an RPO of less than an hour and an RTO of less than 30 seconds.

Availability of Azure Active Directory

Azure does a great job of providing highly-available Active Directory (AD). Azure AD is continuously backed up and geo-replicated with multiple geographically-dispersed read-access copies.

Availability of the Azure App Service

There are high-availability options available for the Azure App Service. This availability is provided by using a geo-redundant configuration for Azure Blob Storage accounts and provisioning an additional instance of the Azure App Service at the secondary site.

If the lowest RTO is required, even in the event of a region-wide outage, the secondary App Service instance can be kept running as a warm standby. Since the time required to provision a new App Service in a failover scenario is relatively small, customers typically don't find the RTO improvement of the warm standby to be worth the ongoing additional cost.

Summary

Veritas recognizes that a backup copy that is inaccessible defeats the purpose of having the backup copy. Therefore, with NetBackup SaaS Protection, Veritas employs multiple technologies to provide different levels of high-availability to customers, enabling customers to select the option(s) that best fit their specific needs.

VERITAS

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

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

V1569 05/22