White Paper

Regional Storage Configuration in SaaS Backup for Office 365

Ankur Sharma | NetApp

Aug 2019 | WP-7306

Abstract

This white paper outlines the details and benefits of a region-specific storage bucket provided by NetApp® SaaS Backup for Office 365 that offers a flexible and scalable backup solution.

TABLE OF CONTENTS

LIST OF FIGURES

1 Introduction

Data backup is important for quick and seamless data restoration following data loss so that users can stay productive. However, running additional software in the SaaS infrastructure is not an option.

1.1 NetApp SaaS Backup for Office 365

NetApp® SaaS Backup for Office 365 is a secure, encrypted, cloud-native offering that protects Microsoft Office 365, an online, subscription-based service for email, collaboration, and other functions. SaaS Backup protects Office 365 data from accidental deletion or malicious activity and provides storage options in Amazon AWS and Microsoft Azure, with a choice of target locations for backup flexibility. It manages backup for Exchange Online, SharePoint Online, OneDrive for Business,Teams, and O365 Groups

2 Choose a Geographical Location for Your Backup Data

SaaS Backup allows you to choose storage buckets in specific regions to meet local compliance and security requirements. Region-specific storage buckets offer the following benefits:

- Ensuring that data residing in a country meets the security and compliance requirements of that country.
- Choosing a nearby location means reduced latency for backup data access (in the form of restore or export).
- Choosing a nearby location also increases bandwidth, providing faster data access.
- Selecting a more distant location protects data from geographical disaster.

2.1 SaaS Backup Managed Storage

SaaS Backup offers two types of managed storage to backup your Office 365 data.

Figure 1) Storage options in SaaS backup.

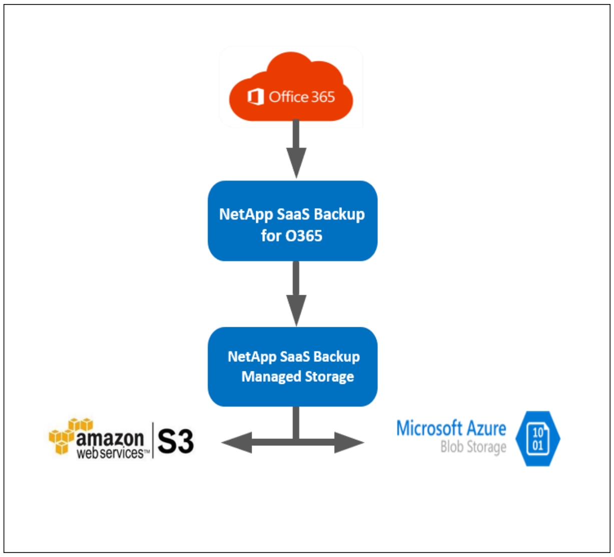
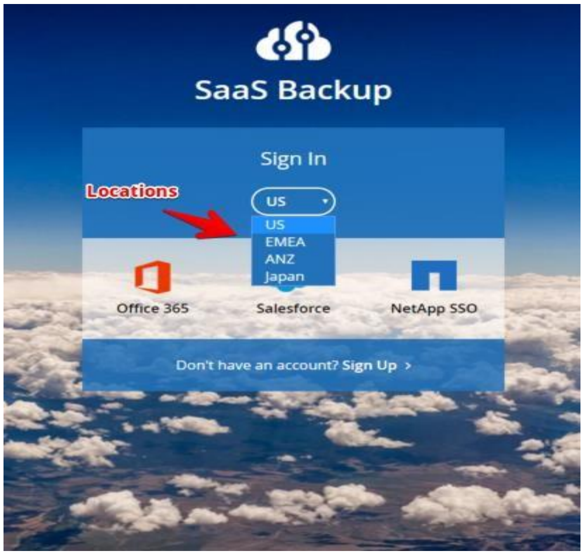

Office 365
NetApp SaaS Backup for O365
NetApp SaaS Backup Managed Storage
amazon web services S3
Microsoft Azure Blob Storage
10 01

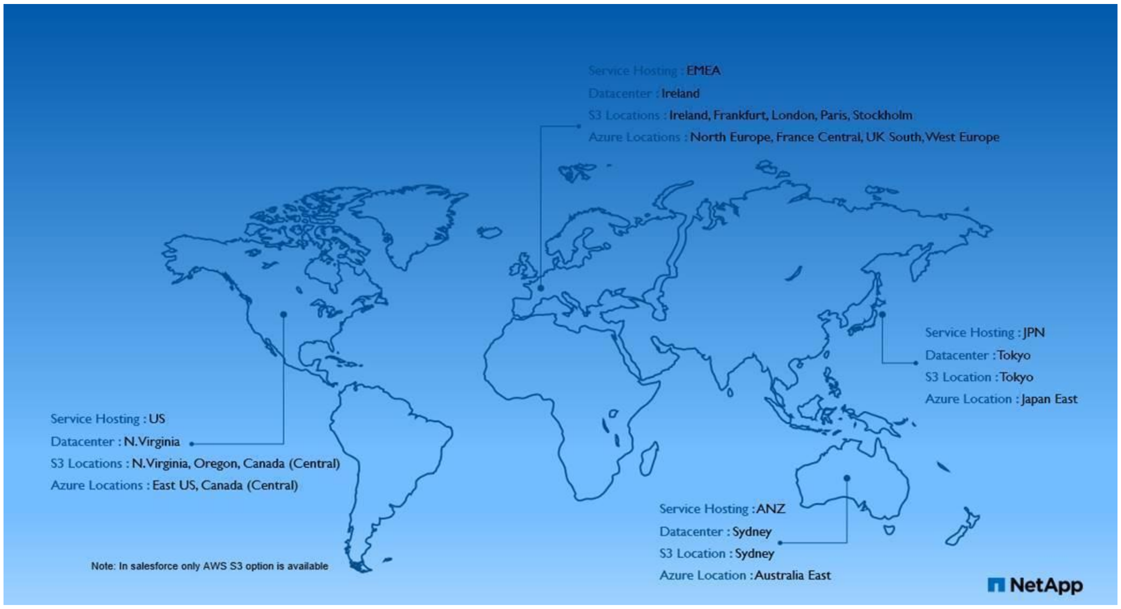
Figure 2) Locations available in SaaS backup.



As per the location selected during the sign-up process, NetApp SaaS Backup for Office 365 offers the flexibility of choosing the complete range of target locations for backup storage in the registered location. The service is currently offered in the US, EMEA, ANZ, and Japan.

2.2 Locations Available For SaaS Backup

Figure 3) SaaS backup locations.


Service Hosting : EMEA
Datacenter : Ireland
S3 Locations : Ireland, Frankfurt, London, Paris, Stockholm
Azure Locations : North Europe, France Central, UK South, West Europe
Service Hosting : JPN
Datacenter : Tokyo
S3 Location : Tokyo
Azure Location : Japan East
Service Hosting : US
Datacenter : N.Virginia
S3 Locations : N.Virginia, Oregon, Canada (Central)
Azure Locations : East US, Canada (Central)
Service Hosting : ANZ
Datacenter : Sydney
S3 Location : Sydney
Azure Location : Australia East
NetApp

Note: In salesforce only AWS S3 option is available

Note: Region selection is a tenant-level configuration and cannot be applied to a specific tier/user.

3 Considerations When Choosing a Storage Type

Organizations should consider these factors when choosing a storage bucket:

- Select a storage bucket in a region closest to the SaaS Backup user for increased bandwidth and reduced latency.
- Choose a storage bucket in a region farther from your location if it is prone to frequent geographical disasters.
- Consider compliance and legal requirements when choosing the storage bucket location.
- Both storage options use object storage (also called object-based storage), which is an approach to addressing and manipulating data storage as discrete units, called objects.

Note: NetApp does not recommend one cloud provider over the other for SaaS Backup.

4 Security and Encryption of Storage Buckets

Data is encrypted in-flight and at-rest. Data in transit is encrypted and secured using Transport Layer Security (TLS v1.2). Data at rest is encrypted using Amazon S3 SSE 256-bit Advanced Encryption Standard (AES-256). With Amazon S3 SSE, every protected object is encrypted with a unique encryption key.

Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available. SaaS backup uses the OAuth mechanism, which redirects the user to the Office 365 login page.

Therefore, SaaS Backup does not store any username or password information.

5 Conclusion

NetApp SaaS Backup for Microsoft Office 365 is a fully managed cloud solution specifically designed to back up and restore crucial data associated with Office 365 services. Region-based backup functionality can help your organization keep data secure and meet your security and compliance requirements.

To find out more about the product and the data residency described in this white paper, sign up for a trial with SaaS Backup for Office 365.

Click here for more information about NetApp SaaS Backup for Office 365.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Trademark Information