



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

1	Introduction	3
1.1	NetApp SaaS Backup for Office 365	3
2	Choose a Geographical Location for Your Backup Data	3
2.1	SaaS Backup Managed Storage	3
2.2	Locations Available For SaaS Backup	4
3	Considerations When Choosing a Storage Type	4
4	Security and Encryption of Storage Buckets	5
5	Conclusion	5

LIST OF FIGURES

Figure 1)	Storage options in SaaS backup	3
Figure 2)	Locations available in SaaS backup	4
Figure 3)	SaaS Backup Locations	4

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.

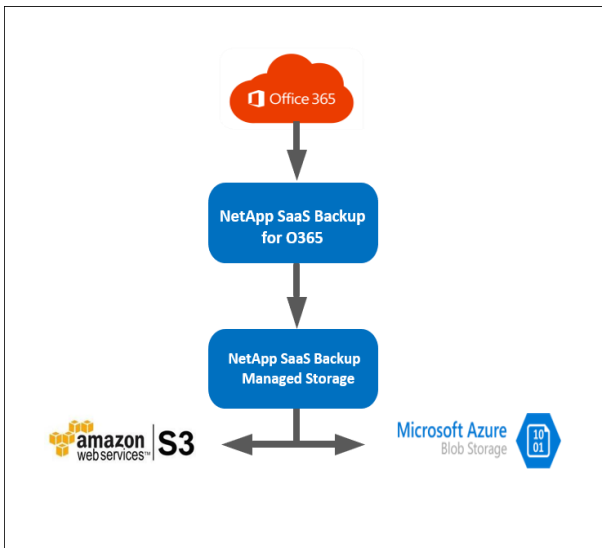


Figure 2) Locations available in SaaS backup.



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.



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

Copyright © 2019 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer: THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice.

NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.