



Manage S3 buckets

Amazon S3 storage

NetApp

February 23, 2024

Table of Contents

- Manage S3 buckets 1
 - Add S3 buckets 1
 - Change S3 bucket settings 2
 - Use NetApp data services with S3 buckets 4

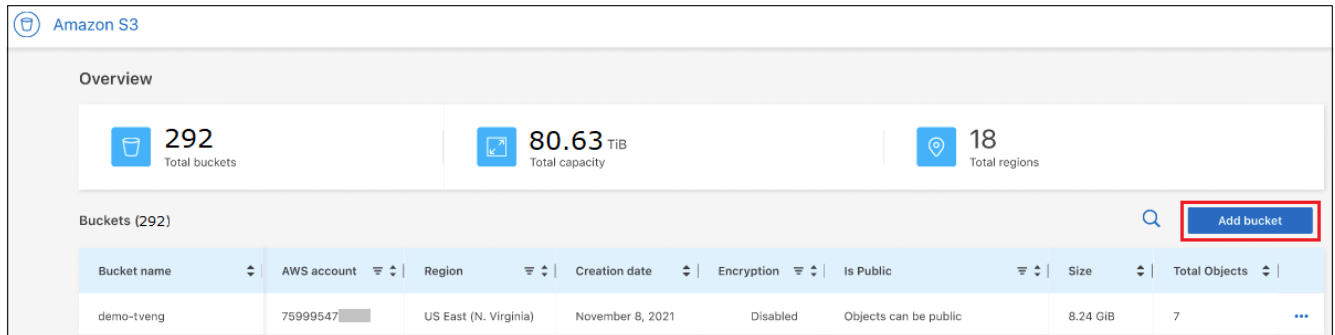
Manage S3 buckets

Add S3 buckets

Once your Amazon S3 working environment is available in the Canvas, you can add additional buckets directly from BlueXP.

Steps

1. From the Canvas, double-click the Amazon S3 working environment to view the Amazon S3 buckets Overview page, and click **Add bucket**.



The *Add bucket* page is displayed.

The screenshot shows the 'Add bucket' page. It has a header 'Add bucket' and a section 'Details and object lock'. Below this, there is a text prompt: 'Enter the following information to create the bucket. You can customize additional bucket settings after it is created.' The form includes a 'Bucket name' text input field, an 'AWS account' dropdown menu (currently showing 'Select account'), and a 'Bucket region' dropdown menu (currently showing 'Select region'). Below these is the 'Object lock' section, which has a toggle switch set to 'Disabled' and a note: 'You can only enable Object Lock for a bucket when you create it, and you can't disable it later. Enabling Object Lock also enables versioning for the bucket.' At the bottom of the form, there are three expandable sections: 'Versioning' (set to 'Disabled'), 'Tags' (set to 'N/A'), and 'Encryption' (set to 'Disabled'). The 'Apply' button is highlighted with a red box.

2. In the Add bucket page, enter the required information to create the bucket and click **Apply**.
 - a. Enter the name you want to use for the bucket.
 - b. Select the AWS account that will be the owner of the bucket. This can be the primary account where the Connector was deployed, or it can be a [different account that you have added to BlueXP](#).

- c. Select the AWS region where the bucket will be created.
- d. Optionally, you can enable S3 object locking on the bucket to store objects using a write-once-read-many (WORM) model. If you plan to use object locking, you must enable it when creating the bucket. Enabling Object Lock also enables Versioning. [Learn more about object locking from the Amazon S3 documentation.](#)

The bucket is created.

What's next

You can't manually configure Versioning, Tags, or Encryption when initially adding a bucket. After the bucket is created you can configure these other properties of the bucket. [Learn more about changing bucket settings.](#)

Change S3 bucket settings

Once your Amazon S3 working environment is available in the Canvas, you can change some bucket properties directly from BlueXP.


Note that you can't change the bucket name, AWS account, region, or object lock setting.


The bucket properties you can change include:


- Whether Versioning is enabled or disabled for all objects in the bucket.
- You can choose to apply tags to the objects that are added to the bucket.
- Whether or not new objects added to the bucket are Encrypted, and the option used for encryption.

You can change these bucket settings directly from BlueXP by clicking ... for a bucket.

Overview

 178
Total Buckets

 3.47 TiB
Total Capacity

 19
Total Regions

178 Buckets Search Add bucket

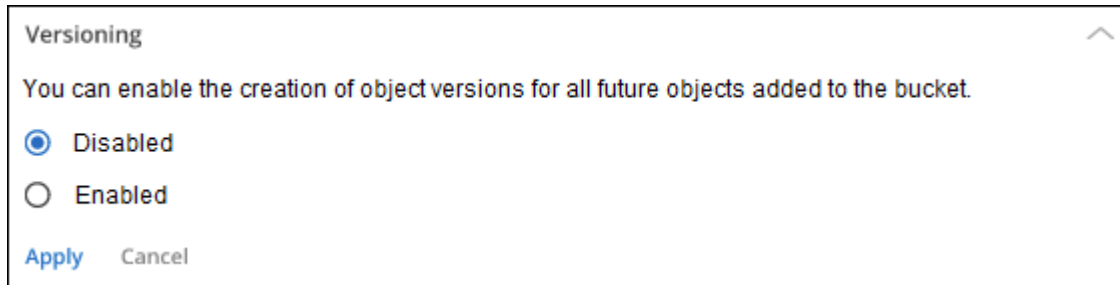
Bucket Name	AWS Account	Region	Creation Date	Encryption	Is Public	
compliance-dataset22	7599954	US West (Oregon)	March 1, 2020	Enabled ⓘ	Bucket and ob	⋮
fabric-pool-8b18cf1e-6d64	7599954	US West (Oregon)	March 24, 2020	Enabled ⓘ	Bucket a	View details
motor-vehicle-bucket01	7599954	US West (Oregon)	June 3, 2020	Enabled ⓘ	Objects	Edit versioning
fabric-pool-a548f122-a681	7599958	US West (Oregon)	June 5, 2020	Enabled ⓘ	Objects	Edit tags
motor-vehicle-bucket64	7599958	US West (Oregon)	June 10, 2020	Enabled ⓘ	Objects	Edit encryption

Change the versioning setting

Versioning enables you to keep multiple versions of an object in a bucket so that you can restore objects that are accidentally deleted or overwritten. You can change the versioning setting for future objects when they are added to the bucket. Changing the versioning setting does not change the value for existing objects.

Versioning is disabled by default in new buckets created by BlueXP, unless you enabled Object Lock when you created the bucket. [Learn more about versioning from the Amazon S3 documentation.](#)

Once enabled, if you want to stop versioning temporarily or permanently, you can choose the "Suspended" state. You can't disable versioning once it has been enabled.

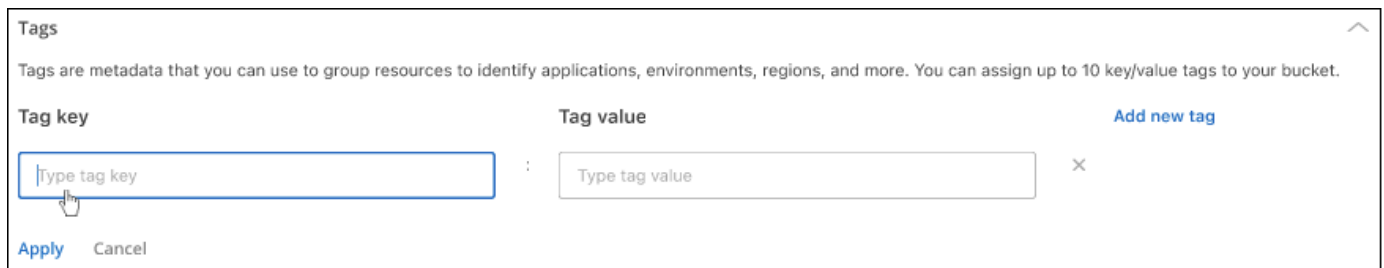


The screenshot shows a dialog box titled "Versioning" with a close button in the top right corner. The text inside says, "You can enable the creation of object versions for all future objects added to the bucket." Below this text are two radio buttons: "Disabled" (which is selected) and "Enabled". At the bottom of the dialog are two buttons: "Apply" and "Cancel".

Add or change tags for objects in the bucket

Tags are metadata that you can use to group resources to identify applications, environments, regions, cloud providers, and more. Tags consists of a tag key and a tag value. You can add tags to a bucket so that the tags are applied to objects when they are added to the bucket. You can also change and delete tags and tag values.

Tags are disabled by default in new buckets created by BlueXP. [Learn more about tagging from the Amazon S3 documentation.](#)



The screenshot shows a dialog box titled "Tags" with a close button in the top right corner. The text inside says, "Tags are metadata that you can use to group resources to identify applications, environments, regions, and more. You can assign up to 10 key/value tags to your bucket." Below this text are two input fields: "Tag key" and "Tag value". The "Tag key" field has a placeholder text "Type tag key" and the "Tag value" field has a placeholder text "Type tag value". To the right of the "Tag value" field is a close button (X). Above the "Tag value" field is a link "Add new tag". At the bottom of the dialog are two buttons: "Apply" and "Cancel".

After you add a tag, click **Apply** to save your changes. If you want to add more tags, click **Add new tag**. You can add up to 10 tags per bucket.

Change the encryption setting

Server-side encryption enables you to encrypt data at the Amazon S3 destination. Amazon S3 encrypts your data at the object level as it writes it to disk, and it decrypts it for you when you access it. You can change the encryption setting used for future objects when they are added to the bucket.

Encryption is enabled by default using "Amazon S3 managed keys (SSE-S3)" in new buckets created by BlueXP. [Learn more about server-side encryption from the Amazon S3 documentation.](#)

Alternatively, you can choose to enable encryption using the "AWS Key Management Service key (SSE-KMS)". Encryption is also possible using your own customer-provided keys (SSE-C), but this functionality is unavailable through the BlueXP UI - you'll need to use the Amazon interface.

Encryption

Server-side encryption is automatically applied to new objects stored in this bucket. [Learn more](#)

Encryption key type i

☒ Amazon S3-managed keys (SSE-S3) ☐ AWS Key Management Service key (SSE-KMS)

Bucket key i

☒ Enabled

[Apply](#) [Cancel](#)

If you choose "AWS Key Management Service key (SSE-KMS)", you can choose an AWS KMS key that you've already created, or you can use an AWS KMS key ARN (Amazon Resource Name).

Encryption

Server-side encryption is automatically applied to new objects stored in this bucket. [Learn more](#)

Encryption key type i

☐ Amazon S3-managed keys (SSE-S3) ☒ AWS Key Management Service key (SSE-KMS)

AWS KMS key

☐ Choose from your AWS KMS keys ☒ Enter AWS KMS key ARN

AWS KMS key ARN i

`arn:aws:kms:<region>:<account-ID>:key/<key-id>`

Bucket key i

☒ Enabled

[Learn more about the AWS Key Management Service from the Amazon S3 documentation](#) and about [using customer keys versus AWS keys](#).

Use NetApp data services with S3 buckets

After you discover S3 buckets in BlueXP, you can use NetApp data services for backup, tiering, classification, and data synchronization.

- Use **BlueXP backup and recovery** to back up data from your on-premises ONTAP and Cloud Volumes ONTAP systems to S3 object storage.

To get started, go to the Canvas and drag and drop an on-premises ONTAP or Cloud Volumes ONTAP working environment on your Amazon S3 working environment.

[Learn more about backing up ONTAP data to Amazon S3 storage.](#)

- Use **BlueXP tiering** to tier inactive data from on-premises ONTAP clusters to S3 object storage.

To get started, go to the Canvas and drag and drop an on-premises ONTAP working environment on your Amazon S3 working environment.

[Learn more about tiering ONTAP data to Amazon S3 storage.](#)

- Use **BlueXP copy and sync** to synchronize data to or from S3 buckets.

To get started, go to the Canvas and drag and drop the source working environment on the target working environment. Your Amazon S3 working environment can be either the source or target.

You can also select your Amazon S3 working environment and click **Copy & sync** from the Services panel to synchronize data to or from S3 buckets.

[Learn more about the BlueXP copy and sync service.](#)

- Use **BlueXP classification** to scan your S3 buckets for personal and sensitive data. BlueXP classification can scan any bucket in the account, regardless of whether it was created for a NetApp solution.

To get started, select your Amazon S3 working environment and select the appropriate option from the **Classification** section of the Services panel to initiate scanning of your S3 buckets.

[Learn more about the BlueXP classification service.](#)

Copyright information

Copyright © 2024 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, 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) (FEB 2014).

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.