Setting up Cloud Backup Service for NetApp Cloud Volumes Service for AWS

Beta Release

February 2019

Abstract

This document provides instructions to help beta release users of Cloud Backup Service set up and use the service.

NetApp

Contents

A. Overview of Cloud Backup Service beta release 3
B. Terms for using the Cloud Backup Service beta software 3
C. Requirements and considerations 3
D. Backing up cloud volumes by using Cloud Backup Service 4
1. Configuring a cloud volume snapshot policy 4
2. Configuring Cloud Backup Service for policy-based (scheduled) backups 4
3. Managing a Cloud Backup Service policy 5
4. Restoring a backup to a new cloud volume 5
5. Deleting a backup 5
E. Cloud Backup Service APIs 6
F. Support for beta release 6
Version History 6

A. OVERVIEW OF CLOUD BACKUP SERVICE BETA RELEASE

The purpose of the Cloud Backup Service beta release is to provide users of NetApp Cloud Volumes Service for AWS early access to the Cloud Backup Service add-on feature.

Cloud Backup Service expands the data protection capabilities of Cloud Volumes Service by delivering dedicated backups for long-term recovery, archive, and compliance. Backups created by the service are stored in AWS S3 object storage, independent of cloud volume snapshots that are available for near-term recovery or cloning.

Users are expected to give feedback to NetApp about Cloud Backup Service during the beta period to help NetApp provide the best user experience when the service becomes generally available (GA).

B. TERMS FOR USING THE CLOUD BACKUP SERVICE BETA SOFTWARE

In accordance with NetApp terms and conditions, the Cloud Backup Service beta release does not provide production-level backups and restores. It is highly recommended that you test Cloud Backup Service by using test copies of production data to mimic usage for production workloads. Although you can choose to protect production data during the beta period, you must be aware of and accept the following potential limitations:

- During the service transition from beta release to GA, backups created during the beta period might be destroyed without notification.
- NetApp might determine that software or other changes are necessary to resolve issues prior to GA. The changes might impact your ability to recover backups that were created during the beta period. It is NetApp's intention to not impose this impact.

C. REQUIREMENTS AND CONSIDERATIONS

You need to be aware of several requirements and considerations before deploying Cloud Backup Service:

- You must have subscribed to Cloud Volumes Service for AWS before you can participate in the Cloud Backup Service beta release.

  See the Get a first look at the new NetApp Cloud Volumes Service for AWS page for information about subscribing to Cloud Volumes Service for AWS.

- Your cloud volume must be located in the ***AWS US-WEST-2 (Oregon)*** region.

  You can only use Cloud Backup Service to protect a cloud volume that is located in the AWS US-WEST-2 region. Backups created by the service are sent to AWS S3 object storage that is located also in US-WEST-2. The beta release does not support direct backups or replication to a different region.

  You can select the US-WEST-2 region by using the Cloud Volumes Service for AWS web UI. See Selecting the region for details.

- To set up a backup policy using Cloud Backup Service, your cloud volume must have a corresponding snapshot policy with a minimum retention count of 2.

For example, if you want to configure a daily backup policy, a daily snapshot policy must exist that retains at least two snapshots. If you want to configure a monthly backup policy, a monthly snapshot policy must exist that retains at least two snapshots. If a corresponding snapshot policy does not exist for a given backup frequency, you cannot enable that backup frequency. See Creating or modifying a snapshot policy for details about snapshot policies.

- The Cloud Volumes Service beta release supports only policy-based (scheduled) backups.

  Manual (on-demand) backups are not currently supported by the service. The service will support on-demand backups in an upcoming update.

- The Cloud Backup Service beta release supports only backups and restores of cloud volumes that are deployed with the NFS protocol.

  The service will support SMB and dual (NFS/SMB) protocol in an upcoming update.

D. BACKING UP CLOUD VOLUMES BY USING CLOUD BACKUP SERVICE

For the initial beta release, Cloud Volumes Service supports only policy-based backups for a cloud volume. Policy-based backups require that a snapshot policy be configured.

1. Configuring a cloud volume snapshot policy

If you do not already have a snapshot policy configured for your cloud volume, follow the instructions in Creating or modifying a snapshot policy to configure a snapshot policy with a frequency (daily, weekly, or monthly) that corresponds to the backup policy you plan to create.

Note: Although hourly snapshots are not required for the backups service, you can configure hourly snapshots as needed.

2. Configuring Cloud Backup Service for policy-based (scheduled) backups

A snapshot policy for the cloud volume must already exist before you can enable or modify the corresponding backup policy. See Creating or modifying a snapshot policy for details about snapshot policies.

To enable a policy-based (scheduled) backup:

1. Log in to the Cloud Volumes Service for AWS web UI.
2. Navigate to the **Volumes** page to display the list of available volumes, then select the volume that you want to back up.
   The Volume Details view appears.
3. Select **Backups**.

4. Click the toggle switch to enable the backup policy for the selected volume.
5. Specify the number of restores that you want to keep for daily, weekly, and monthly backups.
   Note: There is no option to select the start time for backups. The service performs the backups based on internal scheduling and optimization logic.
6. Click **Save Changes** to set and enable the backup policy.
   After the backup policy configuration is saved, a temporary backup is created instantly and displayed in the Volume Backups table. When the policy-based backup starts, the temporary backup goes away, and the table displays only the configured policy-based backup.

3. Managing a Cloud Backup Service policy

You can manage an existing Cloud Backup Service policy for a cloud volume as needed. For example, if you need to change the number of retained backups that are protected by the service, you can modify the Cloud Backup Service policy for the volume to revise the number of restores to keep.

To modify the backup policy settings:

1. Navigate to the **Volumes** page to display the list of available volumes, then select the volume whose backup policy you want to manage.
   The Volume Details view appears.
2. Select **Backups**.
3. Update the number of restores you want to keep for daily, weekly, and monthly backups.
   Note: After backups are enabled and have taken effect for the scheduled frequency, you cannot change the backup policy frequency to 0 restore points. A minimum number of 1 is required for the backup policy.
4. Click **Save Changes** to set and update the backup policy.

4. Restoring a backup to a new cloud volume

To restore a cloud volume backup to a new volume:

1. Navigate to the **Volumes** page to display the list of available volumes, then select the volume whose backup you want to restore.
   The Volume Details view appears.
2. Select **Backups**.
3. From the **Volume Backups** list, select the backup that you want to use, then select **Restore to Volume** from the Action column for that backup.
4. In the Restore Volume from Backup page, provide information for the fields in the page as applicable, and click **Create Volume** to begin restoring the backup to a new volume.

   For general information about the fields, see Creating a cloud volume.

   Note: For the **Protocol** field, you can select only NFSv3 for the Cloud Backup Service beta release.

5. Deleting a backup

You can delete scheduled backups for a cloud volume only when one of the following situations occurs:

- The original cloud volume has been deleted.

- The backup policy is disabled.

When either of the above situations occurs, the service asks you whether to keep or delete the backups. If you choose to delete the backups, all created backups are removed. If you choose to keep the backups, you must manually remove the backups from the Backups page if you want to delete them at a later time.

To manually delete a scheduled backup:

1. Navigate to the **Volumes** page to display the list of available volumes, then select the volume whose backup you want to delete.
   The Volume Details view appears.
2. Select **Backups**.
3. Select the backup that you want to delete from the Volume Backups list, then select **Delete Backup** from the Action column for that backup.
4. In the **Delete Backup** pop-up box, type ***delete*** to confirm, and click **Delete** to begin the deletion process.

E. CLOUD BACKUP SERVICE APIS

The Cloud Backup Service capabilities that are available through the web UI are also available through RESTful APIs. The APIs enable you to manage backups and develop scripts as needed.

To see the Cloud Backup Service APIs, go to the Cloud Volumes APIs page directly (https://app.swaggerhub.com/apis/NetApp-Cloud/c-vaa_s/). You can also click **API documentation** on the storage page of the Cloud Volumes Service for AWS web UI.

F. SUPPORT FOR BETA RELEASE

You must have accepted the terms and conditions for using the Cloud Backup Service beta software. Because this is a beta feature, all questions or technical support issues related to Cloud Backup Service must be directed through email at cvs-support@netapp.com. A NetApp engineer will then assist with any problems you are experiencing.

Version History

Version	Date	Document Version History
Version 1.0	February 2019	Initial beta release.

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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.