Back up cloud native applications data

Cloud Backup

NetApp
December 07, 2022

This PDF was generated from https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-discover-applications.html on December 07, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Back up cloud native applications data

Discover the applications

You should discover the databases on the host to assign policies and create backups.

What you will need

- You should have created the FSx for ONTAP working environment and the Connector.
- Ensure that the Connector has connectivity to the FSx for ONTAP working environment and Oracle database hosts.
- Ensure that the BlueXP user has the “Account Admin” role.
- You should have deployed the SnapCenter Plug-in for Oracle. Learn more.

Steps

1. In BlueXP UI, click **Protection** > **Backup and recovery** > **Applications**.
2. Click Discover Applications.
3. Select **Cloud Native** and click **Next**.

   A service account with *SnapCenter System* role is created to perform scheduled data protection operations for all the users in this account.

   - Click **Account** > **Manage Account** > **Members** to view the service account.

     The service account (*SnapCenter-account-<accountid>*) is used for running the scheduled backup operations. You should never delete the service account.

4. In the Specify Host Details page, enter the details of the Oracle database host, select the check box to confirm that the plug-in is installed on the host, and click **Discover**.
   - Displays all the databases on the host. If OS authentication is disabled for the database, you should configure database authentication by clicking **Configure**. For more information, refer to Configure Oracle database credentials.
   - Click **Manage Application**, select **Add** to add a new host, **Refresh** to discover new databases, or **Remove** to remove a database host.
   - Click **Settings** and select **Policies** to view the pre-canned policies. Review the pre-canned policies and if you want you can either edit them to meet your requirement or create a new policy.

Configure Oracle database credentials

You should configure credentials that are used to perform data protection operations on Oracle databases.

Steps

1. If OS authentication is disabled for the database, you should configure database authentication by clicking **Configure**.
2. Specify the username, password, and the port details either in the Database Settings or ASM Settings section.

The Oracle user should have sysdba privileges and ASM user should have sysasm privileges.

3. Click **Configure**.

Create policy

You can create policies if you do not want to edit the pre-canned policies.

Steps

1. In the Applications page, from the Settings drop-down list, select **Policies**.
2. Click **Create policy**.
3. Specify a policy name.
4. (Optional) Edit the format of the backup name.
5. Specify the schedule and retention details.
6. Click **Create**.

Back up the cloud native application data

You can either assign a pre-canned policy or create a policy and then assign it to the database. Once the policy is assigned, the backups are created as per the schedule defined in the policy. You can also create an on-demand backup.

When creating ASM diskgroups for Oracle, ensure that there are no common volumes across diskgroups. Each diskgroup needs to have dedicated volumes.

Steps

1. In the Applications page, if the database is not protected using any policy, click **Assign Policy**.

   If the database is protected using one or more policies, you can assign more policies by clicking ••• > **Assign Policy**.

2. Select the policy and click **Assign**.

   The backups will be created as per the schedule defined in the policy.

   The service account (*SnapCenter-account-<account_id>*) is used for running the scheduled backup operations.

Create on-demand backups

After assigning the policy, you can create an on-demand backup of the application.

Steps

1. In the Applications page, click ••• corresponding to the application and click **On-Demand Backup**.
2. If multiple policies are assigned to the application, select the policy, retention value, and then click **Create Backup**.

Find more information

After restoring a large database (250 GB or more), if you perform a full online backup on the same database the operation might fail with the following error:

```
failed with status code 500, error
{\"error\":{\"code\":\"app_internal_error\",\"message\":\"Failed to create
snapshot. Reason: Snapshot operation not allowed due to clones backed by
snapshots. Try again after sometime.
```

For information on how to fix this issue, refer to: Snapshot operation not allowed due to clones backed by snapshots.

Copyright information

Copyright © 2022 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.