

Cross-account and cross-region configurations

Cloud Manager

NetApp February 22, 2022

Table of Contents

Cross-account and cross-region configurations	 1
Configure backup for multi-account access in AWS	 1
Configure backup for multi-account access in Azure	

Cross-account and cross-region configurations

These topics describe how to configure Cloud Backup for cross account configurations when using different cloud providers.

- Configure Cloud Backup for multi-account access in AWS
- · Configure Cloud Backup for multi-account access in Azure

Configure backup for multi-account access in AWS

Cloud Backup enables you to create backup files in an AWS account that is different than where your source volumes reside. And both of those accounts can be different than the account where the Cloud Manager Connector resides.

Just follow the steps below to set up your configuration in this manner.

Set up VPC peering between accounts

- 1. Log in to second account and Create Peering Connection:
 - a. Select a local VPC: Select the VPC of the second account.
 - b. Select another VPC: Enter the account ID of the first account.
 - c. Select the Region where the Cloud Manager Connector is running. In this test setup both accounts are running in same region.
 - d. VPC ID: Log into first account and enter the acceptor VPC ID. This is the VPC ID of the Cloud Manager Connector.



A Success dialog displays.



The status of the peering connection shows as Pending Acceptance.



2. Log into the first account and accept the peering request:





a. Click Yes.



The connection now shows as Active. We have also added a Name tag to identify the peering connection called cbs-multi-account.



b. Refresh the peering connection in the second account and notice that the status changes to Active.



Add a route to the route tables in both accounts

1. Go to VPC > Subnet > Route table.



2. Click on the Routes tab.



3. Click Edit routes.



- 4. Click **Add route**, and from the Target drop-down list select **Peering Connection**, and then select the peering connection that you created.
 - a. In the Destination, enter the other account's subnet CIDR.



b. Click Save routes and a Success dialog displays.



Add the second AWS account credentials in Cloud Manager

1. Add the second AWS account, for example, Saran-XCP-Dev.



2. In the Discover Cloud Volumes ONTAP page, select the newly added credentials.



3. Select the Cloud Volumes ONTAP system you want to discover from second account. You can also deploy a new Cloud Volumes ONTAP system in the second account.



The Cloud Volumes ONTAP system from the second account is now added to Cloud Manager which is running in a different account.



Enable backup in the other AWS account

1. In Cloud Manager, enable backup for the Cloud Volumes ONTAP system running in the first account, but select the second account as the location for creating the backup files.



2. Then select a backup policy and the volumes you want to back up, and Cloud Backup attempts to create a new bucket in the selected account.

However, adding the bucket to the Cloud Volumes ONTAP system will fail because Cloud Backup uses the instance profile to add the bucket and the Cloud Manager instance profile doesn't have access to the resources in the second account.

3. Get the working environment ID for the Cloud Volumes ONTAP system.



Cloud Backup creates every bucket with the prefix Netapp-backup- and will include the working environment ID; for example: 87ULeA10

4. In the EC2 portal, go to S3 and search for the bucket with name ending with 87uLeA10 and you'll see the bucket name displayed as Netapp-backup-vsa87uLeA10.



5. Click on the bucket, then click the Permissions tab, and then click **Edit** in the Bucket policy section.



6. Add a bucket policy for the newly created bucket to provide access to the Cloud Manager's AWS account, and then Save the changes.

```
"Version": "2012-10-17",
  "Statement": [
      "Sid": "PublicRead",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::464262061435:root"
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      1,
      "Resource": [
        "arn:aws:s3:::netapp-backup-vsa87uleai0",
        "arn:aws:s3:::netapp-backup-vsa87uleai0/*"
  ]
}
```

Note that "AWS": "arn:aws:iam::464262061435:root" gives complete access this bucket for all resources in account 464262061435. If you want to reduce it to specific role, level, you can update the policy with specific role(s). If you are adding individual roles, ensure that occm role also added, otherwise backups will not get updated in the Cloud Backup UI.

For example: "AWS": "arn:aws:iam::464262061435:role/cvo-instance-profile-version10-d8e-lamInstanceRole-IKJPJ1HC2E7R"

7. Retry enabling Cloud Backup on the Cloud Volumes ONTAP system and this time it should be successful.

Configure backup for multi-account access in Azure

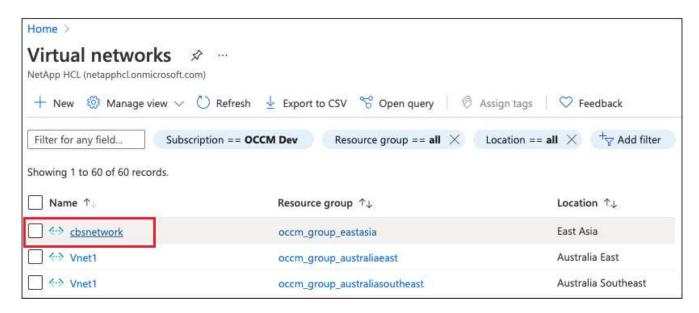
Cloud Backup enables you to create backup files in an Azure account that is different than where your source volumes reside. And both of those accounts can be different than the account where the Cloud Manager Connector resides.

Just follow the steps below to set up your configuration in this manner.

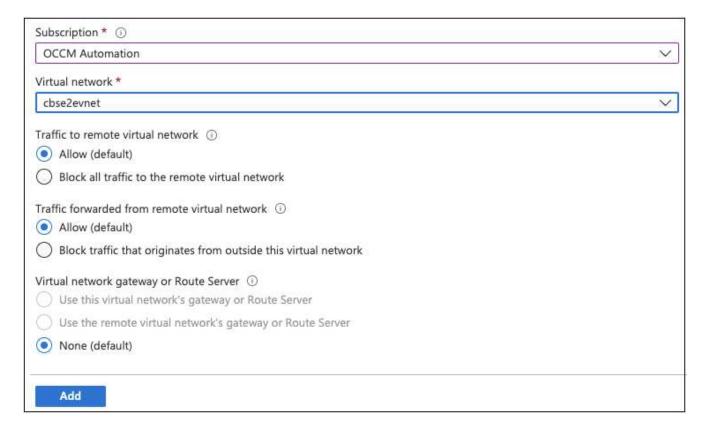
Set up VNet peering between accounts

Note that if you want Cloud Manager to manage your Cloud Volumes ONTAP system in a different account/region, then you need to setup VNet peering. VNet peering is not required for storage account connectivity.

- 1. Log in to the Azure portal and from home, select Virtual Networks.
- 2. Select the subscription you are using as subscription 1 and click on the VNet where you want to set up peering.

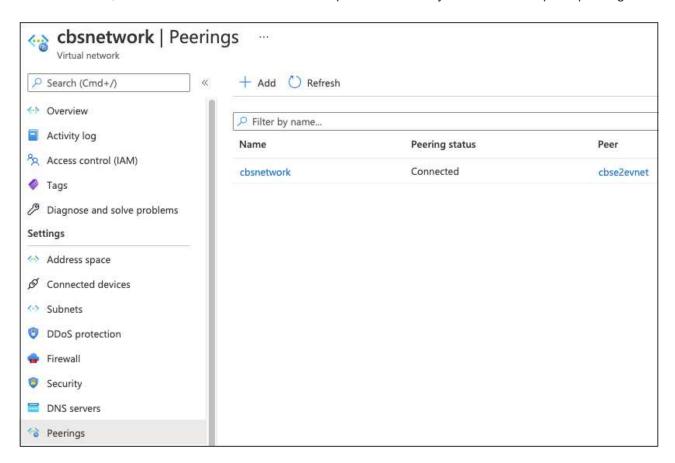


3. Select cbsnetwork and from the left panel, click on Peerings, and then click Add.



- 4. Enter the following information on the Peering page and then click Add.
 - Peering link name for this network: you can give any name to identify the peering connection.
 - Remote virtual network peering link name: enter a name to identify the remote VNet.
 - Keep all the selections as default values.

- Under subscription, select the subscription 2.
- · Virtual network, select the virtual network in subscription 2 to which you want to set up the peering.



5. Perform the same steps in subscription 2 VNet and specify the subscription and remote VNet details of subscription 1.



The peering settings are added.



Create a private endpoint for the storage account

Now you need to create a private endpoint for the storage account. In this example, the storage account is created in subscription 1 and the Cloud Volumes ONTAP system is running in subscription 2.



You need network contributor permission to perform the following action.

```
{
  "id": "/subscriptions/d333af45-0d07-4154-
943dc25fbbce1b18/providers/Microsoft.Authorization/roleDefinitions/4d97b98
b-1d4f-4787-a291-c67834d212e7",
  "properties": {
    "roleName": "Network Contributor",
    "description": "Lets you manage networks, but not access to them.",
    "assignableScopes": [
      11 / 11
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/*/read",
          "Microsoft.Insights/alertRules/*",
          "Microsoft.Network/*",
          "Microsoft.ResourceHealth/availabilityStatuses/read",
          "Microsoft.Resources/deployments/*",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Support/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
    1
}
```

1. Go to the storage account > Networking > Private endpoint connections and click + Private endpoint.



2. In the Private Endpoint *Basics* page:

- Select subscription 2 (where the Cloud Manager Connector and Cloud Volumes ONTAP system are deployed) and the resource group.
- · Enter an endpoint name.
- Select the region.



3. In the Resource page, select Target sub-resource as blob.



- 4. In the Configuration page:
 - Select the virtual network and subnet.
 - Click the Yes radio button to "Integrate with private DNS zone".



5. In the Private DNS zone list, ensure that the Private Zone is selected from the correct Region, and click **Review + Create**.



Now the storage account (in subscription 1) has access to the Cloud Volumes ONTAP system which is running in subscription 2.

6. Retry enabling Cloud Backup on the Cloud Volumes ONTAP system and this time it should be successful.

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.

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.