



Configure backup for multi-account access in Azure

Cloud Manager

Tom Onacki
June 24, 2021

This PDF was generated from https://docs.netapp.com/us-en/occm/reference_backup_multi_account_azure.html on September 14, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- Configure backup for multi-account access in Azure 1
 - Set up VNet peering between accounts 1
 - Create a private endpoint for the storage account 4

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.

Home > Virtual networks ...

NetApp HCL (netapphcl.onmicrosoft.com)

+ New Manage view Refresh Export to CSV Open query | Assign tags | Feedback

Filter for any field... Subscription == OCCM Dev Resource group == all X Location == all X Add filter

Showing 1 to 60 of 60 records.

| <input type="checkbox"/> Name | Resource group | Location |
|--|-------------------------------|---------------------|
| <input type="checkbox"/> cbsnetwork | occm_group_eastasia | East Asia |
| <input type="checkbox"/> Vnet1 | occm_group_australiaeast | Australia East |
| <input type="checkbox"/> Vnet1 | occm_group_australiasoutheast | Australia Southeast |

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

Subscription * ⓘ
OCCM Automation ▼

Virtual network *
cbse2evnet ▼

Traffic to remote virtual network ⓘ
☒ Allow (default)
☐ Block all traffic to the remote virtual network


Traffic forwarded from remote virtual network ⓘ
☒ Allow (default)
☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ
☐ Use this virtual network's gateway or Route Server
☐ Use the remote virtual network's gateway or Route Server
☒ None (default)

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.


cbsnetwork | Peerings
...

Virtual network

<<
+ Add
↻ Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
 - Address space
 - Connected devices
 - Subnets
 - DDoS protection
 - Firewall
 - Security
 - DNS servers
 - Peerings**

| Name | Peering status | Peer |
|------------|----------------|------------|
| cbsnetwork | Connected | cbse2evnet |

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

Subscription * ⓘ

OCCM Dev

Virtual network *

cbsnetwork

Traffic to remote virtual network ⓘ

☒ Allow (default)
 ☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ


☒ Allow (default)
 ☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

☐ Use this virtual network's gateway or Route Server
 ☐ Use the remote virtual network's gateway or Route Server
 ☒ None (default)

Add

The peering settings are added.


cbse2evnet | Peerings
...

Virtual network

<<
+ Add
🔄 Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
 - Address space
 - Connected devices
 - Subnets
 - DDoS protection
 - Firewall
 - Security
 - DNS servers
 - Peerings**

| Name | Peering status | Peer |
|--------------------------------|----------------|----------------------------|
| cbsnetworkpeer | Connected | cbsnetwork |

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.



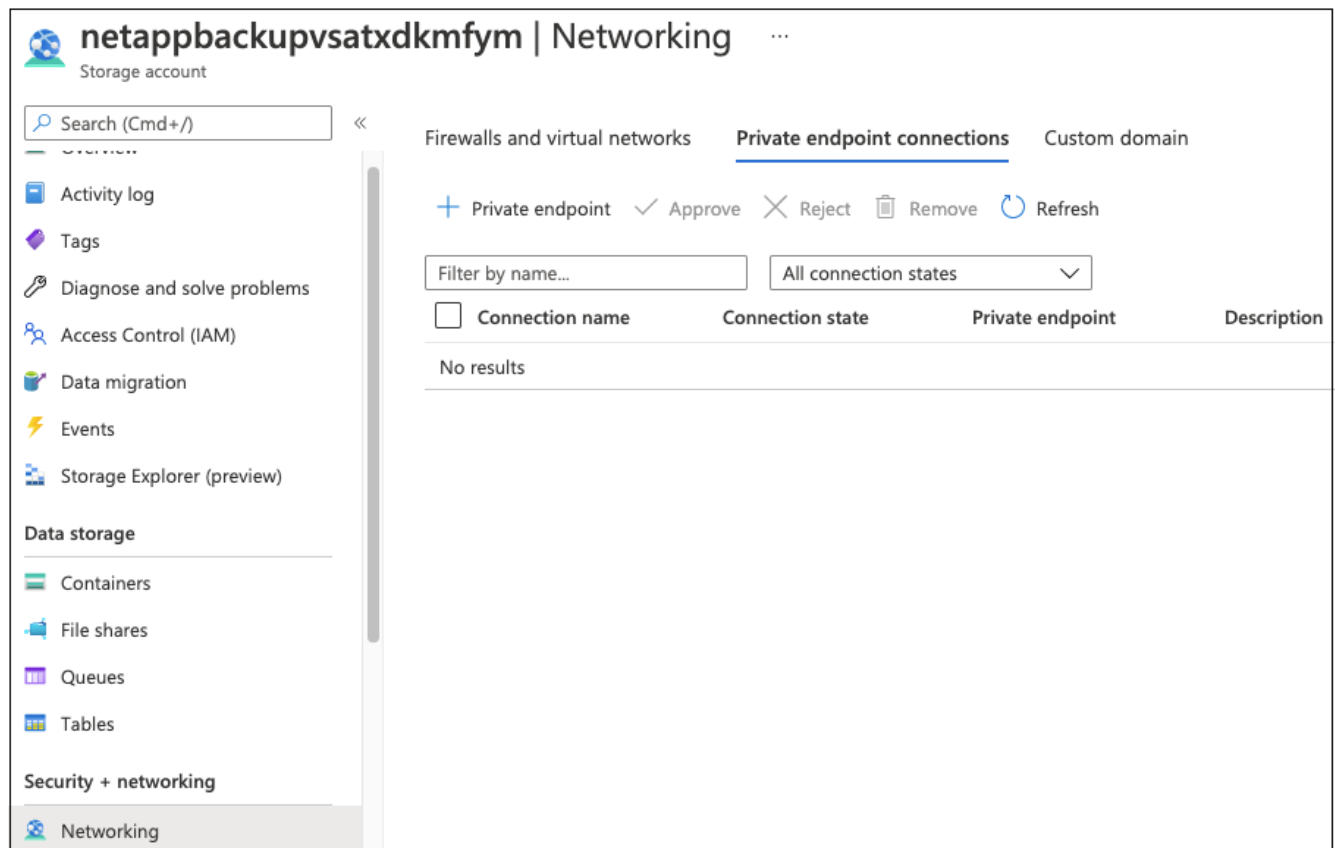
You need network contributor permission to perform the following action.

```

{
  "id": "/subscriptions/d333af45-0d07-4154-943dc25fbbce1b18/providers/Microsoft.Authorization/roleDefinitions/4d97b98b-1d4f-4787-a291-c67834d212e7",
  "properties": {
    "roleName": "Network Contributor",
    "description": "Lets you manage networks, but not access to them.",
    "assignableScopes": [
      "/"
    ],
    "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. 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.

Create a private endpoint

1 Basics 2 Resource 3 Configuration 4 Tags 5 Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

Project details

Subscription * ⓘ OCCM Dev

Resource group * ⓘ cbsoccmdevcvo-rg [Create new](#)

Instance details

Name * cbse2e ✓

Region * (Asia Pacific) East Asia

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

Create a private endpoint ...

✓ Basics **2 Resource** 3 Configuration 4 Tags 5 Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Subscription OCCM Dev (d333af45-0d07-4154-943d-c25fbbce1b18)

Resource type Microsoft.Storage/storageAccounts

Resource test150521

Target sub-resource * ⓘ

blob

4. In the Configuration page:

- Select the virtual network and subnet.
- Click the **Yes** radio button to "Integrate with private DNS zone".

Create a private endpoint ...

✓ Basics ✓ Resource **3 Configuration** 4 Tags 5 Review + create

Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network * ⓘ

cbsnetwork

Subnet * ⓘ

default (10.2.0.0/24)

ⓘ If you have a network security group (NSG) enabled for the subnet above, it will be disabled for private endpoints on this subnet only. Other resources on the subnet will still have NSG enforcement.

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone

☒ Yes ☐ No

Configuration name

Subscription

Private DNS zone

privatelink-blob-core-...

OCCM Dev

privatelink.blob.core.windows.net

[Review + create](#)

[< Previous](#)

[Next : Tags >](#)

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

| Configuration name | Subscription | Private DNS zone |
|---------------------------|--------------|--|
| privatelink-blob-core-... | OCCM Dev | privatelink.blob.core.windows.net |
| | | <input type="text" value="Filter private DNS zones"/> |
| | | <div> <div>occ_m_group_centralus</div> <div>privatelink.blob.core.windows.net</div> </div> |
| | | <div> <div>occ_m_group_eastus</div> <div>privatelink.blob.core.windows.net</div> </div> |
| | | <div> <div>occ_m_group_eastus2</div> <div>privatelink.blob.core.windows.net</div> </div> |

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 © 2021 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.