



Azure でマルチアカウントアクセスのバックアップを 設定する Cloud Manager

Tom Onacki
July 06, 2021

目次

Azure でマルチアカウントアクセスのバックアップを設定する.....	1
アカウント間の VNet ピアリングを設定します	1
ストレージアカウントのプライベートエンドポイントを作成します.....	4

Azure でマルチアカウントアクセスのバックアップを設定する

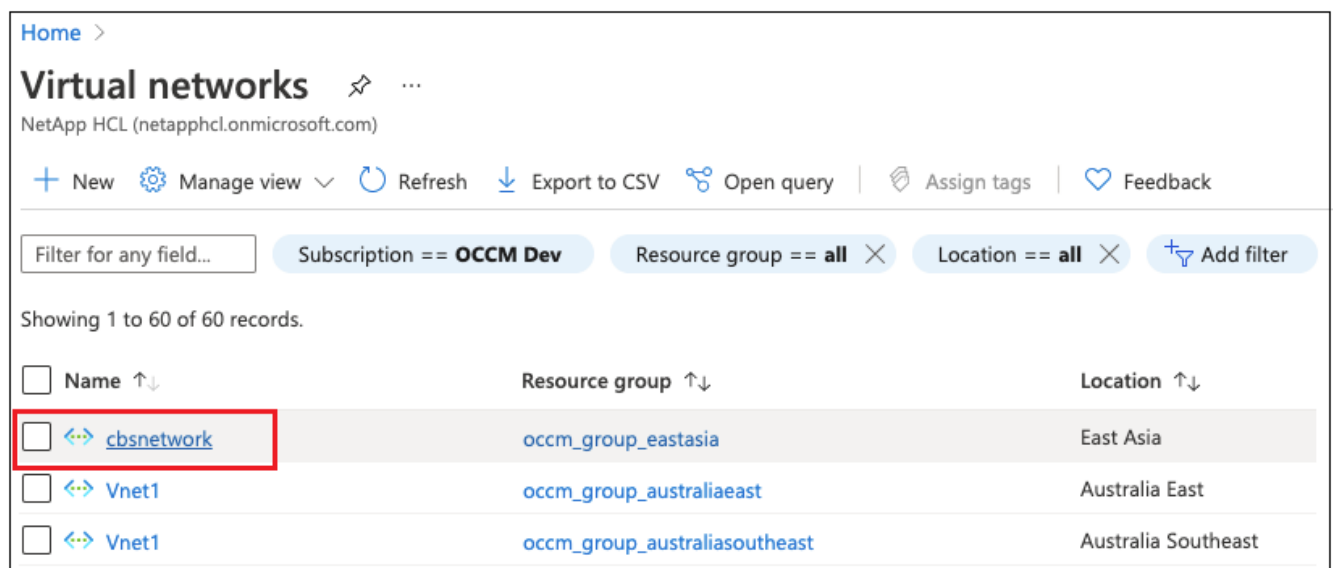
Cloud Backup を使用すると、ソースボリュームとは別の Azure アカウントにバックアップファイルを作成できます。これらのアカウントは、Cloud Manager Connector がインストールされているアカウントとは異なる場合があります。

この方法で設定を行うには、次の手順を実行します。

アカウント間の VNet ピアリングを設定します

Cloud Manager で別のアカウントやリージョンの Cloud Volumes ONTAP システムを管理する場合は、VNet ピアリングを設定する必要があります。ストレージアカウントの接続に VNet ピアリングは必要ありません。

1. Azure ポータルにログインし、ホームから仮想ネットワークを選択します。
2. サブスクリプション 1 として使用するサブスクリプションを選択し、ピアリングを設定する VNet 上でクリックします。



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 × Location == all × + Add filter

Showing 1 to 60 of 60 records.

<input type="checkbox"/> Name ↑↓	Resource group ↑↓	Location ↑↓
<input checked="" 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. **cbsnetwork** を選択し、左パネルから **peerings** をクリックし、* Add * をクリックします。

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. ピアリングページで次の情報を入力し、* 追加 * をクリックします。

- このネットワークのピアリングリンク名：ピアリング接続を識別する任意の名前を指定できます。
- リモート仮想ネットワークピアリングリンク名：リモート VNet を識別するための名前を入力します。
- すべての選択をデフォルト値のままにします。
- [サブスクリプション] で、サブスクリプション 2 を選択します。
- 仮想ネットワーク：ピアリングを設定するサブスクリプション 2 の仮想ネットワークを選択します。


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

5. サブスクリプション 2 VNet 内で同じ手順を実行し、サブスクリプション 1 のサブスクリプションおよびリモート VNet の詳細を指定します。

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

ピアリング設定が追加されます。

cbse2evnet | Peerings

Virtual network

Search (Cmd+ /)

<<

+ 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

Filter by name...

Name	Peering status	Peer
cbsnetworkpeer	Connected	cbsnetwork

ストレージアカウントのプライベートエンドポイントを作成します

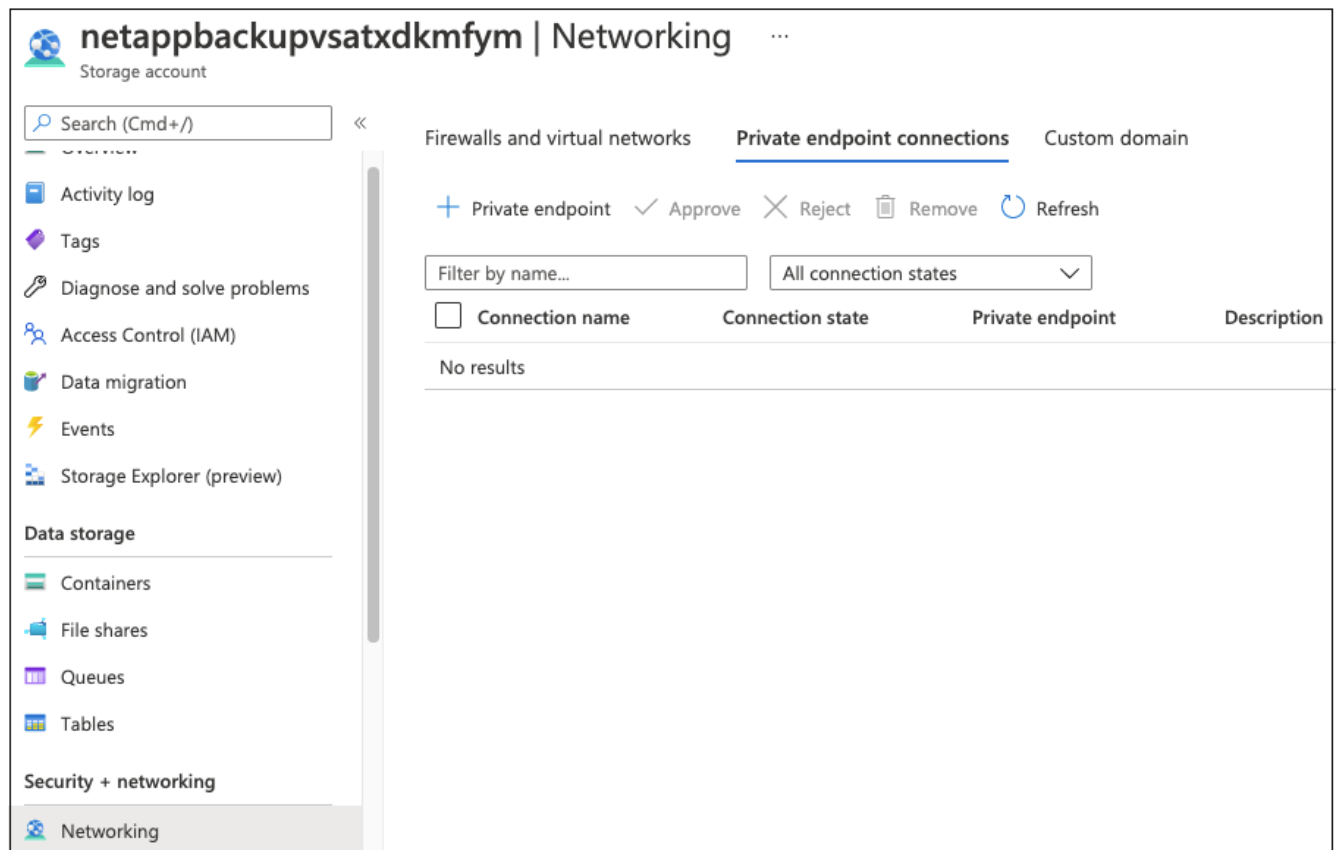
次に、ストレージアカウント用のプライベートエンドポイントを作成する必要があります。この例では、サブスクリプション 1 でストレージアカウントが作成され、Cloud Volumes ONTAP システムはサブスクリプション 2 で実行されています。



次の操作を実行するには、ネットワーク作成者の権限が必要です。

```
{
  "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. ストレージアカウント > ネットワーク > プライベートエンドポイント接続に移動し、 * + プライベートエンドポイント * をクリックします。



2. Private Endpoint_Basics_page で、次の手順を実行します。

- サブスクリプション 2 （ Cloud Manager Connector と Cloud Volumes ONTAP システムを導入する場所）とリソースグループを選択します。
- エンドポイント名を入力します。
- リージョンを選択します。

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. _Resource_page で ' ターゲットサブリソースとして *blob * を選択します

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. 設定ページで、次の操作を行います。

- 仮想ネットワークとサブネットを選択します。
- [はい *] ラジオボタンをクリックして、[プライベート DNS ゾーンと統合] を選択します。

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. [プライベート DNS ゾーン] リストで、正しいリージョンからプライベートゾーンが選択されていることを確認し、[* レビュー + 作成 *] をクリックします。

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>occm_group_centralus</div> <div>privatelink.blob.core.windows.net</div> </div>
		<div> <div>occm_group_eastus</div> <div>privatelink.blob.core.windows.net</div> </div>
		<div> <div>occm_group_eastus2</div> <div>privatelink.blob.core.windows.net</div> </div>

これで、ストレージアカウント（サブスクリプション 1）は、サブスクリプション 2 で実行されている Cloud Volumes ONTAP システムにアクセスできます。

6. Cloud Volumes ONTAP システムでクラウドバックアップの有効化を再度実行して、成功することを確認します。

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.