



跨帳戶和跨區域組態 Cloud Backup

NetApp
May 13, 2022

目錄

跨帳戶和跨區域組態	1
在AWS中設定多帳戶存取的備份	1
在Azure中設定多帳戶存取的備份	9

跨帳戶和跨區域組態

這些主題說明如何在使用不同雲端供應商時、設定跨帳戶組態的Cloud Backup。

- ["在AWS中設定Cloud Backup以進行多帳戶存取"](#)
- ["設定Cloud Backup以在Azure中存取多個帳戶"](#)

在AWS中設定多帳戶存取的備份

Cloud Backup可讓您在AWS帳戶中建立備份檔案、而非來源Cloud Volumes ONTAP 支援區所在的位置。這兩個帳戶可能與Cloud Manager Connector所在的帳戶不同。

只有在您需要時、才需要執行這些步驟 ["將Cloud Volumes ONTAP 不支援的資料備份至Amazon S3"](#)。

請依照下列步驟以這種方式設定組態。

設定帳戶之間的VPC對等關係

1. 登入第二個帳戶並建立對等連線：
 - a. 選取本機VPC：選取第二個帳戶的VPC。
 - b. 選取另一個VPC：輸入第一個帳戶的帳戶ID。
 - c. 選取Cloud Manager Connector執行的區域。在此測試設定中、兩個帳戶都在同一個地區執行。
 - d. VPC ID：登入第一個帳戶、然後輸入接收者VPC ID。這是Cloud Manager Connector的VPC ID。

aws Services ▾

Peering Connections > Create Peering Connection

Create Peering Connection

Peering connection name tag ⓘ

Select a local VPC to peer with

VPC (Requester)* ↕ ↻

CIDRs	CIDR	Status	Status Reason
	10.0.0.0/16	● associated	

Select another VPC to peer with

Account ☐ My account ☒ Another account

Account ID*

Region ☒ This region (us-east-1) ☐ Another Region

VPC ID (Accepter)*

隨即顯示「成功」對話方塊。

Success

A VPC peering connection (pcx-049758069d9b7c140) has been requested.
The owner of **vpc-116d9174** must accept the peering connection.

Requester VPC owner	733004784675 (This account)	Accepter VPC owner	464262061435
Requester VPC ID	vpc-82f55afa	Accepter VPC ID	vpc-116d9174
Requester VPC Region	us-east-1	Accepter VPC Region	us-east-1
Requester VPC CIDRs	10.0.0.0/16	Accepter VPC CIDRs	-

對等連線的狀態顯示為「等待接受」。

	Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
<input checked="" type="checkbox"/>	cbs-multi-ac...	pcx-049758069d9...	● Pending Acceptance	vpc-82f55afa VP...	vpc-116d9174	10.0.0.0/16	-	733004784675	464262061435
<input type="checkbox"/>	cbs-multi-peer	pcx-05f2d310cb7f...	● Deleted	vpc-82f55afa VP...	vpc-116d9174	-	-	733004784675	464262061435
<input type="checkbox"/>	New_Peering	pcx-6d55ca04	● Active	vpc-b16c90d4 V...	vpc-fc2aa39a De...	172.31.0.0/16	192.168.0.0/16	733004784675	733004784675

2. 登入第一個帳戶並接受對等要求：

Create Peering Connection		Actions									
<div>Filter by tags and attributes</div>											
<div><div></div></div>	Name	<div>Delete VPC Peering Connection</div> <div>Edit ClassicLink Settings</div> <div>Edit DNS Settings</div> <div>Add/Edit Tags</div>	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner		
<div><div></div></div>			Active	vpc-0647747d M...	vpc-116d9174	10.2.0.0/24	172.31.0.0/16	464262061435	464262061435		
<div><div></div></div>	estycvoconnect		Active	vpc-116d9174	vpc-445d4f21	172.31.0.0/16	10.129.0.0/20	464262061435	759995470648		
<div><div></div></div>			Pending Acceptance	vpc-82f55afa	vpc-116d9174	10.0.0.0/16	-	733004784675	464262061435		
<div><div></div></div>	hlll-vpc-peer-chen		Active	vpc-0d0e5c7fc4360254d	vpc-824dc0e4 nf...	10.0.0.0/24	10.20.30.0/24	464262061435	464262061435		

Accept VPC Peering Connection Request

×

Are you sure you want to accept this VPC peering connection request (pcx-049758069d9b7c140)?

Requester Account ID

733004784675

Requester VPC ID

vpc-82f55afa

Requester VPC Region

us-east-1

Requester VPC CIDR

10.0.0.0/16

Accepter Account ID

464262061435 (This account)

Accepter VPC ID

vpc-116d9174

Accepter VPC Region

us-east-1

Accepter VPC CIDR

-

Cancel

Yes, Accept

a. 按一下「是」。

Accept VPC Peering Connection Request

×

Your VPC Peering Connection has been established.

To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables. [Learn more](#)

[Modify my route tables now](#)

Close

連線現在顯示為「作用中」。我們也新增了名稱標記、以識別稱為「CBS多帳戶」的對等連線。

	Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
<input type="checkbox"/>		pcx-004715531514cb0d8	Active	vpc-0647747d M...	vpc-116d9174	10.2.0.0/24	172.31.0.0/16	464262061435	464262061435
<input type="checkbox"/>	estycvoconnect	pcx-0305041f9cc2dfbdb	Active	vpc-116d9174	vpc-445d4f21	172.31.0.0/16	10.129.0.0/20	464262061435	759995470648
<input checked="" type="checkbox"/>	cbs-multi-account	pcx-049758069d9b7c140	Active	vpc-82f55afa	vpc-116d9174	10.0.0.0/16	172.31.0.0/16	733004784675	464262061435
<input type="checkbox"/>	hlli-vpc-peer-chen	pcx-0d0e5c7fc4360254d	Active	vpc-0d12df59528f...	vpc-824dc0e4 nf...	10.0.0.0/24	10.20.30.0/24	464262061435	464262061435

a. 重新整理第二個帳戶的對等連線、並注意狀態變更為「作用中」。

	Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
<input checked="" type="checkbox"/>	cbs-multi-account	pcx-049758069d9b7c140	Active	vpc-82f55afa VP...	vpc-116d9174	10.0.0.0/16	172.31.0.0/16	733004784675	464262061435
<input type="checkbox"/>	New_Peering	pcx-6d55ca04	Active	vpc-b16c90d4 V...	vpc-fc2aa39a De...	172.31.0.0/16	192.168.0.0/16	733004784675	733004784675

將路由新增至兩個帳戶中的路由表

1. 前往VPC >子網路>路由表。

VPC > Subnets > subnet-4d315328

subnet-4d315328 / The Subnet created

Details

Subnet ID subnet-4d315328	State Available	VPC vpc-116d9174	IPv4 CIDR 172.31.64.0/20
Available IPv4 addresses 3587	IPv6 CIDR -	Availability Zone us-east-1a	Availability Zone ID use1-az1
Network border group us-east-1	Route table rtb-4da55528	Network ACL acl-c37384a6	Default subnet Yes
Auto-assign public IPv4 address Yes	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool -
Outpost ID -	Owner 464262061435	Subnet ARN arn:aws:ec2:us-east-1:464262061435:subnet/subnet-4d315328	

[Flow logs](#)
[Route table](#)
[Network ACL](#)
[Sharing](#)
[Tags](#)

2. 按一下「路由」索引標籤。

Route Table ID : rtb-4da55528 Add filter

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
rtb-4da55528	subnet-4d315328	-		Yes	vpc-116d9174	464262061435

Route Table: rtb-4da55528

[Summary](#)
[Routes](#)
[Subnet Associations](#)
[Edge Associations](#)
[Route Propagation](#)
[Tags](#)

[Edit routes](#)

View All routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
pl-63a5400a	vpce-098587ed33c36408c	active	No

3. 按一下*編輯路由*。

Edit routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
10.20.30.0/24	pcx-0791b47f6f9a27d65	active	No
10.129.0.0/20	pcx-0305041f9cc2dfbdb	active	No

[Add route](#)

* Required

[Cancel](#)
[Save routes](#)

4. 按一下「新增路由」、然後從「目標」下拉式清單中選取「對等連線」、再選取您建立的對等連線。

a. 在目的地中、輸入其他帳戶的子網路CIDR。

Edit routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
10.20.30.0/24	pcx-0791b47f6f9a27d65	active	No
10.129.0.0/20	pcx-0305041f9cc2dfbdb	active	No
10.0.0.0/24	pcx-		No

Add route

* Required

pcx-05f2d310cb7f49843

pcx-004715531514cb0d8

pcx-049758069d9b7c140 cbs-multi-account

pcx-094f9fdb10a2045ea hill-peer-vadim-vpc

pcx-0791b47f6f9a27d65

pcx-0305041f9cc2dfbdb estycvoconnect

Cancel Save routes

b. 按一下「儲存路由」、就會顯示「成功」對話方塊。

Route Tables > Edit routes

Edit routes

✓ Routes successfully edited

Close

在Cloud Manager中新增第二個AWS帳戶認證資料

1. 新增第二個AWS帳戶、例如_Saran - XCP開發_。

Credentials + Add Credentials

3 Credentials

aws Instance Profile	Credential Type: AWS Keys	aws Saran-XCP-Dev	Credential Type: AWS Keys
464262061435 AWS Account ID	CBS-5R-OCCMOCCM1620912870830... IAM Role	733004784675 AWS Account ID	AKIA2VKT5MQRZRAWW3HI AWS Access Key
aws-sub-a2 Subscription	2 Working Environments	aws-sub-a2 Subscription	0 Working Environments

2. 在「激發Cloud Volumes ONTAP 需求」頁面中、選取新增的認證資料。

Choose an AWS region and then select the working environment that you want to discover.

AWS Region
US East | N. Virginia

aws AWS Credentials

Credential Name

Saran-XCP-Dev | Account ID: 733004784675

Instance Profile | Account ID: 464262061435

To add new AWS credentials, go to the [Credentials settings](#).

Apply Cancel

3. 選取Cloud Volumes ONTAP 您要從第二個帳戶探索的這個系統。您也可以在Cloud Volumes ONTAP 第二個帳戶中部署新的更新系統。

Add an Existing Cloud Volumes ONTAP Region

↑ Previous Step This working environment will be created in Cloud Provider Account: **Saran-XCP-Dev** | Account ID: 733004784675 | [Switch Account](#)

Choose an AWS region and then select the working environment that you want to discover.

AWS Region
US East | N. Virginia

Cloud Volumes ONTAP instances found

Name	VPC Name	Availability Zone	Subnet Id	Cloud Formation Name	Cluster Address	Type
cbscv001	VPC-NAT	us-east-1f	subnet-68e8d464	cbscv001	10.0.0.80	Cloud Volumes ONTAP
testbyolliraz	VPC for VSA	us-east-1a	subnet-c1d99699	testbyolliraz	172.31.5.142	Cloud Volumes ONTAP
ldanAwsHa991001	VPC for VSA	us-east-1a	subnet-c1d99699	ldanAwsHa991001	172.31.5.234,172.31.5.110	HA Cloud Volumes ONTAP

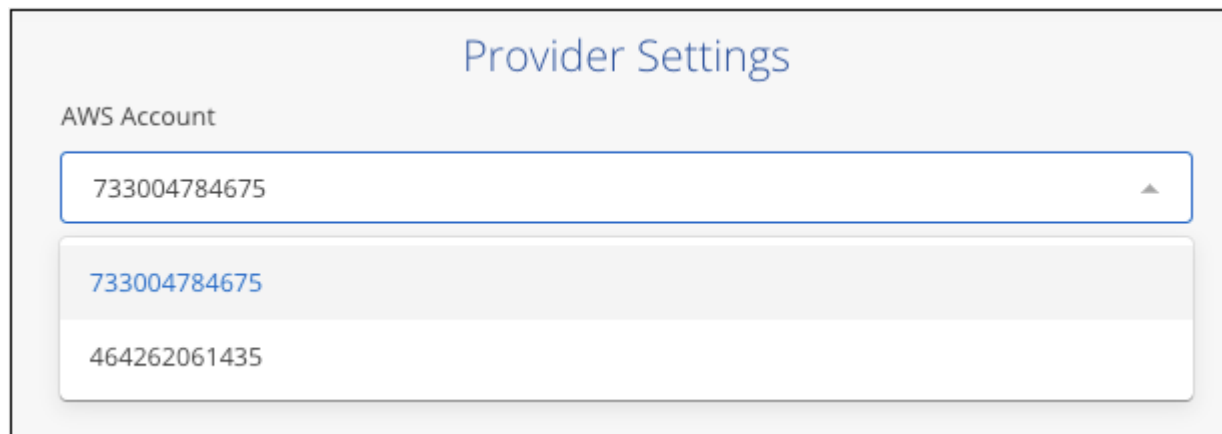
Continue

第二個帳戶的這個系統現在會新增至雲端管理程式、而Cloud Manager則是以不同的帳戶執行。Cloud Volumes ONTAP



在其他AWS帳戶中啟用備份

1. 在Cloud Manager中、為Cloud Volumes ONTAP 第一個帳戶中執行的作業系統啟用備份、但選取第二個帳戶作為建立備份檔案的位置。



2. 然後選取備份原則和您要備份的磁碟區、Cloud Backup會嘗試在選取的帳戶中建立新的儲存區。

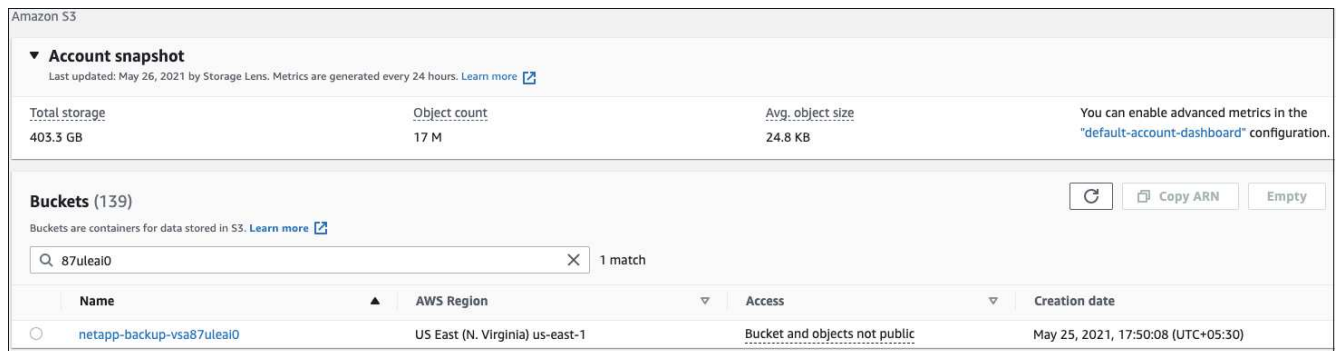
不過、將儲存庫新增Cloud Volumes ONTAP 至支援庫系統將會失敗、因為Cloud Backup會使用執行個體設定檔來新增儲存庫、而Cloud Manager執行個體設定檔則無法存取第二個帳戶中的資源。

3. 取得Cloud Volumes ONTAP 適用於此系統的工作環境ID。

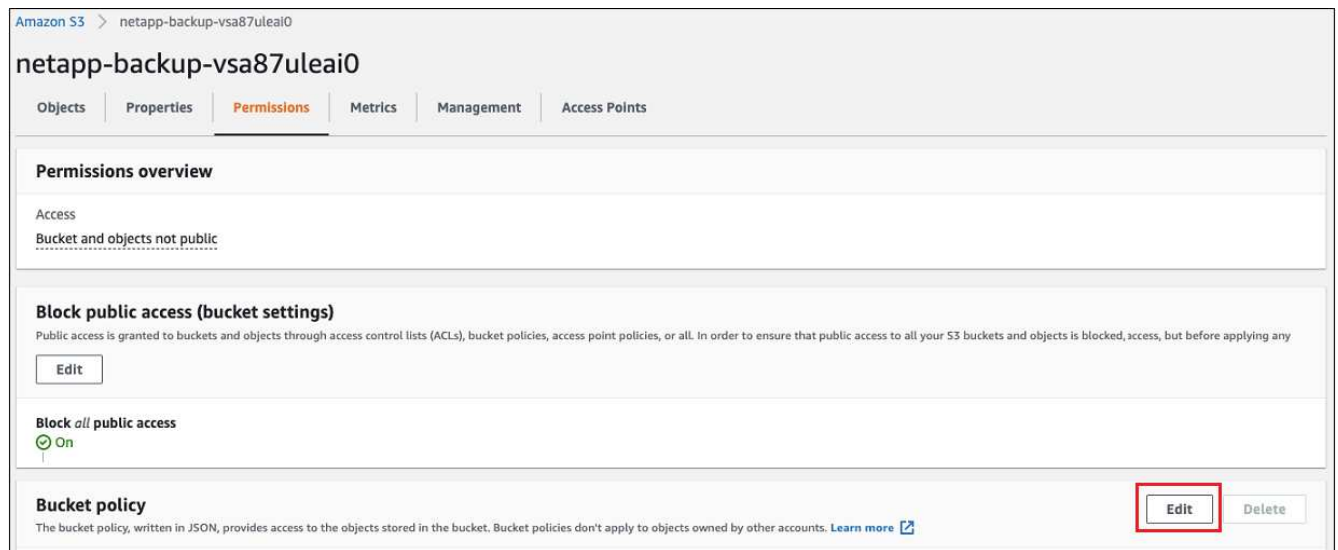


Cloud Backup會以「NetApp-Backup」開頭建立每個儲存區、並包含工作環境ID、例如：「87ULeA10」

- 在EC2入口網站中、前往S3搜尋以「87uLeA10」結尾的儲存區、您會看到儲存區名稱顯示為「NetApp-backup-vsa87uLeA10」。



- 按一下儲存庫、然後按一下「權限」索引標籤、再按一下「儲存庫原則」區段中的「編輯」。



- 為新建立的儲存庫新增儲存庫原則、以提供Cloud Manager AWS帳戶的存取權、然後儲存變更。

```
{
  "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"
      ],
      "Resource": [
        "arn:aws:s3:::netapp-backup-vsa87uleai0",
        "arn:aws:s3:::netapp-backup-vsa87uleai0/*"
      ]
    }
  ]
}
```

請注意、「AWS」：「arn:aws:iam:464262061435:root」可讓帳戶464262061435中的所有資源都能完整存取此儲存區。如果您想要將其縮減為特定角色、層級、可以使用特定角色來更新原則。如果您要新增個別角色、請務必同時新增occm角色、否則Cloud Backup UI不會更新備份。

例如：「AWS」：「arn:aws:iam::464262061435:role / CVO執行個體設定檔版本10-d8e-lamInstanceROE-IKJPJ1HC2E7R」

7. 請重試啟用Cloud Volumes ONTAP 支援整個系統的Cloud Backup、這次應該會成功。

在Azure中設定多帳戶存取的備份

Cloud Backup可讓您在Azure帳戶中建立備份檔案、而該帳戶與來源Cloud Volumes ONTAP 的支援區不同。這兩個帳戶可能與Cloud Manager Connector所在的帳戶不同。

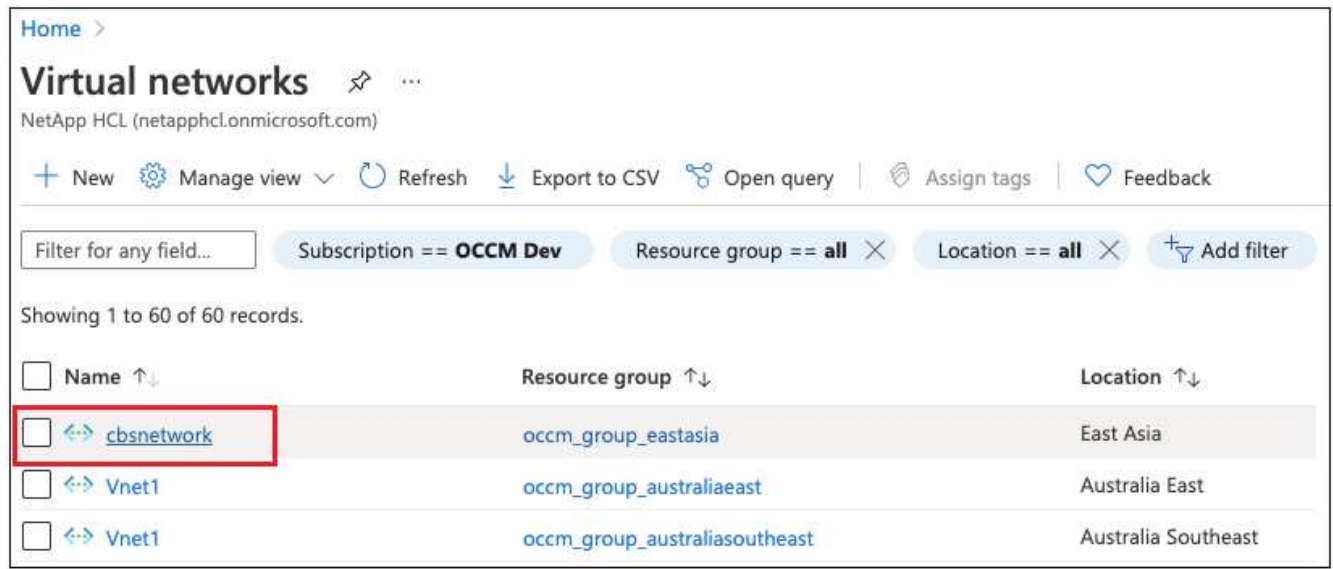
只有在您需要時、才需要執行這些步驟 ["將Cloud Volumes ONTAP 不支援的資料備份到Azure Blob儲存設備"](#)。

只要遵循下列步驟、就能以這種方式設定組態。

在帳戶之間設定vnet對等關係

請注意、如果您想要Cloud Manager在Cloud Volumes ONTAP 不同的帳戶/地區管理您的不一致系統、則必須設定vnet對等關係。儲存帳戶連線不需要vnet對等。

1. 登入Azure入口網站、然後從家中選取「Virtual Networks（虛擬網路）」。
2. 選取您要作為訂閱1使用的訂閱、然後按一下要設定對等的vnet。



3. 選取「* cbsnetwork*」、然後從左側面板按一下「服務」、再按一下「新增」。

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. 在對等頁面上輸入下列資訊、然後按一下「新增」。
 - 此網路的對等連結名稱：您可以指定任何名稱來識別對等連線。
 - 遠端虛擬網路對等連結名稱：輸入名稱以識別遠端Vnet。
 - 將所有選取項目保留為預設值。

- 在「訂購」下、選取「訂購2」。
- 虛擬網路、請在訂購2中選取您要設定對等的虛擬網路。

cbsnetwork | Peerings

Virtual network

Search (Cmd+/) + Add Refresh

Filter by name...

Name	Peering status	Peer
cbsnetwork	Connected	cbse2evnet

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

5. 在訂購2 vnet中執行相同步驟、並指定訂購1的訂閱和遠端vnet詳細資料。

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

系統會新增對等設定。

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

為儲存帳戶建立私有端點

現在您需要為儲存帳戶建立私有端點。在此範例中、儲存帳戶是在訂閱1中建立、Cloud Volumes ONTAP 而該系統正在訂閱2中執行。



您需要網路參與者權限才能執行下列動作。

```

{
  "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. 前往儲存帳戶>網路>私有端點連線、然後按一下*+私有端點*。



2. 在Private Endpoint_Basics頁面：

- 選擇訂購2（部署Cloud Manager Connector和Cloud Volumes ONTAP 一套功能完善的系統）和資源群組。
- 輸入端點名稱。
- 選取區域。

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 * ① OCCM Dev

Resource group * ① cbsoccmdevco-rg [Create new](#)

Instance details

Name * cbse2e ✓

Region * (Asia Pacific) East Asia

3. 在「資源_」頁面中、選取「目標子資源」做為* 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 * ⓘ

4. 在「組態」頁面中：
- 選取虛擬網路和子網路。
 - 按一下「是」選項按鈕以「與私有DNS區域整合」。

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 * ⓘ

Subnet * ⓘ

i 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. 在「私有DNS區域」清單中、確定已從正確的「區域」選取「私有區域」、然後按一下「檢閱+建立」。

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

現在儲存帳戶（訂閱1）可以存取Cloud Volumes ONTAP 以訂閱2執行的作業系統。

6. 請重試啟用Cloud Volumes ONTAP 支援整個系統的Cloud Backup、這次應該會成功。

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.