



Azure administration

Cloud Volumes ONTAP

NetApp
July 11, 2022

Table of Contents

- Azure administration. 1
 - Change the Azure VM type for Cloud Volumes ONTAP. 1
 - Overriding CIFS locks for Cloud Volumes ONTAP HA pairs in Azure 1
 - Use an Azure Private Link or service endpoints. 2

Azure administration

Change the Azure VM type for Cloud Volumes ONTAP

You can choose from several VM types when you launch Cloud Volumes ONTAP in Microsoft Azure. You can change the VM type at any time if you determine that it is undersized or oversized for your needs.

About this task

- Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

[ONTAP 9 Documentation: Commands for configuring automatic giveback](#)

- Changing the VM type can affect Microsoft Azure service charges.
- The operation restarts Cloud Volumes ONTAP.

For single node systems, I/O is interrupted.

For HA pairs, the change is nondisruptive. HA pairs continue to serve data.



Cloud Manager gracefully changes one node at a time by initiating takeover and waiting for give back. NetApp's QA team tested both writing and reading files during this process and didn't see any issues on the client side. As connections changed, we did see retries on the I/O level, but the application layer overcame these short "re-wire" of NFS/CIFS connections.

Steps

1. From the working environment, click the menu icon, and then select **Change VM**.
2. If you are using a node-based PAYGO license, you can optionally choose a different license.
3. Select a VM type, select the check box to confirm that you understand the implications of the change, and then click **OK**.

Result

Cloud Volumes ONTAP reboots with the new configuration.

Overriding CIFS locks for Cloud Volumes ONTAP HA pairs in Azure

The Account Admin can enable a setting in Cloud Manager that prevents issues with Cloud Volumes ONTAP storage giveback during Azure maintenance events. When you enable this setting, Cloud Volumes ONTAP vetoes CIFS locks and resets active CIFS sessions.

About this task

Microsoft Azure schedules periodic maintenance events on its virtual machines. When a maintenance event occurs on a Cloud Volumes ONTAP HA pair, the HA pair initiates storage takeover. If there are active CIFS sessions during this maintenance event, the locks on CIFS files can prevent storage giveback.

If you enable this setting, Cloud Volumes ONTAP will veto the locks and reset the active CIFS sessions. As a result, the HA pair can complete storage giveback during these maintenance events.



This process might be disruptive to CIFS clients. Data that is not committed from CIFS clients could be lost.

What you'll need

You need to create a Connector before you can change Cloud Manager settings. [Learn how.](#)

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Connector Settings**.



2. Under **Azure**, click **Azure CIFS locks for Azure HA working environments**.
3. Click the checkbox to enable the feature and then click **Save**.

Use an Azure Private Link or service endpoints

Cloud Volumes ONTAP uses an Azure Private Link for connections to its associated storage accounts. If needed, you can disable Azure Private Links and use service endpoints instead.

Overview

By default, Cloud Manager enables an Azure Private Link for connections between Cloud Volumes ONTAP and its associated storage accounts. An Azure Private Link secures connections between endpoints in Azure and provides performance benefits.

If required, you can configure Cloud Volumes ONTAP to use service endpoints instead of an Azure Private Link.

With either configuration, Cloud Manager always limits network access for connections between Cloud Volumes ONTAP and storage accounts. Network access is limited to the VNet where Cloud Volumes ONTAP is deployed and the VNet where the Connector is deployed.

Disable Azure Private Links and use service endpoints instead

If required by your business, you can change a setting in Cloud Manager so that it configures Cloud Volumes ONTAP to use service endpoints instead of an Azure Private Link. Changing this setting applies to new Cloud Volumes ONTAP systems that you create.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Connector Settings**.
2. Under **Azure**, click **Use Azure Private Link**.
3. Deselect **Private Link connection between Cloud Volumes ONTAP and storage accounts**.

4. Click **Save**.

Work with Azure Private Links

In most cases, there's nothing that you need to do to set up Azure Private links with Cloud Volumes ONTAP. Cloud Manager manages Azure Private Links for you. But if you use Azure Private DNS, then you'll need to edit a configuration file. You should also be aware of a requirement for the Connector location in Azure.

How Private Link connections work

When Cloud Manager deploys Cloud Volumes ONTAP in Azure, it creates a private endpoint in the resource group. The private endpoint is associated with storage accounts for Cloud Volumes ONTAP. As a result, access to Cloud Volumes ONTAP storage travels through the Microsoft backbone network.

Client access goes through the private link when clients are within the same VNet as Cloud Volumes ONTAP, within peered VNets, or in your on-premises network when using a private VPN or ExpressRoute connection to the VNet.

Here's an example that shows client access over a private link from within the same VNet and from an on-prem network that has either a private VPN or ExpressRoute connection.



Connector location in Azure

The Connector should be deployed in the same Azure region as the Cloud Volumes ONTAP systems that it manages, or in the [Azure region pair](#) for the Cloud Volumes ONTAP systems. This requirement ensures that an Azure Private Link connection is used between Cloud Volumes ONTAP and its associated storage accounts.

Provide Cloud Manager with details about your Azure Private DNS

If you use [Azure Private DNS](#), then you need to modify a configuration file on each Connector. Otherwise, Cloud Manager can't enable the Azure Private Link connection between Cloud Volumes ONTAP and its associated storage accounts.

Note that the DNS name must match Azure DNS naming requirements [as shown in Azure documentation](#).

Steps

1. SSH to the Connector host and log in.
2. Navigate to the following directory: `/opt/application/netapp/cloudmanager/docker_occm/data`
3. Edit `app.conf` by modifying the following parameters as shown:

```
"user-private-dns-zone-settings": {  
  "use-existing": true,  
  "resource-group": "<resource group name of the DNS zone>",  
  "subscription": "<subscription ID>"  
}
```

The subscription parameter is required only if the Private DNS Zone exists in a different subscription than the Connector.

4. Save the file and log off the Connector.

A reboot isn't required.

Enable rollback on failures

If Cloud Manager fails to create an Azure Private Link as part of specific actions, it completes the action without the Azure Private Link connection. This can happen when creating a new working environment (single node or HA pair), or when the following actions occur on an HA pair: creating a new aggregate, adding disks to an existing aggregate, or creating a new storage account when going above 32 TiB.

You can change this default behavior by enabling rollback if Cloud Manager fails to create the Azure Private Link. This can help to ensure that you're fully compliant with your company's security regulations.

If you enable rollback, Cloud Manager stops the action and rolls back all resources that were created as part of the action.

Enabling rollback is supported through the API only.

Step

1. Use the `PUT /occm/config` API call with the following request body:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

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.