



OnCommand® Cloud Manager 3.2

Release Notes

February 2017 | 215-12029_A0_ur001
doccomments@netapp.com

Contents

Product overview	4
New in this release	5
Upgrade notes	6
Known limitations	8
Known issues	10
Changes to published documentation	11
Identifying IP addresses for NAS data access on HA pairs in multiple AZs	11
Where to get help and find more information	13
Copyright information	14
Trademark information	15
How to send comments about documentation and receive update notifications	16

Product overview

OnCommand Cloud Manager enables you to deploy ONTAP Cloud systems, which provide enterprise-class features for your cloud storage, and to easily replicate data across hybrid clouds built on NetApp.

When you set up Cloud Manager in standard Amazon Web Services (AWS) regions, you can choose between two management views: the Storage System View and the Volume View. The Storage System View is the default view for Microsoft Azure and the AWS GovCloud (US) region.

Storage System View

You can use Cloud Manager in this view to have full control of ONTAP Cloud systems:

- Configure and launch ONTAP Cloud instances in AWS and in Azure
- Provision NFS and CIFS storage
- Replicate data across a hybrid cloud and multi-cloud environment: between on-premises ONTAP clusters, ONTAP Cloud systems, and NetApp Private Storage for Cloud configurations
- Manage ONTAP Cloud systems as needed, which includes capacity allocation decisions, simplified upgrades, cost monitoring, and several other tasks

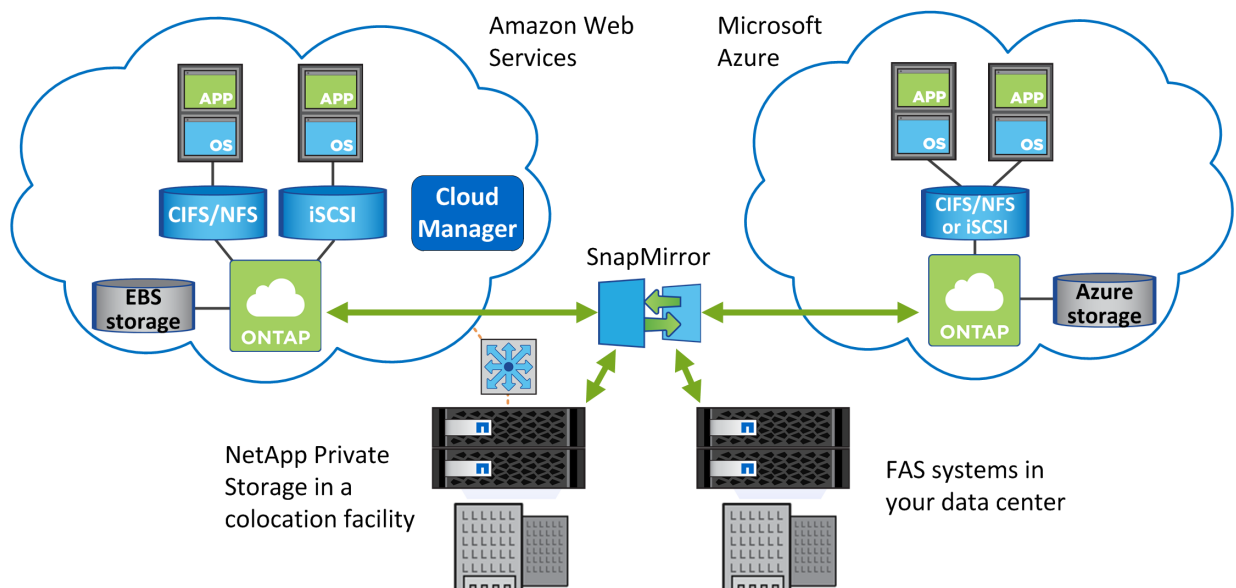
Volume View

The Volume View enables you to simply specify the NFS volumes that you need in AWS and then Cloud Manager handles the rest: it deploys ONTAP Cloud systems as needed and it makes capacity allocation decisions as volumes grow. This view gives you the benefits of enterprise-class storage in the cloud with very little storage management.

Where to deploy Cloud Manager

Cloud Manager can run in the cloud or in your network—it just needs a connection to the networks in which you want to deploy ONTAP Cloud systems.

The following image shows Cloud Manager running in AWS and managing ONTAP Cloud systems in AWS and Azure. It also shows data replication across a hybrid cloud.



New in this release

OnCommand Cloud Manager 3.2 includes several new features and enhancements.

Support for ONTAP Cloud HA in a single Availability Zone

A new high availability (HA) deployment model enables you to deploy an ONTAP Cloud HA configuration in a single AWS Availability Zone (AZ). This configuration, which uses private IP addresses instead of floating IP addresses, ensures high availability of your data if an instance that runs an ONTAP Cloud node fails. It does not protect against AZ failures. All data is natively accessible from outside of the VPC.

[Learning about Cloud Manager and ONTAP Cloud](#)

[Deploying and managing ONTAP Cloud systems](#)

Support for adding private IP addresses to an HA configuration using documented instructions

When you deploy an ONTAP Cloud HA configuration in multiple Availability Zones, the configuration uses floating IP addresses for NFS and CIFS data access. Data is not accessible from outside the VPC when using floating IPs.

Cloud Manager documentation now includes instructions for adding NAS *private* IP addresses to an ONTAP Cloud HA configuration deployed in multiple Availability Zones. Adding private IPs enables NFS and CIFS data access from outside of the VPC. However, the private IP addresses do not automatically fail over between nodes if a failure occurs. You must manually remount volumes to clients using the IP address on the other node.

Note: You should continue using the *floating* IP addresses for NAS client access from within the VPC.

Note: The ONTAP Cloud HA pair must be running the general availability release of ONTAP Cloud 9.1. If you launched an HA configuration using Cloud Manager 3.1 or earlier, you must first upgrade to Cloud Manager 3.2, ONTAP Cloud 9.1, and update the IAM permissions for the HA mediator.

[Upgrade notes](#) on page 6

[Learning about Cloud Manager and ONTAP Cloud](#)

[Deploying and managing ONTAP Cloud systems](#)

Integration with the Data Fabric Cloud Sync service

You can now sync ONTAP volumes to an AWS S3 bucket by integrating a working environment with the NetApp Data Fabric Cloud Sync service. You can then use the synced data as a secondary copy or for data processing using AWS services like EMR and Redshift.

The integration works with ONTAP Cloud working environments, as well as ONTAP clusters that are on-premises or part of a NetApp Private Storage (NPS) configuration.

[Deploying and managing ONTAP Cloud systems](#)

[NetApp Data Fabric Cloud Sync Service](#)

Amazon EBS encryption using customer-managed CMKs

When you set up an ONTAP Cloud system in AWS, you can choose AWS-managed encryption using the AWS Key Management Service (KMS). You can now choose the customer master key (CMK) that you want to use with an ONTAP Cloud system. The CMK can be an AWS-managed CMK or a customer-managed CMK.

Getting up and running

Deploying and managing ONTAP Cloud systems

New Documentation Center for Cloud Manager

The new Cloud Manager Documentation Center provides one-stop access to information that was previously in separate PDFs. You can search for information more easily, filter search results to show only the content you want, and get to your answers more quickly.

OnCommand Cloud Manager Documentation Center

Support for new AWS regions

You can now launch Cloud Manager and ONTAP Cloud instances in the Canada (Central) and EU (London) regions. You can view the full list of supported regions in the [NetApp Interoperability Matrix Tool](#).

Support for new ONTAP Cloud configurations

- Additional AWS instance types are available.
ONTAP Cloud 9.1 for Amazon Web Services Release Notes
- An additional Azure virtual machine type and a new licensing option is available.
ONTAP Cloud 9.1 for Microsoft Azure Release Notes

Support for dedicated EC2 instances

When you select an EC2 instance type for ONTAP Cloud, you can now specify whether it is a shared instance or a dedicated instance.

Cloud Manager now verifies connectivity to VPCs

Immediately after you create an AWS working environment, Cloud Manager launches a test instance in the specified VPC to verify connectivity. If successful, Cloud Manager immediately terminates the instance and then starts deploying the ONTAP Cloud system.

If Cloud Manager cannot verify connectivity, creation of the working environment fails. The test instance is either t2.nano (for default VPC tenancy) or m3.medium (for dedicated VPC tenancy).

New option to recreate failed working environments

If Cloud Manager fails to create a working environment, you can now use the **Recreate Environment** action to return to the wizard and modify the request.

Support for adding and editing more AWS tags

After you launch an ONTAP Cloud instance, you can now specify up to 20 AWS tags and you can edit the tags, as well.

New API to configure CIFS servers in workgroup mode

A new Cloud Manager API enables you to configure an existing ONTAP Cloud CIFS server as a member of a workgroup.

The API operation is: `/vsa/working-environments/{workingEnvironmentID}/cifs-workgroup`

OnCommand Cloud Manager 3.2 API Developer Guide

Related information

Find the Release Notes for your version of ONTAP Cloud

Upgrade notes

Upgrade notes describe new requirements and changes in support between the last release of the product and this one, including any deprecated features. Review this information carefully before

upgrading to the new release. See the NetApp Interoperability Matrix (IMT) for supported configurations and the product user documentation for complete system requirements.

IAM policy changes required for Cloud Manager

The Cloud Manager AWS Identity and Access Management (IAM) policy was updated for the 3.2 release.

Cloud Manager now uses the following actions to manage EC2 tags, to obtain information about keys from the AWS Key Management Service (KMS), and to obtain information from AWS S3 when integrating with the Cloud Sync service:

- “ec2:DeleteTags ”
- “ec2:DescribeTags”
- “kms:List*”
- “kms:Describe*”
- “s3:GetBucketTagging”
- “s3:GetBucketLocation”
- “s3:ListAllMyBuckets”

You should update your IAM policy before you update to this Cloud Manager release.

[NetApp OnCommand Cloud Manager: AWS and Azure Policies](#)

IAM role policy changes required for HA mediator before adding private IPs

If you deployed an ONTAP Cloud HA configuration using Cloud Manager 3.1 or earlier and you want to add private NAS IP addresses to that configuration, you must edit the IAM role policy associated with the HA mediator instance. New permissions are required to manage the private IP addresses.

You can find the role in the IAM console by searching for “mediator”. The role name is prefixed with the name of the working environment.

When you edit the role, you must add the following permissions:

- “ec2:AssignPrivateIpAddresses”
- “ec2:DescribeNetworkInterfaces”
- “ec2:UnassignPrivateIpAddresses”

[New in this release](#) on page 5

Changes to web browser requirements

- The minimum required version of Google Chrome is now 52.
- The minimum required version of Mozilla Firefox is now 49.
- Internet Explorer is no longer supported.

For the full list of supported web browser versions, see the [NetApp Interoperability Matrix Tool](#).

Updating Cloud Manager to this release

You can update Cloud Manager directly from the console by clicking the **New version available** notification or by going to the Software Update page. If you enabled automatic updates, Cloud Manager automatically updates itself to this release.

[Updating and administering Cloud Manager](#)

Known limitations

Known limitations identify platforms, devices, or functions that are not supported by this release of the product, or that do not interoperate correctly with it. Review these limitations carefully.

The Mount Command action is not supported with HA configurations that use floating and private IP addresses

When you select a volume in Cloud Manager, you can click **Mount Command** to view the IP address to use when mounting the volume. The correct IP address might not appear for an ONTAP Cloud HA configuration that is in multiple Availability Zones and uses both floating and private IP addresses.

If you need to identify the correct IP address, you must use the ONTAP Cloud CLI.

[Identifying IP addresses for NAS data access on HA pairs in multiple AZs](#) on page 11

Limitations with the AWS GovCloud (US) region

- Cloud Manager must be deployed in the AWS GovCloud (US) region if you want to launch ONTAP Cloud instances in the AWS GovCloud (US) region.
- The ONTAP Cloud pay-as-you-go AMI is not supported in the AWS GovCloud (US) region.
- When deployed in the AWS GovCloud (US) region, Cloud Manager cannot discover ONTAP clusters in a NetApp Private Storage for Microsoft Azure configuration or a NetApp Private Storage for SoftLayer configuration.

Volume View limitations

- The Volume View is not supported in the AWS GovCloud (US) region and in Microsoft Azure.
- The Volume View enables you to create NFS volumes only.
- Cloud Manager does not launch ONTAP Cloud BYOL instances in the Volume View.
- ONTAP Cloud encryption is not available in the Volume View.

Note: All instances use Amazon EBS encryption.

Cloud Manager does not verify IP addresses of key managers

When you add a key manager to Cloud Manager, it does not verify the IP address that you entered because Cloud Manager does not communicate with key managers. If the IP address is incorrect, you are notified later when you try to create an ONTAP Cloud working environment. Be sure to verify key manager IP addresses after you enter them.

Cloud Manager does not set up iSCSI volumes

When you create a volume in Cloud Manager using the Storage System View, you can choose the NFS or CIFS protocol. You must use OnCommand System Manager to create a volume for iSCSI.

EC2 instance name changes do not change ONTAP Cloud working environment names or cluster names

If you change the name of an ONTAP Cloud instance from the AWS EC2 console, the ONTAP Cloud working environment name and the ONTAP Cloud cluster name do not change.

Documentation Center limitation

Although the application for the OnCommand Cloud Manager Documentation Center is localized for Japanese and Simplified Chinese, the Cloud Manager technical content is available in English only.

Known issues

There are no known issues in this release.

Changes to published documentation

Additional information became available after the documentation provided with this release was published. The information in this section should be used in conjunction with the materials originally published for this release.

Identifying IP addresses for NAS data access on HA pairs in multiple AZs

If you deployed an ONTAP Cloud HA configuration in multiple Availability Zones and use both *floating* IP addresses and *private* IP addresses for NFS and CIFS, you must use the correct IP address for data access.

About this task

Using the correct IP address for data access to a volume is important for two reasons:

1. Using an IP address that belongs to the other node results in unnecessary data traffic between the nodes. This traffic impacts system performance and stability.
2. You must use the floating IP address for traffic *within* the VPC and the private IP address for traffic that *leaves* the VPC.

You cannot identify the correct IP address using Cloud Manager. You must use the ONTAP Cloud CLI at this time.

Steps

1. Connect to the ONTAP Cloud CLI.
2. Use the `volume show` command to identify the ONTAP Cloud node that owns the volume.

Example

In this example, the name of the node is `workingEnvName-01`:

```
workingEnvName::> volume show -volume test -fields
volume,junction-path,node

vserver          volume junction-path node
-----
svm_workingEnvName test    /test          workingEnvName-01
```

3. Use the `network interface show` command to find the NFS and CIFS IP addresses on that ONTAP Cloud node.

The name of the LIF for the floating IP address follows the format
 “svm_*WorkingEnvironmentName*_data_lif1” for node 1 and
 “svm_*WorkingEnvironmentName*_data_lif2” for node 2.

The other LIF is the private IP address, which you named when you created the LIF.

Example

In this example, the floating IP address is 192.168.100.2 and the private IP address is 172.30.0.227:

```
workingEnvName::> network interface show -data-protocol
nfs,cifs -fields lif,address -home-node workingEnvName-01
```

vserver	lif	address
svm_workingEnvName	svm_workingEnvName_data_lif1	192.168.100.2
svm_workingEnvName	svm_workingEnvName_data_lif1_priv	172.30.0.227

2 entries were displayed.

Where to get help and find more information

You can get help and find more information by going to the NetApp Support Site and the NetApp Community forums.

- [*NetApp Support*](#)
Access troubleshooting tools, product documentation, and technical support assistance.
- [*NetApp ONTAP Cloud Support*](#)
Access support resources to get help and troubleshoot issues with ONTAP Cloud.
- [*NetApp Community: Hybrid Cloud*](#)
Connect with peers, ask questions, exchange ideas, find resources, and share best practices.
- [*NetApp ONTAP Cloud Resources*](#)
Access additional documentation and videos for Cloud Manager and ONTAP Cloud.

Copyright information

Copyright © 1994–2017 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

Active IQ, AltaVault, Arch Design, ASUP, AutoSupport, Campaign Express, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Element, Fitness, Flash Accel, Flash Cache, Flash Pool, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, Fueled by SolidFire, GetSuccessful, Helix Design, LockVault, Manage ONTAP, MetroCluster, MultiStore, NetApp, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANscreen, SANshare, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, SolidFire, SolidFire Helix, StorageGRID, SyncMirror, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277