



# **AWS and Azure permissions for Cloud Manager**

Cloud Manager 3.5

Ben Cammett  
November 01, 2018

This PDF was generated from [https://docs.netapp.com/us-en/occm35/reference\\_permissions.html](https://docs.netapp.com/us-en/occm35/reference_permissions.html) on February 15, 2021. Always check docs.netapp.com for the latest.

# Table of Contents

- AWS and Azure permissions for Cloud Manager ..... 1
  - What Cloud Manager does with AWS permissions ..... 1
  - What Cloud Manager does with Azure permissions..... 3

# AWS and Azure permissions for Cloud Manager

Cloud Manager requires permissions to perform actions in AWS and Azure on your behalf. These permissions are included in [the policies provided by NetApp](#). You might want to understand what Cloud Manager does with these permissions.

## What Cloud Manager does with AWS permissions

Cloud Manager uses an AWS account to make API calls to several AWS services, including EC2, S3, CloudFormation, IAM, the Security Token Service (STS), and the Key Management Service (KMS).

| Actions   | Purpose  |
|---|--|
| "ec2:StartInstances",<br>"ec2:StopInstances",<br>"ec2:DescribeInstances",<br>"ec2:DescribeInstanceStatus",<br>"ec2:RunInstances",<br>"ec2:TerminateInstances",<br>"ec2:ModifyInstanceAttribute",  | Launches a Cloud Volumes ONTAP instance and stops, starts, and monitors the instance.  |
| "ec2:DescribeInstanceAttribute",  | Verifies that enhanced networking is enabled for supported instance types.   |
| "ec2:DescribeRouteTables",<br>"ec2:DescribeImages",   | Launches a Cloud Volumes ONTAP HA configuration.   |
| "ec2:CreateTags",   | Tags every resource that Cloud Manager creates with the "WorkingEnvironment" and "WorkingEnvironmentId" tags. Cloud Manager uses these tags for maintenance and cost allocation. |
| "ec2:CreateVolume",<br>"ec2:DescribeVolumes",<br>"ec2:ModifyVolumeAttribute",<br>"ec2:AttachVolume",<br>"ec2:DeleteVolume",<br>"ec2:DetachVolume",  | Manages the EBS volumes that Cloud Volumes ONTAP uses as back-end storage.   |
| "ec2:CreateSecurityGroup",<br>"ec2>DeleteSecurityGroup",<br>"ec2:DescribeSecurityGroups",<br>"ec2:RevokeSecurityGroupEgress",<br>"ec2:AuthorizeSecurityGroupEgress",<br>"ec2:AuthorizeSecurityGroupIngress",<br>"ec2:RevokeSecurityGroupIngress", | Creates predefined security groups for Cloud Volumes ONTAP.  |
| "ec2:CreateNetworkInterface",<br>"ec2:DescribeNetworkInterfaces",<br>"ec2>DeleteNetworkInterface",<br>"ec2:ModifyNetworkInterfaceAttribute",  | Creates and manages network interfaces for Cloud Volumes ONTAP in the target subnet.   |


| Actions   | Purpose  |
|---|--|
| "ec2:DescribeSubnets",<br>"ec2:DescribeVpcs",   | Gets the list of destination subnets and security groups, which is needed when creating a new working environment for Cloud Volumes ONTAP. |
| "ec2:DescribeDhcpOptions",  | Determines DNS servers and the default domain name when launching Cloud Volumes ONTAP instances.   |
| "ec2:CreateSnapshot",<br>"ec2:DeleteSnapshot",<br>"ec2:DescribeSnapshots",  | Takes snapshots of EBS volumes during initial setup and whenever a Cloud Volumes ONTAP instance is stopped.                                |
| "ec2:GetConsoleOutput",   | Captures the Cloud Volumes ONTAP console, which is attached to AutoSupport messages.   |
| "ec2:DescribeKeyPairs",   | Obtains the list of available key pairs when launching instances.  |
| "ec2:DescribeRegions",  | Gets a list of available AWS regions.  |
| "ec2:DeleteTags",<br>"ec2:DescribeTags",  | Manages tags for resources associated with Cloud Volumes ONTAP instances.  |
| "cloudformation:CreateStack",<br>"cloudformation:DeleteStack",<br>"cloudformation:DescribeStacks",<br>"cloudformation:DescribeStackEvents",<br>"cloudformation:ValidateTemplate",   | Launches Cloud Volumes ONTAP instances.  |
| "iam:PassRole",<br>"iam:CreateRole",<br>"iam:DeleteRole",<br>"iam:PutRolePolicy",<br>"iam:CreateInstanceProfile",<br>"iam:DeleteRolePolicy",<br>"iam:AddRoleToInstanceProfile",<br>"iam:RemoveRoleFromInstanceProfile",<br>"iam:DeleteInstanceProfile", | Launches a Cloud Volumes ONTAP HA configuration.   |
| "iam:ListInstanceProfiles",<br>"sts:DecodeAuthorizationMessage",<br>"ec2:AssociateIamInstanceProfile",<br>"ec2:DescribeIamInstanceProfileAssociations",<br>"ec2:DisassociateIamInstanceProfile",  | Manages instance profiles for Cloud Volumes ONTAP instances.   |
| "s3:GetObject",<br>"s3:ListBucket"  | Obtains AWS cost data for Cloud Volumes ONTAP.   |
| "s3:GetBucketTagging",<br>"s3:GetBucketLocation",<br>"s3:ListAllMyBuckets",   | Obtains information about AWS S3 buckets so Cloud Manager can integrate with the NetApp Data Fabric Cloud Sync service.                    |

| Actions  | Purpose  |
|--|--|
| "s3:CreateBucket",<br>"s3:DeleteBucket",<br>"s3:GetLifecycleConfiguration",<br>"s3:PutLifecycleConfiguration",<br>"s3:PutBucketTagging",<br>"s3:ListBucketVersions", | Manages the S3 bucket that a Cloud Volumes ONTAP system uses as a capacity tier. |
| "kms:List*",<br>"kms:Describe*"  | Obtains information about keys from the AWS Key Management Service.              |

## What Cloud Manager does with Azure permissions

The Cloud Manager Azure policy includes the permissions that Cloud Manager needs to deploy and manage Cloud Volumes ONTAP in Azure.

| Actions   | Purpose   |
|---|---|
| "Microsoft.Compute/locations/operations/read",<br>"Microsoft.Compute/locations/vmSizes/read",<br>"Microsoft.Compute/operations/read",<br>"Microsoft.Compute/virtualMachines/instanceView/read",<br>"Microsoft.Compute/virtualMachines/powerOff/action",<br>"Microsoft.Compute/virtualMachines/read",<br>"Microsoft.Compute/virtualMachines/restart/action",<br>"Microsoft.Compute/virtualMachines/start/action",<br>"Microsoft.Compute/virtualMachines/deallocate/action",<br>"Microsoft.Compute/virtualMachines/vmSizes/read",<br>"Microsoft.Compute/virtualMachines/write", | Creates Cloud Volumes ONTAP and stops, starts, deletes, and obtains the status of the system. |
| "Microsoft.Compute/images/write",<br>"Microsoft.Compute/images/read",   | Enables Cloud Volumes ONTAP deployment from a VHD.  |
| "Microsoft.Compute/disks/delete",<br>"Microsoft.Compute/disks/read",<br>"Microsoft.Compute/disks/write",<br>"Microsoft.Storage/checknameavailability/read",<br>"Microsoft.Storage/operations/read",<br>"Microsoft.Storage/storageAccounts/listkeys/action",<br>"Microsoft.Storage/storageAccounts/read",<br>"Microsoft.Storage/storageAccounts/regeneratekey/action",<br>"Microsoft.Storage/storageAccounts/write"  | Manages Azure storage accounts and disks, and attaches the disks to Cloud Volumes ONTAP.      |
| "Microsoft.Network/networkInterfaces/read",<br>"Microsoft.Network/networkInterfaces/write",<br>"Microsoft.Network/networkInterfaces/join/action",   | Creates and manages network interfaces for Cloud Volumes ONTAP in the target subnet.          |
| "Microsoft.Network/networkSecurityGroups/read",<br>"Microsoft.Network/networkSecurityGroups/write",<br>"Microsoft.Network/networkSecurityGroups/join/action",   | Creates predefined network security groups for Cloud Volumes ONTAP.                           |

| Actions   | Purpose  |
|---|--|
| "Microsoft.Resources/subscriptions/locations/read",<br>"Microsoft.Network/locations/operationResults/read",<br>"Microsoft.Network/locations/operations/read",<br>"Microsoft.Network/virtualNetworks/read",<br>"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",<br>"Microsoft.Network/virtualNetworks/subnets/read",<br>"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",<br>"Microsoft.Network/virtualNetworks/virtualMachines/read",<br>"Microsoft.Network/virtualNetworks/subnets/join/action", | Gets network information about regions, the target VNet and subnet, and adds Cloud Volumes ONTAP to VNets. |
| <div data-bbox="181 772 246 835"></div> <div data-bbox="321 703 773 905"> <p>If your network configuration uses route tables, then Cloud Manager also requires the following permission:</p> <p>Microsoft.Network/routeTables/join/action</p> </div>   | Enables VNet service endpoints for data tiering.   |
| "Microsoft.Resources/deployments/operations/read",<br>"Microsoft.Resources/deployments/read",<br>"Microsoft.Resources/deployments/write",   | Deploys Cloud Volumes ONTAP from a template.   |
| "Microsoft.Resources/deployments/operations/read",<br>"Microsoft.Resources/deployments/read",<br>"Microsoft.Resources/deployments/write",<br>"Microsoft.Resources/resources/read",<br>"Microsoft.Resources/subscriptions/operationresults/read",<br>"Microsoft.Resources/subscriptions/resourceGroups/delete",<br>"Microsoft.Resources/subscriptions/resourceGroups/read",<br>"Microsoft.Resources/subscriptions/resourcegroups/resources/read",<br>"Microsoft.Resources/subscriptions/resourceGroups/write",                         | Creates and manages resource groups for Cloud Volumes ONTAP.   |
| "Microsoft.Compute/snapshots/write",<br>"Microsoft.Compute/snapshots/read",<br>"Microsoft.Compute/disks/beginGetAccess/action"  | Creates and manages Azure managed snapshots.   |
| "Microsoft.Compute/availabilitySets/write",<br>"Microsoft.Compute/availabilitySets/read",   | Creates and manages availability sets for Cloud Volumes ONTAP.   |
| "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",<br>"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write"  | Enables programmatic deployments from the Azure Marketplace.   |

| Actions                           | Purpose                                     |
|-----------------------------------|---|
| "Microsoft.Authorization/locks/*" | Enables management of locks on Azure disks. |

## 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.