



AWS and Azure permissions for Cloud Manager

Cloud Manager 3.5

NetApp
11/01/2018

Table of Contents

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

1. 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.

1.1. 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", "ec2:StopInstances", "ec2:DescribeInstances", "ec2:DescribeInstanceStatus", "ec2:RunInstances", "ec2:TerminateInstances", "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", "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", "ec2:DescribeVolumes", "ec2:ModifyVolumeAttribute", "ec2:AttachVolume", "ec2:DeleteVolume", "ec2:DetachVolume",	Manages the EBS volumes that Cloud Volumes ONTAP uses as back-end storage.

Actions	Purpose
"ec2:CreateSecurityGroup", "ec2:DeleteSecurityGroup", "ec2:DescribeSecurityGroups", "ec2:RevokeSecurityGroupEgress", "ec2:AuthorizeSecurityGroupEgress", "ec2:AuthorizeSecurityGroupIngress", "ec2:RevokeSecurityGroupIngress",	Creates predefined security groups for Cloud Volumes ONTAP.
"ec2:CreateNetworkInterface", "ec2:DescribeNetworkInterfaces", "ec2:DeleteNetworkInterface", "ec2:ModifyNetworkInterfaceAttribute",	Creates and manages network interfaces for Cloud Volumes ONTAP in the target subnet.
"ec2:DescribeSubnets", "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", "ec2:DeleteSnapshot", "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", "ec2:DescribeTags",	Manages tags for resources associated with Cloud Volumes ONTAP instances.
"cloudformation:CreateStack", "cloudformation:DeleteStack", "cloudformation:DescribeStacks", "cloudformation:DescribeStackEvents", "cloudformation:ValidateTemplate",	Launches Cloud Volumes ONTAP instances.
"iam:PassRole", "iam:CreateRole", "iam:DeleteRole", "iam:PutRolePolicy", "iam:CreateInstanceProfile", "iam:DeleteRolePolicy", "iam:AddRoleToInstanceProfile", "iam:RemoveRoleFromInstanceProfile", "iam:DeleteInstanceProfile",	Launches a Cloud Volumes ONTAP HA configuration.


Actions	Purpose
"iam:ListInstanceProfiles", "sts:DecodeAuthorizationMessage", "ec2:AssociateIamInstanceProfile", "ec2:DescribeIamInstanceProfileAssociations", "ec2:DisassociateIamInstanceProfile",	Manages instance profiles for Cloud Volumes ONTAP instances.
"s3:GetObject", "s3:ListBucket"	Obtains AWS cost data for Cloud Volumes ONTAP.
"s3:GetBucketTagging", "s3:GetBucketLocation", "s3:ListAllMyBuckets",	Obtains information about AWS S3 buckets so Cloud Manager can integrate with the NetApp Data Fabric Cloud Sync service.
"s3:CreateBucket", "s3:DeleteBucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutBucketTagging", "s3:ListBucketVersions",	Manages the S3 bucket that a Cloud Volumes ONTAP system uses as a capacity tier.
"kms:List*", "kms:Describe*"	Obtains information about keys from the AWS Key Management Service.

1.2. 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", "Microsoft.Compute/locations/vmSizes/read", "Microsoft.Compute/operations/read", "Microsoft.Compute/virtualMachines/instanceView/read", "Microsoft.Compute/virtualMachines/powerOff/action", "Microsoft.Compute/virtualMachines/read", "Microsoft.Compute/virtualMachines/restart/action", "Microsoft.Compute/virtualMachines/start/action", "Microsoft.Compute/virtualMachines/deallocate/action", "Microsoft.Compute/virtualMachines/vmSizes/read", "Microsoft.Compute/virtualMachines/write",	Creates Cloud Volumes ONTAP and stops, starts, deletes, and obtains the status of the system.

Actions	Purpose
"Microsoft.Compute/images/write", "Microsoft.Compute/images/read",	Enables Cloud Volumes ONTAP deployment from a VHD.
"Microsoft.Compute/disks/delete", "Microsoft.Compute/disks/read", "Microsoft.Compute/disks/write", "Microsoft.Storage/checknameavailability/read", "Microsoft.Storage/operations/read", "Microsoft.Storage/storageAccounts/listkeys/action", "Microsoft.Storage/storageAccounts/read", "Microsoft.Storage/storageAccounts/regeneratekey/action", "Microsoft.Storage/storageAccounts/write"	Manages Azure storage accounts and disks, and attaches the disks to Cloud Volumes ONTAP.
"Microsoft.Network/networkInterfaces/read", "Microsoft.Network/networkInterfaces/write", "Microsoft.Network/networkInterfaces/join/action",	Creates and manages network interfaces for Cloud Volumes ONTAP in the target subnet.
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/networkSecurityGroups/write", "Microsoft.Network/networkSecurityGroups/join/action",	Creates predefined network security groups for Cloud Volumes ONTAP.
"Microsoft.Resources/subscriptions/locations/read", "Microsoft.Network/locations/operationResults/read", "Microsoft.Network/locations/operations/read", "Microsoft.Network/virtualNetworks/read", "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read", "Microsoft.Network/virtualNetworks/subnets/read", "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read", "Microsoft.Network/virtualNetworks/virtualMachines/read", "Microsoft.Network/virtualNetworks/subnets/join/action",	Gets network information about regions, the target VNet and subnet, and adds Cloud Volumes ONTAP to VNets.

Actions	Purpose
<p>"Microsoft.Network/virtualNetworks/subnets/write",</p> <div data-bbox="183 383 248 445">  </div> <p>If your network configuration uses route tables, then Cloud Manager also requires the following permission: Microsoft.Network/routeTables/join/action</p>	Enables VNet service endpoints for data tiering.
<p>"Microsoft.Resources/deployments/operations/read", "Microsoft.Resources/deployments/read", "Microsoft.Resources/deployments/write",</p>	Deploys Cloud Volumes ONTAP from a template.
<p>"Microsoft.Resources/deployments/operations/read", "Microsoft.Resources/deployments/read", "Microsoft.Resources/deployments/write", "Microsoft.Resources/resources/read", "Microsoft.Resources/subscriptions/operationresults/read", "Microsoft.Resources/subscriptions/resourceGroups/delete", "Microsoft.Resources/subscriptions/resourceGroups/read", "Microsoft.Resources/subscriptions/resourceGroups/resources/read", "Microsoft.Resources/subscriptions/resourceGroups/write",</p>	Creates and manages resource groups for Cloud Volumes ONTAP.
<p>"Microsoft.Compute/snapshots/write", "Microsoft.Compute/snapshots/read", "Microsoft.Compute/disks/beginGetAccess/action"</p>	Creates and manages Azure managed snapshots.
<p>"Microsoft.Compute/availabilitySets/write", "Microsoft.Compute/availabilitySets/read",</p>	Creates and manages availability sets for Cloud Volumes ONTAP.
<p>"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read", "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write"</p>	Enables programmatic deployments from the Azure Marketplace.
<p>"Microsoft.Authorization/locks/*"</p>	Enables management of locks on Azure disks.