Reference

Set up and administration

NetApp
April 14, 2022

Table of Contents

Reference

Required permissions for the Connector in AWS

Cloud Manager requires permissions to perform actions in your cloud provider. These permissions are included in the policies provided by NetApp. You might want to understand what Cloud Manager does with these 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.
"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.

Actions	Purpose
"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.
"iam:ListInstanceProfiles", "sts:DecodeAuthorizationMessage", "ec2:AssociateIamInstanceProfile", "ec2:DescribeIamInstanceProfileAssociations", "ec2:DisassociateIamInstanceProfile",	Manages instance profiles for Cloud Volumes ONTAP instances.
"s3:GetBucketTagging", "s3:GetBucketLocation", "s3:ListAllMyBuckets", "s3:ListBucket"	Obtains information about AWS S3 buckets so Cloud Manager can integrate with the NetApp Data Fabric Cloud Sync service.

Actions	Purpose
"s3:CreateBucket", "s3:DeleteBucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutBucketTagging", "s3:ListBucketVersions", "s3:GetBucketPolicyStatus", "s3:GetBucketPublicAccessBlock", "s3:GetBucketAcl", "s3:GetBucketPolicy", "s3:PutBucketPublicAccessBlock"	Manages the S3 bucket that a Cloud Volumes ONTAP system uses as a capacity tier for data tiering.
"kms:List*", "kms:ReEncrypt*", "kms:Describe*", "kms:CreateGrant",	Enables data encryption of Cloud Volumes ONTAP using the AWS Key Management Service (KMS).
"ce:GetReservationUtilization", "ce:GetDimensionValues", "ce:GetCostAndUsage", "ce:GetTags"	Obtains AWS cost data for Cloud Volumes ONTAP.
"ec2:CreatePlacementGroup", "ec2:DeletePlacementGroup"	When you deploy an HA configuration in a single AWS Availability Zone, Cloud Manager launches the two HA nodes and the mediator in an AWS spread placement group.
"ec2:DescribeReservedInstancesOfferings"	Cloud Manager uses the permission as part of Cloud Data Sense deployment to choose which instance type to use.
"ec2:CreateTags", "ec2:DeleteTags", "ec2:DescribeTags", "tag:getResources", "tag:getTagKeys", "tag:getTagValues", "tag:TagResources", "tag:UntagResources"	Enables you to manage tags on your AWS resources using the Cloud Manager Tagging service.

Actions	Purpose
"s3:DeleteBucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutBucketTagging", "s3:ListBucketVersions", "s3:GetObject", "s3:ListBucket", "s3:ListAllMyBuckets", "s3:GetBucketTagging", "s3:GetBucketLocation" "s3:GetBucketPolicyStatus", "s3:GetBucketPublicAccessBlock", "s3:GetBucketAcl", "s3:GetBucketPolicy", "s3:PutBucketPublicAccessBlock"	Cloud Manager uses these permissions when you enable the Backup to S3 service.
"eks:ListClusters", "eks:DescribeCluster", "iam:GetInstanceProfile"	Enables discovery of Amazon EKS clusters.

Required permissions for the Connector in Azure

Cloud Manager requires permissions to perform actions in your cloud provider. These permissions are included in the policies provided by NetApp. You might want to understand what Cloud Manager does with these 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.
"Microsoft.Compute/images/write", "Microsoft.Compute/images/read",	Enables Cloud Volumes ONTAP deployment from a VHD.

Actions	Purpose
"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" "Microsoft.Storage/storageAccounts/delete", "Microsoft.Storage/usages/read",	Manages Azure storage accounts and disks, and attaches the disks to Cloud Volumes ONTAP.
"Microsoft.Storage/storageAccounts/blobServices/containers/read", "Microsoft.KeyVault/vaults/read", "Microsoft.KeyVault/vaults/accessPolicies/write"	Enables backups to Azure Blob storage and encryption of storage accounts
"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.
"Microsoft.Network/virtualNetworks/subnets/write", "Microsoft.Network/routeTables/join/action",	Enables VNet service endpoints for data tiering.
"Microsoft.Resources/deployments/operations/read", "Microsoft.Resources/deployments/read", "Microsoft.Resources/deployments/write",	Deploys Cloud Volumes ONTAP from a template.

Actions	Purpose
"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",	Creates and manages resource groups for Cloud Volumes ONTAP.
"Microsoft.Compute/snapshots/write", "Microsoft.Compute/snapshots/read", "Microsoft.Compute/snapshots/delete", "Microsoft.Compute/disks/beginGetAccess/action",	Creates and manages Azure managed snapshots.
"Microsoft.Compute/availabilitySets/write", "Microsoft.Compute/availabilitySets/read",	Creates and manages availability sets for Cloud Volumes ONTAP.
"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read", "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",	Enables programmatic deployments from the Azure Marketplace.
"Microsoft.Network/loadBalancers/read", "Microsoft.Network/loadBalancers/write", "Microsoft.Network/loadBalancers/delete", "Microsoft.Network/loadBalancers/backendAddressPools/read", "Microsoft.Network/loadBalancers/backendAddressPools/join/action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/read", "Microsoft.Network/loadBalancers/loadBalancingRules/read", "Microsoft.Network/loadBalancers/probes/read", "Microsoft.Network/loadBalancers/probes/join/action",	Manages an Azure load balancer for HA pairs.
"Microsoft.Authorization/locks/*",	Enables management of locks on Azure disks.
"Microsoft.Authorization/roleDefinitions/write", "Microsoft.Authorization/roleAssignments/write", "Microsoft.Web/sites/*"	Manages failover for HA pairs.

Actions	Purpose
"Microsoft.Network/privateEndpoints/write", "Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action", "Microsoft.Storage/storageAccounts/privateEndpointConnections/read", "Microsoft.Network/privateEndpoints/read", "Microsoft.Network/privateDnsZones/write", "Microsoft.Network/privateDnsZones/virtualNetworkLinks/write", "Microsoft.Network/virtualNetworks/join/action", "Microsoft.Network/privateDnsZones/A/write", "Microsoft.Network/privateDnsZones/read", "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",	Enables the management of private endpoints. Private endpoints are used when connectivity isn't provided to outside the subnet. Cloud Manager creates the storage account for HA with only internal connectivity within the subnet.
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",	Enables Cloud Manager to delete volumes for Azure NetApp Files.
"Microsoft.Resources/deployments/operationStatuses/read"	Azure requires this permission for some virtual machine deployments (it depends on the underlying physical hardware that's used during deployment).
"Microsoft.Resources/deployments/operationStatuses/read", "Microsoft.Insights/Metrics/Read", "Microsoft.Compute/virtualMachines/extensions/write", "Microsoft.Compute/virtualMachines/extensions/read", "Microsoft.Compute/virtualMachines/extensions/delete", "Microsoft.Compute/virtualMachines/delete", "Microsoft.Network/networkInterfaces/delete", "Microsoft.Network/networkSecurityGroups/delete", "Microsoft.Resources/deployments/delete",	Enables you to use Global File Cache.
"Microsoft.Network/privateEndpoints/delete", "Microsoft.Compute/availabilitySets/delete",	Enables Cloud Manager to remove resources from a resource group that belong to Cloud Volumes ONTAP in case of deployment failure or deletion.
"Microsoft.Compute/diskEncryptionSets/read" "Microsoft.Compute/diskEncryptionSets/write", "Microsoft.Compute/diskEncryptionSets/delete" "Microsoft.KeyVault/vaults/deploy/action", "Microsoft.KeyVault/vaults/read", "Microsoft.KeyVault/vaults/accessPolicies/write",	Enables use of customer-managed encryption keys with Cloud Volumes ONTAP. This feature is supported using APIs.
"Microsoft.Resources/tags/read", "Microsoft.Resources/tags/write", "Microsoft.Resources/tags/delete"	Enables you to manage tags on your Azure resources using the Cloud Manager Tagging service.

Actions	Purpose
"Microsoft.Network/applicationSecurityGroups/write", "Microsoft.Network/applicationSecurityGroups/read", "Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action", "Microsoft.Network/networkSecurityGroups/securityRules/write", "Microsoft.Network/applicationSecurityGroups/delete", "Microsoft.Network/networkSecurityGroups/securityRules/delete"	Enables Cloud Manager to configure an application security group for an HA pair, which isolates the HA interconnect and cluster network NICs.

Required permissions for the Connector in Google Cloud

Cloud Manager requires permissions to perform actions in your cloud provider. These permissions are included in the policies provided by NetApp. You might want to understand what Cloud Manager does with these permissions.

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

Actions	Purpose
- compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use	To create and manage disks for Cloud Volumes ONTAP.
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	To create firewall rules for Cloud Volumes ONTAP.
- compute.globalOperations.get	To get the status of operations.
- compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly	To get images for VM instances.
- compute.instances.attachDisk - compute.instances.detachDisk	To attach and detach disks to Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	To create and delete Cloud Volumes ONTAP VM instances.
- compute.instances.get	To list VM instances.
- compute.instances.getSerialPortOutput	To get console logs.
- compute.instances.list	To retrieve the list of instances in a zone.
- compute.instances.setDeletionProtection	To set deletion protection on the instance.

Actions	Purpose
- compute.instances.setLabels	To add labels.
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	To change the machine type for Cloud Volumes ONTAP.
- compute.instances.setMetadata	To add metadata.
- compute.instances.setTags	To add tags for firewall rules.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	To start and stop Cloud Volumes ONTAP.
- compute.machineTypes.get	To get the numbers of cores to check qoutas.
- compute.projects.get	To support multi-projects.
- compute.snapshots.create - compute.snapshots.delete - compute.snapshots.get - compute.snapshots.list - compute.snapshots.setLabels	To create and manage persistent disk snapshots.
- compute.networks.get - compute.networks.list - compute.regions.get - compute.regions.list - compute.subnetworks.get - compute.subnetworks.list - compute.zoneOperations.get - compute.zones.get - compute.zones.list	To get the networking information needed to create a new Cloud Volumes ONTAP virtual machine instance.
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifests.get - deploymentmanager.manifests.list - deploymentmanager.operations.get - deploymentmanager.operations.list - deploymentmanager.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProviders.get - deploymentmanager.typeProviders.list - deploymentmanager.types.get - deploymentmanager.types.list	To deploy the Cloud Volumes ONTAP virtual machine instance using Google Cloud Deployment Manager.
- logging.logEntries.list - logging.privateLogEntries.list	To get stack log drives.
- resourcemanager.projects.get	To support multi-projects.

Actions	Purpose
- storage.buckets.create - storage.buckets.delete - storage.buckets.get - storage.buckets.list - storage.buckets.update	To create and manage a Google Cloud Storage bucket for data tiering.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.list - cloudkms.keyRings.list	To use customer-managed encryption keys from the Cloud Key Management Service with Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - storage.objects.get - storage.objects.list	To set a service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket.
- compute.addresses.list - compute.backendServices.create - compute.networks.updatePolicy - compute.regionBackendServices.create - compute.regionBackendServices.get - compute.regionBackendServices.list	To deploy HA pairs.
- compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	To enable Cloud Data Sense.
- container.clusters.get - container.clusters.list	To discover Kubernetes clusters running in Google Kubernetes Engine.