Important changes in Cloud Manager

Cloud Manager

Ben Cammett, Tom Onacki
September 01, 2021

Table of Contents

Important changes in Cloud Manager

This page highlights important changes in Cloud Manager that can help you use the service as we introduce new enhancements. You should continue to read the What's new page to learn about all new features and enhancements.

Cloud Volumes ONTAP AMI change

Starting with the 9.8 release, the Cloud Volumes ONTAP PAYGO AMI is no longer available in the AWS Marketplace. If you use the Cloud Manager API to deploy Cloud Volumes ONTAP PAYGO, you'll need to subscribe to the Cloud Manager subscription in the AWS Marketplace before deploying a 9.8 system.

SaaS changes

We have introduced a software-as-a-service experience for Cloud Manager. This new experience makes it easier for you to use Cloud Manager and enables us to provide additional features to manage your hybrid cloud infrastructure.

- Cloud Manager transition to SaaS
- Learn how Cloud Manager works

Machine type changes

To ensure that adequate resources are available for new and upcoming features in Cloud Manager, we've changed the minimum required instance, VM, and machine type as follows:

- AWS: t3.xlarge
- Azure: DS3 v2
- GCP: n1-standard-4

When you upgrade the machine type, you'll get access to features like a new Kubernetes experience, Global File Cache, Monitoring, and more.

These default sizes are the minimum supported based on CPU and RAM requirements.

Cloud Manager will prompt you with instructions to change the machine type of the Connector.

Account settings

We introduced Cloud Central accounts to provide multi-tenancy, to help you organize users and resources in isolated workspaces, and to manage access to Connectors and subscriptions.

- Learn about Cloud Central accounts: users, workspaces, Connectors, and subscriptions
- Learn how to get started with your account
- Learn how to manage your account after you set it up

New permissions

Cloud Manager occasionally requires additional cloud provider permissions as we introduce new features and enhancements. This section identifies new permissions that are now required.

You can find the latest list of permissions on the Cloud Manager policies page.

AWS

- Starting with the 3.9.9 release, the following permissions are required for the tagging service:

```
{
                                    "Action": [
                                      "ec2:CreateTags",
                                      "ec2:DeleteTags",
                                      "ec2:DescribeTags",
                                      "tag:getResources",
                                      "tag:getTagKeys",
                                      "tag:getTagValues",
                                      "tag:TagResources",
                                      "tag:UntagResources"
                                    ],
                                    "Resource": "*",
                                    "Effect": "Allow",
                                    "Sid": "tagServicePolicy"
                                },
```

- Starting with the 3.8.1 release, the following permissions are required to use Cloud Backup with Cloud Volumes ONTAP. Learn more.

```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "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"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

Azure

- Starting with the 3.9.10 release, you can use customer-managed encryption keys with Cloud Volumes ONTAP. A Connector requires these new permissions to set up an encryption key with a single node Cloud Volumes ONTAP system:

```
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.Compute/diskEncryptionSets/delete"
```

- Starting with the 3.9.10 release, you can manage tags on your Azure resources using the Cloud Manager Tagging service. A Connector requires these new permissions for this service:

```
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Resources/tags/delete"
```

- Starting with the 3.9.8 release, Cloud Manager can remove Cloud Volumes ONTAP resources from a

resource group, in case of deployment failure or deletion. Be sure to provide these permissions to each set of Azure credentials that you've added to Cloud Manager:

```
"Microsoft.Network/privateEndpoints/delete",
"Microsoft.Compute/availabilitySets/delete",
```

- Starting with the 3.9.7 release, Cloud Manager can now delete older cloud snapshots of root and boot disks that are created when a Cloud Volumes ONTAP system is deployed and every time its powered down. A Connector requires a new permission to delete Azure snapshots:

```
"Microsoft.Compute/snapshots/delete"
```

- To avoid Azure deployment failures, make sure that your Cloud Manager policy in Azure includes the following permission:

```
"Microsoft.Resources/deployments/operationStatuses/read"
```

- Starting with the 3.8.7 release, the following permission is required to encrypt Azure managed disks on single node Cloud Volumes ONTAP systems using external keys from another account. Learn more.

```
"Microsoft.Compute/diskEncryptionSets/read"
```

- The following permissions are required to enable Global File Cache on Cloud Volumes ONTAP. Learn more.

```
"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",
```

GCP

New permissions to deploy Cloud Data Sense in Google Cloud

Starting with the 3.9.10 release, the following permissions are required to deploy Cloud Data Sense in Google Cloud:

```
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.instances.addAccessConfig
```

New permission for changing machine type

We recently discovered that the following permission is required for Cloud Volumes ONTAP machine type changes when switching between machine type families.

```
- compute.instances.setMinCpuPlatform
```

New permissions for HA pairs

Starting with the 3.9 release, the service account for a Connector requires additional permissions to deploy a Cloud Volumes ONTAP HA pair in GCP:

```
- compute.addresses.list
- compute.backendServices.create
- compute.networks.updatePolicy
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
```

New permissions for data tiering

Starting with the 3.9 release, additional permissions are required 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.

- iam.serviceAccounts.actAs
- storage.objects.get
- storage.objects.list

New permissions for Kubernetes management

Starting with the 3.8.8 release, the service account for a Connector requires additional permissions to discover and manage Kubernetes clusters running in Google Kubernetes Engine (GKE):

```
- container.*
```

New permissions for data tiering

Starting with the 3.8 release, the following permissions are now required to use a service account for data tiering. Learn more about this change.

```
- storage.buckets.update
- compute.instances.setServiceAccount
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
```

New endpoints

The Connector requires outbound internet access to manage resources and processes within your public cloud environment. This section identifies new endpoints that are now required.

You can find the full list of endpoints accessed from your web browser here and the full list of endpoints accessed by the Connector here.

- Users need to access Cloud Manager from a web browser by contacting the following endpoint:

  https://cloudmanager.netapp.com

- Connectors require access to the following endpoint to obtain software images of container components for a Docker infrastructure:

  https://cloudmanagerinfraprod.azurecr.io

  Ensure that your firewall enables access to this endpoint from the Connector.