参考
Set up and administration

NetApp
April 12, 2022

目录

参考

AWS 中连接器的所需权限

Cloud Manager 需要在云提供商中执行操作的权限。中包括这些权限 "NetApp 提供的策略"。您可能希望了解 Cloud Manager 使用这些权限执行的操作。

Cloud Manager 使用 AWS 帐户对几个 AWS 服务进行 API 调用、包括 EC2 、 S3 、 Cloudformation 、 IAM 、 Security Token Service （安全令牌服务， STS ）和密钥管理服务（ KMS ）。

操作	目的
"EC2： StartInstances "， "EC2： StopInstances "， "EC2： Describe Instances "， "EC2： Describe InstanceStatus"， "EC2： RunInstances "， "EC2：终端实例 "， "EC2： ModifyInstanceAttribute"，	启动 Cloud Volumes ONTAP 实例并停止、启动和监控实例。
"EC2：描述实例属性 "、	验证是否已为支持的实例类型启用增强网络。
"EC2：描述图 "、 "EC2：描述图 "、	启动 Cloud Volumes ONTAP HA 配置。
"EC2：创建标记 "、	标记 Cloud Manager 使用 "Workingviron" 和 "Workingvironmid" 标记创建的每个资源。Cloud Manager 使用这些标签进行维护和成本分配。
"EC2： CreateVolume"， "EC2： Describe Volumes"， "EC2： ModifyVolumeAttribute"， "EC2： AttachVolume"， "EC2： DeleteVolume"， "EC2：详细卷 "，	管理 Cloud Volumes ONTAP 用作后端存储的 EBS 卷。
"EC2： CreateSecurityGroup"， "EC2： DeleteSecurityGroup"， "EC2： Describe SecurityGroups"， "EC2： RevokeSecurityGroupEated"， "EC2： AuthorizeSecurityGroupEated"， "EC2： AuthorizeSecurityGroupIn防护 "， "EC2： RevokeSecurityGroupIn防护 "，	为 Cloud Volumes ONTAP 创建预定义的安全组。
"EC2： CreateNetworkInterface"， "EC2： Describe NetworkInterfaces"， "EC2： DeleteNetworkInterface"， "EC2： ModifyNetworkInterfaceAttribute"，	在目标子网中为 Cloud Volumes ONTAP 创建和管理网络接口。
"EC2：描述性子网 "、 "EC2：描述性 VPCS"、	获取目标子网和安全组的列表、在为 Cloud Volumes ONTAP 创建新的工作环境时需要这些子网和安全组。
"EC2：说明 "、	确定启动 Cloud Volumes ONTAP 实例时的 DNS 服务器和默认域名。
"EC2： CreateSnapshot "、 "EC2： DeleteSnapshot "、 "EC2：描述性快照 "、	在初始设置期间和停止 Cloud Volumes ONTAP 实例时拍摄 EBS 卷的快照。
"EC2： GetConsoleOutput "、	捕获附加到 AutoSupport 消息的 Cloud Volumes ONTAP 控制台。
"EC2：描述性密钥对 "、	在启动实例时获取可用密钥对的列表。

操作	目的
"EC2： 描述性 " 、	获得可用 AWS 区域的列表。
"EC2： 删除标记 " 、 "EC2： 描述标记 " 、	管理与 Cloud Volumes ONTAP 实例关联的资源标签。
"CloudFormation： CreateStack"， "CloudFormation： DeleteStack"， "CloudFormation： Describe Stacks"， "CloudFormation： Describe StackEvents "， "CloudFormation： ValidateTemplate"，	启动 Cloud Volumes ONTAP 实例。
"IAM： PassRole"， "iam： CreateRole"， "iam： DeleteRole"， "iam： PutRolePolicy"， "iam： CreateInstanceProfile"， "IAM： DeleteRolePolicy"， "iam： AddRoleToInstanceProfile"， "iam： RemoveRoleFromInstanceProfile"， "iam： DeleteInstanceProfile"，	启动 Cloud Volumes ONTAP HA 配置。
"IAM： ListInstanceProfiles"， "STS： DecodeAuthorizationMessage"， "EC2： AssociateIamInstanceProfile"， "EC2： Describe IamInstanceProfileAssociations"， "EC2： DisassociateIamInstanceProfile"，	管理 Cloud Volumes ONTAP 实例的实例配置文件。
"S3： GetBucketTagging"， "S3： GetBucketLocation"， "S3： ListAllMyBuckets"， "S3： ListBucket"	获取有关 AWS S3 存储槽的信息、以便 Cloud Manager 可以与 NetApp Data Fabric Cloud Sync 服务集成。
"S3： CreateBucket"， "S3： DeleteBucket"， "S3： GetLifeycleConfiguration"， "S3： PutLifeycleConfiguration"， "S3： PutBucketTagging"， "S3： ListBucketVersions"， "S3： GetBucketPolicyStatus"， "S3： GetBucketPublicAccessBlock"， "S3： GetBucketAcl"， "S3： GetBucketPolicy"， "S3： PutBucketPublicAccessBlock"	管理 Cloud Volumes ONTAP 系统用作数据分层容量层的 S3 存储分段。
"kms： List*"， "kms： reencryption*"， "kms： dese*"， "kms： CreateGrant"，	使用 AWS 密钥管理服务（ KMS ）对 Cloud Volumes ONTAP 启用数据加密。
"CE： GetReservationUtilization"， "ce： GetDimensionValues"， "ce： GetCostAndUsage"， "ce： GetTags "	获取有关 Cloud Volumes ONTAP 的 AWS 成本数据。
"EC2： CreatePlacementGroup"， "EC2： DeletePlacementGroup"	在单个 AWS 可用性区域中部署 HA 配置时， Cloud Manager 会启动 AWS 分布式放置组中的两个 HA 节点和调解器。
"EC2： Describe 保留实例服务 "	Cloud Manager 在 Cloud Data sense 部署中使用权限来选择要使用的实例类型。
"EC2： CreateTags "， "EC2： DeleteTags "， "EC2： Describe Tags "， "tag： getResources"， "tag： getTagKeys"， "tag： getTagValues "， "tag： TagResources"， "tag： UnagResources"	用于使用 Cloud Manager 标记服务管理 AWS 资源上的标记。

操作	目的
"S3： DeleteBucket"， "S3： GetLifeycleConfiguration"， "S3： PutLifeycleConfiguration"， "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 会在您启用备份到 S3 服务时使用这些权限。
"EKS： ListClusters"， "EKS： Describe Cluster"， "iam： GetInstanceProfile"	用于发现 Amazon EKS 集群。

Azure 中连接器的所需权限

Cloud Manager 需要在云提供商中执行操作的权限。中包括这些权限 "NetApp 提供的策略"。您可能希望了解 Cloud Manager 使用这些权限执行的操作。

Cloud Manager Azure 策略包括 Cloud Manager 在 Azure 中部署和管理 Cloud Volumes ONTAP 所需的权限。

操作	目的
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"，	创建 Cloud Volumes ONTAP 并停止、启动、删除和获取系统状态。
"Microsoft.compute/images/write"、 "Microsoft.compute/images/read"、	支持从 VHD 部署 Cloud Volumes ONTAP 。
Microsoft.Compute/disks/delete"， Microsoft.Compute/disks/read"， Microsoft.Compute/disks/write"， "microsoft.Storage/SchecknameAvailability /Read"， "microsoft.Storage/operations/Read"， "microsoft.Storage/storageAccounts"， "microsoft.Storage/storageAccouns/Read"， "microsoft.Storage/storageAccounts"， "microsoft.Storage/storageAccounts"， "microsoft.Storage/storageAccounts"， "microsoft.Storage/Acces/ Read"，	管理 Azure 存储帐户和磁盘、并将磁盘连接到 Cloud Volumes ONTAP 。

操作	目的
"microsoft.Storage/storageAccounts/blobServices/contains/read"， "microsoft.KeyVault/vauls/read"，"microsoft.KeyVault/vauls/accessPolicies/write"	可备份到 Azure Blob 存储并对存储帐户进行加密
"microsoft.network/networkinterfaces/read"、"microsoft.network/networkinterfaces/write"、"microsoft.network/networkinterfaces/join/action"、	在目标子网中为 Cloud Volumes ONTAP 创建和管理网络接口。
"microsoft.network/networksecuritygroups/read"、"microsoft.network/networksecuritygroups/write"、"microsoft.network/networksecuritygroups/join/action"、	为 Cloud Volumes ONTAP 创建预定义的网络安全组。
"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"，	获取有关区域、目标 VNet 和子网的网络信息、并将 Cloud Volumes ONTAP 添加到 VNETS 。
Microsoft.Network/virtualNetworks/subnets/write"，Microsoft.Network/routeTables/join/action"，	启用 VNet 服务端点以进行数据分层。
"Microsoft.Resources/deployments/operations/read"、 "Microsoft.Resources/deployments/read"、"Microsoft.Resources/deployments/write"、	从模板部署 Cloud Volumes ONTAP 。
"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/write"，	为 Cloud Volumes ONTAP 创建和管理资源组。
Microsoft.Compute/snapshots/write"，Microsoft.Compute/snapshots/read"，Microsoft.Compute/snapshots/delete"，Microsoft.Compute/disks/beginGetAccess/action"，	创建和管理 Azure 管理的快照。
"microsoft.compute/availabilitysets/write"、"microsoft.compute/availabilitysets/read"、	创建和管理 Cloud Volumes ONTAP 的可用性集。

操作	目的
"Microsoft.Marketplac订购 / 服务类型 / 发布者 / 服务 / 计划 / 协议 / 读取 " 、 "Microsoft.Marketplac订购 / 服务类型 / 发布者 / 服务 / 计划 / 协议 / 写入 "	支持从 Azure Marketplace 进行编程部署。
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" ，	管理 HA 对的 Azure 负载平衡器。
"Microsoft.Authorization/Locks/*"	支持管理 Azure 磁盘上的锁定。
"microsoft.Authorization/roleDefinitions/write" ， "microsoft.Authorization/roleAssignments/write" ， "microsoft.Web/sites/*"	管理 HA 对的故障转移。
Microsoft.Network/privateEndpoints/write" ， "microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/Actions" ， "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" ，	用于管理私有端点。如果未向子网外部提供连接，则会使用私有端点。Cloud Manager 会为 HA 创建存储帐户，但子网中只有内部连接。
" Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete" ，	允许 Cloud Manager 删除 Azure NetApp Files 的卷。
"microsoft.resources/deployments/operationStatuss/Read"	Azure 在某些虚拟机部署中需要此权限（取决于部署期间使用的底层物理硬件）。

操作	目的
"microsoft.resources/deployments/operationStatuss/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" ，	用于使用全局文件缓存。
Microsoft.Network/privateEndpoints/delete" ， Microsoft.Compute/availabilitySets/delete" ，	允许 Cloud Manager 在部署失败或删除时从属于 Cloud Volumes ONTAP 的资源组中删除资源。
Microsoft.Compute/diskEncryptionSets/read" Microsoft.Compute/diskEncryptionSets/write" ， Microsoft.Compute/diskEncryptionSets/delete" "microsoft.KeyVault/vauls/deploy/action" ， "microsoft.KeyVault/vauls/read" ， "microsoft.KeyVault/vauls/accessPolicies/write" ，	支持将客户管理的加密密钥与 Cloud Volumes ONTAP 结合使用。使用 API 支持此功能。
"microsoft.resources/tags /read" ， "microsoft.resources/tags /write" ， "microsoft.resources/tags /delete"	用于使用 Cloud Manager 标记服务管理 Azure 资源上的标记。
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"	通过 Cloud Manager 可以为 HA 对配置应用程序安全组，从而隔离 HA 互连和集群网络 NIC 。

Google Cloud 中连接器的所需权限

Cloud Manager 需要在云提供商中执行操作的权限。中包括这些权限 "NetApp 提供的策略"。您可能希望了解 Cloud Manager 使用这些权限执行的操作。

适用于 GCP 的 Cloud Manager 策略包括 Cloud Manager 部署和管理 Cloud Volumes ONTAP 所需的权限。

操作	目的
— compute.disks.create — compute.disks.createSnapshot — compute.disks.delete — compute.disks.get — compute.disks.list — compute.disks.setLabels — compute.disks.use	为 Cloud Volumes ONTAP 创建和管理磁盘。

操作	目的
— compute.v防火墙 创建— compute.firewalls.delete — compute.v防火墙 .get — compute.v防火墙 列表	为 Cloud Volumes ONTAP 创建防火墙规则。
— compute.globalOperations.get	以获取操作状态。
— compute.images.get — compute.images.getFromFamily — compute.images.list — compute.images.useReadOnly	为 VM 实例获取映像。
— compute.instances.attachDisk — compute.instances.detachDisk	将磁盘连接和断开与 Cloud Volumes ONTAP 的连接。
— compute.instances.create — compute.instances.delete	创建和删除 Cloud Volumes ONTAP VM 实例。
— compute.instances.get	列出 VM 实例。
— compute.instances.getSerialPortOutput	以获取控制台日志。
— compute.instances.list	检索区域中实例的列表。
— compute.instances.setDeletionProtection	为实例设置删除保护。
— compute.instances.setLabels	以添加标签。
— compute.instances.setMachineType — compute.instances.setMinCpuPlatform	更改 Cloud Volumes ONTAP 的计算机类型。
— compute.instances.setMetadata	以添加元数据。
— compute.instances.setTags	为防火墙规则添加标记。
— compute.instances.start — compute.instances.stop — compute.instances.updateDisplayDevice	启动和停止 Cloud Volumes ONTAP 。
— compute.machineTypes.get	获取要检查 qoutas 的核心数。
— compute.projects.get	以支持多个项目。
— compute.snapshots.create — compute.snapshots.delete — compute.snapshots.get — compute.snapshots.list — compute.snapshots.setLabels	创建和管理永久性磁盘快照。
— 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	获取创建新 Cloud Volumes ONTAP 虚拟机实例所需的网络信息。

操作	目的
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifes.get - deploymentmanager.manifes.list - deploymentmanager.operations.get - deploymentmanager.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProvider.get - deploymentmanager.typeProvider.get - deploymentmanager.typeProvider.list - get	使用 Google Cloud 部署管理器部署 Cloud Volumes ONTAP 虚拟机实例。
— logging.logEnrees.list — logging.privateLogEnrees.list	获取堆栈日志驱动器。
— resourcemanager.projects.get	以支持多个项目。
— storage.buctions.create — storage.buckets.delete — storage.buctions.get — storage.buctions.list — storage.buctions.update	创建和管理用于数据分层的 Google Cloud Storage 存储分段。
— cloudkms.cryptoKeyVersions.useToEncrypt — cloudkms.encryptoKeys.get — cloudkms.encryptoKeys.list — cloudkms.keyrings.list	将云密钥管理服务中由客户管理的加密密钥与 Cloud Volumes ONTAP 结合使用。
— compute.instances.setServiceAccount — iam.serviceAccounts.actAs — iam.serviceAccounts.getIamPolicy — iam.serviceAccounts.list — storage.objects.get — storage.objects.list	在 Cloud Volumes ONTAP 实例上设置服务帐户。此服务帐户提供将数据分层到 Google Cloud Storage 存储分段的权限。
— compute.addresses … list — compute.backendServices.create — compute.networks.updatePolicy — compute.regionBackendServices.create — compute.regionBackendServices.get — compute.regionBackendServices.list	部署 HA 对。
— compute.subnetworks.use — compute.subnetworks.useExternalIp — compute.instances.addAccessConfig	启用 Cloud Data sense 。
— container.clusters 。 get — container.clusters 。 list	发现在 Google Kubernetes Engine 中运行的 Kubernetes 集群。