Cloud Manager でクラウドプロバイダの権限が使用される仕組み

Cloud Manager

Ben Cammett, Aksel Davis
May 31, 2021

目次

Cloud Manager でクラウドプロバイダの権限が使用される仕組み

Cloud Manager からクラウドプロバイダの処理を実行するには権限が必要です。これらの権限はに含まれています "ネットアップが提供するポリシー"。このような権限を持つ Cloud Manager の機能を理解しておく必要があるかもしれません。

Cloud Manager が AWS 権限を使用して実行する処理

Cloud Manager は AWS アカウントを使用して、 EC2 、 S3 、 CloudFormation 、 IAM 、 Security Token Service （ STS ）、 Key Management Service （ KMS ）などの複数の AWS サービスへの API コールを行います。

アクション	目的
"EC2:StartInstances" 、 "EC2:StopInstances" 、 "EC2:DescribeInstances" 、 "EC2:DescribeInstanceStatus" 、 "EC2:RunInstances" 、 "EC2:TerminateInstances" 、 "EC2:ModifyInstanceAttribute" 、	Cloud Volumes ONTAP インスタンスを起動し、インスタンスを停止、開始、監視します。
"EC2: DescribeInstanceAttribute" 、	サポートされているインスタンスタイプで Enhanced Networking が有効になっていることを確認します。
「 EC2 ：説明文」、「 EC2 ：説明文」、	Cloud Volumes ONTAP HA 構成を起動します。
EC2 ： createTags 、	Cloud Manager が作成するすべてのリソースに「 workingEnvironment 」タグと「 workingEnvironmId 」タグを付けます。Cloud Manager では、これらのタグを使用してメンテナンスとコスト割り当てを行います。
"EC2:CreateVolume" 、 "EC2:DescribeVolumes" 、 "EC2:ModifyVolumeAttribute" 、 "EC2:AttachVolume" 、 "EC2:DeleteVolume" 、 "EC2:DetachVolume" 、	Cloud Volumes ONTAP がバックエンドストレージとして使用する EBS ボリュームを管理します。
"EC2:CreateSecurityGroup" 、 "EC2:DeleteSecurityGroup" 、 "EC2:RevokeSecurityGroupEgress " 、 "EC2:AuthorizeSecurityGroupEgress " 、 "EC2:RevokeSecurityGroupIngress " 、 "EC2:RevokeSecurityGroupIngress " 、	Cloud Volumes ONTAP 用の定義済みセキュリティグループを作成します。
"EC2:CreateNetworkInterface", "EC2:DescribeNetworkInterfaces ", "EC2:DeleteNetworkInterface", "EC2:ModifyNetworkInterfaceAttribute",	ターゲットサブネット内の Cloud Volumes ONTAP のネットワークインターフェイスを作成および管理します。
「 EC2 ：説明サブネット」、「 EC2 ：説明 VPC 」、	Cloud Volumes ONTAP 用の新しい作業環境を作成するときに必要な、デスティネーションサブネットとセキュリティグループのリストを取得します。
EC2 ： DescribeDHCPOptions	Cloud Volumes ONTAP インスタンスの起動時に DNS サーバとデフォルトのドメイン名を決定します。

アクション	目的
「 EC2 ： CreateSnapshot 」、「 EC2 ： DeleteSnapshot 」、「 EC2 ： DescribeSnapshot 」、	初期セットアップ時、および Cloud Volumes ONTAP インスタンスが停止したときに、 EBS ボリュームのスナップショットを作成します。
"EC2:GetConsoleOutput" 、	AutoSupport メッセージに添付された Cloud Volumes ONTAP コンソールをキャプチャします。
「 EC2 ：説明キーペア」、	インスタンスの起動時に使用可能なキーペアのリストを取得します。
「 EC2 ：説明論」、	使用可能な AWS リージョンのリストを取得します。
EC2 ： DeleteTags 、 EC2 ： DescribeTags 、	Cloud Volumes ONTAP インスタンスに関連付けられたリソースのタグを管理します。
CloudFormation ： CreateStack 」、「 CloudFormation ： DeleteStack 」、「 CloudFormation ： DescribeStack 」、「 CloudFormation ： DescribeStackEvents 」、「 CloudFormation ： ValidateTemplate 」、	Cloud Volumes ONTAP インスタンスを起動します。
"iam ： PassRole" 、 "iam ： CREATEROLE" 、 "iam ： PutRolePolicy " 、 "iam ： CreateInstanceProfile" 、 "iam ： DeleteRolePolicy " 、 "iam ： AddRoleToInstanceProfile" 、 "IAM ： RemoveRoleInstanceFromProfile" 、 "iam ： DeleteInstanceProfile" 、 "iam ： DeleteInstanceProfile	Cloud Volumes ONTAP HA 構成を起動します。
"IAM:ListInstanceProfiles" 、 "STS: DecodeAuthorizationMessage" 、 "EC2:AssociateIamInstanceProfile" 、 "EC2:DescribeIamInstanceProfileAssociations" 、 "EC2:DisassociateIamInstanceProfileProfile" 、	Cloud Volumes ONTAP インスタンスのインスタンスプロファイルを管理します。
「 s3 ： GetBucketTagging 」、「 s3 ： GetBucketLocation 」、「 s3 ： ListAllMyBuckets 」、「 s3 ： ListBucket 」	AWS S3 バケットに関する情報を取得して、 Cloud Manager を NetApp Data Fabric Cloud Sync サービスと統合できるようにします。
s3 ： CreateBucket 、 s3 ： DeleteBucket 、 s3 ： GetLifecycleConfiguration 、 s3 ： PutBucketTagging 、 s3 ： ListBucketVersions 、 s3 ： GetBucketPolicyStatus 、 s3 ： GetBucketPublicAccessBlock 、 s3 ： GetBucketAccessBlock 、 GetBucketAccessBlock	Cloud Volumes ONTAP システムでデータ階層として使用する S3 バケットを管理します。
"kms ：リスト * " 、 "kms ：再暗号化 * " 、 "kms ： DESCRIBE * " 、 "kms ： CreateGrant" 、	AWS Key Management Service （ KMS ；キー管理サービス）を使用した Cloud Volumes ONTAP のデータ暗号化を有効にします。
"CE:GetReservationUtilization" 、 "CE:GetDimensionValues" 、 "CE:GetCostAndUsage", "CE:GetTags"	Cloud Volumes ONTAP の AWS コストデータを取得します。

アクション	目的
"EC2:CreatePlacementGroup" 、 "EC2:DeletePlacementGroup"	単一の AWS アベイラビリティゾーンに HA 構成を導入すると、 Cloud Manager は 2 つの HA ノードと AWS 分散配置グループ内のメディエーターを起動します。
EC2: DescribeReservedInstancesOffers (英語)	Cloud Manager は、 Cloud Compliance の導入の一環としてこの権限を使用して、使用するインスタンスタイプを選択します。
「 s3 ： DeleteBucket 」、「 s3 ： GetLifecycleConfiguration 」、「 s3 ： PutBucketLifeConfiguration 」、「 s3 ： PutBucketTagging 」、「 s3 ： ListBucketVersions 」、「 s3 ： ListBucket 」、「 s3 ： ListAllMyBuckets 」、「 s3 ： GetBucketAccessBuckets3 ： GetBucketAccessBuckets3 、 GetBucketAccessBuckets3 ： GetBucketAccessBlock	Cloud Manager では、 S3 へのバックアップサービスを有効にする際にこれらの権限を使用します。

クラウドマネージャーが **Azure** の権限で行うこと

Cloud Manager Azure ポリシーには、 Cloud Manager が Azure で Cloud Volumes ONTAP を導入および管理するために必要な権限が含まれています。

アクション	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" 」、	Cloud Volumes ONTAP を作成し、システムのステータスを停止、開始、削除、取得します。
「 microsoft.compute/images/write 」、「 microsoft.compute/images/read 」、	VHD から Cloud Volumes ONTAP を導入できます。

アクション	目的
Microsoft.Compute/disks/delete" 、 Microsoft.Compute/disks/read" 、 Microsoft.Compute/disks/write" 、 "Microsoft.Storage/checknameavailability/read" 、 "Microsoft.Storage/operations/read" 、 "microsoft.StorageAccounts/listkeyss/action" 、 "microsoft.Storage/storageAccounts/read" 、 "microsoft.Storage/regenerateAccounts/action" 、 "Microsoft.Storage/storageAccounts/action" 、 "/writeStorageAccounts" 、 "/StorageAccounts/StorageAccounts/write/StorageAccounts" 、 ","Microsoft 。	Azure ストレージアカウントとディスクを管理し、ディスクを Cloud Volumes ONTAP に接続します。
「 microsoft.network/networkinterfaces/read 」、「 microsoft.network/networkinterfaces/write 」、「 microsoft.network/networkinterfaces/join/action 」、	ターゲットサブネット内の Cloud Volumes ONTAP のネットワークインターフェイスを作成および管理します。
「 microsoft.network/networksecuritygroups/read 」、「 microsoft.network/networksecuritygroups/write 」、「 microsoft.network/networksecuritygroups/join/action 」、	Cloud Volumes ONTAP 用の定義済みネットワークセキュリティグループを作成します。
「 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" 」、	リージョン、ターゲット VNet 、およびサブネットに関するネットワーク情報を取得し、 vnet に Cloud Volumes ONTAP を追加します。
「 Microsoft.Network/virtualNetworks/subnets/write" 」、 Microsoft.Network/routeTables/join/action" 、	データ階層化のための VNet サービスエンドポイントを有効にします。
「 Microsoft.Resources/Deployments/Operations/Read 」、「 Microsoft.Resources/Deployments/Read 」、「 Microsoft.Resources/Deployments/Write 」、	テンプレートから Cloud Volumes ONTAP を導入します。

アクション	目的
"microsoft.Resources/Deployments/operations/read" 、 "microsoft.Resources/Deployments/read" 、 "microsoft.Resources/resources/read" 、 "microsoft.resources/resources/operationresults/read" 、 "microsoft.resources/Subscriptions /resourceGroups/delete" 、 "microsoft.resources/Subscriptions /resources/groups/resources/resources/reads/resources/resources/resources/resources/resources/resources/resources/resources/reading" 、 ","," ","resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/groups/	Cloud Volumes ONTAP のリソースグループを作成および管理します。
「 Microsoft.Compute/snapshots/write" 」、「 Microsoft.Compute/snapshots/read" 」、「 Microsoft.Compute/snapshots/delete" 」、「 Microsoft.Compute/disks/beginGetAccess/action" 」、	Azure マネージドスナップショットを作成および管理します。
"microsoft.compute/availabilitySets/write", "microsoft.compute/availabilitySets/read",	Cloud Volumes ONTAP の可用性セットを作成および管理します。
"Microsoft.MarketplaceOrdering/Offered Types/publishers/capers/plans/agreements/read" 、 "Microsoft.MarketplaceOrdering / offerTypes/publishers/capes/plans/agreements/write"	Azure Marketplace からのプログラムによる展開を可能にします。
「 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" 」	HA ペアの Azure ロードバランサを管理します。
"Microsoft 許可 / ロック /*"	Azure ディスクのロックの管理を有効にします。
"Microsoft.Authorization/roleDefinites/write" 、 "Microsoft.Authorization/rolrolわり あて /write" 、 "Microsoft.Web/sites/*"	HA ペアのフェイルオーバーを管理します。

アクション	目的
「 Microsoft.Network/privateEndpoints/write" 」、「 Microsoft.StorageAccounts/PrivateEndpointConnectionsApproval/action 」、「 microsoft.Storage/storageAccounts/privateEndpointConnections/read 」、「 Microsoft.Network/privateEndpoints/read" 」、「 Microsoft.Network/privateDnsZones/write" 」、「 Microsoft.Network/privateDnsZones/virtualNetworkLinks/write" 」、「 Microsoft.Network/privateDnsZones/A/write" 」、「 Microsoft.Network/privateDnsZones/virtualNetworkLinks/read" 」、「 Microsoft.Network/privateDnsZones/read" 」、「 Microsoft.Network/virtualNetworks/join/action" 」、「 」、「 」、「 」	プライベートエンドポイントの管理をイネーブルにします。プライベートエンドポイントは、サブネットの外部への接続が提供されない場合に使用されます。Cloud Manager は、サブネット内で内部接続のみを使用して HA 用のストレージアカウントを作成します。
" Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete" 、	Azure NetApp Files のボリュームを Cloud Manager で削除できます。
"microsoft.Resources/Deployments/operationStatuses/read"	Azure では、一部の仮想マシン環境に対してこの権限が必要です（導入時に使用する基盤となる物理ハードウェアによって異なります）。
"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" 、	グローバルファイルキャッシュを使用できます。
「 Microsoft.Compute/diskEncryptionSets/read"	Cloud Manager で、別のアカウントの外部キーを使用してシングルノード Cloud Volumes ONTAP システムの Azure 管理ディスクを暗号化できます。この機能は API を使用してサポートされます。

Cloud Manager が GCP 権限を使用して実行する処理

GCP の Cloud Manager ポリシーには、 Cloud Volumes ONTAP の導入と管理に Cloud Manager が必要とする権限が含まれています。

アクション	目的
-compute.disks .create -computedisks .createsnapshot - compute.disks.delete -computedisks .get-compute.diskList - compute.disks.setLabels - compute.disks.us	Cloud Volumes ONTAP 用のディスクを作成および管理します。

アクション	目的
-compute-firewalls .create - compute.firewalls.delete -comput領域 .firewalls .get-comput領域 .firewalls リスト	Cloud Volumes ONTAP のファイアウォールルールを作成します。
-computer.globalOperationsGet	処理のステータスを確認できます。
-compute.image.get-compute.image.getFromFamily -compute.image.list - compute.images.useReadOnly	VM インスタンスのイメージを取得します。
- compute.instances.attachDisk - compute.instances.detachDisk	ディスクを Cloud Volumes ONTAP に接続して接続解除します。
- compute.instances.create - compute.instances.delete	Cloud Volumes ONTAP VM インスタンスを作成および削除します。
- compute.instances.get	VM インスタンスを一覧表示します。
- compute.instances.getSerialPortOutput	をクリックしてコンソールログを取得してください
- compute.instances.list	ゾーン内のインスタンスのリストを取得します。
- compute.instances.setDeletionProtection	インスタンスに削除保護を設定します。
- compute.instances.setLabels	ラベルを追加します。
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	Cloud Volumes ONTAP のマシンタイプを変更します。
- compute.instances.setMetadata	をクリックしてください。
- compute.instances.setTags	ファイアウォールルールのタグを追加します。
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Cloud Volumes ONTAP を開始および停止します。
-computesCompute .machineTypes.get	コア数を取得して qoutas をチェックしてください。
- compute.projects.get	複数のプロジェクトをサポートするため。
-compute-snapshots-create - compute.snapshots.delete -compute-snapshots -getCompute-snapshots-list - compute.snapshots.setLabels	永続ディスクスナップショットを作成および管理するには、次の手順に従います。
- compute.networks.get - compute.networks.list - comput.regions.Get-comput領域 .list-comput領域 .subnetworks -compute.subnetworks .listCompute.zoneOperations-get-compute.zones .get-compute.zones リスト	新しい Cloud Volumes ONTAP 仮想マシンインスタンスの作成に必要なネットワーク情報を取得するため。

アクション	目的
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list -deploymentmanager. マニフェスト .get-deploymentmanager. マニフェスト .list-list-deploymentmanager. operations-get-deploymentmanager. operationlist -deploymentmanager. resources.get-deploymentmanager. resources.list-deploymentmanager. typeProviders.get-deploymentmanager. typeProviders.list-deploymentmanager. -deploymentmanager. types] リスト	Google Cloud Deployment Manager を使用して Cloud Volumes ONTAP 仮想マシンインスタンスを導入します。
-logging.logEntries.list-logging.privateLogEntries.list	スタックログドライブを取得する方法
- resourcemanager.projects.get	複数のプロジェクトをサポートするため。
-storag/バケット 。 create - storage.buckets.delete -storag/バケット .get-storag/バケット .list-storag/バケット .buckets-update	Google Cloud Storage バケットを作成して管理し、データを階層化します。
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms .cryptoKeys.get-cloudkms .cryptoKeys.list-cloudkm.keyringlist.list	Cloud Volumes ONTAP でクラウドキー管理サービスからお客様が管理する暗号化キーを使用するため。
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - storage.objects-get -storage.objectlist	Cloud Volumes ONTAP インスタンスにサービスアカウントを設定します。このサービスアカウントは、Google Cloud Storage バケットへのデータ階層化の権限を提供します。
-compute.address.listCompute.backendServices. create -compute.networks.updatePolicy -compute.regionBackendServices.create -compute.regionBackendServices.get -compute.regionBackendServices.list	をクリックしてください。