



參考資料

Set up and administration

NetApp

May 04, 2022

目錄

參考資料	1
AWS中Connector的必要權限	1
Azure中Connector的必要權限	3
Google Cloud中Connector的必要權限	6

參考資料

AWS中Connector的必要權限

Cloud Manager 需要權限、才能在雲端供應商中執行動作。這些權限包含在中 ["NetApp 提供的原則"](#)。您可能想要瞭解 Cloud Manager 使用這些權限的功能。

Cloud Manager 使用 AWS 帳戶來撥打 API 呼叫數項 AWS 服務、包括 EC2 、 S3 、 CloudFormation 、 IAM 、 安全性權杖服務 (STS) 和金鑰管理服務 (KMS) 。

行動	目的
"EC2 : StartInstances" 、 "EC2 : 停止 Instances" 、 "EC2 : 說明資訊 " 、 "EC2 : 說明資訊狀態 " 、 "EC2 : 執行資訊 " 、 "EC2 : 終端實例 " 、 "EC2 : 修改實例屬性 " 、	啟動 Cloud Volumes ONTAP 一個執行個體、並停止、啟動及監控執行個體。
"EC2 : 取消訂閱實例屬性 " 、	驗證是否已針對支援的執行個體類型啟用增強式網路功能。
"EC2 : 取消航線表 " 、 "EC2 : 取消航線影像 " 、	啟動 Cloud Volumes ONTAP 功能不只是功能不一的 HA 組態。
"EC2 : 建立標記 " 、	標記 Cloud Manager 所建立的每個資源、並加上「 WorkingEnvironment 」和「 WorkingEnvironment Id 」標記。Cloud Manager 會使用這些標籤來進行維護和成本分配。
"EC2 : 建立磁碟區 " 、 "EC2 : 指定磁碟區 " 、 "EC2 : 修改磁碟區屬性 " 、 "EC2 : 附加磁碟區 " 、 "EC2 : 刪除磁碟區 " 、 "EC2 : 分離磁碟區 " 、	管理 Cloud Volumes ONTAP EBS 磁碟區、這些磁碟區可作為後端儲存設備使用。
EC2 : CreateSecurity Group 、 「 EC2 : 刪除安全性群組」 、 「 EC2 : 取消安全性群組」 、 「 EC2 : 重新執行安全性群組 Egress 」 、 「 EC2 : 授權安全性群組 Egress 」 、 "EC2 : AuthorizeSecurity GroupIngress" 、 "EC2 : RevokeSecurity GroupIngress" 、	建立預先定義 Cloud Volumes ONTAP 的安全性群組以供使用。
"EC2 : 建立網路介面 " 、 "EC2 : 指定網路介面 " 、 "EC2 : 刪除網路介面 " 、 "EC2 : 修改網路介面屬性 " 、	建立並管理 Cloud Volumes ONTAP 目標子網路中的網路介面以供其使用。
"EC2 : 取消訂閱子網路 " 、 "EC2 : 取消訂閱 Vpcs" 、	取得目的地子網路和安全群組的清單、這是建立 Cloud Volumes ONTAP 新的功能環境時所需的。
"EC2 : 脫色器 DhcpOptions " 、	在啟動 Cloud Volumes ONTAP Instance 執行個體時、決定 DNS 伺服器 and 預設網域名稱。
"EC2 : 建立 Snapshot " 、 "EC2 : 刪除 Snapshot " 、 "EC2 : 取消快照 " 、	在初始設定期間及 Cloud Volumes ONTAP 停止執行個體時、都會擷取 EBS Volume 的快照。
"EC2 : GetConsole 輸出 " 、	擷取 Cloud Volumes ONTAP 附加於 AutoSupport 不檢訊息的功能。
「 EC2 : 免持鑰匙會議」 、	在啟動執行個體時取得可用的金鑰配對清單。

行動	目的
"EC2：取消註冊"、	取得可用 AWS 區域的清單。
"EC2：刪除標記"、"EC2：取消標記"、	管理 Cloud Volumes ONTAP 與實例有關的資源標記。
「雲端形成：建立堆疊」、「雲端形成：刪除堆疊」、「雲端形成：取消堆疊」、「雲端形成：雲端堆疊」、「雲端形成：取消堆疊事件」、「雲端形成：驗證範本」、	啟動 Cloud Volumes ONTAP 執行個體。
「IAM：PassRole」、「iam：CreeRole」、「iam：Delete 角色」、「iam：PuttrolePolicy」、「iam：CrestanceProfile」、「IAM：刪除角色原則」、「iam：AddRoleToInstanceProfile」、「iam：RemoveRoleFromInstanceProfile」、「iam：刪除實例設定檔」、	啟動 Cloud Volumes ONTAP 功能不只是功能不一的 HA 組態。
「IAM：清單實例設定檔」、「STS:DecodeAuthorizationMessage」、「EC2：Associate IamInstanceProfile」、「EC2：說明程式碼產生關聯性關聯性」、「EC2：關聯性 IamInstanceProfile」、	管理 Cloud Volumes ONTAP 執行個體的執行個體設定檔。
「S3：GetBucketTagging」、「S3：GetBucketLocation」、「S3：ListAllMyBucket」、「S3：清單 Bucket」	取得 AWS S3 儲存區的相關資訊、讓 Cloud Manager 能夠與 NetApp Data Fabric Cloud Sync 的功能整合。
「S3：建立 Bucket」、「S3：刪除 Bucket」、「S3：GetLifecycleConfiguration」、「S3：PuttlifecycleConfiguration」、「S3：PuttBucketting 標記」、「S3：listBucketVerions」、「S3：GetBucketPolicyStatus」、「S3：GetBucketPublicAccessBlock」、「S3：GetBucketAcl」、「S3：GetBucketPolicy」、「S3：PuttBucketPublicAccessBlock」	管理 Cloud Volumes ONTAP 作為資料分層容量層的 S3 儲存區。
「kms：List *」、「kms：ReEncrypt *」、「kms：vesk *」、「kms：Create Grant」、	使用 Cloud Volumes ONTAP AWS 金鑰管理服務（KMS）啟用資料加密功能。
"CE:GetReservationUtilization"、 "CE:GetDimensionValues"、"CE:GetCostAndusage"、 "CE:GetTags"	取得 AWS 成本資料 Cloud Volumes ONTAP 以供使用。
"EC2：建立位置群組"、"EC2：刪除位置群組"	當您在單一 AWS 可用性區域中部署 HA 組態時、Cloud Manager 會在 AWS 分散配置群組中啟動兩個 HA 節點和中介器。
「EC2：取消訂閱保留服務」	Cloud Manager將權限作為Cloud Data Sense部署的一部分、用於選擇要使用的執行個體類型。
"EC2：建立標記"、"EC2：刪除標記"、"EC2：取消標記"、 "tag:getResources"、"tag:getTagKeys"、 「標記：getTagValues」、「標記：TagResources」、「標記：UntagResources」	可讓您使用Cloud Manager標記服務來管理AWS資源上的標記。

行動	目的
「 S3 : 刪除 Bucket 」、「 S3 : GetLifecycleConfiguration 」、「 S3 : PutLifecycleConfiguration 」、「 S3 : PutObject 」、「 S3 : listBucketVersions 」、「 S3 : GetObject 」、「 S3 : 清單桶 」、「 S3 : 清單 AllMyBucket 」、「 S3 : GetBucketTagging 」、「 S3 : GetBucketLocation 」、「 S3 : GetBucketPolicyStatus 」、「 S3 : GetBucketPublicAccessBlock 」、「 S3 : GetBucketAcl 」、「 S3 : GetBucketPolicy 」、「 S3 : PutBucketPublicAccessBlock 」	啟用「備份到 S3」服務時、Cloud Manager 會使用這些權限。
"EKS: listClusters"、"EKS: DescribeCluster"、"iam: GetInstanceProfile"、	可探索 Amazon EKS 叢集。
"EC2: 取消程序位置群組"、"iam: GetPolicy"、	為部署在單一可用度區域 (AZ) 的 HA 配對建立 AWS 分散配置群組。

Azure 中 Connector 的必要權限

Cloud Manager 需要權限、才能在雲端供應商中執行動作。這些權限包含在中 ["NetApp 提供的原則"](#)。您可能想要瞭解 Cloud Manager 使用這些權限的功能。

Cloud Manager Azure 原則包含 Cloud Manager 在 Cloud Volumes ONTAP Azure 中部署及管理功能所需的權限。

行動	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"、	建立 Cloud Volumes ONTAP 不同時停止、啟動、刪除及取得系統狀態。
「 Microsoft.Compute/images/write"、 Microsoft.Compute/images/read"、	可 Cloud Volumes ONTAP 從 VHD 進行支援功能性部署。

行動	目的
Microsoft.Compute/disks/delete" 、 "Microsoft.Compute/disks/read" 、 "Microsoft.Compute/disks/write" 、 "microsoft.Storage/checkamed可用度 / 讀取 " 、 "microsoft.Storage/operations / 讀取 " 、 "Microsoft.Storage/storageAccounts/listkeys/action" 、 "Microsoft.Storage/storageAccounts/read" 、 "Microsoft.Storage/storageAccounts/再生金鑰 / 行動 " 、 "Microsoft.Storage/storageAccounts/write" 、 "Microsoft.Storage/storageAccounts/storageAccounts/delete" 、 "Microsoft.Storage/改用 / 讀取 " 、	管理 Azure 儲存帳戶和磁碟、並將磁碟附加 Cloud Volumes ONTAP 至
"Microsoft.Storage/storageAccounts/blobServices/containers/read" 、 "Microsoft.KeyVault/Vaults/read" 、 "Microsoft.KeyVault/Vaults/accessPolicies/write"	可備份至 Azure Blob 儲存設備、並加密儲存帳戶
"Microsoft.Network/networkInterfaces/read" 、 "Microsoft.Network/networkInterfaces/write" 、 "Microsoft.Network/networkInterfaces/join/action" 、	建立並管理 Cloud Volumes ONTAP 目標子網路中的網路介面以供其使用。
"Microsoft.Network/networkSecurityGroups/read" 、 "Microsoft.Network/networkSecurityGroups/write" 、 "Microsoft.Network/networkSecurityGroups/join/action" 、	建立預先定義 Cloud Volumes ONTAP 的網路安全群組以供使用。
"Microsoft.Resources/訂購 / 位置 / 讀取 " 、 "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" 、	取得區域、目標 Vnet 和子網路的網路資訊、並將 Cloud Volumes ONTAP 之新增至 VNets 。
"Microsoft.Network/virtualNetworks/subnets/write" 、 "Microsoft.Network/routeTables/join/action" 、	啟用 vnet 服務端點以進行資料分層。
"microsoft.Resources/edges/operations / read" 、 "microsoft.Resources/edges/read" 、 "microsoft.Resources/edges/write" 、	從 Cloud Volumes ONTAP 範本部署功能。
"microsoft.Resources/edations/operations/read" 、 "microsoft.Resources/edations/read" 、 "microsoft.Resources/dations/read" 、 "microsoft.Resources/read" 、 "microsoft.Resources/dations/operations/read" 、 "Microsoft.Resources / 訂閱 / 資源群組 / 刪除 " 、 "Microsoft.Resources / 訂閱 / 資源群組 / 讀取 " 、 "Microsoft.Resources / 訂閱 / 資源群組 / 資源 / 讀取 " 、 "Microsoft.Resources / 訂閱 / 資源群組 / 寫入 " 、	建立及管理 Cloud Volumes ONTAP 資源群組以供參考。

行動	目的
「Microsoft.Compute/snapshots/write"、Microsoft.Compute/snapshots/read"、「Microsoft.Compute/snapshots/delete"、Microsoft.Compute/disks/beginGetAccess/action"、	建立及管理 Azure 託管快照。
「Microsoft.Compute/availabilitySets/write"、Microsoft.Compute/availabilitySets/read"、	建立及管理 Cloud Volumes ONTAP 可用度集以供使用。
"Microsoft.MarketplaceOrdnation/offersTypes / 出版商/服務/方案/協議/讀取" 、"Microsoft.MarketplaceOrdnations/offersTypes / 出版商/服務/計畫/協議/寫入"、	可從 Azure Marketplace 進程式化部署。
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 Azure 負載平衡器以供 HA 配對使用。
"Microsoft.Authorization/Locks/*、	可管理 Azure 磁碟上的鎖定。
"Microsoft.Authorization/RoleDefinitions/write (Microsoft 授權 / 角色指派 / 寫入) "、 "Microsoft.Web/sites/* (Microsoft 網站 / 網站 / *) "	管理 HA 配對的容錯移轉。
Microsoft.Network/privateEndpoints/write"、 "Microsoft.Storage/storageAccounts/privateEndpointConnectionsApproval / AC 巨集指令"、 "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"、	可管理私有端點。未將連線提供給子網路外部時、會使用私有端點。Cloud Manager 會為 HA 建立儲存帳戶、但僅在子網路內建立內部連線功能。
「 Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete"、	讓 Cloud Manager 能夠刪除 Volume 以 Azure NetApp Files 供使用。
"Microsoft.Resources / 部署 / 作業狀態 / 讀取 "	Azure 在某些虛擬機器部署中需要此權限（視部署期間所使用的基礎實體硬體而定）。

行動	目的
"microsoft.Resources/edges/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/edges/delete" 、	可讓您使用全域檔案快取。
「Microsoft.Network/privateEndpoints/delete" 、 Microsoft.Compute/availabilitySets/delete" 、	可讓Cloud Manager在Cloud Volumes ONTAP 部署失敗或刪除時、從屬於支援的資源群組移除資源。
Microsoft.Compute/diskEncryptionSets/read" 「Microsoft.Compute/diskEncryptionSets/write"」 、 「Microsoft.Compute/diskEncryptionSets/delete" "microsoft.KeyVault/Vaults/Deploy / action 」 、 「microsoft.KeyVault/Vaults/read」 、 「microsoft.KeyVault/Vaults/accesss/write」 、	可搭配Cloud Volumes ONTAP 使用客戶管理的加密金鑰。API 支援此功能。
"Microsoft.Resources/標記/讀取" 、 "Microsoft.Resources/標記/寫入" 、 "Microsoft.Resources/標記/刪除"	可讓您使用Cloud Manager標記服務來管理Azure資源上的標記。
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"	可讓Cloud Manager設定HA配對的應用程式安全群組、隔離HA互連和叢集網路NIC。

Google Cloud中Connector的必要權限

Cloud Manager 需要權限、才能在雲端供應商中執行動作。這些權限包含在中 ["NetApp 提供的原則"](#)。您可能想要瞭解 Cloud Manager 使用這些權限的功能。

適用於 GCP 的 Cloud Manager 原則包含 Cloud Manager 部署和管理 Cloud Volumes ONTAP 功能所需的權限。

行動	目的
- compute 、 disks.create - compute 、 disks.createSnapshot - compute.disks.delete - compute 、 disks.Get - compute 、 disks.list - compute.disks.setLabels - compute.disks.use	建立及管理 Cloud Volumes ONTAP 磁碟以供使用。
- compute 、 防火牆、 create - compute.firewalls.delete - compute 、 防火牆、 Get - compute 、 防火牆、 list	建立 Cloud Volumes ONTAP 防火牆規則以供使用。

行動	目的
運算： globalOperations 。 Get	以取得作業狀態。
- compiler.images.Get - compile.images.getFromFamily - compile.images.list - compute.images.useReadOnly	取得 VM 執行個體的映像。
- compute.instances.attachDisk - compute.instances.detachDisk	可將磁碟安裝到 Cloud Volumes ONTAP 實體上、並將其拆離。
- compute.instances.create - compute.instances.delete	建立及刪除 Cloud Volumes ONTAP 不顯示的 VM 執行個體。
- compute.instances.get	列出 VM 執行個體。
- compute.instances.getSerialPortOutput	以取得主控台記錄。
- compute.instances.list	可檢索區域中的實例列表。
- compute.instances.setDeletionProtection	設定執行個體的刪除保護。
- compute.instances.setLabels	以新增標籤。
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	變更 Cloud Volumes ONTAP 機器類型以供使用。
- compute.instances.setMetadata	新增中繼資料。
- compute.instances.setTags	新增防火牆規則的標記。
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	開始和停止 Cloud Volumes ONTAP 功能。
- compute 。 machineTypes 。 Get	取得要檢查 quotas 的核心數量。
- compute.projects.get	支援多個專案。
- compute 、 snapshots.create - compute.snapshots.delete - compute 、 snapshots.Get - compute 、 snapshots.list - compute.snapshots.setLabels	以建立及管理持續磁碟快照。
- compute.networks.get - compute.networks.list - compute .regions.Get - compute .regions.list - compute .subnetworks .Get - compute .subnetworks .list - compute .zonewores.Get - compute .zones.list	取得建立全新 Cloud Volumes ONTAP 的物件虛擬機器執行個體所需的網路資訊。

行動	目的
deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.in清單 - deploymentmanager.in 清單 - deploymentmanager.in清單 - deploymentmanager.operations - deploymentmanager.operations .list - deploymentmanager.sepaes.Get - deploymentmanager.operations - deploymentmanager.types.list - deploymentmanager.list	使用 Cloud Volumes ONTAP Google Cloud Deployment Manager 部署物件虛擬機器執行個體。
- logging.logEntries .list - logging.privateLogEntries .list	以取得堆疊記錄磁碟機。
- resourceManager.projects.get	支援多個專案。
- storage 、 buckets 、 create - storage.buckets.delete - storage 、 buckets 、 storage 、 buckets 、 list - storage 、 buckets 、 update	建立及管理 Google Cloud Storage 儲存庫以進行資料分層。
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.Get - cloudkms.cryptoKeys.list - cloudkms.keycycles.list	搭配 Cloud Volumes ONTAP 使用 Cloud Key Management Service 的客戶管理加密金鑰。
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - 儲存空間 .objects.Get - 儲存 空間 .objects.list	在 Cloud Volumes ONTAP 整個過程中設定服務帳戶。此服務帳戶提供資料分層至 Google Cloud Storage 儲存庫的權限。
- compute 、 addresses.list - compute 、 backendServices.create - compute.networks.updatePolicy - compute 、 Region. 、 BackendServices.create - compute 、 Region. 、 BackendServices.list	部署 HA 配對。
- compute.subnetworks.use - compute.subnetworks.useExternallp - compute.instances.addAccessConfig	以實現Cloud Data Sense。
- container 。叢集 。Get - container 。叢集 。清單	探索在Google Kubernetes Engine中執行的Kubernetes叢集。

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.