權限

Setup and administration

NetApp
April 26, 2024

目錄

權限

BlueXP的權限摘要

若要使用 BlueXP 功能和服務、您必須提供權限、讓 BlueXP 能夠在雲端環境中執行作業。使用此頁面上的連結、根據您的目標快速存取所需的權限。

AWS 權限

BlueXP 需要連接器和個別服務的 AWS 權限。

連接器

目標	說明	連結
從 BlueXP 部署 Connector	從BlueXP建立Connector的使用者需要特定權限、才能在AWS中部署執行個體。	"設定 AWS 權限"
提供 Connector 的權限	當BlueXP啟動Connector時、它會將原則附加至執行個體、以提供管理AWS帳戶中資源和處理程序所需的權限。 如果您是從 AWS Marketplace 啟動 Connector 、手動安裝 Connector 、或是您需要自行設定原則 "將更多AWS認證資料新增至Connector"。 您也必須確保在後續版本中新增權限時、原則保持在最新狀態。	"Connector的AWS權限"

備份與還原

目標	說明	連結
將內部部署 ONTAP 叢集備份至 Amazon S3	在 ONTAP 磁碟區上啟動備份時、 BlueXP 備份與還原會提示您為具有特定權限的 IAM 使用者輸入存取金鑰與密碼。	"設定 S3 備份權限"

Cloud Volumes ONTAP

目標	說明	連結
提供 Cloud Volumes ONTAP 節點的權限	必須將IAM角色附加至Cloud Volumes ONTAP AWS中的每個節點。HA中介者也是如此。預設選項是讓 BlueXP 為您建立 IAM 角色、但您可以在建立工作環境時使用自己的角色。	"瞭解如何自行設定IAM角色"

複製與同步

目標	說明	連結
在 AWS 中部署資料代理程式	您用來部署資料代理的 AWS 使用者帳戶必須具有特定權限。	"在 AWS 中部署資料代理程式所需的權限"

目標	說明	連結
提供資料代理程式的權限	當 BlueXP 複製與同步部署資料代理程式時、它會為資料代理程式執行個體建立 IAM 角色。您可以視需要使用自己的 IAM 角色來部署資料代理程式。	"將您自己的 IAM 角色用於 AWS 資料代理程式的要求"
為手動安裝的資料代理程式啟用 AWS 存取	如果您使用的資料代理程式具有包含 S3 儲存區的同步關係、則應準備 Linux 主機以供 AWS 存取。安裝資料代理程式時、您需要為具有程式化存取權和特定權限的 IAM 使用者提供 AWS 金鑰。	"可存取 AWS"

FSX ONTAP

目標	說明	連結
建立及管理 ONTAP 的 FSX	若要建立或管理適用於 NetApp ONTAP 工作環境的 Amazon FSX 、您需要將 AWS 認證新增至 BlueXP 、方法是提供 IAM 角色的 ARN 、讓 BlueXP 擁有建立工作環境所需的權限。	"瞭解如何設定適用於 FSX 的 AWS 認證"

分層

目標	說明	連結
將內部部署的 ONTAP 叢集分層至 Amazon S3	當您啟用 BlueXP 分層至 AWS 時、精靈會提示您輸入存取金鑰和秘密金鑰。這些認證資料會傳遞ONTAP 到S庫 叢集、ONTAP 以便讓S庫 將資料分層傳送到S3儲存庫。	"設定 S3 分層權限"

Azure權限

BlueXP 需要連接器和個別服務的 Azure 權限。

連接器

目標	說明	連結
從 BlueXP 部署 Connector	從BlueXP部署Connector時、您需要使用Azure帳戶或服務主體、該用戶必須具有在Azure中部署Connector VM的權限。	"設定 Azure 權限"
提供 Connector 的權限	當BlueXP在Azure中部署Connector VM時、它會建立自訂角色、提供必要的權限來管理該Azure訂閱中的資源和程序。 如果您是從市場啟動 Connector 、手動安裝 Connector 、或是您需要自行設定自訂角色 "將更多Azure認證資料新增至 Connector"。 您也必須確保在後續版本中新增權限時、原則保持在最新狀態。	"連接器的Azure權限"

複製與同步

目標	說明	連結
在 Azure 中部署資料代理程式	您用來部署資料代理的 Azure 使用者帳戶必須具有必要的權限。	"在Azure中部署資料代理程式所需的權限"

Google Cloud權限

BlueXP 需要 Google Cloud 權限才能使用 Connector 和個別服務。

連接器

目標	說明	連結
從 BlueXP 部署 Connector	從BlueXP部署Connector的Google Cloud使用者需要特定權限、才能在Google Cloud中部署Connector。	"設定建立 Connector 的權限"
提供 Connector 的權限	Connector VM執行個體的服務帳戶必須具有特定的日常作業權限。在部署期間、您需要將服務帳戶與 Connector 建立關聯。 您也必須確保在後續版本中新增權限時、原則保持在最新狀態。	"設定 Connector 的權限"

備份與還原

目標	說明	連結
備份Cloud Volumes ONTAP 到Google Cloud	使用 BlueXP 備份與還原來備份 Cloud Volumes ONTAP 時、您需要在下列案例中新增 Connector 的權限： • 您想要使用「搜尋與還原」功能 • 您想要使用客戶管理的加密金鑰（CMEK）	• "搜尋擴大機的權限；還原功能" • "CMEK 的權限"
將內部部署的 ONTAP 叢集備份至 Google Cloud	使用 BlueXP 備份與還原備份內部部署 ONTAP 叢集時、您需要新增 Connector 的權限、才能使用「搜尋與還原」功能。	"搜尋擴大機的權限；還原功能"

適用於 **Google Cloud Cloud Volumes Service**

目標	說明	連結
探索 Cloud Volumes Service for Google Cloud	BlueXP需要透過Cloud Volumes Service Google Cloud服務帳戶存取功能、以及適當的權限。	"設定服務帳戶"

複製與同步

目標	說明	連結
在 Google Cloud 中部署資料代理程式	確保部署資料代理程式的 Google Cloud 使用者擁有必要的權限。	"在Google Cloud中部署資料代理商所需的權限"

目標	說明	連結
為手動安裝的資料代理程式啟用 Google Cloud 存取	如果您計畫使用資料代理商的同步關係、包括Google Cloud Storage儲存庫、則應準備Linux主機以進行Google Cloud存取。安裝資料代理程式時、您必須提供具有特定權限的服務帳戶金鑰。	"可存取 Google Cloud"

StorageGRID 權限

BlueXP 需要兩項服務的 StorageGRID 權限。

備份與還原

目標	說明	連結
將內部部署 ONTAP 叢集備份至 StorageGRID	當您準備將 StorageGRID 做為 ONTAP 叢集的備份目標時、BlueXP 備份與還原會提示您輸入具有特定權限的 IAM 使用者的存取金鑰和密碼。	"準備 StorageGRID 做為備份目標"

分層

目標	說明	連結
將內部部署的 ONTAP 叢集分層至 StorageGRID	當您設定 BlueXP 分層到 StorageGRID 時、您需要提供 BlueXP 分層、並提供 S3 存取金鑰和秘密金鑰。BlueXP 分層使用金鑰來存取您的貯體。	"準備分層至 StorageGRID"

Connector的AWS權限

當BlueXP在AWS中啟動Connector執行個體時、它會將原則附加到執行個體、讓Connector有權限管理該AWS帳戶內的資源和程序。連接器使用權限來撥打API呼叫數個AWS服務、包括EC2、S3、CloudForecation、IAM、 金鑰管理服務（KMS）等。

IAM 原則

以下提供的IAM原則提供Connector所需的權限、可讓您根據AWS區域來管理公有雲環境中的資源和程序。

請注意下列事項：

- 如果您直接從BlueXP在標準AWS區域中建立連接器、則BlueXP會自動將原則套用至連接器。在這種情況下、您不需要執行任何動作。
- 如果您是從AWS Marketplace部署Connector、在Linux主機上手動安裝Connector、或是想要新增額外的AWS認證到BlueXP、則必須自行設定原則。
- 您也必須確保原則在後續版本中新增權限時保持最新狀態。
- 如有需要、您可以使用IAM來限制IAM原則 `Condition` 元素。 "AWS文件：條件元素"
- 若要檢視使用這些原則的逐步指示、請參閱下列頁面：
  - "設定 AWS Marketplace 部署的權限"

- "設定內部部署的權限"
- "設定受限模式的權限"
- "設定私有模式的權限"

選取您所在的地區以檢視所需的原則：

標準區域

對於標準區域、權限分佈在兩個原則之間。由於AWS中受管理原則的字元大小上限、因此需要兩個原則。

第一個原則提供下列服務的權限：

- Amazon S3 儲存區探索
- 備份與還原
- 分類
- Cloud Volumes ONTAP
- FSX ONTAP
- 分層

第二個原則提供下列服務的權限：

- 邊緣快取
- Kubernetes

原則1

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DescribeTags",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:CreatePlacementGroup",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DescribeVpcs",
```

```
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteRoute",
                "ec2:DeletePlacementGroup",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeVolumesModifications",
                "ec2:ModifyVolume",
                "cloudformation:CreateStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "cloudformation:DeleteStack",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:ListInstanceProfiles",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DeleteInstanceProfile",
                "iam:GetRolePolicy",
                "iam:GetRole",
                "sts:DecodeAuthorizationMessage",
                "sts:AssumeRole",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketPolicy",
                "s3:GetBucketAcl",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:PutObject",
                "s3:ListAllMyBuckets",
```

```
                "s3:GetObject",
                "s3:GetEncryptionConfiguration",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "fsx:Describe*",
                "fsx:List*",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "cvoServicePolicy"
        },
        {
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "kms:List*",
                "kms:Describe*",
                "ec2:DescribeVpcEndpoints",
                "kms:ListAliases",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
```

```
                "glue:BatchDeletePartition"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "backupPolicy"
        },
        {
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketAcl",
                "s3:PutBucketPublicAccessBlock",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",
                "s3:DeleteBucket",
                "s3:GetObjectVersionTagging",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:PutObjectVersionTagging",
                "s3:PutObjectRetention",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketVersioning",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:PutBucketPolicy",
                "s3:PutBucketOwnershipControls"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::netapp-backup-*"
            ],
            "Effect": "Allow",
            "Sid": "backupS3Policy"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:DeleteBucket"
            ],
            "Resource": [
                "arn:aws:s3:::fabric-pool*"
            ],
            "Effect": "Allow",
            "Sid": "fabricPoolS3Policy"
        },
        {
            "Action": [
                "ec2:DescribeRegions"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "fabricPoolPolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/netapp-adc-manager": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
```

```
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume",
                "ec2:StopInstances",
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        }
```

```
    ]
}
```

原則 **#2**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeRegions",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "iam:GetInstanceProfile"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "K8sServicePolicy"
        },
        {
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudwatch:GetMetricStatistics",
                "cloudformation:ListStacks"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "GFCservicePolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GFCInstance": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
```

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

GovCloud（美國）地區

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListInstanceProfiles",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "ec2:ModifyVolumeAttribute",
                "sts:DecodeAuthorizationMessage",
                "ec2:DescribeImages",
                "ec2:DescribeRouteTables",
                "ec2:DescribeInstances",
                "iam:PassRole",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
```

```
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:StopInstances",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:CreateBucket",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
```

```
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::fabric-pool*"
            ]
        },
        {
            "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-us-gov:s3:::netapp-backup-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
```

```
            "Resource": [
                "arn:aws-us-gov:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-us-gov:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

秘密區域

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
```

```
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
```

```
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

最高機密區域

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
```

```
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
```

```
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

AWS權限的使用方式

下列各節說明如何將權限用於每項 BlueXP 服務。如果您的企業原則規定只有在需要時才提供權限、此資訊就很有幫助。

Amazon FSX for ONTAP Sf

Connector 會提出下列 API 要求、以管理 Amazon FSX for ONTAP ：

- EC2：資料說明
- EC2：取消訂閱即時狀態
- EC2：取消訂閱實例屬性
- EC2：取消功能表
- EC2：取消影像
- EC2：建立標記
- EC2：減量磁碟區
- EC2：取消安全性群組
- EC2：網路介面

- EC2：無資料子網路
- EC2：取消功能Vpcs
- EC2：取消功能DhcpOptions
- EC2：取消快照
- EC2：評量會議
- EC2：取消註冊
- EC2：取消標示
- EC2：解讀IamInstanceProfileAssociations
- EC2：取消訂閱保留服務
- EC2：取消資料VpcEndpoints
- EC2：取消功能Vpcs
- EC2：說明體積修改
- EC2：取消目標位置群組
- 公里：清單*
- 公里：描述*
- 公里：建立授予
- kms：清單別名
- FSX：說明*
- FSX：清單*

Amazon S3 儲存區探索

Connector提出下列API要求以探索Amazon S3儲存區：

S3：GetEncryptionConfiguration

備份與還原

Connector會提出下列API要求、以管理Amazon S3中的備份：

- S3：GetBucketLocation
- S3：ListAllMyb桶
- S3：清單庫
- S3：建立桶
- S3：Get生命 週期組態
- S3：Putt升降 器組態
- S3：PuttBucketting
- S3：listBucketVerions

- S3：GetBucketAcl
- S3：PuttBucketPublicAccessBlock
- 公里：清單*
- 公里：描述*
- S3：GetObject
- EC2：取消資料VpcEndpoints
- kms：清單別名
- S3：PuttEncryptionConfiguration

當您使用搜尋與還原方法還原磁碟區和檔案時、Connector會發出下列API要求：

- S3：建立桶
- S3：刪除物件
- S3：刪除ObjectVersion
- S3：GetBucketAcl
- S3：清單庫
- S3：listBucketVerions
- S3：listBucketMultiPartUploads
- S3：PuttObject
- S3：PuttBucketAcl
- S3：Putt升降 器組態
- S3：PuttBucketPublicAccessBlock
- S3：中止多重角色上傳
- S3：列出多個零件上傳零件
- Athena ： StartQueryExecution
- Athena：GetQueryResults
- Athena：GetQueryExecution
- Athena：停止查詢執行
- 黏著劑：建立資料庫
- 黏著劑：CreateTable
- 黏著劑：批字刪除分割區

當您使用DataLock和勒索軟體保護來進行Volume備份時、Connector會發出下列API要求：

- S3：GetObjectVersion標記
- S3：GetBucketObjectLockConfiguration
- S3：GetObjectVerionAcl

- S3：PuttObjectTagging
- S3：刪除物件
- S3：刪除ObjectTagging
- S3：GetObjectRetention
- S3：刪除ObjectVersion標記
- S3：PuttObject
- S3：GetObject
- S3：PuttBucketObjectLockConfiguration
- S3：Get生命 週期組態
- S3：listBucketByTags
- S3：GetBucketting
- S3：刪除ObjectVersion
- S3：listBucketVerions
- S3：清單庫
- S3：PuttBucketting
- S3：GetObjectTagging
- S3：PuttBucketVersion
- S3：PuttObjectVersion標記
- S3：GetBucketVersion
- S3：GetBucketAcl
- S3：BypassGovernanceRetention
- S3：PuttObjectRetention
- S3：GetBucketLocation
- S3：GetObjectVersion

如果Cloud Volumes ONTAP 您使用不同的AWS帳戶來進行還原備份、而非用於來源磁碟區、Connector會發出下列API要求：

- S3：PuttBucketPolicy
- S3：PuttBucketOwnershipControl

分類

Connector 會提出下列 API 要求、以部署 BlueXP 分類執行個體：

- EC2：資料說明
- EC2：取消訂閱即時狀態
- EC2：RunInstances

- EC2：終端安裝
- EC2：建立標記
- EC2：建立磁碟區
- EC2：AttachVolume
- EC2：建立安全性群組
- EC2：刪除安全性群組
- EC2：取消安全性群組
- EC2：建立網路介面
- EC2：網路介面
- EC2：刪除網路介面
- EC2：無資料子網路
- EC2：取消功能Vpcs
- EC2：建立Snapshot
- EC2：取消註冊
- 雲端：建立堆疊
- 雲端：刪除堆疊
- 雲端：無標準堆疊
- 雲端：取消功能堆疊事件
- IAM：AddRoleToInstanceProfile
- EC2：Associate IamInstanceProfile
- EC2：解讀IamInstanceProfileAssociations

當您使用 BlueXP 分類時、 Connector 會發出下列 API 要求來掃描 S3 貯體：

- IAM：AddRoleToInstanceProfile
- EC2：Associate IamInstanceProfile
- EC2：解讀IamInstanceProfileAssociations
- S3：GetBucketting
- S3：GetBucketLocation
- S3：ListAllMyb桶
- S3：清單庫
- S3：GetBucketPolicyStatus
- S3：GetBucketPolicy
- S3：GetBucketAcl
- S3：GetObject
- IAM：GetRole

- S3：刪除物件
- S3：刪除ObjectVersion
- S3：PuttObject
- STS: Assume勞力

Cloud Volumes ONTAP

Connector會提出下列API要求、要求在Cloud Volumes ONTAP AWS中部署及管理功能。

目的	行動	用於部署？	用於日常營運？	用於刪除？
建立及管理IAM角色及Cloud Volumes ONTAP 執行個體設定檔以利執行個體	IAM：清單執行設定檔	是的	是的	否
	IAM：建立角色	是的	否	否
	IAM：刪除角色	否	是的	是的
	IAM：Putt角色 原則	是的	否	否
	IAM：CreatanceProfile	是的	否	否
	IAM：刪除角色原則	否	是的	是的
	IAM：AddRoleToInstanceProfile	是的	否	否
	IAM：RemoveRoleFromInstanceProfile	否	是的	是的
	IAM：刪除InstanceProfile	否	是的	是的
	IAM：密碼	是的	否	否
	EC2：Associate IamInstanceProfile	是的	是的	否
	EC2：解讀IamInstanceProfile Associations	是的	是的	否
	EC2：中斷IamInstanceProfile	否	是的	否
解碼授權狀態訊息	STS:解碼授權訊息	是的	是的	否
說明帳戶可使用的指定映像（Amis）	EC2：取消影像	是的	是的	否
描述VPC中的路由表（僅HA配對需要）	EC2：取消功能表	是的	否	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
停止、啟動及監控執行個體	EC2：啟動安裝	是的	是的	否
	EC2：停止執行	是的	是的	否
	EC2：資料說明	是的	是的	否
	EC2：取消訂閱即時狀態	是的	是的	否
	EC2：RunInstances	是的	否	否
	EC2：終端安裝	否	否	是的
	EC2：修改實例屬性	否	是的	否
確認已針對支援的執行個體類型啟用增強式網路功能	EC2：取消訂閱實例屬性	否	是的	否
使用「WorkingEnvironment」和「WorkingEnvironmentId」標記來標記資源、這些標記用於維護和成本分配	EC2：建立標記	是的	是的	否
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：建立磁碟區	是的	是的	否
	EC2：減量磁碟區	是的	是的	是的
	EC2：修改Volume屬性	否	是的	是的
	EC2：AttachVolume	是的	是的	否
	EC2：刪除Volume	否	是的	是的
	EC2：分離Volume	否	是的	是的

目的	行動	用於部署？	用於日常營運？	用於刪除？
建立及管理安全性群組Cloud Volumes ONTAP 以利執行	EC2：建立安全性群組	是的	否	否
	EC2：刪除安全性群組	否	是的	是的
	EC2：取消安全性群組	是的	是的	是的
	EC2 ：RevokeSecurity GroupEgress	是的	否	否
	EC2：授權安全性群組出口	是的	否	否
	EC2：授權安全性群組入口	是的	否	否
	EC2 ：RevokeSecurity GroupIngress	是的	是的	否
在Cloud Volumes ONTAP 目標子網路中建立及管理用於實現效能不中斷的網路介面	EC2：建立網路介面	是的	否	否
	EC2：網路介面	是的	是的	否
	EC2：刪除網路介面	否	是的	是的
	EC2：修改網路互連屬性	否	是的	否
取得目的地子網路和安全性群組清單	EC2：無資料子網路	是的	是的	否
	EC2：取消功能Vpcs	是的	是的	否
取得DNS伺服器和Cloud Volumes ONTAP 預設的網域名稱以供執行個體使用	EC2：取消功能DhcpOptions	是的	否	否
拍攝EBS Volume的快照Cloud Volumes ONTAP 以供其使用	EC2：建立Snapshot	是的	是的	否
	EC2：刪除Snapshot	否	是的	是的
	EC2：取消快照	否	是的	否
擷取Cloud Volumes ONTAP 附加於AutoSupport 資訊畫面的功能	EC2：GetConsole輸出	是的	是的	否
取得可用金鑰組的清單	EC2：評量會議	是的	否	否
取得可用AWS區域的清單	EC2：取消註冊	是的	是的	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
管理Cloud Volumes ONTAP 與實例相關的資源標記	EC2：刪除標記	否	是的	是的
	EC2：取消標示	否	是的	否
建立及管理AWS CloudForation範本的堆疊	雲端：建立堆疊	是的	否	否
	雲端：刪除堆疊	是的	否	否
	雲端：無標準堆疊	是的	是的	否
	雲端：取消功能堆疊事件	是的	否	否
	cloudformation：驗證範本	是的	否	否
建立並管理Cloud Volumes ONTAP S3儲存區、讓整個系統做為資料分層的容量層	S3：建立桶	是的	是的	否
	S3：刪除資源桶	否	是的	是的
	S3：Get生命 週期組態	否	是的	否
	S3：Putt升降 器組態	否	是的	否
	S3：PuttBucketting	否	是的	否
	S3：listBucketVerions	否	是的	否
	S3：GetBucketPolicyStatus	否	是的	否
	S3：GetBucketPublicAccessBlock	否	是的	否
	S3：GetBucketAcl	否	是的	否
	S3：GetBucketPolicy	否	是的	否
	S3：PuttBucketPublicAccessBlock	否	是的	否
	S3：GetBucketting	否	是的	否
	S3：GetBucketLocation	否	是的	否
	S3：ListAllMyb桶	否	否	否
	S3：清單庫	否	是的	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
使用Cloud Volumes ONTAP AWS金鑰管理服務（KMS）啟用資料加密功能	公里：清單*	是的	是的	否
	公里：ReEncrypt *	是的	否	否
	公里：描述*	是的	是的	否
	公里：建立授予	是的	是的	否
	KMS ：GenerateDataKeyWithoutPlaintext	是的	是的	否
在單一AWS可用性區域中、為兩個HA節點建立並管理AWS分散放置群組、以及協調器	EC2：建立位置群組	是的	否	否
	EC2：刪除位置群組	否	是的	是的
建立報告	FSX：說明*	否	是的	否
	FSX：清單*	否	是的	否
建立及管理可支援Amazon EBS彈性Volume功能的集合體	EC2：說明體積修改	否	是的	否
	EC2：修改Volume	否	是的	否

邊緣快取

Connector 會在部署期間提出下列 API 要求、以部署 BlueXP 邊緣快取執行個體：

- 雲端：無標準堆疊
- cloudwatch：GetMetricStatistics
- 雲端：清單堆疊

Kubernetes

Connector會提出下列API要求、以探索及管理Amazon EKS叢集：

- EC2：取消註冊
- EKS：清單叢集
- EKS：取消叢集
- IAM：GetInstanceProfile

變更記錄

新增和移除權限時、我們會在下方各節中加以註記。

2024 年 3 月 8 日

Connector 原則現在包含下列權限：

EC2 ：去除可用性區域

即將發行的版本需要此權限。我們會在發行版本推出時更新版本資訊、提供更多詳細資料。

2023 年 6 月 6 日

Cloud Volumes ONTAP 現在需要下列權限：

KMS ： GenerateDataKeyWithoutPlaintext

2023 年 2 月 14 日

BlueXP 分層現在需要下列權限：

EC2：取消資料VpcEndpoints

連接器的Azure權限

當BlueXP在Azure中啟動Connector VM時、它會將自訂角色附加至VM、讓Connector有權管理該Azure訂閱中的資源和程序。Connector會使用權限來撥打API呼叫數個Azure服務。

自訂角色權限

下列自訂角色提供Connector管理Azure網路中資源與程序所需的權限。

直接從BlueXP建立連接器時、BlueXP會自動將此自訂角色套用至連接器。

如果您從Azure Marketplace部署Connector、或是在Linux主機上手動安裝Connector、則必須自行設定自訂角色。

若要檢視使用這些原則的逐步指示、請參閱下列頁面：

- "設定 Azure Marketplace 部署的權限"
- "設定內部部署的權限"
- "設定受限模式的權限"
- "設定私有模式的權限"

您也必須確保在後續版本中新增權限時、該角色是最新的。

```
{
    "Name": "BlueXP Operator",
    "Actions": [
                    "Microsoft.Compute/disks/delete",
                    "Microsoft.Compute/disks/read",
                    "Microsoft.Compute/disks/write",
                    "Microsoft.Compute/locations/operations/read",
                    "Microsoft.Compute/locations/vmSizes/read",
```

```
                    "Microsoft.Resources/subscriptions/locations/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/deallocate/action",
                    "Microsoft.Compute/virtualMachines/start/action",
                    "Microsoft.Compute/virtualMachines/vmSizes/read",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/images/read",
                    "Microsoft.Network/locations/operationResults/read",
                    "Microsoft.Network/locations/operations/read",
                    "Microsoft.Network/networkInterfaces/read",
                    "Microsoft.Network/networkInterfaces/write",
                    "Microsoft.Network/networkInterfaces/join/action",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/networkSecurityGroups/write",
                    "Microsoft.Network/networkSecurityGroups/join/action",
                    "Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
                    "Microsoft.Network/virtualNetworks/subnets/read",
                    "Microsoft.Network/virtualNetworks/subnets/write",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",

"Microsoft.Network/virtualNetworks/virtualMachines/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
                    "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",
                    "Microsoft.Storage/checknameavailability/read",
                    "Microsoft.Storage/operations/read",
```

```
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Storage/storageAccounts/read",
                    "Microsoft.Storage/storageAccounts/delete",
                    "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/listAccountSas/action",
                    "Microsoft.Storage/usages/read",
                    "Microsoft.Compute/snapshots/write",
                    "Microsoft.Compute/snapshots/read",
                    "Microsoft.Compute/availabilitySets/write",
                    "Microsoft.Compute/availabilitySets/read",
                    "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write",
                    "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/loadBalancingRules/read",
                    "Microsoft.Network/loadBalancers/probes/read",
                    "Microsoft.Network/loadBalancers/probes/join/action",
                    "Microsoft.Authorization/locks/*",
                    "Microsoft.Network/routeTables/join/action",
                    "Microsoft.NetApp/netAppAccounts/read",
                    "Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
                    "Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acti
on",
```

```
"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
                    "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",

"Microsoft.Resources/deployments/operationStatuses/read",
                    "Microsoft.Insights/Metrics/Read",
                    "Microsoft.Compute/virtualMachines/extensions/write",
                    "Microsoft.Compute/virtualMachines/extensions/delete",
                    "Microsoft.Compute/virtualMachines/extensions/read",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Network/networkInterfaces/delete",
                    "Microsoft.Network/networkSecurityGroups/delete",
                    "Microsoft.Resources/deployments/delete",
                    "Microsoft.Compute/diskEncryptionSets/read",
                    "Microsoft.Compute/snapshots/delete",
                    "Microsoft.Network/privateEndpoints/delete",
                    "Microsoft.Compute/availabilitySets/delete",
                    "Microsoft.KeyVault/vaults/read",
                    "Microsoft.KeyVault/vaults/accessPolicies/write",
                    "Microsoft.Compute/diskEncryptionSets/write",
                    "Microsoft.KeyVault/vaults/deploy/action",
                    "Microsoft.Compute/diskEncryptionSets/delete",
                    "Microsoft.Resources/tags/read",
                    "Microsoft.Resources/tags/write",
                    "Microsoft.Resources/tags/delete",
                    "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",
```

```
"Microsoft.ContainerService/managedClusters/listClusterUserCredential/acti
on",
                    "Microsoft.ContainerService/managedClusters/read",
                    "Microsoft.Synapse/workspaces/write",
                    "Microsoft.Synapse/workspaces/read",
                    "Microsoft.Synapse/workspaces/delete",
                    "Microsoft.Synapse/register/action",
                    "Microsoft.Synapse/checkNameAvailability/action",
                    "Microsoft.Synapse/workspaces/operationStatuses/read",
                    "Microsoft.Synapse/workspaces/firewallRules/read",

"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
                    "Microsoft.Synapse/workspaces/operationResults/read",

"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",

"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
                    "Microsoft.Compute/images/write",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "BlueXP Permissions",
    "IsCustom": "true"
}
```

Azure權限的使用方式

下列各節說明如何將權限用於每項 BlueXP 服務。如果您的企業原則規定只有在需要時才提供權限、此資訊就很有幫助。

Azure NetApp Files

當您使用 BlueXP 分類來掃描 Azure NetApp Files 資料時、 Connector 會提出下列 API 要求：

- Microsoft.NetApp/netAppAccounts/read
- Microsoft.NetApp/netAppAccounts/capacityPools/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete

備份與還原

Connector 會針對 BlueXP 備份與還原提出下列 API 要求：

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/contains/read
- Microsoft.Storage/storageAccounts/listAccountSas /行動
- Microsoft.KeyVault/Vault/Read
- Microsoft.KeyVault/Vault/accessPolicys/write
- Microsoft.Network/networkInterfaces/read
- Microsoft.Resources /訂閱/位置/讀取
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- 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
- Microsoft授權/鎖定/*
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/privateEndpoints/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/write
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Network/privateDnsZones/A/write
- Microsoft.Network/privateDnsZones/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/read
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft資源/部署/刪除
- Microsoft.ManagedIdentity /使用者身分識別/指派/行動

使用搜尋與還原功能時、Connector會發出下列API要求：

- Microsoft.Synapse /工作區/寫入
- Microsoft.Synapse /工作區/讀取
- Microsoft.Synapse /工作區/刪除
- Microsoft.Synapse /登錄/行動
- Microsoft.Synape/checksNameAvailability /行動
- Microsoft.Synapse /工作區/作業狀態/讀取
- Microsoft.Synapse /工作區/防火牆規則/讀取
- Microsoft.Synapse /工作區/替代AllIpFiretallRules /行動

- Microsoft.Synapse /工作區/作業結果/讀取
- Microsoft.Synapse /工作區/私有端點連線核准/行動

分類

當您使用 BlueXP 分類時、 Connector 會提出下列 API 要求。

行動	用於設定？	用於日常營運？
Microsoft.Compute/locations/operations/read	是的	是的
Microsoft.Compute/locations/vmSizes/read	是的	是的
Microsoft.Compute/operations/read	是的	是的
Microsoft.Compute/virtualMachines/instanceView/read	是的	是的
Microsoft.Compute/virtualMachines/powerOff/action	是的	否
Microsoft.Compute/virtualMachines/read	是的	是的
Microsoft.Compute/virtualMachines/restart/action	是的	否
Microsoft.Compute/virtualMachines/start/action	是的	否
Microsoft.Compute/virtualMachines/vmSizes/read	否	是的
Microsoft.Compute/virtualMachines/write	是的	否
Microsoft.Compute/images/read	是的	是的
Microsoft.Compute/disks/delete	是的	否
Microsoft.Compute/disks/read	是的	是的
Microsoft.Compute/disks/write	是的	否
Microsoft.Storage/測試可用度/讀取	是的	是的
Microsoft.Storage/operations /讀取	是的	是的
Microsoft.Storage/storageAccounts/listkeys/action	是的	否
Microsoft.Storage/storageAccounts/read	是的	是的
Microsoft.Storage/storageAccounts/write	是的	否
Microsoft.Storage/storageAccounts/blobServices/contains/read	是的	是的

行動	用於設定？	用於日常營運？
Microsoft.Network/networkInterfaces/read	是的	是的
Microsoft.Network/networkInterfaces/write	是的	否
Microsoft.Network/networkInterfaces/join/action	是的	否
Microsoft.Network/networkSecurityGroups/read	是的	是的
Microsoft.Network/networkSecurityGroups/write	是的	否
Microsoft.Resources /訂閱/位置/讀取	是的	是的
Microsoft.Network/locations/operationResults/read	是的	是的
Microsoft.Network/locations/operations/read	是的	是的
Microsoft.Network/virtualNetworks/read	是的	是的
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	是的	是的
Microsoft.Network/virtualNetworks/subnets/read	是的	是的
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	是的	是的
Microsoft.Network/virtualNetworks/virtualMachines/read	是的	是的
Microsoft.Network/virtualNetworks/subnets/join/action	是的	否
Microsoft.Network/virtualNetworks/subnets/write	是的	否
Microsoft.Network/routeTables/join/action	是的	否
Microsoft.Resources /部署/作業/讀取	是的	是的
Microsoft.Resources /部署/讀取	是的	是的
Microsoft.Resources /部署/寫入	是的	否
Microsoft.Resources /資源/讀取	是的	是的
Microsoft.Resources /訂閱/作業結果/讀取	是的	是的

行動	用於設定？	用於日常營運？
Microsoft.Resources /訂閱/資源群組/刪除	是的	否
Microsoft.Resources /訂閱/資源群組/讀取	是的	是的
Microsoft.Resources /訂閱/資源群組/資源/讀取	是的	是的
Microsoft.Resources /訂閱/資源群組/寫入	是的	否

Cloud Volumes ONTAP

Connector會提出下列API要求、要求在Cloud Volumes ONTAP Azure中部署及管理功能。

目的	行動	用於部署？	用於日常營運？	用於刪除？
建立及管理VM	Microsoft.Compute/locations/operations/read	是的	是的	否
	Microsoft.Compute/locations/vmSizes/read	是的	是的	否
	Microsoft.Resources/訂閱/位置/讀取	是的	否	否
	Microsoft.Compute/operations/read	是的	是的	否
	Microsoft.Compute/virtualMachines/instanceView/read	是的	是的	否
	Microsoft.Compute/virtualMachines/powerOff/action	是的	是的	否
	Microsoft.Compute/virtualMachines/read	是的	是的	否
	Microsoft.Compute/virtualMachines/restart/action	是的	是的	否
	Microsoft.Compute/virtualMachines/start/action	是的	是的	否
	Microsoft.Compute/virtualMachines/deallocate/action	否	是的	是的
	Microsoft.Compute/virtualMachines/vmSizes/read	否	是的	否
	Microsoft.Compute/virtualMachines/write	是的	是的	否
	Microsoft.Compute/virtualMachines/delete	是的	是的	是的
	Microsoft資源/部署/刪除	是的	否	否
從VHD啟用部署	Microsoft.Compute/images/read	是的	否	否
	Microsoft.Compute/images/write	是的	否	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
在目標子網路中建立及管理網路介面	Microsoft.Network/networkInterfaces/read	是的	是的	否
	Microsoft.Network/networkInterfaces/write	是的	是的	否
	Microsoft.Network/networkInterfaces/join/action	是的	是的	否
	Microsoft.Network/networkInterfaces/delete	是的	是的	否
建立及管理網路安全群組	Microsoft.Network/networkSecurityGroups/read	是的	是的	否
	Microsoft.Network/networkSecurityGroups/write	是的	是的	否
	Microsoft.Network/networkSecurityGroups/join/action	是的	否	否
	Microsoft.Network/networkSecurityGroups/delete	否	是的	是的

目的	行動	用於部署？	用於日常營運？	用於刪除？
取得區域、目標Vnet和子網路的網路資訊、並將VM新增至VNets	Microsoft.Network/locations/operationResults/read	是的	是的	否
	Microsoft.Network/locations/operations/read	是的	是的	否
	Microsoft.Network/virtualNetworks/read	是的	否	否
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	是的	否	否
	Microsoft.Network/virtualNetworks/subnets/read	是的	是的	否
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	是的	是的	否
	Microsoft.Network/virtualNetworks/virtualMachines/read	是的	是的	否
	Microsoft.Network/virtualNetworks/subnets/join/action	是的	是的	否
建立及管理資源群組	Microsoft.Resources/部署/作業/讀取	是的	是的	否
	Microsoft.Resources/部署/讀取	是的	是的	否
	Microsoft.Resources/部署/寫入	是的	是的	否
	Microsoft.Resources/資源/讀取	是的	是的	否
	Microsoft.Resources/訂閱/作業結果/讀取	是的	是的	否
	Microsoft.Resources/訂閱/資源群組/刪除	是的	是的	是的
	Microsoft.Resources/訂閱/資源群組/讀取	否	是的	否
	Microsoft.Resources/訂閱/資源群組/資源/讀取	是的	是的	否
	Microsoft.Resources/訂閱/資源群組/寫入	是的	是的	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
管理Azure儲存帳戶與磁碟	Microsoft.Compute/disks/read	是的	是的	是的
	Microsoft.Compute/disks/write	是的	是的	否
	Microsoft.Compute/disks/delete	是的	是的	是的
	Microsoft.Storage/測試可用度/讀取	是的	是的	否
	Microsoft.Storage/operations /讀取	是的	是的	否
	Microsoft.Storage/storageAccounts/listkeys/action	是的	是的	否
	Microsoft.Storage/storageAccounts/read	是的	是的	否
	Microsoft.Storage/storageAccounts/DELETE	否	是的	是的
	Microsoft.Storage/storageAccounts/write	是的	是的	否
	Microsoft.Storage/改用/讀取	否	是的	否
可備份至Blob儲存設備、並加密儲存帳戶	Microsoft.Storage/storageAccounts/blobServices/contains/read	是的	是的	否
	Microsoft.KeyVault/Vault/Read	是的	是的	否
	Microsoft.KeyVault/Vault/accessPolicys/write	是的	是的	否
啟用vnet服務端點以進行資料分層	Microsoft.Network/virtualNetworks/subnets/write	是的	是的	否
	Microsoft.Network/routeTables/join/action	是的	是的	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
建立及管理Azure託管快照	Microsoft.Compute/snapshots/write	是的	是的	否
	Microsoft.Compute/snapshots/read	是的	是的	否
	Microsoft.Compute/snapshots/delete	否	是的	是的
	Microsoft.Compute/disks/beginGetAccess/action	否	是的	否
建立及管理可用度集	Microsoft.Compute/availabilitySets/write	是的	否	否
	Microsoft.Compute/availabilitySets/read	是的	否	否
從市場進行程式化部署	Microsoft.MarketplaceOrdination/offersTypes /出版商/優惠/計畫/協議/讀取	是的	否	否
	Microsoft.MarketplaceOrder/OfferTypes /出版商/服務/計畫/協議/寫入	是的	是的	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
管理HA配對的負載平衡器	Microsoft.Network/loadBalancers/read	是的	是的	否
	Microsoft.Network/loadBalancers/write	是的	否	否
	Microsoft.Network/loadBalancers/delete	否	是的	是的
	Microsoft.Network/loadBalancers/backendAddressPools/read	是的	否	否
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	是的	否	否
	Microsoft.Network/loadBalancers/frontendIPConfigurations/read	是的	是的	否
	Microsoft.Network/loadBalancers/loadBalancingRules/read	是的	否	否
	Microsoft.Network/loadBalancers/probes/read	是的	否	否
	Microsoft.Network/loadBalancers/probes/join/action	是的	否	否
可管理Azure磁碟上的鎖定	Microsoft授權/鎖定/*	是的	是的	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
在子網路外沒有連線時、為HA配對啟用私有端點	Microsoft.Network/privateEndpoints/write	是的	是的	否
	Microsoft儲存設備/儲存帳戶/權限端點連線核准/動作	是的	否	否
	Microsoft.Storage/storageAccounts/privateEndpointConnections/read	是的	是的	是的
	Microsoft.Network/privateEndpoints/read	是的	是的	是的
	Microsoft.Network/privateDnsZones/write	是的	是的	否
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/write	是的	是的	否
	Microsoft.Network/virtualNetworks/join/action	是的	是的	否
	Microsoft.Network/privateDnsZones/A/write	是的	是的	否
	Microsoft.Network/privateDnsZones/read	是的	是的	否
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/read	是的	是的	否
某些VM部署所需的資源、視基礎實體硬體而定	Microsoft.Resources/部署/作業狀態/讀取	是的	是的	否
如果部署失敗或刪除、請從資源群組移除資源	Microsoft.Network/privateEndpoints/delete	是的	是的	否
	Microsoft.Compute/availabilitySets/delete	是的	是的	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
使用API時、可啟用客戶管理的加密金鑰	Microsoft.Compute/diskEncryptionSets/read	是的	是的	是的
	Microsoft.Compute/diskEncryptionSets/write	是的	是的	否
	Microsoft.KeyVault/Vault/Deploy /行動	是的	否	否
	Microsoft.Compute/diskEncryptionSets/delete	是的	是的	是的
設定HA配對的應用程式安全性群組、以隔離HA互連和叢集網路NIC	Microsoft.Network/applicationSecurityGroups/write	否	是的	否
	Microsoft.Network/applicationSecurityGroups/read	否	是的	否
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	否	是的	否
	Microsoft.Network/networkSecurityGroups/securityRules/write	是的	是的	否
	Microsoft.Network/applicationSecurityGroups/delete	否	是的	是的
	Microsoft.Network/networkSecurityGroups/securityRules/delete	否	是的	是的
讀取、寫入及刪除Cloud Volumes ONTAP 與資源相關的標記	Microsoft.Resources/標記/讀取	否	是的	否
	Microsoft.Resources/標記/寫入	是的	是的	否
	Microsoft.Resources/標記/刪除	是的	否	否
在建立期間加密儲存帳戶	Microsoft.ManagedIdentity /使用者身分識別/指派/行動	是的	是的	否

邊緣快取

當您使用 BlueXP 邊緣快取時、 Connector 會發出下列 API 要求：

- Microsoft.Insights /指標/讀取
- 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資源/部署/刪除

Kubernetes

Connector會提出下列API要求、以探索及管理Azure Kubernetes Service（KS）中執行的叢集：

- Microsoft.Compute/virtualMachines/read
- Microsoft.Resources /訂閱/位置/讀取
- Microsoft.Resources /訂閱/作業結果/讀取
- Microsoft.Resources /訂閱/資源群組/讀取
- Microsoft.Resources /訂閱/資源群組/資源/讀取
- Microsoft.ContainerService/管理叢集/讀取
- Microsoft.ContainerService/managedClusters/listClusterUserCredentials/action

分層

當您設定 BlueXP 分層時、 Connector 會發出下列 API 要求。

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Resources /訂閱/資源群組/讀取
- Microsoft.Resources /訂閱/位置/讀取

Connector會針對日常作業提出下列API要求。

- Microsoft.Storage/storageAccounts/blobServices/contains/read
- Microsoft.Storage/storageAccounts/managementPolicys/read
- Microsoft.Storage/storageAccounts/managementPolicys/write
- Microsoft.Storage/storageAccounts/read

變更記錄

新增和移除權限時、我們會在下方各節中加以註記。

2023 年 12 月 5 日

將 Volume 資料備份至 Azure Blob 儲存設備時、 BlueXP 備份與還原不再需要下列權限：

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete

其他 BlueXP 儲存服務需要這些權限、因此如果您使用其他儲存服務、這些權限仍會保留在 Connector 的自訂角色中。

2023 年 5 月 12 日

下列權限已新增至 JSON 原則、因為 Cloud Volumes ONTAP 管理需要這些權限：

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read

下列權限已從Json原則中移除、因為不再需要這些權限：

- Microsoft.Storage/storageAccounts/blobServices/contains/write
- Microsoft.Network/publicIPAddresses/delete

2023 年 3 月 23 日

BlueXP 分類不再需要「 Microsoft.Storage/storageAccounts/delete 」權限。

此權限仍為Cloud Volumes ONTAP 必填項目。

2023年1月5日

下列權限已新增至Json原則：

- Microsoft.Storage/storageAccounts/listAccountSas /行動
- Microsoft.Synapse /工作區/私有端點連線核准/行動

  BlueXP 備份與還原需要這些權限。

- Microsoft.Network/loadBalancers/backendAddressPools/join/action

  此權限是Cloud Volumes ONTAP 進行非必要部署所需的權限。

Connector的Google Cloud權限

BlueXP需要權限才能在Google Cloud中執行動作。這些權限包含在NetApp提供的自訂角色中。您可能想要瞭解BlueXP使用這些權限的功能。

服務帳戶權限

下方顯示的自訂角色提供Connector在Google Cloud網路中管理資源和程序所需的權限。

您必須將此自訂角色套用至連接器VM的服務帳戶。

- "設定標準模式的 Google Cloud 權限"
- "設定受限模式的權限"
- "設定私有模式的權限"

您也必須確保在後續版本中新增權限時、該角色是最新的。

```
title: NetApp BlueXP
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.addAccessConfig
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
```

```
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
- compute.instanceGroups.get
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- 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
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
```

如何使用Google Cloud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。
運算： globalOperations 。 Get	以取得作業狀態。
- compute 、 images.get - compile.images.getFromFamily - compute 。 images.list - compute.images.useReadOnly	取得 VM 執行個體的映像。

行動	目的
- 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 qoutas 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 。 subnets.get -compute 。 subnets.list - competing.zoneOperations 。 GET - compute 、 zones 、 get - compute 。 sites.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.inits.get - deploymentmanager.lists.list - deploymentmanager.operations.get - deploymentmanager.operations.list - deploymentmanager.edes.get - deploymentmanager.edes.list - deploymentmanager.typeProviders.get - deploymentmanager.typeProviders.list - deploymentmanager.types.get - deploymentmanager.types.list	使用 Cloud Volumes ONTAP Google Cloud Deployment Manager 部署物件虛擬機器執行個體。
- logging.logEntries 清單 - logging.privateLogEntries 清單	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 - 儲存、貯體、取得 - 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.keyclings 。 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、物件、 GET 儲存、物件、清單	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。
運算.addresses.list	在部署HA配對時擷取區域中的位址。
- compute 。 backendServices.create - compute 。 RegionBackendServices.create - compute 、 Region.BackendServices.get -compute 。 RegionBackendServices.list	設定後端服務以在HA配對中分配流量。
- compute.networks.updatePolicy	將防火牆規則套用至HA配對的VPC和子網路。
- compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	以啟用 BlueXP 分類。
- container 。叢集。 get - container 。叢集清單	探索在Google Kubernetes Engine中執行的Kubernetes叢集。

行動	目的
- compute.instanceGroups.get - compute 、 addresses.get - compute.instances.updateNetworkInterface	在Cloud Volumes ONTAP 以各種方式建立及管理儲存VM的整組。
-monitoring.timeSeries.list - storage 。 buckets 。 getIamPolicy	探索Google Cloud Storage儲存桶的相關資訊。
- cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.getIamPolicy - cloudkms.cryptoKeys.list - cloudkms.cryptoKeys.setIamPolicy - cloudkms.keycloues.get - cloudkms.keyclogs.getIamPolicy - cloudkms.keyclings 。 list - cloudkms.keyRings.setIamPolicy	可在 BlueXP 備份和恢復激活嚮導中選擇您自己的客戶託管密鑰，而無需使用默認的 Google 託管加密密鑰。

變更記錄

新增和移除權限時、我們會在下方各節中加以註記。

2023 年 **2** 月 **6** 日

已將下列權限新增至此原則：

- compute.instances.updateNetworkInterface

此權限為Cloud Volumes ONTAP 必填欄位。

2023 年 **1** 月 **27** 日

已將下列權限新增至原則：

- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyclous.Get
- cloudkms.keyclas.getIamPolicy
- cloudkms.keyRings.setIamPolicy

BlueXP 備份與還原需要這些權限。