権限

Setup and administration

NetApp
April 26, 2024

目次

権限

BlueXPの権限の概要

BlueXPの機能やサービスを使用するには、権限を指定してBlueXPがクラウド環境で処理を実行できるようにする必要があります。このページのリンクを使用して、目的に応じて必要な権限にすばやくアクセスできます。

AWS権限

BlueXPでは、コネクタと個 々 のサービスにAWS権限が必要です。

コネクタ

目標	説明	リンク
BlueXPからコネクタを導入	BlueXPからConnectorを作成するユーザには、AWSにインスタンスを導入するための特別な権限が必要です。	"AWS権限を設定"
コネクタの権限を指定します	BlueXPがConnectorを起動すると、AWSアカウントのリソースとプロセスの管理に必要な権限を提供するポリシーがインスタンスに関連付けられます。 AWS Marketplaceからコネクタを起動した場合、コネクタを手動でインストールした場合、または "AWSクレデンシャルをコネクタに追加します"。 また、新しい権限が以降のリリースで追加されるときに、ポリシーが最新の状態であることを確認する必要があります。	"Connector の AWS 権限"

バックアップとリカバリ

目標	説明	リンク
オンプレミスのONTAPクラスタをAmazon S3にバックアップ	ONTAPボリュームでバックアップをアクティブ化すると、特定の権限を持つIAMユーザのアクセスキーとシークレットを入力するように求められます。	"バックアップのS3権限を設定"

Cloud Volumes ONTAP

目標	説明	リンク
Cloud Volumes ONTAPノードの権限を付与する	AWSの各Cloud Volumes ONTAP ノードにIAMロールを関連付ける必要があります。HAメディエーターについても同様です。デフォルトではBlueXPにIAMロールが作成されますが、作業環境の作成時に独自のロールを使用することもできます。	"IAMロールを自分で設定する方法について説明します"

コピーと同期

目標	説明	リンク
データブローカーをAWSに導入	データブローカーの導入に使用するAWSユーザアカウントには、特定の権限が必要です。	"AWS にデータブローカーを展開するために必要な権限"
データブローカーの権限を指定	BlueXPのコピーと同期でデータブローカーを導入すると、データブローカーインスタンス用のIAMロールが作成されます。必要に応じて、独自の IAM ロールを使用してデータブローカーを展開できます。	"AWS データブローカーで独自の IAM ロールを使用するための要件"
手動でインストールしたデータブローカーに対してAWSへのアクセスを有効にする	データブローカーをS3バケットを含む同期関係で使用する場合は、AWSにアクセスできるLinuxホストを準備する必要があります。データブローカーをインストールするときは、プログラムによるアクセスと特定の権限を持つIAMユーザにAWSキーを指定する必要があります。	"AWS へのアクセスを有効化"

FSX for ONTAP の略

目標	説明	リンク
FSx for ONTAPの作成と管理	Amazon FSx for NetApp ONTAP作業環境を作成または管理するには、作業環境の作成に必要な権限をBlueXPに付与するIAMロールのARNを指定して、AWSクレデンシャルをBlueXPに追加する必要があります。	"FSx用のAWSクレデンシャルの設定方法をご確認ください"

階層化

目標	説明	リンク
オンプレミスのONTAPクラスタをAmazon S3に階層化	AWSへのBlueXPの階層化を有効にすると、アクセスキーとシークレットキーを入力するように求められます。これらのクレデンシャルは、ONTAP がS3バケットにデータを階層化できるようにONTAP クラスタに渡されます。	"階層化のためのS3権限を設定する"

Azure権限

BlueXPでは、コネクタと個 々 のサービスにAzure権限が必要です。

コネクタ

目標	説明	リンク
BlueXPからコネクタを導入	BlueXPからConnectorを導入する場合は、AzureにConnector VMを導入する権限を持つAzureアカウントまたはサービスプリンシパルを使用する必要があります。	"Azure権限を設定する"

目標	説明	リンク
コネクタの権限を指定します	BlueXPがConnector VMをAzureに導入すると、そのAzureサブスクリプション内でリソースとプロセスを管理するために必要な権限を提供するカスタムロールが作成されます。 Marketplaceからコネクタを起動する場合、コネクタを手動でインストールする場合、またはカスタムロールを自分で設定する必要があります。 "Azureクレデンシャルをコネクタに追加します"。 また、新しい権限が以降のリリースで追加されるときに、ポリシーが最新の状態であることを確認する必要があります。	"Connector の Azure 権限"

コピーと同期

目標	説明	リンク
Azureにデータブローカーを導入	データブローカーの導入に使用するAzureユーザアカウントに、必要な権限が付与されている必要があります。	"Azureにデータブローカーを導入するための権限が必要です"

Google Cloud権限

BlueXPでは、コネクタと個 々 のサービスにGoogle Cloudの権限が必要です。

コネクタ

目標	説明	リンク
BlueXPからコネクタを導入	BlueXPからConnectorを導入するGoogle Cloudユーザーには、Google CloudにConnectorを導入するための特定の権限が必要です。	"コネクタを作成するための権限を設定する"
コネクタの権限を指定します	Connector VMインスタンスのサービスアカウントには、日常処理に対する特定の権限が必要です。導入時にサービスアカウントをコネクタに関連付ける必要があります。 また、新しい権限が以降のリリースで追加されるときに、ポリシーが最新の状態であることを確認する必要があります。	"コネクタの権限を設定します"

バックアップとリカバリ

目標	説明	リンク
Cloud Volumes ONTAP を Google Cloud にバックアップ	BlueXPのバックアップとリカバリを使用してCloud Volumes ONTAPをバックアップする場合は、次のシナリオでコネクタに権限を追加する必要があります。 • 「検索と復元」機能を使用する場合 • 顧客管理の暗号化キー（CMEK）を使用する場合	• "検索と復元機能の権限" • "CMEKの権限"
オンプレミスのONTAPクラスタをGoogle Cloudにバックアップ	BlueXPのバックアップとリカバリを使用してオンプレミスのONTAPクラスタをバックアップする場合は、「検索とリストア」機能を使用するためにコネクタに権限を追加する必要があります。	"検索と復元機能の権限"

Cloud Volumes Service for Google Cloud

目標	説明	リンク
Cloud Volumes Service for Google Cloudの詳細	BlueXPでは、Google Cloudサービスアカウントを使用してCloud Volumes Service APIにアクセスし、適切な権限を付与する必要があります。	"サービスアカウントを設定します"

コピーと同期

目標	説明	リンク
Google Cloudにデータブローカーを導入	データブローカーを導入するGoogle Cloudユーザに必要な権限が割り当てられていることを確認します。	"Google Cloud にデータブローカーを導入するための権限が必要です"
手動でインストールしたデータブローカーに対してGoogle Cloudへのアクセスを有効にする	Google Cloud Storage バケットを含む同期関係でデータブローカーを使用する場合は、 Google Cloud アクセス用の Linux ホストを準備しておく必要があります。データブローカーをインストールする場合、特定の権限を持つサービスアカウントにキーを提供する必要があります。	"Google Cloud へのアクセスを有効にします"

StorageGRIDケンケン

BlueXPでは、2つのサービスに対してStorageGRID権限が必要です。

バックアップとリカバリ

目標	説明	リンク
オンプレミスのONTAPクラスタをStorageGRIDにバックアップ	StorageGRIDをONTAPクラスタのバックアップターゲットとして準備する際、特定の権限を持つIAMユーザのアクセスキーとシークレットを入力するように求められます。	"バックアップターゲットとしてStorageGRIDを準備します"

階層化

目標	説明	リンク
オンプレミスのONTAPクラスタをStorageGRIDに階層化	StorageGRIDへのBlueXPの階層化をセットアップするときは、S3のアクセスキーとシークレットキーを使用してBlueXPの階層化を提供する必要があります。BlueXPの階層化サービスでは、このキーを使用してバケットにアクセスします。	"StorageGRIDへの階層化を準備"

Connector の AWS 権限

BlueXPがAWSでConnectorインスタンスを起動すると、そのAWSアカウント内のリソースとプロセスを管理するための権限をConnectorに提供するポリシーがインスタンスにアタッチされます。Connectorでは、権限を使用してAPI呼び出しを実行することで、EC2、S3、CloudFormation、IAM、 Key Management Service（KMS；キー管理サービス）など。

IAMポリシー

以下のIAMポリシーは、ConnectorがAWSリージョンに基づいてパブリッククラウド環境内のリソースとプロセスを管理するために必要な権限を提供します。

次の点に注意してください。

- BlueXPから直接、標準のAWSリージョンでコネクタを作成すると、BlueXPによって自動的にそのコネクタにポリシーが適用されます。この場合、何も行う必要はありません。
- AWS Marketplaceからコネクタを導入する場合、Linuxホストにコネクタを手動でインストールする場合、またはBlueXPにAWSクレデンシャルを追加する場合は、ポリシーを自分で設定する必要があります。
- また、新しい権限が以降のリリースで追加されるときに、ポリシーが最新の状態であることを確認する必要があります。
- 必要に応じて、IAMを使用してIAMポリシーを制限できます `Condition` 要素（Element）："AWSドキュメント：Condition要素"
- これらのポリシーの使用手順については、次のページを参照してください。
  - "AWS Marketplace環境の権限を設定する"
  - "オンプレミス環境の権限を設定する"
  - "制限モードの権限を設定します"
  - "プライベートモードの権限を設定します"

必要なポリシーを表示する地域を選択します。

標準領域

標準のリージョンでは、権限は2つのポリシーに分散されます。AWSの管理対象ポリシーの最大文字数に制限されているため、2つのポリシーが必要です。

1つ目のポリシーでは、次のサービスに対する権限を付与します。

- Amazon S3 バケットの検出
- バックアップとリカバリ
- 分類
- Cloud Volumes ONTAP
- FSX for ONTAP の略
- 階層化

2つ目のポリシーは、次のサービスに対する権限を提供します。

- エッジキャッシュ
- Kubernetes

ポリシー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"
        }
```

```
    ]
}
```

ポリシー#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（US）リージョン

```
{
    "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/*"
            ]
        }
    ]
}
```

シークレットリージョン

```
{
    "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/*"
            ]
        }
    ]
}
```

Top Secret領域

```
{
    "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権限の使用方法

以降のセクションでは、各BlueXPサービスでの権限の使用方法について説明します。この情報は、企業のポリシーによって、必要な場合にのみアクセス許可が指定されるように指定されている場合に役立ちます。

ONTAP 対応の Amazon FSX

コネクタは、Amazon FSx for ONTAP を管理するための次のAPI要求を行います。

- EC2: DescribeInstances
- EC2: DescribeInstanceStatus
- EC2: DescribeInstanceAttributeのこと
- EC2: DescribeRouteTables
- EC2: DescribeImages
- ec2：CreateTags
- EC2: DescribeVolumesの場合
- EC2: DescribeSecurityGroups
- EC2: DescribeNetworkInterfaces

- EC2: DescribeSubnets
- EC2: DescribeVpcs
- EC2: DescribeDhcpOptions
- ec2: DescribeSnapshots
- EC2：DescribeKeyPairs
- EC2: DescribeRegions (説明領域
- EC2: DescribeTags (説明タグ)
- EC2: DescribeIamInstanceProfileAssociations
- EC2: DescribeReservedInstancesOfferings
- EC2: DescribeVpcEndpoints
- EC2: DescribeVpcs
- EC2: DescribeVolumesModifications (EC2 : DescribeVolumesMod
- EC2: DescribePlacementGroups
- KMS：リスト*
- KMS：説明*
- KMS：CreateGrant
- KMS：エイリアスを確認する
- FSx：説明*
- FSx：リスト*

Amazon S3 バケットの検出

コネクタは、Amazon S3バケットを検出するために次のAPI要求を実行します。

S3 ： GetEncryptionConfiguration

バックアップとリカバリ

Connectorは、Amazon S3でバックアップを管理するために次のAPI要求を実行します。

- S3 ： GetBucketLocation
- S3 ： ListAllMyBuckets
- S3 ： ListBucket
- S3 ： CreateBucket を指定します
- S3 ： GetLifecycleConfiguration
- S3 ： PutLifecycleConfiguration
- S3 ： PutBucketTagging
- S3 ： ListBucketVersions
- S3 ： GetBucketAcl

- S3：PutBucketPublicAccessBlock
- KMS：リスト*
- KMS：説明*
- S3 ： GetObject
- EC2: DescribeVpcEndpoints
- KMS：エイリアスを確認する
- S3 ： PutEncryptionConfiguration

コネクタは、Search & Restoreメソッドを使用してボリュームとファイルをリストアする場合に次のAPI要求を実行します。

- S3 ： CreateBucket を指定します
- S3 ： DeleteObject
- S3 ： DeleteObjectVersion
- S3 ： GetBucketAcl
- S3 ： ListBucket
- S3 ： ListBucketVersions
- S3 ： ListBucketMultipartUploads
- S3 ： PutObject
- S3：PutBucketAcl
- S3 ： PutLifecycleConfiguration
- S3：PutBucketPublicAccessBlock
- S3 ： AbortMultipartUpload
- S3 ： ListMultipartUploadParts
- Athena：StartQueryExecution
- Athena: GetQueryResults.
- Athena: GetQueryExecution
- Athena：StopQueryExecution
- グルー：データベースを作成します
- グルー: CreateTable
- グルー: BatchDeletePartition

このコネクタは、データロックとランサムウェア保護を使用してボリュームのバックアップを行う際に次のAPI要求を実行します。

- S3 ： GetObjectVersionTagging
- S3 ： GetBucketObjectLockConfiguration
- S3：GetObjectVersionAcl

- S3 ： PutObjectTagging
- S3 ： DeleteObject
- S3 ： DeleteObjectTagging
- S3 ： GetObjectRetention
- S3 ： DeleteObjectVersionTagging
- S3 ： PutObject
- S3 ： GetObject
- S3 ： PutBucketObjectLockConfiguration
- S3 ： GetLifecycleConfiguration
- S3：ListBucketByTags
- S3 ： GetBucketTagging
- S3 ： DeleteObjectVersion
- S3 ： ListBucketVersions
- S3 ： ListBucket
- S3 ： PutBucketTagging
- S3 ： GetObjectTagging
- S3 ： PutBucketVersioning
- S3 ： PutObjectVersionTagging
- S3 ： GetBucketVersioning
- S3 ： GetBucketAcl
- S3：Bypassガバナー 保持
- S3 ： PutObjectRetention
- S3 ： GetBucketLocation
- S3 ： GetObjectVersion

Cloud Volumes ONTAP バックアップにソースボリュームとは異なるAWSアカウントを使用する場合、Connectorは次のAPI要求を実行します。

- S3 ： PutBucketPolicy
- S3：PutBucketOwnershipControls

分類

コネクタは、BlueXP分類インスタンスを導入するために次のAPI要求を行います。

- EC2: DescribeInstances
- EC2: DescribeInstanceStatus
- EC2：RunInstances

- EC2：TerminateInstances
- ec2：CreateTags
- EC2：CreateVolume
- EC2：AttachVolume
- EC2：CreateSecurityGroup
- EC2: DeleteSecurityGroup
- EC2: DescribeSecurityGroups
- EC2：CreateNetworkInterface
- EC2: DescribeNetworkInterfaces
- EC2：DeleteNetworkInterface
- EC2: DescribeSubnets
- EC2: DescribeVpcs
- EC2: CreateSnapshotの作成
- EC2: DescribeRegions (説明領域
- CloudFormation：CreateStack
- CloudFormation：DeleteStack
- CloudFormation：DescribeStack
- CloudFormation：DescribeStackEvents
- IAM：AddRoleToInstanceProfile
- EC2: AssociateIamInstanceProfile
- EC2: DescribeIamInstanceProfileAssociations

BlueXP分類を使用する場合、コネクタはS3バケットをスキャンするために次のAPI要求を行います。

- IAM：AddRoleToInstanceProfile
- EC2: AssociateIamInstanceProfile
- EC2: DescribeIamInstanceProfileAssociations
- S3 ： GetBucketTagging
- S3 ： GetBucketLocation
- S3 ： ListAllMyBuckets
- S3 ： ListBucket
- S3：GetBucketPolicyStatus
- S3 ： GetBucketPolicy
- S3 ： GetBucketAcl
- S3 ： GetObject
- IAM：GetRole

- S3 ： DeleteObject
- S3 ： DeleteObjectVersion
- S3 ： PutObject
- STS: AssumeRole

Cloud Volumes ONTAP

Connectorは、AWSでのCloud Volumes ONTAP の導入と管理に対して次のAPI要求を実行します。

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
Cloud Volumes ONTAP インスタンスのIAMロールとインスタンスプロファイルを作成および管理します	IAM ：ListInstanceProfiles	はい。	はい。	いいえ
	IAM ：CREATEROLE	はい。	いいえ	いいえ
	IAM：DeleteRole	いいえ	はい。	はい。
	IAM：PutRolePolicy	はい。	いいえ	いいえ
	IAM ：CreateInstanceProfile	はい。	いいえ	いいえ
	IAM ：DeleteRolePolicy	いいえ	はい。	はい。
	IAM ：AddRoleToInstanceProfile	はい。	いいえ	いいえ
	IAM ：RemoveRoleFromInstanceProfile	いいえ	はい。	はい。
	IAM ：DeleteInstanceProfile	いいえ	はい。	はい。
	IAM：PassRole	はい。	いいえ	いいえ
	EC2: AssociateIamInstanceProfile	はい。	はい。	いいえ
	EC2: DescribeIamInstanceProfileAssociations	はい。	はい。	いいえ
	EC2: DisassociateIamInstanceProfile	いいえ	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
読み取り許可ステータスメッセージ	STS: DecodeAuthorizationMessage	はい。	はい。	いいえ
アカウントで使用可能な指定イメージ（AMIS）について説明します	EC2: DescribeImages	はい。	はい。	いいえ
VPC内のルーティングテーブルの説明（HAペアの場合のみ必要）	EC2: DescribeRouteTables	はい。	いいえ	いいえ
インスタンスの停止、開始、監視	EC2：StartInstances（EC2：開始インスタンス	はい。	はい。	いいえ
	EC2：StopInstances	はい。	はい。	いいえ
	EC2: DescribeInstances	はい。	はい。	いいえ
	EC2: DescribeInstanceStatus	はい。	はい。	いいえ
	EC2：RunInstances	はい。	いいえ	いいえ
	EC2：TerminateInstances	いいえ	いいえ	はい。
	EC2：ModifyInstanceAttribute	いいえ	はい。	いいえ
サポートされるインスタンスタイプに対して拡張ネットワークが有効になっていることを確認します	EC2: DescribeInstanceAttributeのこと	いいえ	はい。	いいえ
メンテナンスとコストの割り当てに使用する「WorkingEnvironment」タグと「WorkingEnvironmentId」タグを使用してリソースにタグを付けます	ec2：CreateTags	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
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：CreateVolume	はい。	はい。	いいえ
	EC2: DescribeVolumesの場合	はい。	はい。	はい。
	EC2 ：ModifyVolumeAttributeのことです	いいえ	はい。	はい。
	EC2：AttachVolume	はい。	はい。	いいえ
	EC2：DeleteVolume	いいえ	はい。	はい。
	EC2 ：DetachVolumeの場合	いいえ	はい。	はい。
Cloud Volumes ONTAP のセキュリティグループを作成および管理します	EC2 ：CreateSecurityGroup	はい。	いいえ	いいえ
	EC2: DeleteSecurityGroup	いいえ	はい。	はい。
	EC2: DescribeSecurityGroups	はい。	はい。	はい。
	EC2: RevokeSecurityGroupEgress	はい。	いいえ	いいえ
	ec2 ：AuthorizeSecurityGroupEgress	はい。	いいえ	いいえ
	ec2 ：AuthorizeSecurityGroupIngress	はい。	いいえ	いいえ
	EC2: RevokeSecurityGroupIngress	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
ターゲットサブネットの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：CreateNetworkInterface	はい。	いいえ	いいえ
	EC2: DescribeNetworkInterfaces	はい。	はい。	いいえ
	EC2：DeleteNetworkInterface	いいえ	はい。	はい。
	EC2:ModifyNetworkInterfaceAttributeのいずれかです	いいえ	はい。	いいえ
デスティネーションのサブネットとセキュリティグループの一覧を取得します	EC2: DescribeSubnets	はい。	はい。	いいえ
	EC2: DescribeVpcs	はい。	はい。	いいえ
Cloud Volumes ONTAP インスタンスのDNSサーバおよびデフォルトのドメイン名を取得します	EC2: DescribeDhcpOptions	はい。	いいえ	いいえ
Cloud Volumes ONTAP 用のEBSボリュームのSnapshotを作成します	EC2: CreateSnapshotの作成	はい。	はい。	いいえ
	EC2：DeleteSnapshot	いいえ	はい。	はい。
	ec2: DescribeSnapshots	いいえ	はい。	いいえ
AutoSupport メッセージに添付されているCloud Volumes ONTAP コンソールをキャプチャします	EC2: GetConsoleOutput	はい。	はい。	いいえ
使用可能なキーペアのリストを取得します	EC2：DescribeKeyPairs	はい。	いいえ	いいえ
使用可能なAWSリージョンのリストを取得します	EC2: DescribeRegions (説明領域	はい。	はい。	いいえ
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	EC2:タグを削除します	いいえ	はい。	はい。
	EC2: DescribeTags (説明タグ)	いいえ	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
AWS CloudFormationテンプレートのスタックの作成と管理	CloudFormation：CreateStack	はい。	いいえ	いいえ
	CloudFormation：DeleteStack	はい。	いいえ	いいえ
	CloudFormation：DescribeStack	はい。	はい。	いいえ
	CloudFormation：DescribeStackEvents	はい。	いいえ	いいえ
	CloudFormation：ValidateTemplate	はい。	いいえ	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
Cloud Volumes ONTAP システムでデータ階層として使用するS3バケットを作成および管理します	S3 ： CreateBucket を指定します	はい。	はい。	いいえ
	S3 ： DeleteBucket	いいえ	はい。	はい。
	S3 ： GetLifecycleConfiguration	いいえ	はい。	いいえ
	S3 ： PutLifecycleConfiguration	いいえ	はい。	いいえ
	S3 ： PutBucketTagging	いいえ	はい。	いいえ
	S3 ： ListBucketVersions	いいえ	はい。	いいえ
	S3 ：GetBucketPolicyStatus	いいえ	はい。	いいえ
	S3 ：GetBucketPublicAccessBlock	いいえ	はい。	いいえ
	S3 ： GetBucketAcl	いいえ	はい。	いいえ
	S3 ： GetBucketPolicy	いいえ	はい。	いいえ
	S3 ：PutBucketPublicAccessBlock	いいえ	はい。	いいえ
	S3 ： GetBucketTagging	いいえ	はい。	いいえ
	S3 ： GetBucketLocation	いいえ	はい。	いいえ
	S3 ： ListAllMyBuckets	いいえ	いいえ	いいえ
	S3 ： ListBucket	いいえ	はい。	いいえ
AWS Key Management Service（KMS；キー管理サービス）を使用してCloud Volumes ONTAP のデータ暗号化を有効にする	KMS：リスト*	はい。	はい。	いいえ
	KMS：再暗号化*	はい。	いいえ	いいえ
	KMS：説明*	はい。	はい。	いいえ
	KMS：CreateGrant	はい。	はい。	いいえ
	KMS ：GenerateDataKeyWithoutPlaintext	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
2つのHAノードとメディエーター用のAWS分散配置グループを1つのAWSアベイラビリティゾーンに作成して管理します	EC2：CreatePlacementGroup	はい。	いいえ	いいえ
	EC2: DeletePlacementGroup	いいえ	はい。	はい。
レポートを作成します	FSx：説明*	いいえ	はい。	いいえ
	FSx：リスト*	いいえ	はい。	いいえ
Amazon EBS Elastic Volumes機能をサポートするアグリゲートを作成して管理します	EC2: DescribeVolumesModifications (EC2 : DescribeVolumesMod	いいえ	はい。	いいえ
	EC2：ModifyVolume	いいえ	はい。	いいえ

エッジキャッシュ

コネクタは、導入時にBlueXPエッジキャッシュインスタンスを導入するために次のAPI要求を行います。

- CloudFormation：DescribeStack
- CloudWatch：GetMetricStatistics
- CloudFormation：リストスタック

Kubernetes

コネクタは、次のAPI要求を実行してAmazon EKSクラスタを検出および管理します。

- EC2: DescribeRegions (説明領域
- EKS：リストクラスタ
- EKS：DescribeCluster
- IAM：GetInstanceProfile

変更ログ

権限が追加および削除されると、以下のセクションにそれらの権限が表示されます。

2024年3月8日

次の権限がコネクタポリシーに含まれるようになりました。

EC2：説明AvailabilityZones

この権限は、今後のリリースで必要になります。リリースノートの詳細については、リリースノートを更新し

ます。

2023年6月6日

Cloud Volumes ONTAPには次の権限が必要です。

KMS：GenerateDataKeyWithoutPlaintext

2023年2月14日

BlueXPの階層化には次の権限が必要です。

EC2: DescribeVpcEndpoints

Connector の Azure 権限

BlueXPがAzureでConnector VMを起動すると、そのAzureサブスクリプション内のリソースとプロセスを管理するための権限をConnectorに提供するカスタムロールがVMに割り当てられます。Connectorは、権限を使用して複数のAzureサービスに対してAPI呼び出しを実行します。

カスタムロールの権限

以下のカスタムロールには、Azureネットワーク内のリソースとプロセスを管理するためにConnectorで必要となる権限が含まれています。

BlueXPからコネクタを直接作成すると、BlueXPは自動的にこのカスタムロールをコネクタに適用します。

Azure MarketplaceからConnectorを導入する場合、またはLinuxホストにConnectorを手動でインストールする場合は、カスタムロールを自分で設定する必要があります。

これらのポリシーの使用手順については、次のページを参照してください。

- "Azure Marketplace環境の権限を設定する"
- "オンプレミス環境の権限を設定する"
- "制限モードの権限を設定します"
- "プライベートモードの権限を設定します"

また、新しい権限が以降のリリースで追加されるときに、ロールが最新の状態であることを確認する必要があります。

```
{
    "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権限の使用方法

以降のセクションでは、各BlueXPサービスでの権限の使用方法について説明します。この情報は、企業のポリシーによって、必要な場合にのみアクセス許可が指定されるように指定されている場合に役立ちます。

Azure NetApp Files の特長

BlueXP分類を使用してAzure NetApp Filesデータをスキャンする場合、コネクタは次のAPI要求を行います。

- 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

バックアップとリカバリ

コネクタは、BlueXPのバックアップとリカバリ用に次のAPI要求を行います。

- microsoft.Storage/storageAccounts/listkeys/action
- microsoft.Storage/storageAccounts/read
- microsoft.Storage/storageAccounts/write
- microsoft.Storage/storageAccounts/blobServices/container/read
- microsoft.Storage/storageAccountSas/action
- microsoft.KeyVault/vaults/read
- Microsoft。KeyVault/vaults/accessPolicies/write
- Microsoft.Network/networkInterfaces/read
- microsoft.Resources/Subscriptions /locations /read
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- microsoft.Resources/Subscriptions /resourceGroups/read
- microsoft.resources/Subscriptions /resourcegroups/resources/read
- microsoft.Resources/Subscriptions /resourceGroups/write
- Microsoft 。許可/ロック/
- 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.Resources/Deployments/delete
- microsoft.ManagedIdentity/userAssignedIdentities/assign/action

検索とリストア機能を使用すると、コネクタは次のAPI要求を実行します。

- Microsoft .Synapse/workspaces /書き込み
- Microsoft . Synapse/workspaces / read
- Microsoft .Synapse/workspaces /削除
- 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 /操作結果/読み取り
- Microsoft .Synapse/workspaces /privateEndpointConnectionsApproval / action

分類

BlueXP分類を使用する場合、コネクタは次のAPI要求を行います。

アクション	セットアップに使用？	日々の業務に使用されるか？
Microsoft.Compute/locations/operations/read	はい。	はい。
Microsoft.Compute/locations/vmSizes/read	はい。	はい。
Microsoft.Compute/operations/read	はい。	はい。
Microsoft.Compute/virtualMachines/instanceView/read	はい。	はい。
Microsoft.Compute/virtualMachines/powerOff/action	はい。	いいえ
Microsoft.Compute/virtualMachines/read	はい。	はい。
Microsoft.Compute/virtualMachines/restart/action	はい。	いいえ
Microsoft.Compute/virtualMachines/start/action	はい。	いいえ
Microsoft.Compute/virtualMachines/vmSizes/read	いいえ	はい。
Microsoft.Compute/virtualMachines/write	はい。	いいえ
Microsoft.Compute/images/read	はい。	はい。
Microsoft.Compute/disks/delete	はい。	いいえ
Microsoft.Compute/disks/read	はい。	はい。
Microsoft.Compute/disks/write	はい。	いいえ
Microsoft. Storage/checknameavailability/read	はい。	はい。
Microsoft。ストレージ/運用/読み取り	はい。	はい。
microsoft.Storage/storageAccounts/listkeys/action	はい。	いいえ
microsoft.Storage/storageAccounts/read	はい。	はい。

アクション	セットアップに使用？	日々の業務に使用されるか？
microsoft.Storage/storageAccounts/write	はい。	いいえ
microsoft.Storage/storageAccounts/blobServices/container/read	はい。	はい。
Microsoft.Network/networkInterfaces/read	はい。	はい。
Microsoft.Network/networkInterfaces/write	はい。	いいえ
Microsoft.Network/networkInterfaces/join/action	はい。	いいえ
Microsoft.Network/networkSecurityGroups/read	はい。	はい。
Microsoft.Network/networkSecurityGroups/write	はい。	いいえ
microsoft.Resources/Subscriptions/locations /read	はい。	はい。
Microsoft.Network/locations/operationResults/read	はい。	はい。
Microsoft.Network/locations/operations/read	はい。	はい。
Microsoft.Network/virtualNetworks/read	はい。	はい。
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	はい。	はい。
Microsoft.Network/virtualNetworks/subnets/read	はい。	はい。
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	はい。	はい。
Microsoft.Network/virtualNetworks/virtualMachines/read	はい。	はい。
Microsoft.Network/virtualNetworks/subnets/join/action	はい。	いいえ
Microsoft.Network/virtualNetworks/subnets/write	はい。	いいえ
Microsoft.Network/routeTables/join/action	はい。	いいえ
microsoft.Resources/Deployments/operations/read	はい。	はい。
Microsoft .Resources/Deployments/read	はい。	はい。

アクション	セットアップに使用？	日々の業務に使用されるか？
Microsoft .Resources/Deployments/write	はい。	いいえ
microsoft.resources/resources/read	はい。	はい。
microsoft.Resources/Subscriptions /operationresults/read	はい。	はい。
microsoft.Resources/Subscriptions /resourceGroups/delete	はい。	いいえ
microsoft.Resources/Subscriptions /resourceGroups/read	はい。	はい。
microsoft.resources/Subscriptions /resourcegroups/resources/read	はい。	はい。
microsoft.Resources/Subscriptions /resourceGroups/write	はい。	いいえ

Cloud Volumes ONTAP

Connectorは、AzureでCloud Volumes ONTAP の導入と管理を行うために次のAPI要求を実行します。

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
VMの作成と管理	Microsoft.Compute/locations/operations/read	はい。	はい。	いいえ
	Microsoft.Compute/locations/vmSizes/read	はい。	はい。	いいえ
	microsoft.Resources/Subscriptions/locations /read	はい。	いいえ	いいえ
	Microsoft.Compute/operations/read	はい。	はい。	いいえ
	Microsoft.Compute/virtualMachines/instanceView/read	はい。	はい。	いいえ
	Microsoft.Compute/virtualMachines/powerOff/action	はい。	はい。	いいえ
	Microsoft.Compute/virtualMachines/read	はい。	はい。	いいえ
	Microsoft.Compute/virtualMachines/restart/action	はい。	はい。	いいえ
	Microsoft.Compute/virtualMachines/start/action	はい。	はい。	いいえ
	Microsoft.Compute/virtualMachines/deallocate/action	いいえ	はい。	はい。
	Microsoft.Compute/virtualMachines/vmSizes/read	いいえ	はい。	いいえ
	Microsoft.Compute/virtualMachines/write	はい。	はい。	いいえ
	Microsoft.Compute/virtualMachines/delete	はい。	はい。	はい。
	microsoft.Resources/Deployments/delete	はい。	いいえ	いいえ
VHDからの導入を有効にします	Microsoft.Compute/images/read	はい。	いいえ	いいえ
	Microsoft.Compute/images/write	はい。	いいえ	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
ターゲットサブネット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/networkInterfaces/read	はい。	はい。	いいえ
	Microsoft.Network/networkInterfaces/write	はい。	はい。	いいえ
	Microsoft.Network/networkInterfaces/join/action	はい。	はい。	いいえ
	Microsoft.Network/networkInterfaces/delete	はい。	はい。	いいえ
ネットワークセキュリティグループを作成および管理します	Microsoft.Network/networkSecurityGroups/read	はい。	はい。	いいえ
	Microsoft.Network/networkSecurityGroups/write	はい。	はい。	いいえ
	Microsoft.Network/networkSecurityGroups/join/action	はい。	いいえ	いいえ
	Microsoft.Network/networkSecurityGroups/delete	いいえ	はい。	はい。

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
リージョンおよびターゲットのVNetとサブネットのネットワーク情報を取得し、VMをVNetに追加します	Microsoft.Network/locations/operationResults/read	はい。	はい。	いいえ
	Microsoft.Network/locations/operations/read	はい。	はい。	いいえ
	Microsoft.Network/virtualNetworks/read	はい。	いいえ	いいえ
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	はい。	いいえ	いいえ
	Microsoft.Network/virtualNetworks/subnets/read	はい。	はい。	いいえ
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	はい。	はい。	いいえ
	Microsoft.Network/virtualNetworks/virtualMachines/read	はい。	はい。	いいえ
	Microsoft.Network/virtualNetworks/subnets/join/action	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
リソースグループを作成および管理する	microsoft.Resources/Deployments/operations/read	はい。	はい。	いいえ
	Microsoft.Resources/Deployments/read	はい。	はい。	いいえ
	Microsoft.Resources/Deployments/write	はい。	はい。	いいえ
	microsoft.resources/resources/read	はい。	はい。	いいえ
	microsoft.Resources/Subscriptions/operationresults/read	はい。	はい。	いいえ
	microsoft.Resources/Subscriptions/resourceGroups/delete	はい。	はい。	はい。
	microsoft.Resources/Subscriptions/resourceGroups/read	いいえ	はい。	いいえ
	microsoft.resources/Subscriptions/resourcegroups/resources/read	はい。	はい。	いいえ
	microsoft.Resources/Subscriptions/resourceGroups/write	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
Azureストレージアカウントおよびディスクを管理する	Microsoft.Compute/disks/read	はい。	はい。	はい。
	Microsoft.Compute/disks/write	はい。	はい。	いいえ
	Microsoft.Compute/disks/delete	はい。	はい。	はい。
	Microsoft.Storage/checknameavailability/read	はい。	はい。	いいえ
	Microsoft。ストレージ/運用/読み取り	はい。	はい。	いいえ
	microsoft.Storage/storageAccounts/listkeys/action	はい。	はい。	いいえ
	microsoft.Storage/storageAccounts/read	はい。	はい。	いいえ
	microsoft.Storage/storageAccounts/delete	いいえ	はい。	はい。
	microsoft.Storage/storageAccounts/write	はい。	はい。	いいえ
	Microsoft.Storage/uses/read：ストレージ/使用状況/読み取り	いいえ	はい。	いいえ
ストレージアカウントのBLOBストレージへのバックアップと暗号化を有効にします	microsoft.Storage/storageAccounts/blobServices/container/read	はい。	はい。	いいえ
	microsoft.KeyVault/vaults/read	はい。	はい。	いいえ
	Microsoft。KeyVault/vaults/accessPolicies/write	はい。	はい。	いいえ
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.Network/virtualNetworks/subnets/write	はい。	はい。	いいえ
	Microsoft.Network/routeTables/join/action	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
Azureで管理されるSnapshotを作成および管理します	Microsoft.Compute/snapshots/write	はい。	はい。	いいえ
	Microsoft.Compute/snapshots/read	はい。	はい。	いいえ
	Microsoft.Compute/snapshots/delete	いいえ	はい。	はい。
	Microsoft.Compute/disks/beginGetAccess/action	いいえ	はい。	いいえ
アベイラビリティセットを作成および管理します	Microsoft.Compute/availabilitySets/write	はい。	いいえ	いいえ
	Microsoft.Compute/availabilitySets/read	はい。	いいえ	いいえ
市場からのプログラムによる導入を可能にします	"Microsoft.MarketplaceOrdering/offerTypes/publisher/offers/plans/agrees/read	はい。	いいえ	いいえ
	"Microsoft.MarketplaceOrdering/offerTypes/publisher/offers/plans/agrees/write	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
HAペアのロードバランサを管理します	Microsoft.Network/loadBalancers/read	はい。	はい。	いいえ
	Microsoft.Network/loadBalancers/write	はい。	いいえ	いいえ
	Microsoft.Network/loadBalancers/delete	いいえ	はい。	はい。
	Microsoft.Network/loadBalancers/backendAddressPools/read	はい。	いいえ	いいえ
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	はい。	いいえ	いいえ
	Microsoft.Network/loadBalancers/frontendIPConfigurations/read	はい。	はい。	いいえ
	Microsoft.Network/loadBalancers/loadBalancingRules/read	はい。	いいえ	いいえ
	Microsoft.Network/loadBalancers/probes/read	はい。	いいえ	いいえ
	Microsoft.Network/loadBalancers/probes/join/action	はい。	いいえ	いいえ
Azureディスク上のロックの管理を有効にします	Microsoft 。許可/ロック/	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
サブネット外に接続がない場合は、HAペアのプライベートエンドポイントを有効にします	Microsoft.Network/privateEndpoints/write	はい。	はい。	いいえ
	microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval / action	はい。	いいえ	いいえ
	microsoft.Storage/storageAccounts/privateEndpointConnections/ read	はい。	はい。	はい。
	Microsoft.Network/privateEndpoints/read	はい。	はい。	はい。
	Microsoft.Network/privateDnsZones/write	はい。	はい。	いいえ
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/write	はい。	はい。	いいえ
	Microsoft.Network/virtualNetworks/join/action	はい。	はい。	いいえ
	Microsoft.Network/privateDnsZones/A/write	はい。	はい。	いいえ
	Microsoft.Network/privateDnsZones/read	はい。	はい。	いいえ
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/read	はい。	はい。	いいえ
基盤となる物理ハードウェアに応じて、一部のVM環境で必要です	microsoft.Resources/Deployments/operationStatuses /read	はい。	はい。	いいえ
導入に失敗した場合やリソースを削除した場合は、リソースグループからリソースを削除します	Microsoft.Network/privateEndpoints/delete	はい。	はい。	いいえ
	Microsoft.Compute/availabilitySets/delete	はい。	はい。	いいえ

目的	アクション	導入に使用	日々の業務に使用されるか？	削除しますか？
APIを使用する際に、お客様が管理する暗号化キーの使用を有効にします	Microsoft.Compute/diskEncryptionSets/read	はい。	はい。	はい。
	Microsoft.Compute/diskEncryptionSets/write	はい。	はい。	いいえ
	microsoft.KeyVault/vaults/deploy/action	はい。	いいえ	いいえ
	Microsoft.Compute/diskEncryptionSets/delete	はい。	はい。	はい。
HAペアのアプリケーションセキュリティグループを設定して、HAインターコネクトのNICとクラスタネットワークのNICを分離します	Microsoft.Network/applicationSecurityGroups/write	いいえ	はい。	いいえ
	Microsoft.Network/applicationSecurityGroups/read	いいえ	はい。	いいえ
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	いいえ	はい。	いいえ
	Microsoft.Network/networkSecurityGroups/securityRules/write	はい。	はい。	いいえ
	Microsoft.Network/applicationSecurityGroups/delete	いいえ	はい。	はい。
	Microsoft.Network/networkSecurityGroups/securityRules/delete	いいえ	はい。	はい。
Cloud Volumes ONTAP リソースに関連付けられたタグの読み取り、書き込み、および削除	microsoft.Resources/tags/read	いいえ	はい。	いいえ
	microsoft.Resources/tags/write	はい。	はい。	いいえ
	microsoft.Resources/tags/delete	はい。	いいえ	いいえ
作成時にストレージアカウントを暗号化	microsoft.ManagedIdentity/userAssignedIdentities/assign/action	はい。	はい。	いいえ

エッジキャッシュ

BlueXPエッジキャッシングを使用する場合、コネクタは次のAPI要求を行います。

- 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

Kubernetes

Connectorは、Azure Kubernetes Service（AKS）で実行されているクラスタを検出し管理するために次のAPI要求を実行します。

- Microsoft.Compute/virtualMachines/read
- microsoft.Resources/Subscriptions /locations /read
- microsoft.Resources/Subscriptions /operationresults/read
- microsoft.Resources/Subscriptions /resourceGroups/read
- microsoft.resources/Subscriptions /resourcegroups/resources/read
- Microsoft .ContainerService/managedClusters/read
- Microsoft .ContainerService/managedClusters/listClusterUserCredential/action

階層化

BlueXP階層化のセットアップ時に、コネクタは次のAPI要求を行います。

- microsoft.Storage/storageAccounts/listkeys/action
- microsoft.Resources/Subscriptions /resourceGroups/read
- microsoft.Resources/Subscriptions /locations /read

このコネクタは、次のAPI要求を日々の処理に送信します。

- microsoft.Storage/storageAccounts/blobServices/container/read
- Microsoft。Storage/storageAccounts/managementPolicies/read
- microsoft.StorageAccounts/managementPolicies/write
- microsoft.Storage/storageAccounts/read

変更ログ

権限が追加および削除されると、以下のセクションにそれらの権限が表示されます。

2023年12月5日

Azure BLOBストレージにボリュームデータをバックアップする場合、BlueXPのバックアップとリカバリに次の権限は不要になりました。

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

これらの権限は他のBlueXPストレージサービスに必要なため、他のストレージサービスを使用している場合はコネクタのカスタムロールが引き続き使用されます。

2023年5月12日

次の権限はCloud Volumes ONTAP の管理に必要なため、JSONポリシーに追加されました。

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

JSONポリシーから次の権限が削除されました。これらの権限は不要になりました。

- microsoft.Storage/storageAccounts/blobServices/container/write
- Microsoft.Network/publicIPAddresses/delete

2023年3月23日

BlueXPの分類に「Microsoft.Storage/storageAccounts/delete」権限は不要になりました。

この権限はCloud Volumes ONTAP では引き続き必要です。

2023年1月5日

JSONポリシーに次の権限が追加されました。

- microsoft.Storage/storageAccountSas/action
- Microsoft .Synapse/workspaces /privateEndpointConnectionsApproval / action

  これらの権限はBlueXPのバックアップとリカバリに必要です。

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

  この権限はCloud Volumes ONTAP の導入に必要です。

Connector の Google Cloud 権限

BlueXPには、Google Cloudでアクションを実行するための権限が必要です。これらの権

限は、ネットアップが提供するカスタムロールに含まれています。これらの権限でBlue XPが何を実行するのかを理解しておくとよいでしょう。

サービスアカウントの権限

次のカスタムロールは、ConnectorがGoogle Cloudネットワーク内のリソースとプロセスを管理するために必要な権限を提供します。

このカスタムロールは、Connector VMに関連付けられているサービスアカウントに適用する必要があります。

- "標準モードのGoogle Cloud権限を設定します"
- "制限モードの権限を設定します"
- "プライベートモードの権限を設定します"

また、新しい権限が以降のリリースで追加されるときに、ロールが最新の状態であることを確認する必要があります。

```
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
```

Google Cloud権限の使用方法

アクション	目的
- compute.disks.create - compute.disks.createsnapshot - compute.disks.delete -コンピューティング、ディスク、取得 - compute.disksリスト - 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。
- compute.firewalls.create - compute.firewalls.delete -コンピューティング、ファイアウォール、取得 - compute.firewalls.list	Cloud Volumes ONTAP のファイアウォールルールを作成します。

アクション	目的
-computer.globalOperationsGet	処理のステータスを確認できます。
-計算画像取得 - compute.images.getFromFamily - compute.images.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 -コンピュートスナップショット取得 - compute.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 - compute.regions.get - compute.regions.list - compute.subnetworks.get - compute.subnetworks.list - compute.zoneOperations.get -コンピュートゾーン取得 - compute.zones.list	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.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	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。
-storage.buckets.create - storage.buckets.delete -ストレージ、バケツ、取得します -storage.buckets.list -storage.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 - cloudkms.keyrings.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.objects.list	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-addresslist	HAペアを導入する際にリージョン内のアドレスを取得する。
-compute.backendServices.create -compute.regionBackendServices.create -compute.regionBackendServices.get -compute.regionBackendServices.list	HAペアでトラフィックを分散するためのバックエンドサービスを設定するには、次の手順を実行します。
- compute.networks.updatePolicy	HAペアのVPCおよびサブネットにファイアウォールルールを適用する。
- compute.subnetworks.us - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	してBlueXPの分類を有効にします。

アクション	目的
-container.clusters.get -container.clusters.list	Google Kubernetes Engine で実行されている Kubernetes クラスタを検出する。
- compute.instanceGroups.get -計算アドレス取得 - compute.instances.updateNetworkInterface	Cloud Volumes ONTAP HAペアでStorage VMを作成および管理する方法。
- monitoring.timeseries.list -storage.buckets.getIamPolicy	をクリックして、Google Cloud Storageバケットに関する情報を確認してください。
- cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.getIamPolicy - cloudkms.cryptoKeys.list - cloudkms.cryptoKeys.setIamPolicy - cloudkmsキーリング取得 - cloudkms.keyrings.getIamPolicy - cloudkms.keyrings.list - cloudkms.keyRings.setIamPolicy	Googleが管理するデフォルトの暗号化キーを使用する代わりに、BlueXPのバックアップとリカバリのアクティブ化ウィザードでお客様が管理する独自のキーを選択します。

変更ログ

権限が追加および削除されると、以下のセクションにそれらの権限が表示されます。

2023年2月6日

このポリシーには次の権限が追加されています：

- compute.instances.updateNetworkInterface

この権限はCloud Volumes ONTAP に必要です。

2023年1月27日

ポリシーに追加された権限は次のとおりです。

- Cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- Cloudkms.keyrings.get
- cloudks.keyrings.getIamPolicyを参照してください
- cloudkms.keyRings.setIamPolicy

これらの権限はBlueXPのバックアップとリカバリに必要です。