참조하십시오

Setup and administration

NetApp
April 26, 2024

목차

참조하십시오

권한

BlueXP에 대한 권한 요약

BlueXP 기능 및 서비스를 사용하려면 BlueXP가 클라우드 환경에서 작업을 수행할 수 있도록 권한을 제공해야 합니다. 이 페이지의 링크를 사용하여 목표에 따라 필요한 사용 권한에 빠르게 액세스할 수 있습니다.

AWS 권한

BlueXP를 사용하려면 Connector 및 개별 서비스에 대한 AWS 권한이 필요합니다.

커넥터

목표	설명	링크
BlueXP에서 Connector를 구축합니다	BlueXP에서 Connector를 생성하는 사용자는 AWS에 인스턴스를 배포하기 위한 특정 권한이 필요합니다.	"AWS 권한을 설정합니다"
커넥터에 대한 사용 권한을 제공합니다	BlueXP에서 Connector를 시작하면 해당 인스턴스에 정책을 연결하여 AWS 계정의 리소스와 프로세스를 관리하는 데 필요한 권한을 제공합니다. AWS Marketplace에서 Connector를 시작하거나 커넥터를 수동으로 설치한 경우 또는 직접 정책을 설정해야 합니다 "Connector에 AWS 자격 증명을 더 추가합니다". 또한 새 권한이 후속 릴리스에 추가될 때 정책이 최신 상태인지 확인해야 합니다.	"Connector에 대한 AWS 권한"

백업 및 복구

목표	설명	링크
사내 ONTAP 클러스터를 Amazon S3에 백업	ONTAP 볼륨에서 백업을 활성화할 때 특정 권한이 있는 IAM 사용자에 대한 액세스 키와 암호를 입력하라는 메시지가 BlueXP 백업 및 복구에 표시됩니다.	"백업에 대한 S3 권한을 설정합니다"

Cloud Volumes ONTAP

목표	설명	링크
Cloud Volumes ONTAP 노드에 대한 권한을 제공합니다	IAM 역할은 AWS의 각 Cloud Volumes ONTAP 노드에 연결되어야 합니다. HA 중재자의 경우도 마찬가지입니다. 기본 옵션은 BlueXP가 IAM 역할을 생성할 수 있도록 하는 것이지만, 작업 환경을 생성할 때는 자신의 역할을 사용할 수 있습니다.	"IAM 역할을 직접 설정하는 방법에 대해 알아봅니다"

복사 및 동기화

목표	설명	링크
AWS에서 데이터 브로커를 구축합니다	데이터 브로커를 구축하는 데 사용하는 AWS 사용자 계정에는 특정 권한이 있어야 한다.	"AWS에서 데이터 브로커를 구축하는 데 필요한 권한입니다"
데이터 브로커에 대한 권한을 제공한다	BlueXP 복사 및 동기화가 데이터 브로커를 배포할 때 데이터 브로커 인스턴스에 대해 IAM 역할을 생성합니다. 원할 경우 자체 IAM 역할을 사용하여 데이터 브로커를 배포할 수 있습니다.	"AWS 데이터 브로커와 함께 IAM 역할을 사용해야 합니다"
수동으로 설치된 데이터 브로커에 대해 AWS 액세스가 활성화됩니다	S3 버킷이 포함된 동기화 관계에서 데이터 브로커를 사용하는 경우 AWS 액세스를 위해 Linux 호스트를 준비해야 합니다. 데이터 브로커를 설치할 때 프로그래밍 방식 액세스 및 특정 권한이 있는 IAM 사용자에게 AWS 키를 제공해야 합니다.	"AWS에 대한 액세스 설정"

ONTAP용 FSX

목표	설명	링크
FSx for ONTAP을 생성하고 관리합니다	Amazon FSx for NetApp ONTAP 작업 환경을 생성하거나 관리하려면 작업 환경을 생성하는 데 필요한 권한을 BlueXP에 제공하는 IAM 역할의 ARN을 제공하여 AWS 자격 증명을 BlueXP에 추가해야 합니다.	"FSx용 AWS 자격 증명을 설정하는 방법을 알아보십시오"

계층화

목표	설명	링크
사내 ONTAP 클러스터를 Amazon S3에 계층화	BlueXP 계층화를 AWS에 활성화하면 마법사에서 액세스 키와 비밀 키를 입력하라는 메시지가 표시됩니다. 이러한 자격 증명은 ONTAP 클러스터에 전달되므로 ONTAP은 데이터를 S3 버킷으로 계층화할 수 있습니다.	"계층화에 S3 사용 권한 설정"

Azure 권한

BlueXP를 사용하려면 Connector 및 개별 서비스에 대한 Azure 권한이 필요합니다.

커넥터

목표	설명	링크
BlueXP에서 Connector를 구축합니다	BlueXP에서 Connector를 배포하는 경우 Azure에 Connector VM을 배포할 수 있는 권한이 있는 Azure 계정 또는 서비스 보안 주체를 사용해야 합니다.	"Azure 권한을 설정합니다"

목표	설명	링크
커넥터에 대한 사용 권한을 제공합니다	BlueXP는 Azure에 Connector VM을 배포할 때 Azure 구독 내에서 리소스와 프로세스를 관리하는 데 필요한 권한을 제공하는 사용자 지정 역할을 생성합니다. 마켓플레이스에서 커넥터를 시작하거나 커넥터를 수동으로 설치한 경우 또는 사용자 지정 역할을 직접 설정해야 합니다 "Connector에 Azure 자격 증명을 더 추가합니다". 또한 새 권한이 후속 릴리스에 추가될 때 정책이 최신 상태인지 확인해야 합니다.	"Connector에 대한 Azure 권한"

복사 및 동기화

목표	설명	링크
Azure에서 데이터 브로커를 배포합니다	데이터 브로커를 배포하는 데 사용하는 Azure 사용자 계정에는 필요한 권한이 있어야 합니다.	"Azure에서 데이터 브로커를 배포하는 데 필요한 권한입니다"

Google Cloud 권한

BlueXP를 사용하려면 Connector 및 개별 서비스에 대한 Google Cloud 권한이 필요합니다.

커넥터

목표	설명	링크
BlueXP에서 Connector를 구축합니다	BlueXP의 Connector를 배포하는 Google Cloud 사용자는 Google Cloud에 Connector를 배포하기 위한 특정 권한이 필요합니다.	"커넥터를 만들 수 있는 권한을 설정합니다"
커넥터에 대한 사용 권한을 제공합니다	Connector VM 인스턴스의 서비스 계정에는 일상적인 작업에 대한 특정 권한이 있어야 합니다. 배포 중에 서비스 계정을 커넥터에 연결해야 합니다. 또한 새 권한이 후속 릴리스에 추가될 때 정책이 최신 상태인지 확인해야 합니다.	"Connector에 대한 권한을 설정합니다"

백업 및 복구

목표	설명	링크
Cloud Volumes ONTAP을 Google Cloud에 백업합니다	BlueXP 백업 및 복구를 사용하여 Cloud Volumes ONTAP를 백업할 때 다음 시나리오에서 커넥터에 권한을 추가해야 합니다. • "검색 및 복원" 기능을 사용하려고 합니다 • 고객 관리 암호화 키(CMEK)를 사용하려는 경우	• "검색 및 표시 권한; 복원 기능" • "CMEK에 대한 권한"

목표	설명	링크
사내 ONTAP 클러스터를 Google Cloud로 백업	BlueXP 백업 및 복구를 사용하여 온프레미스 ONTAP 클러스터를 백업하는 경우 "검색 및 복원" 기능을 사용하려면 커넥터에 권한을 추가해야 합니다.	"검색 및 표시 권한; 복원 기능"

Google Cloud용 Cloud Volumes Service

목표	설명	링크
Google Cloud용 Cloud Volumes Service를 만나보세요	BlueXP는 Google Cloud 서비스 계정을 통해 Cloud Volumes Service API 및 올바른 사용 권한에 액세스해야 합니다.	"서비스 계정을 설정합니다"

복사 및 동기화

목표	설명	링크
Google Cloud에서 데이터 브로커를 배포합니다	데이터 브로커를 구축하는 Google Cloud 사용자에게 필요한 권한이 있는지 확인한다.	"Google Cloud에서 데이터 브로커를 배포하는 데 필요한 권한입니다"
수동으로 설치된 데이터 브로커에 대해 Google Cloud 액세스 활성화	Google Cloud Storage 버킷을 포함하여 동기화 관계에 데이터 브로커를 사용할 계획이라면, Google Cloud 액세스를 위한 Linux 호스트를 준비해야 합니다. 데이터 브로커를 설치할 때 특정 권한이 있는 서비스 계정에 대한 키를 제공해야 합니다.	"Google Cloud에 대한 액세스를 활성화합니다"

StorageGRID 권한

BlueXP를 사용하려면 2가지 서비스에 대한 StorageGRID 권한이 필요합니다.

백업 및 복구

목표	설명	링크
사내 ONTAP 클러스터를 StorageGRID로 백업	StorageGRID를 ONTAP 클러스터의 백업 대상으로 준비할 때 BlueXP 백업 및 복구 시 특정 권한이 있는 IAM 사용자에 대한 액세스 키와 암호를 입력하라는 메시지가 표시됩니다.	"StorageGRID를 백업 타겟으로 준비합니다"

계층화

목표	설명	링크
사내 ONTAP 클러스터를 StorageGRID로 계층화	StorageGRID에 BlueXP 계층화를 설정할 경우 S3 액세스 키와 비밀 키를 사용하여 BlueXP 계층화를 제공해야 합니다. BlueXP 계층화는 키를 사용하여 버킷에 액세스합니다.	"StorageGRID에 계층화할 준비를 합니다"

Connector에 대한 **AWS** 권한

BlueXP가 AWS에서 Connector 인스턴스를 시작하면 Connector에 해당 AWS 계정 내의 리소스와 프로세스를 관리할 수 있는 권한을 제공하는 인스턴스에 정책을 연결합니다.

Connector는 권한을 사용하여 EC2, S3, CloudFormation, IAM, KMS(키 관리 서비스) 등

IAM 정책

아래에서 사용할 수 있는 IAM 정책은 Connector가 AWS 지역에 따라 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리하는 데 필요한 권한을 제공합니다.

다음 사항에 유의하십시오.

- BlueXP에서 직접 표준 AWS 영역에 커넥터를 생성하는 경우 BlueXP는 자동으로 Connector에 정책을 적용합니다. 이 경우에는 아무 작업도 수행할 필요가 없습니다.
- AWS Marketplace에서 Connector를 배포하거나, Linux 호스트에 Connector를 수동으로 설치하거나, BlueXP에 추가 AWS 자격 증명을 추가하려는 경우 직접 정책을 설정해야 합니다.
- 또한 새 권한이 후속 릴리스에 추가될 때 정책이 최신 상태인지 확인해야 합니다.
- 필요한 경우 IAM을 사용하여 IAM 정책을 제한할 수 있습니다 `Condition` 요소. "AWS 설명서:조건 요소"
- 이러한 정책 사용에 대한 단계별 지침을 보려면 다음 페이지를 참조하십시오.
  - "AWS Marketplace 구축에 대한 사용 권한을 설정합니다"
  - "온프레미스 배포에 대한 권한을 설정합니다"
  - "제한된 모드에 대한 권한을 설정합니다"
  - "비공개 모드에 대한 권한을 설정합니다"

필요한 정책을 보려면 지역을 선택하십시오.

표준 영역

표준 영역의 경우 권한이 두 정책에 분산됩니다. AWS에서 관리되는 정책의 최대 문자 크기 제한으로 인해 두 개의 정책이 필요합니다.

첫 번째 정책은 다음 서비스에 대한 권한을 제공합니다.

- Amazon S3 버킷 검색
- 백업 및 복구
- 분류
- Cloud Volumes ONTAP
- ONTAP용 FSX
- 계층화

두 번째 정책은 다음 서비스에 대한 권한을 제공합니다.

- 에지 캐싱
- 쿠버네티스

정책 **#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"
        }
```

```
    ]
}
```

정책 **#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(미국) 지역

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

비밀 영역

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

주요 비밀 지역

```
{
    "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 사용 권한

다음 섹션에서는 각 BlueXP 서비스에 대한 사용 권한이 어떻게 사용되는지 설명합니다. 이 정보는 기업 정책에 따라 사용 권한이 필요한 경우에만 제공된다는 내용이 지정되어 있는 경우에 유용합니다.

ONTAP용 Amazon FSx

Connector는 ONTAP용 Amazon FSx를 관리하기 위해 다음과 같은 API 요청을 수행합니다.

- EC2: DescribeInstances(지시 인스턴스)
- EC2: DescribeInstanceStatus
- EC2: DescribeInstanceAttribute
- EC2: 설명표
- EC2: DescribeImages(설명 영상)
- EC2: CreateTags(태그 생성)
- EC2: 설명 볼륨을 참조하십시오
- EC2: DescribeSecurityGroups
- EC2: DescribeNetworkInterfaces를 참조하십시오

- EC2: DescribeSubnet
- EC2: 설명
- EC2: DescribeDhcpOptions
- EC2: 설명
- EC2: 설명
- EC2: 설명
- EC2: DescribeTags(설명 태그)
- EC2: DescribeIamInstanceProfileAssociations
- EC2: DescribeReservedInstancesOffbised
- EC2: DescribeVpcEndpoints
- EC2: 설명
- EC2: 볼륨 수정 설명
- EC2: DescribePlacementGroups
- KMS: 목록 *
- KMS: 설명 *
- KMS: CreateGrant
- KMS: ListAliases
- FSX: 설명 *
- FSX:목록 *

Amazon S3 버킷 검색

Connector는 Amazon S3 버킷을 검색하기 위해 다음과 같은 API 요청을 수행합니다.

S3:GetEncryptionConfiguration

백업 및 복구

Connector는 Amazon S3에서 백업을 관리하기 위해 다음과 같은 API 요청을 수행합니다.

- S3:GetBucketLocation
- S3:ListAllMyBucket
- S3:목록 버킷
- S3:생성 버킷
- S3:GetLifecycleConfiguration
- S3: PutLifecycleConfiguration
- S3: PutBucketTagging
- S3:목록 BuckketVersions
- S3:GetBuckketAcl
- S3: PutBucketPublicAccessBlock

- KMS: 목록 *
- KMS: 설명 *
- S3:GetObject
- EC2: DescribeVpcEndpoints
- KMS: ListAliases
- S3:PutEncryptionConfiguration

Connector는 검색 및 복원 방법을 사용하여 볼륨 및 파일을 복원할 때 다음과 같은 API 요청을 수행합니다.

- S3:생성 버킷
- S3:DeleteObject 를 선택합니다
- S3:DeleteObjectVersion
- S3:GetBuckketAcl
- S3:목록 버킷
- S3:목록 BuckketVersions
- S3:ListBuckketMultipartUploads
- S3:PutObject
- S3: PutBucketAcl
- S3: PutLifecycleConfiguration
- S3: PutBucketPublicAccessBlock
- S3:중단멀티업로드입니다
- S3:ListMultipartUploadParts(S3:ListMultimpartUploadParts) 를
- Athena: StartQueryExecution
- Athena:GetQueryResults
- Athena:GetQueryExecution을 참조하십시오
- Athena: StopQueryExecution
- 글루:CreateDatabase
- 글루:CreateTable
- GLUE:BatchDeletePartition

Connector는 볼륨 백업에 DataLock 및 랜섬웨어 보호를 사용할 때 다음과 같은 API 요청을 수행합니다.

- S3:GetObjectVersionTagging
- S3:GetBuckketObjectLockConfiguration
- S3:GetObjectVersionAcl
- S3:PutObjectTagging
- S3:DeleteObject 를 선택합니다
- S3:삭제 ObjectTagging
- S3:GetObjectRetention

- S3:DeleteObjectVersionTagging
- S3:PutObject
- S3:GetObject
- S3:PutBucketObjectLockConfiguration
- S3:GetLifecycleConfiguration
- S3:ListBucketByTags
- S3:GetBucketTagging
- S3:DeleteObjectVersion
- S3:목록 BuckketVersions
- S3:목록 버킷
- S3: PutBucketTagging
- S3:GetObjectTagging
- S3: PutBucketVersioning
- S3:PutObjectVersionTagging
- S3:GetBucketVersioning
- S3:GetBuckketAcl
- S3:BypassGovernanceRetention
- S3:PutObjectRetention
- S3:GetBucketLocation
- S3:GetObjectVersion

소스 볼륨에 사용 중인 것과 다른 Cloud Volumes ONTAP 백업 계정을 사용하는 경우 Connector에서 다음 API 요청을 수행합니다.

- S3: PutBucketPolicy
- S3: PutBucketOwnershipControls

분류

Connector는 다음과 같은 API 요청을 수행하여 BlueXP 분류 인스턴스를 배포합니다.

- EC2: DescribeInstances(지시 인스턴스)
- EC2: DescribeInstanceStatus
- EC2: 런인스턴스
- EC2: 터미네이스
- EC2: CreateTags(태그 생성)
- EC2: CreateVolume
- EC2: AttachVolume
- EC2:CreateSecurityGroup입니다
- EC2: DeleteSecurityGroup

- EC2: DescribeSecurityGroups
- EC2: CreateNetworkInterface입니다
- EC2: DescribeNetworkInterfaces를 참조하십시오
- EC2: DeleteNetworkInterface
- EC2: DescribeSubnet
- EC2: 설명
- EC2: 스냅샷을 만듭니다
- EC2: 설명
- CloudFormation:CreateStack
- CloudFormation:DeleteStack
- CloudFormation: DescribeStacks
- CloudFormation: DescribeStackEvents
- IAM:AddRoleToInstanceProfile 을 참조하십시오
- EC2: AssociateIamInstanceProfile 을 참조하십시오
- EC2: DescribeIamInstanceProfileAssociations

Connector는 BlueXP 분류를 사용할 때 S3 버킷을 스캔하기 위해 다음과 같은 API 요청을 수행합니다.

- IAM:AddRoleToInstanceProfile 을 참조하십시오
- EC2: AssociateIamInstanceProfile 을 참조하십시오
- EC2: DescribeIamInstanceProfileAssociations
- S3:GetBucketTagging
- S3:GetBucketLocation
- S3:ListAllMyBucket
- S3:목록 버킷
- S3:GetBuckketPolicyStatus를 참조하십시오
- S3:GetBuckketPolicy를 참조하십시오
- S3:GetBuckketAcl
- S3:GetObject
- IAM:GetRole
- S3:DeleteObject 를 선택합니다
- S3:DeleteObjectVersion
- S3:PutObject
- STS:AssumeRole

Cloud Volumes ONTAP

Connector는 AWS에서 Cloud Volumes ONTAP를 구축 및 관리하기 위해 다음과 같은 API 요청을 수행합니다.

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
Cloud Volumes ONTAP 인스턴스에 대한 IAM 역할 및 인스턴스 프로필을 생성하고 관리합니다	IAM: ListInstanceProfiles(인스턴스 프로필)	예	예	아니요
	IAM: CreateRole	예	아니요	아니요
	IAM: DeleteRole	아니요	예	예
	IAM: PutRolePolicy(입수 정책)	예	아니요	아니요
	IAM:CreateInstanceProfile	예	아니요	아니요
	IAM: DeleteRolePolicy(삭제 RolePolicy	아니요	예	예
	IAM:AddRoleToInstanceProfile 을 참조하십시오	예	아니요	아니요
	IAM:RemoveRoleFromInstanceProfile 을 참조하십시오	아니요	예	예
	IAM: DeleteInstanceProfile	아니요	예	예
	IAM: 암호 역할	예	아니요	아니요
	EC2: AssociateIamInstanceProfile 을 참조하십시오	예	예	아니요
	EC2: DescribeIamInstanceProfileAssociations	예	예	아니요
	EC2: DiscassociateIamInstanceProfile 을 참조하십시오	아니요	예	아니요
인증 상태 메시지를 디코딩합니다	STS:DecodeAuthorizationMessage 를 참조하십시오	예	예	아니요
계정에 사용할 수 있는 지정된 영상(AMI)을 설명합니다	EC2: DescribeImages(설명 영상)	예	예	아니요
VPC의 라우트 테이블 설명(HA 쌍에만 필요)	EC2: 설명표	예	아니요	아니요

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
인스턴스를 중지, 시작 및 모니터링합니다	EC2: StartInstances(시작 인스턴스)	예	예	아니요
	EC2: StopInstances(중지 인스턴스)	예	예	아니요
	EC2: DescribeInstances(지시 인스턴스)	예	예	아니요
	EC2: DescribeInstanceStatus	예	예	아니요
	EC2: 런인스턴스	예	아니요	아니요
	EC2: 터미네이스	아니요	아니요	예
	EC2: ModifyInstanceAttribute	아니요	예	아니요
지원되는 인스턴스 유형에 대해 향상된 네트워킹이 활성화되어 있는지 확인합니다	EC2: DescribeInstanceAttribute	아니요	예	아니요
유지 관리 및 비용 할당에 사용되는 "WorkingEnvironment" 및 "WorkingEnvironmentId" 태그로 리소스에 태그를 지정합니다	EC2: CreateTags(태그 생성)	예	예	아니요
Cloud Volumes ONTAP가 백엔드 스토리지로 사용하는 EBS 볼륨을 관리합니다	EC2: CreateVolume	예	예	아니요
	EC2: 설명 볼륨을 참조하십시오	예	예	예
	EC2: ModifyVolumeAttribute	아니요	예	예
	EC2: AttachVolume	예	예	아니요
	EC2: DeleteVolume(삭제 볼륨)	아니요	예	예
	EC2: DetachVolume(분리 볼륨)	아니요	예	예

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
Cloud Volumes ONTAP에 대한 보안 그룹을 만들고 관리합니다	EC2:CreateSecurityGroup입니다	예	아니요	아니요
	EC2: DeleteSecurityGroup	아니요	예	예
	EC2: DescribeSecurityGroups	예	예	예
	EC2: RevokeSecurityGroupEgress	예	아니요	아니요
	EC2: AuthorizeSecurityGroupEgress 를 참조하십시오	예	아니요	아니요
	EC2: AuthorizeSecurityGroupIngress 를 참조하십시오	예	아니요	아니요
	EC2: RevokeSecurityGroupIngress 를 참조하십시오	예	예	아니요
대상 서브넷에서 Cloud Volumes ONTAP에 대한 네트워크 인터페이스를 생성하고 관리합니다	EC2: CreateNetworkInterface입니다	예	아니요	아니요
	EC2: DescribeNetworkInterfaces를 참조하십시오	예	예	아니요
	EC2: DeleteNetworkInterface	아니요	예	예
	EC2: ModifyNetworkInterfaceAttribute 입니다	아니요	예	아니요
대상 서브넷 및 보안 그룹 목록을 가져옵니다	EC2: DescribeSubnet	예	예	아니요
	EC2: 설명	예	예	아니요
Cloud Volumes ONTAP 인스턴스의 DNS 서버와 기본 도메인 이름을 가져옵니다	EC2: DescribeDhcpOptions	예	아니요	아니요

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
Cloud Volumes ONTAP용 EBS 볼륨의 스냅샷을 생성합니다	EC2: 스냅샷을 만듭니다	예	예	아니요
	EC2: DeleteSnapshot	아니요	예	예
	EC2: 설명	아니요	예	아니요
AutoSupport 메시지에 첨부된 Cloud Volumes ONTAP 콘솔을 캡처합니다	EC2:GetConsoleOutput 을 참조하십시오	예	예	아니요
사용 가능한 키 쌍 목록을 가져옵니다	EC2: 설명	예	아니요	아니요
사용 가능한 AWS 지역 목록을 확인하십시오	EC2: 설명	예	예	아니요
Cloud Volumes ONTAP 인스턴스와 연결된 리소스의 태그를 관리합니다	EC2: 삭제 태그	아니요	예	예
	EC2: DescribeTags(설명 태그)	아니요	예	아니요
AWS CloudFormation 템플릿을 위한 스택을 만들고 관리합니다	CloudFormation:CreateStack	예	아니요	아니요
	CloudFormation:DeleteStack	예	아니요	아니요
	CloudFormation: DescribeStacks	예	예	아니요
	CloudFormation: DescribeStackEvents	예	아니요	아니요
	CloudFormation:ValidateTemplate 을 참조하십시오	예	아니요	아니요

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
Cloud Volumes ONTAP 시스템이 데이터 계층화를 위한 용량 계층으로 사용하는 S3 버킷을 생성 및 관리합니다	S3:생성 버킷	예	예	아니요
	S3:삭제 버킷	아니요	예	예
	S3:GetLifecycleConfiguration	아니요	예	아니요
	S3: PutLifecycleConfiguration	아니요	예	아니요
	S3: PutBucketTagging	아니요	예	아니요
	S3:목록 BuckketVersions	아니요	예	아니요
	S3:GetBuckketPolicyStatus를 참조하십시오	아니요	예	아니요
	S3:GetBuckketPublicAccessBlock	아니요	예	아니요
	S3:GetBuckketAcl	아니요	예	아니요
	S3:GetBuckketPolicy를 참조하십시오	아니요	예	아니요
	S3: PutBucketPublicAccessBlock	아니요	예	아니요
	S3:GetBucketTagging	아니요	예	아니요
	S3:GetBucketLocation	아니요	예	아니요
	S3:ListAllMyBucket	아니요	아니요	아니요
	S3:목록 버킷	아니요	예	아니요
AWS KMS(키 관리 서비스)를 사용하여 Cloud Volumes ONTAP의 데이터 암호화 지원	KMS: 목록 *	예	예	아니요
	KMS: 재암호화 *	예	아니요	아니요
	KMS: 설명 *	예	예	아니요
	KMS: CreateGrant	예	예	아니요
	KMS: GenerateDataKeyWithoutPlaintext	예	예	아니요

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
단일 AWS Availability Zone에서 2개의 HA 노드를 위한 AWS 분산 배치 그룹과 중재자를 생성하고 관리합니다	EC2: CreatePlacementGroup(배치 그룹 생성)	예	아니요	아니요
	EC2: DeletePlacementGroup	아니요	예	예
보고서 작성	FSX: 설명 *	아니요	예	아니요
	FSX:목록 *	아니요	예	아니요
Amazon EBS Elastic Volumes 기능을 지원하는 애그리게이트를 생성 및 관리합니다	EC2: 볼륨 수정 설명	아니요	예	아니요
	EC2: ModifyVolume(수정 볼륨)	아니요	예	아니요

에지 캐싱

Connector는 배포 중에 다음과 같은 API 요청을 수행하여 BlueXP 에지 캐싱 인스턴스를 배포합니다.

- CloudFormation: DescribeStacks
- CloudWatch: GetMetricStatistics
- CloudFormation: ListStacks

쿠버네티스

Connector는 다음과 같은 API 요청을 수행하여 Amazon EKS 클러스터를 검색하고 관리합니다.

- EC2: 설명
- EKS: ListClusters
- EKS: DescribeCluster
- IAM:GetInstanceProfile 을 참조하십시오

변경 로그

권한이 추가되고 제거됨에 따라 아래 섹션에 해당 권한이 표시됩니다.

2024년 3월 8일

이제 커넥터 정책에 다음 권한이 포함됩니다.

EC2:가용성 영역 설명

이 권한은 다음 릴리스에 필요합니다. 해당 릴리스가 출시되면 릴리스 노트를 더 자세히 업데이트하겠습니다.

2023년 6월 6일

이제 Cloud Volumes ONTAP에 대해 다음 권한이 필요합니다.

KMS: GenerateDataKeyWithoutPlaintext

2023년 2월 14일

이제 BlueXP 계층화에 대해 다음 권한이 필요합니다.

EC2: DescribeVpcEndpoints

Connector에 대한 Azure 권한

BlueXP가 Azure에서 Connector VM을 시작하면 Connector에 Azure 구독 내의 리소스 및 프로세스를 관리할 수 있는 권한을 제공하는 사용자 지정 역할을 VM에 연결합니다. Connector는 사용 권한을 사용하여 여러 Azure 서비스에 대한 API 호출을 수행합니다.

사용자 지정 역할 권한

아래 표시된 사용자 지정 역할은 Connector가 Azure 네트워크 내의 리소스 및 프로세스를 관리하는 데 필요한 권한을 제공합니다.

BlueXP에서 직접 커넥터를 만들면 BlueXP에서 자동으로 이 사용자 정의 역할을 커넥터에 적용합니다.

Azure Marketplace에서 Connector를 배포하거나 Linux 호스트에 Connector를 수동으로 설치하는 경우 사용자 지정 역할을 직접 설정해야 합니다.

이러한 정책 사용에 대한 단계별 지침을 보려면 다음 페이지를 참조하십시오.

- "Azure Marketplace 배포에 대한 사용 권한을 설정합니다"
- "온프레미스 배포에 대한 권한을 설정합니다"
- "제한된 모드에 대한 권한을 설정합니다"
- "비공개 모드에 대한 권한을 설정합니다"

또한 후속 릴리스에 새 권한이 추가되므로 역할이 최신 상태인지 확인해야 합니다.

```
{
    "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 사용 권한 사용 방법

다음 섹션에서는 각 BlueXP 서비스에 대한 사용 권한이 어떻게 사용되는지 설명합니다. 이 정보는 기업 정책에 따라 사용 권한이 필요한 경우에만 제공된다는 내용이 지정되어 있는 경우에 유용합니다.

Azure NetApp Files

BlueXP 분류를 사용하여 Azure NetApp Files 데이터를 스캔할 때 커넥터는 다음과 같은 API 요청을 합니다.

- 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

백업 및 복구

Connector는 BlueXP 백업 및 복구를 위해 다음과 같은 API 요청을 수행합니다.

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/read를 참조하십시오
- Microsoft.Storage/storageAccounts/write입니다

- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.KeyVault/볼트/읽기
- Microsoft.KeyVault/vaults/accessPolicies/write
- Microsoft.Network/networkInterfaces/read
- Microsoft.Resources/서브스크립션/위치/읽기
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Resources/Subscriptions/resourceGroups/read
- Microsoft.Resources/Subscriptions/resourcegroups/resources/read
- Microsoft.Resources/Subscriptions/resourceGroups/write입니다
- Microsoft.인증/잠금/ *
- 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 를 참조하십시오
- Microsoft.ManagedIdentity/userAssignedIdentities/assign/action 을 참조하십시오

Connector는 검색 및 복원 기능을 사용할 때 다음과 같은 API 요청을 수행합니다.

- Microsoft.Synapse/작업 공간/쓰기
- Microsoft.Synapse/작업 공간/읽기
- Microsoft.Synapse/작업 공간/삭제
- Microsoft.Synapse/등록/조치
- Microsoft.Synapse/checkNameAvailability/action
- Microsoft.Synapse/작업 공간/작업 상태/읽기
- Microsoft.Synapse/작업 공간/firewallwules/read
- Microsoft.Synapse/작업 공간/교체 eAllIpFirewallRules/action
- Microsoft.Synapse/작업 공간/작업 결과/읽기
- Microsoft.Synapse/작업 공간/privateEndpointConnectionsApproval/action

분류

Connector는 BlueXP 분류를 사용할 때 다음과 같은 API 요청을 수행합니다.

조치	설정에 사용됩니까?	일상적 운영에 사용됩니까?
Microsoft.Compute/locations/operations/read	예	예
Microsoft.Compute/locations/vmSizes/read	예	예
Microsoft.Compute/operations/read	예	예
Microsoft.Compute/virtualMachines/instanceView/read	예	예
Microsoft.Compute/virtualMachines/powerOff/action	예	아니요
Microsoft.Compute/virtualMachines/read	예	예
Microsoft.Compute/virtualMachines/restart/action	예	아니요
Microsoft.Compute/virtualMachines/start/action	예	아니요
Microsoft.Compute/virtualMachines/vmSizes/read	아니요	예
Microsoft.Compute/virtualMachines/write	예	아니요
Microsoft.Compute/images/read	예	예
Microsoft.Compute/disks/delete	예	아니요
Microsoft.Compute/disks/read	예	예
Microsoft.Compute/disks/write	예	아니요
Microsoft.Storage/CheckknameAvailability/read	예	예
Microsoft.스토리지/작업/읽기	예	예
Microsoft.Storage/storageAccounts/listkeys/action	예	아니요
Microsoft.Storage/storageAccounts/read를 참조하십시오	예	예
Microsoft.Storage/storageAccounts/write입니다	예	아니요
Microsoft.Storage/storageAccounts/blobServices/containers/read	예	예
Microsoft.Network/networkInterfaces/read	예	예

조치	설정에 사용됩니까?	일상적 운영에 사용됩니까?
Microsoft.Network/networkInterfaces/write	예	아니요
Microsoft.Network/networkInterfaces/join/action	예	아니요
Microsoft.Network/networkSecurityGroups/read	예	예
Microsoft.Network/networkSecurityGroups/write	예	아니요
Microsoft.Resources/서브스크립션/위치/읽기	예	예
Microsoft.Network/locations/operationResults/read	예	예
Microsoft.Network/locations/operations/read	예	예
Microsoft.Network/virtualNetworks/read	예	예
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	예	예
Microsoft.Network/virtualNetworks/subnets/read	예	예
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	예	예
Microsoft.Network/virtualNetworks/virtualMachines/read	예	예
Microsoft.Network/virtualNetworks/subnets/join/action	예	아니요
Microsoft.Network/virtualNetworks/subnets/write	예	아니요
Microsoft.Network/routeTables/join/action	예	아니요
Microsoft.Resources/Deployments/Operations/Read 를 참조하십시오	예	예
Microsoft.Resources/Deployments/Read 를 참조하십시오	예	예
Microsoft.Resources/Deployments/Write 를 참조하십시오	예	아니요
Microsoft.Resources/resources/read	예	예
Microsoft.Resources/서브스크립션/운영 결과/읽기	예	예

조치	설정에 사용됩니까?	일상적 운영에 사용됩니까?
Microsoft.Resources/Subscriptions/resourceGroups/delete	예	아니요
Microsoft.Resources/Subscriptions/resourceGroups/read	예	예
Microsoft.Resources/Subscriptions/resourcegroups/resources/read	예	예
Microsoft.Resources/Subscriptions/resourceGroups/write입니다	예	아니요

Cloud Volumes ONTAP

Connector는 Azure에서 Cloud Volumes ONTAP를 배포 및 관리하기 위해 다음과 같은 API 요청을 수행합니다.

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
VM을 생성하고 관리합니다	Microsoft.Compute/locations/operations/read	예	예	아니요
	Microsoft.Compute/locations/vmSizes/read	예	예	아니요
	Microsoft.Resources/서브스크립션/위치/읽기	예	아니요	아니요
	Microsoft.Compute/operations/read	예	예	아니요
	Microsoft.Compute/virtualMachines/instanceView/read	예	예	아니요
	Microsoft.Compute/virtualMachines/powerOff/action	예	예	아니요
	Microsoft.Compute/virtualMachines/read	예	예	아니요
	Microsoft.Compute/virtualMachines/restart/action	예	예	아니요
	Microsoft.Compute/virtualMachines/start/action	예	예	아니요
	Microsoft.Compute/virtualMachines/deallocate/action	아니요	예	예
	Microsoft.Compute/virtualMachines/vmSizes/read	아니요	예	아니요
	Microsoft.Compute/virtualMachines/write	예	예	아니요
	Microsoft.Compute/virtualMachines/delete	예	예	예
	Microsoft.Resources/Deployments/Delete를 참조하십시오	예	아니요	아니요
VHD에서 배포를 활성화합니다	Microsoft.Compute/images/read	예	아니요	아니요
	Microsoft.Compute/images/write	예	아니요	아니요

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
대상 서브넷에서 네트워크 인터페이스를 생성하고 관리합니다	Microsoft.Network/networkInterfaces/read	예	예	아니요
	Microsoft.Network/networkInterfaces/write	예	예	아니요
	Microsoft.Network/networkInterfaces/join/action	예	예	아니요
	Microsoft.Network/networkInterfaces/delete	예	예	아니요
네트워크 보안 그룹을 만들고 관리합니다	Microsoft.Network/networkSecurityGroups/read	예	예	아니요
	Microsoft.Network/networkSecurityGroups/write	예	예	아니요
	Microsoft.Network/networkSecurityGroups/join/action	예	아니요	아니요
	Microsoft.Network/networkSecurityGroups/delete	아니요	예	예

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
지역, 대상 VNET 및 서브넷에 대한 네트워크 정보를 얻고 VM을 VNets에 추가합니다	Microsoft.Network/locations/operationResults/read	예	예	아니요
	Microsoft.Network/locations/operations/read	예	예	아니요
	Microsoft.Network/virtualNetworks/read	예	아니요	아니요
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	예	아니요	아니요
	Microsoft.Network/virtualNetworks/subnets/read	예	예	아니요
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	예	예	아니요
	Microsoft.Network/virtualNetworks/virtualMachines/read	예	예	아니요
	Microsoft.Network/virtualNetworks/subnets/join/action	예	예	아니요

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
자원 그룹을 만들고 관리합니다	Microsoft.Resources/Deployments/Operations/Read 를 참조하십시오	예	예	아니요
	Microsoft.Resources/Deployments/Read 를 참조하십시오	예	예	아니요
	Microsoft.Resources/Deployments/Write 를 참조하십시오	예	예	아니요
	Microsoft.Resources/resources/read	예	예	아니요
	Microsoft.Resources/서브스크립션/운영 결과/읽기	예	예	아니요
	Microsoft.Resources/Subscriptions/resourceGroups/delete	예	예	예
	Microsoft.Resources/Subscriptions/resourceGroups/read	아니요	예	아니요
	Microsoft.Resources/Subscriptions/resourcegroups/resources/read	예	예	아니요
	Microsoft.Resources/Subscriptions/resourceGroups/write입니다	예	예	아니요

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
Azure 스토리지 계정 및 디스크를 관리합니다	Microsoft.Compute/disks/read	예	예	예
	Microsoft.Compute/disks/write	예	예	아니요
	Microsoft.Compute/disks/delete	예	예	예
	Microsoft.Storage/CheckknameAvailability/read	예	예	아니요
	Microsoft.스토리지/작업/읽기	예	예	아니요
	Microsoft.Storage/storageAccounts/listkeys/action	예	예	아니요
	Microsoft.Storage/storageAccounts/read를 참조하십시오	예	예	아니요
	Microsoft.Storage/storageAccounts/delete	아니요	예	예
	Microsoft.Storage/storageAccounts/write입니다	예	예	아니요
	Microsoft.스토리지/용도/읽기	아니요	예	아니요
Blob 저장소로 백업 및 스토리지 계정 암호화 지원	Microsoft.Storage/storageAccounts/blobServices/containers/read	예	예	아니요
	Microsoft.KeyVault/볼트/읽기	예	예	아니요
	Microsoft.KeyVault/vaults/accessPolicies/write	예	예	아니요
데이터 계층화를 위해 VNET 서비스 엔드포인트를 활성화합니다	Microsoft.Network/virtualNetworks/subnets/write	예	예	아니요
	Microsoft.Network/routeTables/join/action	예	예	아니요

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
Azure 관리 스냅샷을 생성하고 관리합니다	Microsoft.Compute/snapshots/write	예	예	아니요
	Microsoft.Compute/snapshots/read	예	예	아니요
	Microsoft.Compute/snapshots/delete	아니요	예	예
	Microsoft.Compute/disks/beginGetAccess/action	아니요	예	아니요
가용성 세트 생성 및 관리	Microsoft.Compute/availabilitySets/write	예	아니요	아니요
	Microsoft.Compute/availabilitySets/read	예	아니요	아니요
시장에서 프로그래밍 방식으로 배포할 수 있습니다	Microsoft.MarketplaceOrdering/offerstypes/publishers/Offers/Plans/Agreement/read	예	아니요	아니요
	Microsoft.MarketplaceOrdering/offersTypes/publishers/Offers/Plans/Agreement/write	예	예	아니요

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
HA 쌍에 대한 로드 밸런서를 관리합니다	Microsoft.Network/loadBalancers/read	예	예	아니요
	Microsoft.Network/loadBalancers/write	예	아니요	아니요
	Microsoft.Network/loadBalancers/delete	아니요	예	예
	Microsoft.Network/loadBalancers/backendAddressPools/read	예	아니요	아니요
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	예	아니요	아니요
	Microsoft.Network/loadBalancers/frontendIPConfigurations/read	예	예	아니요
	Microsoft.Network/loadBalancers/loadBalancingRules/read	예	아니요	아니요
	Microsoft.Network/loadBalancers/probes/read	예	아니요	아니요
	Microsoft.Network/loadBalancers/probes/join/action	예	아니요	아니요
Azure 디스크에서 잠금 관리를 활성화합니다	Microsoft.인증/잠금/ *	예	예	아니요

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
서브넷 외부에 연결이 없는 경우 HA 쌍에 대한 개인 끝점을 설정합니다	Microsoft.Network/privateEndpoints/write	예	예	아니요
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action 을 참조하십시오	예	아니요	아니요
	Microsoft.Storage/storageAccounts/privateEndpointConnections/read	예	예	예
	Microsoft.Network/privateEndpoints/read	예	예	예
	Microsoft.Network/privateDnsZones/write	예	예	아니요
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/write	예	예	아니요
	Microsoft.Network/virtualNetworks/join/action	예	예	아니요
	Microsoft.Network/privateDnsZones/A/write	예	예	아니요
	Microsoft.Network/privateDnsZones/read	예	예	아니요
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/read	예	예	아니요
기본 물리적 하드웨어에 따라 일부 VM 배포에 필요합니다	Microsoft.Resources/Deployments/operationStates/read 를 참조하십시오	예	예	아니요
배포 실패 또는 삭제 시 리소스 그룹에서 리소스를 제거합니다	Microsoft.Network/privateEndpoints/delete	예	예	아니요
	Microsoft.Compute/availabilitySets/delete	예	예	아니요

목적	조치	배포에 사용되었습니까?	일상적 운영에 사용됩니까?	삭제에 사용되었습니까?
API를 사용할 때 고객이 관리하는 암호화 키를 사용할 수 있도록 설정합니다	Microsoft.Compute/diskEncryptionSets/read	예	예	예
	Microsoft.Compute/diskEncryptionSets/write	예	예	아니요
	Microsoft.KeyVault/볼트/배포/작업	예	아니요	아니요
	Microsoft.Compute/diskEncryptionSets/delete	예	예	예
HA 인터커넥트 및 클러스터 네트워크 NIC를 격리하도록 HA 쌍에 대한 애플리케이션 보안 그룹을 구성합니다	Microsoft.Network/applicationSecurityGroups/write	아니요	예	아니요
	Microsoft.Network/applicationSecurityGroups/read	아니요	예	아니요
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	아니요	예	아니요
	Microsoft.Network/networkSecurityGroups/securityRules/write	예	예	아니요
	Microsoft.Network/applicationSecurityGroups/delete	아니요	예	예
	Microsoft.Network/networkSecurityGroups/securityRules/delete	아니요	예	예
Cloud Volumes ONTAP 리소스와 연결된 태그를 읽고, 쓰고, 삭제합니다	Microsoft.Resources/tags/read	아니요	예	아니요
	Microsoft.Resources/tags/write(Microsoft.리소스/태그/쓰기	예	예	아니요
	Microsoft.Resources/tags/delete(Microsoft.리소스/태그/삭제	예	아니요	아니요
생성 중에 스토리지 계정을 암호화합니다	Microsoft.ManagedIdentity/userAssignedIdentities/assign/action 을 참조하십시오	예	예	아니요

에지 캐싱

Connector는 BlueXP 에지 캐싱을 사용할 때 다음과 같은 API 요청을 수행합니다.

- Microsoft.Insights/메트릭/읽기
- 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 를 참조하십시오

쿠버네티스

Connector는 Azure Kubernetes Service(AKS)에서 실행 중인 클러스터를 검색하고 관리하기 위해 다음과 같은 API 요청을 수행합니다.

- Microsoft.Compute/virtualMachines/read
- Microsoft.Resources/서브스크립션/위치/읽기
- Microsoft.Resources/서브스크립션/운영 결과/읽기
- Microsoft.Resources/Subscriptions/resourceGroups/read
- Microsoft.Resources/Subscriptions/resourcegroups/resources/read
- Microsoft.ContainerService/managedClusters/read
- Microsoft.ContainerService/managedClusters/listClusterUserCredential/action입니다

계층화

Connector는 BlueXP 계층화를 설정할 때 다음과 같은 API 요청을 수행합니다.

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Resources/Subscriptions/resourceGroups/read
- Microsoft.Resources/서브스크립션/위치/읽기

Connector는 일상적인 작업에 대해 다음과 같은 API 요청을 수행합니다.

- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/managementPolicies/read를 참조하십시오
- Microsoft.Storage/storageAccounts/managementPolicies/write를 참조하십시오
- Microsoft.Storage/storageAccounts/read를 참조하십시오

변경 로그

권한이 추가되고 제거됨에 따라 아래 섹션에 해당 권한이 표시됩니다.

2023년 12월 5일

볼륨 데이터를 Azure Blob 스토리지에 백업할 때 BlueXP 백업 및 복구에 더 이상 다음 권한이 필요하지 않습니다.

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

이러한 권한은 다른 BlueXP 스토리지 서비스에 필요하므로 다른 스토리지 서비스를 사용하는 경우에도 Connector의 사용자 지정 역할이 유지됩니다.

2023년 5월 12일

JSON 정책에는 Cloud Volumes ONTAP 관리에 필요한 다음과 같은 권한이 추가되었습니다.

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

다음 권한은 더 이상 필요하지 않으므로 JSON 정책에서 제거되었습니다.

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

2023년 3월 23일

BlueXP 분류에는 "Microsoft.Storage/storageAccounts/delete" 권한이 더 이상 필요하지 않습니다.

이 권한은 Cloud Volumes ONTAP에 여전히 필요합니다.

2023년 1월 5일

JSON 정책에 다음 권한이 추가되었습니다.

- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Synapse/작업 공간/privateEndpointConnectionsApproval/action

  이러한 권한은 BlueXP 백업 및 복구에 필요합니다.

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

  이 권한은 Cloud Volumes ONTAP 배포에 필요합니다.

Connector에 대한 **Google Cloud** 권한

BlueXP는 Google Cloud에서 작업을 수행할 수 있는 권한이 필요합니다. 이러한 사용 권한은 NetApp에서 제공하는 사용자 지정 역할에 포함됩니다. BlueXP가 이러한 권한을 통해 수행하는 작업을 이해하기를 원할 수 있습니다.

서비스 계정 권한

아래 표시된 사용자 지정 역할은 Connector가 Google Cloud 네트워크 내의 리소스 및 프로세스를 관리하는 데 필요한 권한을 제공합니다.

Connector VM에 연결되는 서비스 계정에 이 사용자 지정 역할을 적용해야 합니다.

- "표준 모드에 대한 Google Cloud 권한을 설정합니다"
- "제한된 모드에 대한 권한을 설정합니다"
- "비공개 모드에 대한 권한을 설정합니다"

또한 후속 릴리스에 새 권한이 추가되므로 역할이 최신 상태인지 확인해야 합니다.

```
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 사용 권한 사용 방법

작업	목적
-compute.disks.create를 참조하십시오 -compute.disks.createSnapshot을 참조하십시오 compute.disks.delete 으로 문의하십시오 -compute.disks.get을 참조하십시오 -compute.disks.list 를 참조하십시오 compute.disks.setLabels 으로 문의하십시오 compute.disks.us e	Cloud Volumes ONTAP용 디스크를 생성하고 관리합니다.
-컴퓨팅.방화벽.create compute.firewalls.delete 으로 문의하십시오 바로 컴퓨팅, 방화벽, GET입니다 -compute.방화벽.list 를 참조하십시오	Cloud Volumes ONTAP에 대한 방화벽 규칙을 만듭니다.
-compute.globalOperations.get	작업 상태를 확인합니다.
-compute.images.get -compute.images.getFromFamily 를 참조하십시오 -compute.images.list 를 선택합니다 compute.images.useReadOnly 으로 문의하십시오	VM 인스턴스의 이미지를 가져옵니다.

작업	목적
compute.instances.attachDisk 으로 문의하십시오 compute.instances.detachDisk 으로 문의하십시오	Cloud Volumes ONTAP에 디스크를 연결 및 분리합니다.
compute.instances.create 으로 문의하십시오 compute.instances.delete 으로 문의하십시오	Cloud Volumes ONTAP VM 인스턴스를 생성 및 삭제합니다.
compute.instances.get 으로 문의하십시오	VM 인스턴스를 나열합니다.
compute.instances.getSerialPortOutput 으로 문의하십시오	콘솔 로그를 가져옵니다.
compute.instances.list 으로 문의하십시오	영역에 있는 인스턴스 목록을 검색합니다.
compute.instances.setDeletionProtection 으로 문의하십시오	인스턴스에 대한 삭제 보호를 설정합니다.
compute.instances.setLabels 으로 문의하십시오	를 눌러 라벨을 추가합니다.
compute.instances.setMachineType 으로 문의하십시오 compute.instances.setMinCpuPlatform 으로 문의하십시오	Cloud Volumes ONTAP의 기계 유형을 변경합니다.
compute.instances.setMetadata 으로 문의하십시오	를 눌러 메타데이터를 추가합니다.
compute.instances.setTags 으로 문의하십시오	방화벽 규칙에 대한 태그를 추가하려면
compute.instances.start 으로 문의하십시오 compute.instances.stop 으로 문의하십시오 compute.instances.updateDisplayDevice 으로 문의하십시오	Cloud Volumes ONTAP를 시작 및 중지합니다.
-compute.machineTypes.get	를 클릭하여 qoutas를 확인하십시오.
compute.projects.get 으로 문의하십시오	여러 프로젝트를 지원합니다.
-compute.snapshots.create를 참조하십시오 compute.snapshots.delete 으로 문의하십시오 -compute.snapshots.get -compute.snapshots.list 를 참조하십시오 compute.snapshots.setLabels 으로 문의하십시오	영구 디스크 스냅샷을 생성하고 관리합니다.
compute.networks.get 으로 문의하십시오 compute.networks.list 으로 문의하십시오 -compute.regions.get 을 선택합니다 -compute.regions.list 를 선택합니다 -compute.subnetworks.get -compute.subnetworks.list 를 참조하십시오 -compute.zoneOperations.get -compute.zone.get을 입력합니다 -compute.zones.list를 입력합니다	새 Cloud Volumes ONTAP 가상 머신 인스턴스를 생성하는 데 필요한 네트워킹 정보를 가져옵니다.

작업	목적
deploymentmanager.compositeTypes.get 으로 문의하십시오 deploymentmanager.compositeTypes.list 으로 문의하십시오 deploymentmanager.deployments.create 으로 문의하십시오 deploymentmanager.deployments.delete 으로 문의하십시오 deploymentmanager.deployments.get 으로 문의하십시오 deploymentmanager.deployments.list 으로 문의하십시오 -deploymentmanager.manifests.get -deploymentmanager.manifests.list 를 참조하십시오 -deploymentmanager.operations.get -deploymentmanager.operations.list 를 참조하십시오 -deploymentmanager.resources.get -deploymentmanager.resources.list 를 참조하십시오 -deploymentmanager.typeProviders.get -deploymentmanager.typeProviders.list 를 참조하십시오 -deploymentmanager.types.get -deploymentmanager.types.list 를 참조하십시오	Google Cloud Deployment Manager를 사용하여 Cloud Volumes ONTAP 가상 머신 인스턴스를 구축합니다.
-logging.logEntrries.list 를 참조하십시오 -logging.privateLogEntrs.list 를 참조하십시오	스택 로그 드라이브를 가져옵니다.
resourcemanager.projects.get 으로 문의하십시오	여러 프로젝트를 지원합니다.
-storage.버킷.create storage.buckets.delete 으로 문의하십시오 버킷.GET -storage.버킷.list -storage.버킷.update	데이터 계층화를 위한 Google Cloud Storage 버킷 생성 및 관리
cloudkms.cryptoKeyVersions.useToEncrypt 으로 문의하십시오 -클라우드킬로미터.암호화 키.가져오기 -cloudkms.cryptoKeys.list -cloudkms.keyRings.list를 선택합니다	클라우드 키 관리 서비스(Cloud Volumes ONTAP 포함)에서 고객이 관리하는 암호화 키를 사용하려면
compute.instances.setServiceAccount 으로 문의하십시오 iam.serviceAccounts.actAs 으로 문의하십시오 iam.serviceAccounts.getIamPolicy 으로 문의하십시오 iam.serviceAccounts.list 으로 문의하십시오 -storage.objects.get 을 선택합니다 -storage.objects.list 를 선택합니다	Cloud Volumes ONTAP 인스턴스에서 서비스 계정을 설정하려면 이 서비스 계정은 Google Cloud Storage 버킷에 대한 데이터 계층화 권한을 제공합니다.
-compute.addresses.list 를 참조하십시오	HA 쌍을 구축할 때 영역의 주소를 검색합니다.
-compute.backendServices.create 를 참조하십시오 -compute.regionBackendServices.create -compute.regionBackendServices.get -compute.regionBackendServices.list 를 참조하십시오	HA 쌍으로 트래픽을 분산하기 위한 백엔드 서비스를 구성합니다.

작업	목적
compute.networks.updatePolicy 으로 문의하십시오	HA 쌍에 대한 VPC 및 서브넷에 방화벽 규칙을 적용합니다.
compute.subnetworks.us e compute.subnetworks.useExternalIp 으로 문의하십시오 compute.instances.addAccessConfig 으로 문의하십시오	BlueXP 분류를 사용하도록 설정합니다.
container.clusters.get을 선택합니다 -container.clusters.list 를 선택합니다	Google Kubernetes Engine에서 실행 중인 Kubernetes 클러스터를 검색할 수 있습니다.
compute.instanceGroups.get 으로 문의하십시오 -compute.addresses.get compute.instances.updateNetworkInterface 으로 문의하십시오	Cloud Volumes ONTAP HA 쌍에서 스토리지 VM을 생성하고 관리합니다.
-monitoring.timeseries.list 를 참조하십시오 -storage.버킷.getIamPolicy	Google Cloud Storage 버킷에 대한 정보를 검색할 수 있습니다.
-클라우드킬로미터.암호화 키.가져오기 -cloudkms.cryptoKeys.getIamPolicy -cloudkms.cryptoKeys.list cloudkms.cryptoKeys.setIamPolicy 으로 문의하십시오 -cloudkms.keyrings.get -cloudkms.keyRings.getIamPolicy -cloudkms.keyRings.list를 선택합니다 cloudkms.keyRings.setIamPolicy 으로 문의하십시오	Google에서 관리하는 기본 암호화 키를 사용하는 대신 BlueXP 백업 및 복구 활성화 마법사에서 고객이 관리하는 키를 직접 선택할 수 있습니다.

변경 로그

권한이 추가되고 제거됨에 따라 아래 섹션에 해당 권한이 표시됩니다.

2023년 2월 6일

이 정책에 다음 권한이 추가되었습니다.

- compute.instances.updateNetworkInterface

이 권한은 Cloud Volumes ONTAP에 필요합니다.

2023년 1월 27일

다음 권한이 정책에 추가되었습니다.

- cloudkms.cryptoKeys.getIamPolicy를 참조하십시오
- cloudkms.cryptoKeys.setIamPolicy
- 클라우드킬로미터.키링.GET
- cloudkms.keyRings.getIamPolicy를 참조하십시오
- cloudkms.keyRings.setIamPolicy

이러한 권한은 BlueXP 백업 및 복구에 필요합니다.

포트

AWS의 커넥터 보안 그룹 규칙

Connector의 AWS 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다. BlueXP에서 커넥터를 만들면 이 보안 그룹이 자동으로 생성됩니다. 다른 모든 설치 옵션에 대해 이 보안 그룹을 설정해야 합니다.

인바운드 규칙

프로토콜	포트	목적
SSH를 클릭합니다	22	커넥터 호스트에 대한 SSH 액세스를 제공합니다
HTTP	80	• 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공합니다 • Cloud Volumes ONTAP 업그레이드 프로세스 중에 사용됩니다
HTTPS	443	클라이언트 웹 브라우저에서 로컬 사용자 인터페이스에 대한 HTTPS 액세스 및 BlueXP 분류 인스턴스의 연결을 제공합니다
TCP	3128	Cloud Volumes ONTAP에서 인터넷에 액세스하여 AutoSupport 메시지를 NetApp 지원으로 보냅니다. 배포 후에는 이 포트를 수동으로 열어야 합니다. "커넥터가 AutoSupport 메시지의 프록시로 사용되는 방법에 대해 알아봅니다"
TCP	9060, 9061	정부 지역에서 BlueXP 분류 및 BlueXP 백업 및 복구를 활성화하고 사용할 수 있는 기능을 제공합니다.

아웃바운드 규칙

Connector에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

기본 아웃바운드 규칙

Connector에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

프로토콜	포트	목적
모든 TCP	모두	모든 아웃바운드 트래픽
모든 UDP	모두	모든 아웃바운드 트래픽

고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Connector의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

> 소스 IP 주소는 커넥터 호스트입니다.

서비스	프로토콜	포트	목적지	목적
API 호출 및 AutoSupport	HTTPS	443	아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF	API에서는 AWS, ONTAP, BlueXP 분류 및 AutoSupport 메시지를 NetApp에 전송하는 데 호출됩니다
API 호출	TCP	3000입니다	ONTAP HA 중재자	ONTAP HA 중재인과의 커뮤니케이션
	TCP	8080	BlueXP 분류	배포 중에 BlueXP 분류 인스턴스를 조사합니다
DNS	UDP입니다	53	DNS	BlueXP에서 DNS Resolve에 사용됩니다

Azure의 커넥터 보안 그룹 규칙

Connector의 Azure 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다. BlueXP에서 커넥터를 만들면 이 보안 그룹이 자동으로 생성됩니다. 다른 모든 설치 옵션에 대해 이 보안 그룹을 설정해야 합니다.

인바운드 규칙

프로토콜	포트	목적
SSH를 클릭합니다	22	커넥터 호스트에 대한 SSH 액세스를 제공합니다
HTTP	80	• 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공합니다 • Cloud Volumes ONTAP 업그레이드 프로세스 중에 사용됩니다
HTTPS	443	클라이언트 웹 브라우저에서 로컬 사용자 인터페이스에 대한 HTTPS 액세스 및 BlueXP 분류 인스턴스의 연결을 제공합니다
TCP	3128	Cloud Volumes ONTAP에서 인터넷에 액세스하여 AutoSupport 메시지를 NetApp 지원으로 보냅니다. 배포 후에는 이 포트를 수동으로 열어야 합니다. "커넥터가 AutoSupport 메시지의 프록시로 사용되는 방법에 대해 알아봅니다"

프로토콜	포트	목적
TCP	9060, 9061	정부 지역에서 BlueXP 분류 및 BlueXP 백업 및 복구를 활성화하고 사용할 수 있는 기능을 제공합니다.

아웃바운드 규칙

Connector에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

기본 아웃바운드 규칙

Connector에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

프로토콜	포트	목적
모든 TCP	모두	모든 아웃바운드 트래픽
모든 UDP	모두	모든 아웃바운드 트래픽

고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Connector의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

소스 IP 주소는 커넥터 호스트입니다.

서비스	프로토콜	포트	목적지	목적
API 호출 및 AutoSupport	HTTPS	443	아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF	API에서는 Azure, ONTAP, BlueXP 분류 및 AutoSupport 메시지를 NetApp에 전송합니다
API 호출	TCP	8080	BlueXP 분류	배포 중에 BlueXP 분류 인스턴스를 조사합니다
DNS	UDP입니다	53	DNS	BlueXP에서 DNS Resolve에 사용됩니다

Google Cloud의 커넥터 방화벽 규칙

Connector에 대한 Google Cloud 방화벽 규칙에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다. BlueXP에서 커넥터를 만들면 이 보안 그룹이 자동으로 생성됩니다. 다른 모든 설치 옵션에 대해 이 보안 그룹을 설정해야 합니다.

인바운드 규칙

프로토콜	포트	목적
SSH를 클릭합니다	22	커넥터 호스트에 대한 SSH 액세스를 제공합니다
HTTP	80	• 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공합니다 • Cloud Volumes ONTAP 업그레이드 프로세스 중에 사용됩니다
HTTPS	443	클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTPS 액세스를 제공합니다
TCP	3128	Cloud Volumes ONTAP에서 인터넷에 액세스하여 AutoSupport 메시지를 NetApp 지원으로 보냅니다. 배포 후에는 이 포트를 수동으로 열어야 합니다. "커넥터가 AutoSupport 메시지의 프록시로 사용되는 방법에 대해 알아봅니다"

아웃바운드 규칙

Connector에 대해 미리 정의된 방화벽 규칙은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

기본 아웃바운드 규칙

Connector에 대해 미리 정의된 방화벽 규칙에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

프로토콜	포트	목적
모든 TCP	모두	모든 아웃바운드 트래픽
모든 UDP	모두	모든 아웃바운드 트래픽

고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Connector의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

> 소스 IP 주소는 커넥터 호스트입니다.

서비스	프로토콜	포트	목적지	목적
API 호출 및 AutoSupport	HTTPS	443	아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF	API에서는 Google Cloud, ONTAP, BlueXP 분류 및 AutoSupport 메시지를 NetApp에 전송합니다
API 호출	TCP	8080	BlueXP 분류	배포 중에 BlueXP 분류 인스턴스를 조사합니다
DNS	UDP입니다	53	DNS	BlueXP에서 DNS Resolve에 사용됩니다

사내 커넥터용 포트

Connector는 온-프레미스 Linux 호스트에 수동으로 설치할 때 _ inbound_ports를 사용합니다. 이러한 포트는 계획 목적으로 참조해야 할 수 있습니다.

이러한 인바운드 규칙은 모든 BlueXP 배포 모델에 적용됩니다.

프로토콜	포트	목적
HTTP	80	• 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공합니다 • Cloud Volumes ONTAP 업그레이드 프로세스 중에 사용됩니다
HTTPS	443	클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTPS 액세스를 제공합니다