Permissões e regras de segurança do agente AWS

NetApp Console setup and administration

NetApp
March 02, 2026

Índice

Permissões e regras de segurança do agente AWS

Permissões da AWS para o agente do Console

Quando o NetApp Console inicia um agente do Console na AWS, ele anexa uma política ao agente que fornece ao agente permissões para gerenciar recursos e processos dentro dessa conta da AWS. O agente usa as permissões para fazer chamadas de API para vários serviços da AWS, incluindo EC2, S3, CloudFormation, IAM, Key Management Service (KMS) e muito mais.

Políticas de IAM

As políticas do IAM disponíveis abaixo fornecem as permissões que um agente do Console precisa para gerenciar recursos e processos dentro do seu ambiente de nuvem pública com base na sua região da AWS.

Observe o seguinte:

- Se você criar um agente do Console em uma região padrão da AWS diretamente do Console, o Console aplicará automaticamente as políticas ao agente.
- Você precisa configurar as políticas sozinho se implantar o agente do AWS Marketplace, se instalar manualmente o agente em um host Linux ou se quiser adicionar credenciais adicionais da AWS ao Console.
- Em ambos os casos, você precisa garantir que as políticas estejam atualizadas à medida que novas permissões forem adicionadas em versões subsequentes. Se novas permissões forem necessárias, elas serão listadas nas notas de versão.
- Se necessário, você pode restringir as políticas do IAM usando o IAM `Condition` elemento. "Documentação da AWS: Elemento Condition"
- Para ver instruções passo a passo sobre como usar essas políticas, consulte as seguintes páginas:
  - "Configurar permissões para uma implantação do AWS Marketplace"
  - "Configurar permissões para implantações locais"
  - "Configurar permissões para o modo restrito"
  - "Configure as permissões para o modo privado"

Selecione sua região para visualizar as políticas necessárias:

Regiões padrão

Para regiões padrão, as permissões são distribuídas em duas políticas. Duas políticas são necessárias devido ao limite máximo de tamanho de caracteres para políticas gerenciadas na AWS.

Política nº 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:ListStacks",
        "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:ReEncrypt*",
            "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",
            "ec2:DescribeVpcEndpoints",
            "kms:ListAliases",
            "glue:GetDatabase",
            "glue:GetTable",
            "glue:GetPartitions"
        ],
        "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"
    }
  ]
}
```

Política nº 2

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "tagServicePolicy"
    }
  ]
}
```

Regiões GovCloud (EUA)

```
{
  "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:ListStacks",
        "cloudformation:ValidateTemplate",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:CreateBucket",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "kms:ReEncrypt*",
        "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/*"
        ]
      }
    ]
}
```

Regiões secretas

```
{
  "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:ListStacks",
```

```
        "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",
        "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/*"
        ]
    }
  ]
}
```

Regiões ultrasecretas

```
{
  "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:ListStacks",
```

```
        "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",
        "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/*"
        ]
      }
    ]
}
```

Como as permissões da AWS são usadas

As seções a seguir descrevem como as permissões são usadas para cada serviço de gerenciamento ou dados do NetApp Console . Essas informações podem ser úteis se suas políticas corporativas determinarem que as permissões sejam fornecidas somente quando necessário.

Amazon FSx para ONTAP

O agente do Console faz as seguintes solicitações de API para gerenciar um sistema de arquivos Amazon FSx para ONTAP :

- ec2:DescreverInstâncias
- ec2:DescreverStatusDaInstancia
- ec2:DescribeInstanceAttribute
- ec2:DescreverTabelas de Rota
- ec2:DescreverImagens
- ec2:CriarTags
- ec2:DescreverVolumes
- ec2:DescreverGruposDeSegurança
- ec2:DescreverInterfacesDeRede

- ec2:DescreverSub-redes
- ec2:DescreverVpcs
- ec2:DescribeDhcpOptions
- ec2:Descrever Instantâneos
- ec2:DescreverParesDeChaves
- ec2:DescreverRegiões
- ec2:DescreverTags
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeReservedInstancesOfferings
- ec2:DescreverVpcEndpoints
- ec2:DescreverVpcs
- ec2:DescribeVolumesModifications
- ec2:DescreverGruposDePosicionamento
- kms:CriarConcessão
- kms:ListAliases
- fsx:Descreva*
- fsx:Lista*

Descoberta de bucket do Amazon S3

O agente do Console faz a seguinte solicitação de API para descobrir buckets do Amazon S3:

s3:ObterConfiguração de Criptografia

NetApp Backup and Recovery

O agente faz as seguintes solicitações de API para gerenciar backups no Amazon S3:

- s3:ObterLocalização do Balde
- s3:ListarTodosOsMeusBuckets
- s3:ListBucket
- s3:CriarBucket
- s3:ObterConfiguração do Ciclo de Vida
- s3:PutLifecycleConfiguration
- s3:PutBucketTagging
- s3:ListBucketVersões
- s3:ObterBucketAcl
- s3:PutBucketBloco de Acesso Público
- s3:ObterObjeto
- ec2:DescreverVpcEndpoints
- kms:ListAliases

- s3:PutEncryptionConfiguration

O agente faz as seguintes solicitações de API quando você usa o método Pesquisar e Restaurar para restaurar volumes e arquivos:

- s3:CriarBucket
- s3:ExcluirObjeto
- s3:ExcluirVersãoDoObjeto
- s3:ObterBucketAcl
- s3:ListBucket
- s3:ListBucketVersões
- s3:ListBucketMultipartUploads
- s3:ColocarObjeto
- s3:ColocarBucketAcl
- s3:PutLifecycleConfiguration
- s3:PutBucketBloco de Acesso Público
- s3:AbortarUploadMultipart
- s3:ListMultipartUploadParts

O agente faz as seguintes solicitações de API quando você usa o DataLock e o NetApp Ransomware Resilience para seus backups de volume:

- s3:ObterTag deVersão do Objeto
- s3:GetBucketObjectLockConfiguration
- s3:ObterVersãoDoObjetoAcl
- s3:PutObjectTagging
- s3:ExcluirObjeto
- s3:ExcluirMarcaçãoDeObjeto
- s3:ObterRetençãoDeObjeto
- s3:ExcluirMarcaçãoDeVersãoDoObjeto
- s3:ColocarObjeto
- s3:ObterObjeto
- s3:PutBucketObjectLockConfiguração
- s3:ObterConfiguração do Ciclo de Vida
- s3:ListBucketPorTags
- s3:Obter marcação de balde
- s3:ExcluirVersãoDoObjeto
- s3:ListBucketVersões
- s3:ListBucket
- s3:PutBucketTagging

- s3:ObterMarcaçãoDeObjeto
- s3:PutBucketVersionamento
- s3:PutObjectVersionTagging
- s3:GetBucketVersionamento
- s3:ObterBucketAcl
- s3:Ignorar Governança Retenção
- s3:PutObjectRetention
- s3:ObterLocalização do Balde
- s3:ObterVersãoDoObjeto

O agente faz as seguintes solicitações de API se você usar uma conta da AWS diferente para seus backups do Cloud Volumes ONTAP do que você está usando para os volumes de origem:

- s3:PolíticaPutBucket
- s3:PutBucketOwnershipControls

Permissões legadas para backup e recuperação.

Você só precisa das seguintes permissões se tiver habilitado os recursos de indexação legados antes do lançamento da versão 2 da indexação:

- kms:Lista*
- kms:Descreva*
- athena:Execução de Consulta Inicial
- athena:ObterResultados da Consulta
- athena:GetQueryExecution
- athena:PararExecuçãoDeConsulta
- cola:CriarBancoDeDados
- cola:CriarTabela
- cola:BatchDeletePartition

NetApp Data Classification

O agente faz as seguintes solicitações de API para implantar a NetApp Data Classification:

- ec2:DescreverInstâncias
- ec2:DescreverStatusDaInstancia
- ec2:ExecutarInstâncias
- ec2:TerminateInstances
- ec2:CriarTags
- ec2:CriarVolume
- ec2:AnexarVolume
- ec2:CriarGrupoDeSegurança

- ec2:ExcluirGrupoDeSegurança
- ec2:DescreverGruposDeSegurança
- ec2:CriarInterface de Rede
- ec2:DescreverInterfacesDeRede
- ec2:ExcluirInterface de Rede
- ec2:DescreverSub-redes
- ec2:DescreverVpcs
- ec2:Criar Instantâneo
- ec2:DescreverRegiões
- formação de nuvem: CreateStack
- formação de nuvem:DeleteStack
- cloudformation:DescribeStacks
- cloudformation:DescreverEventosStack
- cloudformation:ListStacks
- iam:AdicionarFunçãoAoPerfilDaInstancia
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations

O agente faz as seguintes solicitações de API para verificar buckets do S3 quando você usa a NetApp Data Classification:

- iam:AdicionarFunçãoAoPerfilDaInstancia
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations
- s3:Obter marcação de balde
- s3:ObterLocalização do Balde
- s3:ListarTodosOsMeusBuckets
- s3:ListBucket
- s3:ObterStatusdaPolíticaDoBucket
- s3:ObterPolítica deBucket
- s3:ObterBucketAcl
- s3:ObterObjeto
- iam:GetRole
- s3:ExcluirObjeto
- s3:ExcluirVersãoDoObjeto
- s3:ColocarObjeto
- sts:AssumaFunção

Cloud Volumes ONTAP

O agente faz as seguintes solicitações de API para implantar e gerenciar o Cloud Volumes ONTAP na AWS.

Propósito	Ação	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
Crie e gerencie funções do IAM e perfis de instância para instâncias do Cloud Volumes ONTAP	iam:ListInstanceProfiles	Sim	Sim	Não
	iam:CriarFunção	Sim	Não	Não
	iam:ExcluirFunção	Não	Sim	Sim
	iam:PutRolePolicy	Sim	Não	Não
	iam:CriarPerfilDeInstancia	Sim	Não	Não
	iam:DeleteRolePolicy	Não	Sim	Sim
	iam:AdicionarFunçãoAoPerfilDaInstancia	Sim	Não	Não
	iam:RemoveRoleFromInstanceProfile	Não	Sim	Sim
	iam:ExcluirPerfilDeInstance	Não	Sim	Sim
	iam:PassRole	Sim	Não	Não
	ec2:AssociateIamInstanceProfile	Sim	Sim	Não
	ec2:DescribeIamInstanceProfileAssociations	Sim	Sim	Não
	ec2:DesassociarPerfilDeInstanciaIam	Não	Sim	Não
Decodificar mensagens de status de autorização	sts:DecodificarMensagemDeAutorização	Sim	Sim	Não
Descreva as imagens especificadas (AMIs) disponíveis para a conta	ec2:DescreverImagens	Sim	Sim	Não
Descreva as tabelas de rotas em uma VPC (necessário apenas para pares HA)	ec2:DescreverTabelas de Rota	Sim	Não	Não

Propósito	Ação	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
Parar, iniciar e monitorar instâncias	ec2:Instâncias de Início	Sim	Sim	Não
	ec2:StopInstances	Sim	Sim	Não
	ec2:DescreverInstâncias	Sim	Sim	Não
	ec2:DescreverStatusDaInstancia	Sim	Sim	Não
	ec2:ExecutarInstâncias	Sim	Não	Não
	ec2:TerminateInstances	Não	Não	Sim
	ec2:ModificarAtributoDeInstancia	Não	Sim	Não
Verifique se a rede aprimorada está habilitada para os tipos de instância suportados	ec2:DescribeInstanceAttribute	Não	Sim	Não
Marque os recursos com as tags "WorkingEnvironment" e "WorkingEnvironmentId", que são usadas para manutenção e alocação de custos.	ec2:CriarTags	Sim	Sim	Não
Gerenciar volumes EBS que o Cloud Volumes ONTAP usa como armazenamento de backend	ec2:CriarVolume	Sim	Sim	Não
	ec2:DescreverVolumes	Sim	Sim	Sim
	ec2:ModificarAtributoVolume	Não	Sim	Sim
	ec2:AnexarVolume	Sim	Sim	Não
	ec2:ExcluirVolume	Não	Sim	Sim
	ec2:DetachVolume	Não	Sim	Sim

Propósito	Ação	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
Crie e gerencie grupos de segurança para o Cloud Volumes ONTAP	ec2:CriarGrupoDeSegurança	Sim	Não	Não
	ec2:ExcluirGrupoDeSegurança	Não	Sim	Sim
	ec2:DescreverGruposDeSegurança	Sim	Sim	Sim
	ec2:RevokeSecurityGroupEgress	Sim	Não	Não
	ec2:AuthorizeSecurityGroupEgress	Sim	Não	Não
	ec2:AutorizarEntrada de Grupo de Segurança	Sim	Não	Não
	ec2:RevogarIngressoDoGrupoDeSegurança	Sim	Sim	Não
Crie e gerencie interfaces de rede para o Cloud Volumes ONTAP na sub-rede de destino	ec2:CriarInterface de Rede	Sim	Não	Não
	ec2:DescreverInterfacesDeRede	Sim	Sim	Não
	ec2:ExcluirInterface de Rede	Não	Sim	Sim
	ec2:ModificarAtributoDeInterfaceDeRede	Não	Sim	Não
Obtenha a lista de sub-redes de destino e grupos de segurança	ec2:DescreverSub-redes	Sim	Sim	Não
	ec2:DescreverVpcs	Sim	Sim	Não
Obtenha servidores DNS e o nome de domínio padrão para instâncias do Cloud Volumes ONTAP	ec2:DescribeDhcpOptions	Sim	Não	Não
Faça snapshots de volumes EBS para Cloud Volumes ONTAP	ec2:Criar Instantâneo	Sim	Sim	Não
	ec2:ExcluirInstantâneo	Não	Sim	Sim
	ec2:Descrever Instantâneos	Não	Sim	Não

Propósito	Ação	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
Capture o console Cloud Volumes ONTAP , que está anexado às mensagens do AutoSupport	ec2:ObterSaída do Console	Sim	Sim	Não
Obtenha a lista de pares de chaves disponíveis	ec2:DescreverParesDeChaves	Sim	Não	Não
Obtenha a lista de regiões AWS disponíveis	ec2:DescreverRegiões	Sim	Sim	Não
Gerenciar tags para recursos associados a instâncias do Cloud Volumes ONTAP	ec2:ExcluirTags	Não	Sim	Sim
	ec2:DescreverTags	Não	Sim	Não
Criar e gerenciar pilhas para modelos do AWS CloudFormation	formação de nuvem: CreateStack	Sim	Não	Não
	formação de nuvem:DeleteStack	Sim	Não	Não
	cloudformation:DescribeStacks	Sim	Sim	Não
	cloudformation:DescreverEventosStack	Sim	Não	Não
	cloudformation:ValidarModelo	Sim	Não	Não

Propósito	Ação	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
Crie e gerencie um bucket S3 que um sistema Cloud Volumes ONTAP usa como uma camada de capacidade para hierarquização de dados	s3:CriarBucket	Sim	Sim	Não
	s3:ExcluirBucket	Não	Sim	Sim
	s3:ObterConfiguração do Ciclo de Vida	Não	Sim	Não
	s3:PutLifecycleConfiguration	Não	Sim	Não
	s3:PutBucketTagging	Não	Sim	Não
	s3:ListBucketVersões	Não	Sim	Não
	s3:ObterStatusdaPolíticaDoBucket	Não	Sim	Não
	s3:GetBucketBloco de Acesso Público	Não	Sim	Não
	s3:ObterBucketAcl	Não	Sim	Não
	s3:ObterPolíticadeBucket	Não	Sim	Não
	s3:PutBucketBloco de Acesso Público	Não	Sim	Não
	s3:Obter marcação de balde	Não	Sim	Não
	s3:ObterLocalizaçãodo Balde	Não	Sim	Não
	s3:ListarTodosOsMeusBuckets	Não	Não	Não
	s3:ListBucket	Não	Sim	Não
Habilitar a criptografia de dados do Cloud Volumes ONTAP usando o AWS Key Management Service (KMS)	kms:Recriptografar*	Sim	Não	Não
	kms:CriarConcessão	Sim	Sim	Não
	kms:GerarChaveDeDadosSemTextoSimples	Sim	Sim	Não

Propósito	Ação	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
Crie e gerencie um grupo de posicionamento de spread da AWS para dois nós de HA e o mediador em uma única Zona de Disponibilidade da AWS	ec2:CriarGrupoDePosicionamento	Sim	Não	Não
	ec2:ExcluirGrupo de Posicionamento	Não	Sim	Sim
Criar relatórios	fsx:Descreva*	Não	Sim	Não
	fsx:Lista*	Não	Sim	Não
Crie e gerencie agregados que oferecem suporte ao recurso Amazon EBS Elastic Volumes	ec2:DescribeVolumesModifications	Não	Sim	Não
	ec2:ModificarVolume	Não	Sim	Não
Verifique se a Zona de Disponibilidade é uma Zona Local da AWS e valide se todos os parâmetros de implantação são compatíveis	ec2:DescreverZonasDeDisponibilidade	Sim	Não	Sim

Registro de alterações

Conforme as permissões forem adicionadas e removidas, elas serão anotadas nas seções abaixo.

24 fevereiro 2026

A seguinte permissão agora é necessária para Data Classification:

cloudformation:ListStacks

11 de novembro de 2025

As seguintes permissões não são mais necessárias para o NetApp Backup and Recovery, a menos que você utilize a indexação legada. Essas permissões foram removidas das políticas desta página:

- kms:Lista*
- kms:Descreva*
- athena:Execução de Consulta Inicial
- athena:ObterResultados da Consulta
- athena:GetQueryExecution
- athena:ParararExecuçãoDeConsulta
- cola:CriarBancoDeDados

- cola:CriarTabela
- cola:BatchDeletePartition

9 de setembro de 2024

As permissões foram removidas da política nº 2 para regiões padrão porque o NetApp Console não oferece mais suporte ao cache de borda do NetApp , nem à descoberta e ao gerenciamento de clusters do Kubernetes.

Visualizar as permissões que foram removidas da política

```
{
    "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"
}
```

9 de maio de 2024

A seguinte permissão agora é necessária para o Cloud Volumes ONTAP:

ec2:DescreverZonasDeDisponibilidade

6 de junho de 2023

A seguinte permissão agora é necessária para o Cloud Volumes ONTAP:

kms:GerarChaveDeDadosSemTextoSimples

14 de fevereiro de 2023

A seguinte permissão agora é necessária para o NetApp Cloud Tiering:

ec2:DescreverVpcEndpoints

Regras de grupo de segurança do agente de console na AWS

O grupo de segurança da AWS para o agente requer regras de entrada e saída. O NetApp Console cria automaticamente esse grupo de segurança quando você cria um agente do Console a partir do Console. Você precisa configurar este grupo de segurança para todas as outras opções de instalação.

Regras de entrada

Protocolo	Porta	Propósito
SSH	22	Fornece acesso SSH ao host do agente
HTTP	80	• Fornece acesso HTTP dos navegadores da web do cliente para a interface do usuário local • Usado durante o processo de atualização do Cloud Volumes ONTAP
HTTPS	443	Fornece acesso HTTPS à interface do usuário local e conexões da instância de NetApp Data Classification
TCP	3128	Fornece Cloud Volumes ONTAP com acesso à internet. Você deve abrir esta porta manualmente após a implantação.

Regras de saída

O grupo de segurança predefinido para o agente abre todo o tráfego de saída. Se isso for aceitável, siga as regras básicas de saída. Se precisar de regras mais rígidas, use as regras de saída avançadas.

Regras básicas de saída

O grupo de segurança predefinido para o agente inclui as seguintes regras de saída.

Protocolo	Porta	Propósito
Todos TCP	Todos	Todo o tráfego de saída

Protocolo	Porta	Propósito
Todos os UDP	Todos	Todo o tráfego de saída

Regras avançadas de saída

Se você precisar de regras rígidas para o tráfego de saída, poderá usar as seguintes informações para abrir apenas as portas necessárias para a comunicação de saída pelo agente

O endereço IP de origem é o host do agente.

Serviço	Protocolo	Porta	Destino	Propósito
Chamadas de API e AutoSupport	HTTPS	443	Gerenciamento de cluster de Internet de saída e ONTAP LIF	Chamadas de API para AWS, para ONTAP, para NetApp Data Classification e envio de mensagens AutoSupport para NetApp
Chamadas de API	TCP	3000	Mediador ONTAP HA	Comunicação com o mediador ONTAP HA
	TCP	8080	Classificação de Dados	Sondar a instância de classificação de dados durante a implantação
DNS	UDP	53	DNS	Usado para resolução de DNS pelo Console

Informações sobre direitos autorais

Informações sobre marcas comerciais