Autorizzazioni e regole di sicurezza dell'agente AWS

NetApp Console setup and administration

NetApp
February 11, 2026

Sommario

Autorizzazioni e regole di sicurezza dell'agente AWS

Autorizzazioni AWS per l'agente della console

Quando la NetApp Console avvia un agente della console in AWS, associa all'agente una policy che gli fornisce le autorizzazioni per gestire risorse e processi all'interno di quell'account AWS. L'agente utilizza le autorizzazioni per effettuare chiamate API a diversi servizi AWS, tra cui EC2, S3, CloudFormation, IAM, Key Management Service (KMS) e altri ancora.

Politiche IAM

Le policy IAM disponibili di seguito forniscono le autorizzazioni di cui un agente della console ha bisogno per gestire risorse e processi all'interno del tuo ambiente cloud pubblico in base alla tua regione AWS.

Notare quanto segue:

- Se si crea un agente della Console in una regione AWS standard direttamente dalla Console, la Console applica automaticamente le policy all'agente.
- È necessario impostare autonomamente le policy se si distribuisce l'agente da AWS Marketplace, se si installa manualmente l'agente su un host Linux o se si desidera aggiungere ulteriori credenziali AWS alla Console.
- In entrambi i casi, è necessario assicurarsi che i criteri siano aggiornati poiché nelle versioni successive verranno aggiunte nuove autorizzazioni. Se saranno necessarie nuove autorizzazioni, queste saranno elencate nelle note di rilascio.
- Se necessario, è possibile limitare i criteri IAM utilizzando IAM `Condition` elemento. "Documentazione AWS: Elemento Condizione"
- Per visualizzare le istruzioni dettagliate sull'utilizzo di queste policy, fare riferimento alle seguenti pagine:
  - "Impostare le autorizzazioni per una distribuzione AWS Marketplace"
  - "Impostare le autorizzazioni per le distribuzioni in locale"
  - "Imposta le autorizzazioni per la modalità limitata"

Seleziona la tua regione per visualizzare le policy richieste:

Regioni standard

Per le regioni standard, le autorizzazioni sono distribuite su due policy. Sono necessarie due policy a causa del limite massimo di dimensione dei caratteri per le policy gestite in AWS.

Politica n. 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: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"
    }
  ]
}
```

Politica n. 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"
    }
  ]
}
```

Regioni GovCloud (USA)

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

Regioni segrete

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

Regioni top secret

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

Come vengono utilizzate le autorizzazioni AWS

Le sezioni seguenti descrivono come vengono utilizzate le autorizzazioni per ogni servizio dati o di gestione NetApp Console . Queste informazioni possono essere utili se le politiche aziendali stabiliscono che le autorizzazioni vengano concesse solo se necessario.

Amazon FSx per ONTAP

L'agente della console effettua le seguenti richieste API per gestire un file system Amazon FSx for ONTAP :

- ec2:DescriviIstanze
- ec2:DescriviStatoIstanza
- ec2:Descriviattributoistanza
- ec2:DescriviRouteTables
- ec2:DescriviImmagini
- ec2:CreaTag
- ec2:DescriviVolumi
- ec2:Descrivi gruppi di sicurezza
- ec2:DescriviInterfacceDiRete
- ec2:Descrivi sottoreti
- ec2:DescriviVpcs

- ec2:DescriviDhcpOptions
- ec2:Descrivi istantanee
- ec2:Descrivi coppie di chiavi
- ec2:DescriviRegioni
- ec2:DescriviTag
- ec2:DescribeIamInstanceProfileAssociations
- ec2:Descrivi le offerte di istanze riservate
- ec2:DescriviVpcEndpoints
- ec2:DescriviVpcs
- ec2:DescribeVolumesModifications
- ec2:DescribePlacementGroups
- kms:CreateGrant
- kms:ListAliases
- fsx:Descrivi*
- fsx:Elenco*

Rilevamento del bucket Amazon S3

L'agente della console effettua la seguente richiesta API per individuare i bucket Amazon S3:

s3:Ottieni configurazione crittografia

NetApp Backup and Recovery

L'agente effettua le seguenti richieste API per gestire i backup in Amazon S3:

- s3:OttieniPosizioneBucket
- s3:ElencaTuttiIMieBucket
- s3:ElencoBucket
- s3:CreaBucket
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3:PutBucketTagging
- s3:ListBucketVersions
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- s3:OttieniOggetto
- ec2:DescriviVpcEndpoints
- kms:ListAliases
- s3:PutEncryptionConfiguration

L'agente effettua le seguenti richieste API quando si utilizza il metodo Cerca e ripristina per ripristinare volumi

e file:

- s3:CreaBucket
- s3:EliminaOggetto
- s3:EliminaVersioneOggetto
- s3:GetBucketAcl
- s3:ElencoBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLifecycleConfiguration
- s3:PutBucketPublicAccessBlock
- s3:AnnullaCaricamentoMultipart
- s3:ListMultipartUploadParts

L'agente effettua le seguenti richieste API quando si utilizzano DataLock e NetApp Ransomware Resilience per i backup dei volumi:

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:EliminaOggetto
- s3:EliminaTaggingOggetto
- s3:OttieniRitenzioneOggetto
- s3:EliminaObjectVersionTagging
- s3:PutObject
- s3:OttieniOggetto
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:ListBucketByTags
- s3:OttieniTaggingBucket
- s3:EliminaVersioneOggetto
- s3:ListBucketVersions
- s3:ElencoBucket
- s3:PutBucketTagging
- s3:OttieniTaggingOggetto
- s3:PutBucketVersioning
- s3:PutObjectVersionTagging

- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BypassGovernanceRetention
- s3:PutObjectRetention
- s3:OttieniPosizioneBucket
- s3:GetObjectVersion

L'agente effettua le seguenti richieste API se per i backup Cloud Volumes ONTAP utilizzi un account AWS diverso da quello utilizzato per i volumi di origine:

- s3:PoliticaPutBucket
- s3:PutBucketOwnershipControls

Autorizzazioni legacy per backup e ripristino

Sono necessarie solo le seguenti autorizzazioni se sono state abilitate le funzionalità di indicizzazione legacy prima del rilascio dell'indicizzazione v2:

- km:Elenco*
- km:Descrivi*
- athena:StartQueryExecution
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- colla:CreaDatabase
- colla:CreaTabella
- colla:BatchDeletePartition

Classificazione

L'agente effettua le seguenti richieste API per distribuire NetApp Data Classification:

- ec2:DescriviIstanze
- ec2:DescriviStatoIstanza
- ec2:EseguiIstanze
- ec2:Termina le istanze
- ec2:CreaTag
- ec2:CreaVolume
- ec2:AttachVolume
- ec2:CreateSecurityGroup
- ec2:EliminaGruppoDiSicurezza
- ec2:Descrivi gruppi di sicurezza
- ec2:CreateNetworkInterface

- ec2:DescriviInterfacceDiRete
- ec2:EliminaInterfacciaDiRete
- ec2:Descrivi sottoreti
- ec2:DescriviVpcs
- ec2:CreaSnapshot
- ec2:DescriviRegioni
- cloudformation:CreateStack
- cloudformation:EliminaStack
- cloudformation:DescribeStacks
- cloudformation:DescribeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations

L'agente effettua le seguenti richieste API per eseguire la scansione dei bucket S3 quando si utilizza NetApp Data Classification:

- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations
- s3:OttieniTaggingBucket
- s3:OttieniPosizioneBucket
- s3:ElencaTuttiIMieBucket
- s3:ElencoBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy
- s3:GetBucketAcl
- s3:OttieniOggetto
- iam:GetRole
- s3:EliminaOggetto
- s3:EliminaVersioneOggetto
- s3:PutObject
- sts:AssumeRole

Cloud Volumes ONTAP

L'agente effettua le seguenti richieste API per distribuire e gestire Cloud Volumes ONTAP in AWS.

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Crea e gestisci ruoli IAM e profili di istanza per istanze Cloud Volumes ONTAP	iam:ListInstanceProfiles	SÌ	SÌ	NO
	iam:CreateRole	SÌ	NO	NO
	iam:EliminaRuolo	NO	SÌ	SÌ
	iam:PutRolePolicy	SÌ	NO	NO
	iam:CreateInstanceProfile	SÌ	NO	NO
	iam:DeleteRolePolicy	NO	SÌ	SÌ
	iam:AddRoleToInstanceProfile	SÌ	NO	NO
	iam:RemoveRoleFromInstanceProfile	NO	SÌ	SÌ
	iam:DeleteInstanceProfile	NO	SÌ	SÌ
	iam:PassRole	SÌ	NO	NO
	ec2:AssociateIamInstanceProfile	SÌ	SÌ	NO
	ec2:DescribeIamInstanceProfileAssociations	SÌ	SÌ	NO
	ec2:DisassociateIamInstanceProfile	NO	SÌ	NO
Decodifica i messaggi sullo stato di autorizzazione	sts:DecodeAuthorizationMessage	SÌ	SÌ	NO
Descrivi le immagini specificate (AMI) disponibili per l'account	ec2:DescriviImmagini	SÌ	SÌ	NO
Descrivere le tabelle di routing in una VPC (richiesto solo per le coppie HA)	ec2:DescriviRouteTables	SÌ	NO	NO

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Arrestare, avviare e monitorare le istanze	ec2:StartInstances	SÌ	SÌ	NO
	ec2:StopInstances	SÌ	SÌ	NO
	ec2:DescriviIstanze	SÌ	SÌ	NO
	ec2:DescriviStatoIstanza	SÌ	SÌ	NO
	ec2:EseguiIstanze	SÌ	NO	NO
	ec2:Termina le istanze	NO	NO	SÌ
	ec2:ModificaAttributoIstanza	NO	SÌ	NO
Verificare che la rete avanzata sia abilitata per i tipi di istanza supportati	ec2:Descriviattributoistanza	NO	SÌ	NO
Etichettare le risorse con i tag "WorkingEnvironment" e "WorkingEnvironmentId" che vengono utilizzati per la manutenzione e l'allocazione dei costi	ec2:CreaTag	SÌ	SÌ	NO
Gestire i volumi EBS che Cloud Volumes ONTAP utilizza come storage back-end	ec2:CreaVolume	SÌ	SÌ	NO
	ec2:DescriviVolumi	SÌ	SÌ	SÌ
	ec2:ModificaAttributoVolume	NO	SÌ	SÌ
	ec2:AttachVolume	SÌ	SÌ	NO
	ec2:EliminaVolume	NO	SÌ	SÌ
	ec2:DetachVolume	NO	SÌ	SÌ

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Crea e gestisci gruppi di sicurezza per Cloud Volumes ONTAP	ec2:CreateSecurityGroup	SÌ	NO	NO
	ec2:EliminaGruppoDiSicurezza	NO	SÌ	SÌ
	ec2:Descrivi gruppi di sicurezza	SÌ	SÌ	SÌ
	ec2:RevokeSecurityGroupEgress	SÌ	NO	NO
	ec2:AuthorizeSecurityGroupEgress	SÌ	NO	NO
	ec2:AuthorizeSecurityGroupIngress	SÌ	NO	NO
	ec2:RevokeSecurityGroupIngress	SÌ	SÌ	NO
Crea e gestisci le interfacce di rete per Cloud Volumes ONTAP nella subnet di destinazione	ec2:CreateNetworkInterface	SÌ	NO	NO
	ec2:DescriviInterfaccEDiRete	SÌ	SÌ	NO
	ec2:EliminaInterfacciaDiRete	NO	SÌ	SÌ
	ec2:ModificaAttributoInterfacciaRete	NO	SÌ	NO
Ottieni l'elenco delle subnet di destinazione e dei gruppi di sicurezza	ec2:Descrivi sottoreti	SÌ	SÌ	NO
	ec2:DescriviVpcs	SÌ	SÌ	NO
Ottieni i server DNS e il nome di dominio predefinito per le istanze Cloud Volumes ONTAP	ec2:DescriviDhcpOptions	SÌ	NO	NO
Acquisisci snapshot dei volumi EBS per Cloud Volumes ONTAP	ec2:CreaSnapshot	SÌ	SÌ	NO
	ec2:EliminaSnapshot	NO	SÌ	SÌ
	ec2:Descrivi istantanee	NO	SÌ	NO
Acquisisci la console Cloud Volumes ONTAP , che è allegata ai messaggi AutoSupport	ec2:GetConsoleOutput	SÌ	SÌ	NO

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Ottieni l'elenco delle coppie di chiavi disponibili	ec2:Descrivi coppie di chiavi	SÌ	NO	NO
Ottieni l'elenco delle regioni AWS disponibili	ec2:DescriviRegioni	SÌ	SÌ	NO
Gestisci i tag per le risorse associate alle istanze Cloud Volumes ONTAP	ec2:EliminaTag	NO	SÌ	SÌ
	ec2:DescriviTag	NO	SÌ	NO
Crea e gestisci stack per i modelli AWS CloudFormation	cloudformation:CreateStack	SÌ	NO	NO
	cloudformation:EliminaStack	SÌ	NO	NO
	cloudformation:DescribeStacks	SÌ	SÌ	NO
	cloudformation:DescribeStackEvents	SÌ	NO	NO
	cloudformation:ValidateTemplate	SÌ	NO	NO

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Crea e gestisci un bucket S3 che un sistema Cloud Volumes ONTAP utilizza come livello di capacità per la suddivisione in livelli dei dati	s3:CreaBucket	SÌ	SÌ	NO
	s3:EliminaBucket	NO	SÌ	SÌ
	s3:GetLifecycleConfiguration	NO	SÌ	NO
	s3:PutLifecycleConfiguration	NO	SÌ	NO
	s3:PutBucketTagging	NO	SÌ	NO
	s3:ListBucketVersions	NO	SÌ	NO
	s3:GetBucketPolicyStatus	NO	SÌ	NO
	s3:GetBucketPublicAccessBlock	NO	SÌ	NO
	s3:GetBucketAcl	NO	SÌ	NO
	s3:GetBucketPolicy	NO	SÌ	NO
	s3:PutBucketPublicAccessBlock	NO	SÌ	NO
	s3:OttieniTaggingBucket	NO	SÌ	NO
	s3:OttieniPosizioneBucket	NO	SÌ	NO
	s3:ElencaTuttiIMieBucket	NO	NO	NO
	s3:ElencoBucket	NO	SÌ	NO
Abilita la crittografia dei dati di Cloud Volumes ONTAP utilizzando AWS Key Management Service (KMS)	kms:Ricrittografa*	SÌ	NO	NO
	kms:CreateGrant	SÌ	SÌ	NO
	kms:GenerateDataKeyWithoutPlaintext	SÌ	SÌ	NO
Crea e gestisci un gruppo di posizionamento diffuso AWS per due nodi HA e il mediatore in una singola zona di disponibilità AWS	ec2:CreatePlacementGroup	SÌ	NO	NO
	ec2:EliminaGruppoPosizionamento	NO	SÌ	SÌ

Scopo	Azione	Utilizzato per la distribuzione?	Utilizzato per le operazioni quotidiane?	Utilizzato per l'eliminazione?
Crea report	fsx:Descrivi*	NO	SÌ	NO
	fsx:Elenco*	NO	SÌ	NO
Crea e gestisci aggregati che supportano la funzionalità Amazon EBS Elastic Volumes	ec2:DescribeVolumesModifications	NO	SÌ	NO
	ec2:ModificaVolume	NO	SÌ	NO
Verifica se la zona di disponibilità è una zona locale AWS e convalida che tutti i parametri di distribuzione siano compatibili	ec2:Descrivi le zone di disponibilità	SÌ	NO	SÌ

Registro delle modifiche

Man mano che vengono aggiunte o rimosse autorizzazioni, ne daremo nota nelle sezioni seguenti.

11 novembre 2025

Le seguenti autorizzazioni non sono più necessarie per NetApp Backup and Recovery, a meno che non si utilizzi l'indicizzazione legacy. Queste autorizzazioni sono state rimosse dalle policy presenti in questa pagina:

- km:Elenco*
- km:Descrivi*
- athena:StartQueryExecution
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- colla:CreaDatabase
- colla:CreaTabella
- colla:BatchDeletePartition

9 settembre 2024

Le autorizzazioni sono state rimosse dalla policy n. 2 per le regioni standard perché la NetApp Console non supporta più la memorizzazione nella cache edge NetApp e la scoperta e la gestione dei cluster Kubernetes.

Visualizza le autorizzazioni che sono state rimosse dalla policy

```
{
    "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 maggio 2024

Per Cloud Volumes ONTAP è ora richiesta la seguente autorizzazione:

ec2:Descrivi le zone di disponibilità

6 giugno 2023

Per Cloud Volumes ONTAP è ora richiesta la seguente autorizzazione:

kms:GenerateDataKeyWithoutPlaintext

14 febbraio 2023

Per NetApp Cloud Tiering è ora richiesta la seguente autorizzazione:

ec2:DescriviVpcEndpoints

Regole del gruppo di sicurezza dell'agente della console in AWS

Il gruppo di sicurezza AWS per l'agente richiede regole sia in entrata che in uscita. La NetApp Console crea automaticamente questo gruppo di sicurezza quando si crea un agente della console dalla console. È necessario impostare questo gruppo di sicurezza per tutte le altre opzioni di installazione.

Regole in entrata

Protocollo	Porta	Scopo
SSH	22	Fornisce accesso SSH all'host dell'agente
HTTP	80	• Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale • Utilizzato durante il processo di aggiornamento Cloud Volumes ONTAP
HTTPS	443	Fornisce accesso HTTPS all'interfaccia utente locale e connessioni dall'istanza di NetApp Data Classification
TCP	3128	Fornisce a Cloud Volumes ONTAP l'accesso a Internet. Dopo la distribuzione, è necessario aprire manualmente questa porta.

Regole in uscita

Il gruppo di sicurezza predefinito per l'agente apre tutto il traffico in uscita. Se ciò è accettabile, seguite le regole di base per le comunicazioni in uscita. Se hai bisogno di regole più rigide, usa le regole in uscita avanzate.

Regole di base in uscita

Il gruppo di sicurezza predefinito per l'agente include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutto TCP	Tutto	Tutto il traffico in uscita

Protocollo	Porta	Scopo
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole in uscita avanzate

Se hai bisogno di regole rigide per il traffico in uscita, puoi utilizzare le seguenti informazioni per aprire solo le porte necessarie per la comunicazione in uscita da parte dell'agente

L'indirizzo IP di origine è l'host dell'agente.

Servizio	Protocollo	Porta	Destinazione	Scopo
Chiamate API e AutoSupport	HTTPS	443	Gestione cluster ONTAP e Internet in uscita LIF	Chiamate API ad AWS, a ONTAP, a NetApp Data Classification e invio di messaggi AutoSupport a NetApp
chiamate API	TCP	3000	Mediatore ONTAP HA	Comunicazione con il mediatore ONTAP HA
	TCP	8080	Classificazione dei dati	Sonda per l'istanza di classificazione dei dati durante la distribuzione
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS da parte della console

Informazioni sul copyright

Informazioni sul marchio commerciale