Referência

NetApp Console setup and administration

NetApp
January 23, 2026

Índice

Referência

Console de manutenção do agente

Validação do agente com o console de manutenção

Você pode usar o console de manutenção do agente do Console para validar a instalação e a configuração de um agente do Console.

Acesse o console de manutenção do agente

Você pode acessar o Console de manutenção a partir do host do agente do Console. Navegue até o seguinte diretório:

```
/opt/application/netapp/service-manager-2/agent-maint-console
```

verificador de configuração validar

O `config-checker validate` O comando permite validar a configuração de um agente de console.

Parâmetros

`--services <comma-separated list of services to validate>`**--OBRIGATÓRIO--**

Selecione um ou mais serviços para validar. Os nomes de serviço válidos são:*`PLATFORM` que valida a conectividade de rede com os endpoints do Console necessários.

`--validationTypes <comma-separated list validation types to run>`**--OBRIGATÓRIO--**
Escolha um ou mais tipos de validação para executar. Os tipos de validação válidos são: * `NETWORK` que valida a conectividade de rede com os endpoints do Console necessários.

`--proxy <url>`**--OPCIONAL--**

Especifica o URL do servidor proxy a ser usado para a validação. Necessário se o seu agente estiver configurado para usar um servidor proxy.

`--certs <paths>`**--OPCIONAL--**

Especifica o caminho para um ou mais arquivos de certificado a serem usados para a validação. Os arquivos de certificado devem estar no formato PEM. Separe vários caminhos com vírgulas. Este parâmetro é obrigatório se o seu agente usar um certificado personalizado.

Exemplos de validação do verificador de configuração

Validação básica:

```
./agent-maint-console config-checker validate --services PLATFORM
--validationTypes NETWORK
```

Validação quando um servidor proxy é usado para o agente:

```
./agent-maint-console config-checker validate --services PLATFORM
--validationTypes NETWORK --proxy http://proxy.company.com:8080
```

Validação quando um certificado é usado para o agente:

```
./agent-maint-console config-checker validate --services PLATFORM
--validationTypes NETWORK --certs /path/to/cert1.pem,/path/to/cert2.pem
```

Ver ajuda para qualquer comando

Para visualizar a ajuda de qualquer comando, anexe `--help` ao comando. Por exemplo, para visualizar a ajuda para o `proxy add` comando, use o seguinte comando:

```
./agent-maint-console proxy add --help
```

Comandos de proxy transparentes

Você pode usar o console de manutenção do agente do Console para configurar um agente do Console para usar um servidor proxy transparente.

Acesse o console de manutenção do agente

Você pode acessar o Console de manutenção a partir do host do agente do Console. Navegue até o seguinte diretório:

```
/opt/application/netapp/service-manager-2/agent-maint-console
```

Ver ajuda para qualquer comando

Para visualizar a ajuda de qualquer comando, anexe `--help` ao comando. Por exemplo, para visualizar a ajuda para o `proxy add` comando, use o seguinte comando:

```
./agent-maint-console proxy add --help
```

proxy get

O `proxy get` O comando exibe informações sobre a configuração atual do servidor proxy transparente. Para visualizar a configuração atual do servidor proxy transparente, use o seguinte comando:

Exemplo de obtenção de proxy

Para visualizar a configuração atual do servidor proxy transparente, use o seguinte comando:

```
./agent-maint-console proxy get
```

adicionar proxy

O `proxy add` O comando configura o agente para usar um servidor proxy transparente.

Parâmetros

`-c <certificate file>`

Especifica o caminho para o arquivo de certificado do servidor proxy. O arquivo de certificado deve estar no formato PEM. Certifique-se de que o arquivo de certificado esteja no mesmo diretório que o comando ou especifique o caminho completo para o arquivo de certificado.

Exemplo de adição de proxy

Para adicionar um servidor proxy transparente, use o seguinte comando, onde `/home/ubuntu/myCA1.pem` é o caminho para o arquivo de certificado do servidor proxy. O arquivo do certificado deve estar no formato PEM:

```
./agent-maint-console proxy add -c /home/ubuntu/myCA1.pem
```

atualização de proxy

O `proxy update` Este comando permite atualizar o certificado de um proxy transparente.

Parâmetros

`-c <certificate file>`Especifica o caminho para o arquivo de certificado do servidor proxy. O arquivo de certificado deve estar no formato PEM.

Certifique-se de que o arquivo de certificado esteja no mesmo diretório que o comando ou especifique o caminho completo para o arquivo de certificado.

Exemplo de atualização de proxy

Para atualizar o certificado de um servidor proxy transparente, use o seguinte comando, onde `/home/ubuntu/myCA1.pem` é o caminho para o novo arquivo de certificado para o servidor proxy. O arquivo do certificado deve estar no formato PEM:

```
./agent-maint-console proxy update -c /home/ubuntu/myCA1.pem
```

remoção de proxy

O `proxy remove` O comando remove a configuração do servidor proxy transparente do agente.

Exemplo de remoção de proxy

Para remover o servidor proxy transparente, use o seguinte comando:

```
./agent-maint-console proxy remove
```

Permissões do agente do provedor de nuvem e requisitos de rede

Resumo de permissões para o NetApp Console

Você precisará conceder ao agente do Console as permissões adequadas para que ele possa executar operações em seu ambiente de nuvem. Utilize os links nesta página para acessar rapidamente as permissões necessárias de acordo com seu objetivo.

Permissões da AWS

O NetApp Console requer permissões da AWS para um agente do Console e para serviços individuais.

Agentes de console

Meta	Descrição	Link
Implantar um agente do Console a partir do Console Para implantar um agente do Console na AWS, o usuário precisa de permissões específicas.	"Configurar permissões da AWS"	Fornecer permissões para um agente do Console

NetApp Backup and Recovery

Meta	Descrição	Link
Faça backup de clusters ONTAP locais no Amazon S3 com o NetApp Backup and Recovery	Ao ativar backups em seus volumes ONTAP , o NetApp Backup and Recovery solicita que você insira uma chave de acesso e um segredo para um usuário do IAM que tenha permissões específicas.	"Configurar permissões S3 para backups"

Cloud Volumes ONTAP

Meta	Descrição	Link
Fornecer permissões para nós Cloud Volumes ONTAP	Uma função do IAM deve ser anexada a cada nó do Cloud Volumes ONTAP na AWS. O mesmo vale para o mediador HA. A opção padrão é deixar o Console criar as funções do IAM para você, mas você pode usar as suas próprias ao criar o sistema no Console.	"Aprenda a configurar as funções do IAM você mesmo"

NetApp Copy and Sync

Meta	Descrição	Link
Implantar o data broker na AWS	A conta de usuário da AWS que você usa para implantar o agente de dados deve ter as permissões necessárias.	"Permissões necessárias para implantar o data broker na AWS"
Forneça permissões para o corretor de dados	Quando o NetApp Copy and Sync implanta o data broker, ele cria uma função do IAM para a instância do data broker. Você pode implantar o data broker usando sua própria função do IAM, se preferir.	"Requisitos para usar sua própria função do IAM com o AWS Data Broker"
Habilitar acesso à AWS para um data broker instalado manualmente	Se você usar o data broker com um relacionamento de sincronização que inclua um bucket S3, deverá preparar o host Linux para acesso à AWS. Ao instalar o data broker, você precisará fornecer chaves da AWS para um usuário do IAM que tenha acesso programático e permissões específicas.	"Habilitando o acesso à AWS"

FSx para ONTAP

Meta	Descrição	Link
Crie e gerencie FSx para ONTAP	Para criar ou gerenciar um sistema Amazon FSx for NetApp ONTAP , você precisa adicionar credenciais da AWS ao Console fornecendo o ARN de uma função do IAM que concede ao Console as permissões necessárias.	"Aprenda a configurar credenciais da AWS para FSx"

NetApp Cloud Tiering

Meta	Descrição	Link
Clusters ONTAP locais em camadas para o Amazon S3	Ao habilitar o NetApp Cloud Tiering para AWS, você insere uma chave de acesso e uma chave secreta. Essas credenciais são passadas para o cluster ONTAP para que o ONTAP possa organizar os dados em camadas no bucket S3.	"Configurar permissões S3 para camadas"

Permissões do Azure

O Console requer permissões do Azure para um agente do Console e para serviços individuais.

Agente de console

Meta	Descrição	Link
Implantar um agente do Console a partir do Console	Ao implantar um agente do Console a partir do Console, você precisa usar uma conta do Azure ou uma entidade de serviço que tenha permissões para implantar uma VM do agente do Console no Azure.	"Configurar permissões do Azure"
Fornecer permissões para um agente do Console	Quando o Console implanta uma VM de agente do Console no Azure, ele cria uma função personalizada que fornece as permissões necessárias para gerenciar recursos e processos dentro dessa assinatura do Azure. Você precisa configurar a função personalizada se iniciar um agente do Console no marketplace, se instalar manualmente um agente do Console ou se"adicionar mais credenciais do Azure a um agente do Console" . Mantenha a política atualizada, pois novas permissões serão adicionadas em versões posteriores.	"Permissões do Azure para um agente do Console"

NetApp Backup and Recovery

Meta	Descrição	Link
Fazer backup do Cloud Volumes ONTAP no armazenamento de blobs do Azure	Ao usar o NetApp Backup and Recovery para fazer backup do Cloud Volumes ONTAP, você precisa adicionar permissões a um agente do Console nos seguintes cenários: • Você deseja usar a funcionalidade "Pesquisar e Restaurar" • Você deseja usar chaves de criptografia gerenciadas pelo cliente (CMEK)	• "Faça backup dos dados do Cloud Volumes ONTAP no armazenamento de Blobs do Azure com Backup e Recuperação"
Fazer backup de clusters ONTAP locais no armazenamento de blobs do Azure	Ao usar o NetApp Backup and Recovery para fazer backup de clusters ONTAP locais, você precisa adicionar permissões a um agente do console para usar a funcionalidade "Pesquisar e Restaurar".	"Faça backup de dados ONTAP locais no armazenamento de Blobs do Azure com Backup e Recuperação"

Cópia e sincronização do NetApp

Meta	Descrição	Link
Implantar o data broker no Azure	A conta de usuário do Azure que você usa para implantar o data broker deve ter as permissões necessárias.	"Permissões necessárias para implantar o data broker no Azure"

Permissões do Google Cloud

O Console requer permissões do Google Cloud para um agente do Console e para serviços individuais.

Agentes de console

Meta	Descrição	Link
Implantar um agente do Console a partir do Console	O usuário do Google Cloud que implanta um agente do Console a partir do Console precisa de permissões específicas para implantar um agente do Console no Google Cloud.	"Configurar permissões para criar um agente do Console"
Fornecer permissões para um agente do Console	A conta de serviço de um agente do Console deve ter permissões específicas para as operações diárias. Você precisa associar a conta de serviço a um agente do Console durante a implantação. Mantenha a política atualizada, pois novas permissões serão adicionadas em versões posteriores.	"Configurar permissões para um agente do Console"

NetApp Backup and Recovery

Meta	Descrição	Link
Faça backup do Cloud Volumes ONTAP no Google Cloud	Ao usar o NetApp Backup and Recovery para fazer backup do Cloud Volumes ONTAP, você precisa adicionar permissões a um agente do Console nos seguintes cenários: • Você deseja usar a funcionalidade "Pesquisar e Restaurar" • Você deseja usar chaves de criptografia gerenciadas pelo cliente (CMEK)	• "Faça backup dos dados do Cloud Volumes ONTAP no Google Cloud Storage com Backup e Recuperação" • "Permissões para CMEKs"
Faça backup de clusters ONTAP locais no Google Cloud	Ao usar o NetApp Backup and Recovery para fazer backup de clusters ONTAP locais, você precisa adicionar permissões a um agente do console para usar a funcionalidade "Pesquisar e Restaurar".	"Faça backup de dados ONTAP locais no Google Cloud Storage com Backup e Recuperação"

NetApp Copy and Sync

Meta	Descrição	Link
Implantar o data broker no Google Cloud	Certifique-se de que o usuário do Google Cloud que implanta o data broker tenha as permissões necessárias.	"Permissões necessárias para implantar o data broker no Google Cloud"
Habilitar acesso ao Google Cloud para um corretor de dados instalado manualmente	Se você planeja usar o data broker com um relacionamento de sincronização que inclui um bucket do Google Cloud Storage, você deve preparar o host Linux para acesso ao Google Cloud. Ao instalar o data broker, você precisará fornecer uma chave para uma conta de serviço que tenha permissões específicas.	"Habilitando o acesso ao Google Cloud"

Permissões do StorageGRID

O Console requer permissões StorageGRID para dois serviços.

NetApp Backup and Recovery

Meta	Descrição	Link
Faça backup de clusters ONTAP locais no StorageGRID	Ao preparar o StorageGRID como um destino de backup para clusters ONTAP , o NetApp Backup and Recovery solicita que você insira uma chave de acesso e um segredo para um usuário do IAM que tenha permissões específicas.	"Prepare o StorageGRID como seu destino de backup"

NetApp Cloud Tiering

Meta	Descrição	Link
Camada de clusters ONTAP locais para StorageGRID	Ao configurar o NetApp Cloud Tiering para StorageGRID, você precisa fornecer ao Cloud Tiering uma chave de acesso S3 e uma chave secreta. O armazenamento em camadas na nuvem usa as chaves para acessar seus buckets.	"Preparar a hierarquização para StorageGRID"

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"

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: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: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: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: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

Classificação

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
- 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.

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:PararExecuçãoDeConsulta
- 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
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

Permissões do Azure e regras de segurança necessárias

Permissões do Azure para o agente do Console

Quando o NetApp Console inicia um agente de console no Azure, ele anexa uma função personalizada à VM que fornece ao agente permissões para gerenciar recursos e processos dentro dessa assinatura do Azure. O agente usa as permissões para fazer chamadas de API para vários serviços do Azure.

A necessidade ou não de criar essa função personalizada para o agente depende de como você a implantou.

Implantando do NetApp Console

Quando você usa o Console para implantar a máquina virtual do agente no Azure, ele habilita um "identidade gerenciada atribuída pelo sistema" na máquina virtual, cria uma função personalizada e a atribui à máquina virtual. A função fornece ao Console as permissões necessárias para gerenciar recursos e processos dentro dessa assinatura do Azure. As permissões da função são mantidas atualizadas quando o agente é atualizado. Você não precisa criar essa função para o agente ou gerenciar atualizações.

Implantação manual ou do Azure Marketplace

Ao implantar o agente do Azure Marketplace ou instalá-lo manualmente em um host Linux, você precisará configurar a função personalizada e manter suas permissões com quaisquer alterações.

Você precisará garantir que a função esteja atualizada à medida que novas permissões forem adicionadas em

versões subsequentes. Se novas permissões forem necessárias, elas serão listadas nas notas de versão.

- Para ver instruções passo a passo sobre como usar essas políticas, consulte as seguintes páginas:
  - "Configurar permissões para uma implantação do Azure Marketplace"
  - "Configurar permissões para implantações locais"
  - "Configurar permissões para o modo restrito"

```
{
  "Name": "Console 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.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",
    "Microsoft.Compute/virtualMachineScaleSets/write",
    "Microsoft.Compute/virtualMachineScaleSets/read",
    "Microsoft.Compute/virtualMachineScaleSets/delete"
  ],
  "NotActions": [],
  "AssignableScopes": [],
  "Description": "Console Permissions",
  "IsCustom": "true"
}
```

Como as permissões do Azure são usadas

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

Azure NetApp Files

O agente faz as seguintes solicitações de API quando você usa a NetApp Data Classification para verificar dados do Azure NetApp Files :

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

NetApp Backup and Recovery

As seções a seguir descrevem como as permissões são usadas para o NetApp Backup and Recovery.

Permissões mínimas de NetApp Backup and Recovery

O agente do Console faz as seguintes solicitações de API para funcionalidades básicas de NetApp Backup and Recovery :

- Microsoft.Storage/storageAccounts/listkeys/ação
- Microsoft.Storage/storageAccounts/leitura
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/ação
- Microsoft.Recursos/assinaturas/locais/leitura
- Microsoft.Recursos/assinaturas/grupos de recursos/leitura

- Microsoft.Recursos/assinaturas/grupos de recursos/recursos/leitura
- Microsoft.Recursos/assinaturas/grupos de recursos/gravação
- Microsoft.Storage/storageAccounts/managementPolicies/leitura
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Authorization/locks/write
- Microsoft.Authorization/locks/read

A seguir, apresentamos uma política personalizada para Backup e Recuperação que utiliza o mínimo de permissões possível e o escopo mais restrito possível:

```
{
  "id":
"/subscriptions/{subscriptionId}/providers/Microsoft.Authorization/roleDef
initions/{roleDefinitionGuid}",
  "properties": {
    "roleName": "Custom Role",
    "description": "Minimal permissions required for Backup and
Recovery.",
    "assignableScopes": [
      "/subscriptions/{subscriptionId}",

"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupNameContaini
ngConnectorAndStorageAccount}",

"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupNameContaini
ngConnectorAndStorageAccount}/providers/Microsoft.Storage/storageAccounts/
{storageAccountNameWithObjectLockPreprovisioned}"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Storage/storageAccounts/listkeys/action",
          "Microsoft.Storage/storageAccounts/read",
          "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",
          "Microsoft.Storage/storageAccounts/listAccountSas/action",
          "Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
          "Microsoft.Resources/subscriptions/resourceGroups/write",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Storage/storageAccounts/managementPolicies/read",
          "Microsoft.Storage/storageAccounts/managementPolicies/write",
          "Microsoft.Authorization/locks/write",
          "Microsoft.Authorization/locks/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

Permissões avançadas de backup e recuperação

O agente do console faz as seguintes solicitações de API para operações avançadas de backup e recuperação, bem como para recursos de busca e restauração. Essas permissões permitem o gerenciamento de redes, cofres de chaves e identidades gerenciadas:

- Microsoft.KeyVault/vaults/accessPolicies/gravação
- Microsoft.KeyVault/cofres/leitura
- Microsoft.ManagedIdentity/userAssignedIdentities/atribuir/ação
- Microsoft.Network/networkInterfaces/excluir
- Microsoft.Network/networkInterfaces/leitura
- Microsoft.Network/networkSecurityGroups/excluir
- Microsoft.Network/privateDnsZones/leitura
- Microsoft.Network/privateDnsZones/gravação
- Microsoft.Network/privateEndpoints/leitura
- Microsoft.Network/privateEndpoints/gravação
- Microsoft.Network/virtualNetworks/join/ação
- Microsoft.Recursos/implantações/excluir

Permissões legadas para backup e recuperação.

O agente realiza as seguintes solicitações de API quando você utiliza a funcionalidade de Busca e Restauração. Você só precisa dessas permissões se tiver habilitado os recursos de indexação legados antes do lançamento da versão 2 da indexação, em fevereiro de 2025:

- Microsoft.Synapse/espaços de trabalho/gravação
- Microsoft.Synapse/espaços de trabalho/leitura
- Microsoft.Synapse/espaços de trabalho/excluir
- Microsoft.Synapse/registro/ação
- Microsoft.Synapse/checkNameAvailability/ação
- Microsoft.Synapse/espaços de trabalho/status de operação/leitura
- Microsoft.Synapse/espaços de trabalho/regras de firewall/leitura
- Microsoft.Synapse/espaços de trabalho/replaceAllIpFirewallRules/ação
- Microsoft.Synapse/espaços de trabalho/resultadosdaoperação/leitura
- Microsoft.Synapse/workspaces/privateEndpointConnectionsAprovação/ação

NetApp Data Classification

O agente faz as seguintes solicitações de API quando você usa a Classificação de Dados.

Ação	Usado para configuração?	Usado para operações diárias?
Microsoft.Compute/locais/operações/leitura	Sim	Sim

Ação	Usado para configuração?	Usado para operações diárias?
Microsoft.Compute/locais/tamanhos de vm/leitura	Sim	Sim
Microsoft.Compute/operações/leitura	Sim	Sim
Microsoft.Compute/virtualMachines/instanceView/leitura	Sim	Sim
Microsoft.Compute/virtualMachines/powerOff/ação	Sim	Não
Microsoft.Compute/máquinas virtuais/leitura	Sim	Sim
Microsoft.Compute/virtualMachines/reiniciar/ação	Sim	Não
Microsoft.Compute/virtualMachines/iniciar/ação	Sim	Não
Microsoft.Compute/virtualMachines/vmSizes/leitura	Não	Sim
Microsoft.Compute/máquinasvirtuais/gravação	Sim	Não
Microsoft.Compute/imagens/leitura	Sim	Sim
Microsoft.Compute/discos/excluir	Sim	Não
Microsoft.Compute/discos/leitura	Sim	Sim
Microsoft.Compute/discos/gravação	Sim	Não
Microsoft.Storage/checknameavailability/leitura	Sim	Sim
Microsoft.Armazenamento/operações/leitura	Sim	Sim
Microsoft.Storage/storageAccounts/listkeys/ação	Sim	Não
Microsoft.Storage/storageAccounts/leitura	Sim	Sim
Microsoft.Storage/storageAccounts/write	Sim	Não
Microsoft.Storage/storageAccounts/blobServices/containers/read	Sim	Sim
Microsoft.Network/networkInterfaces/leitura	Sim	Sim
Microsoft.Network/networkInterfaces/escrever	Sim	Não
Microsoft.Network/networkInterfaces/join/ação	Sim	Não

Ação	Usado para configuração?	Usado para operações diárias?
Microsoft.Network/networkSecurity Groups/leitura	Sim	Sim
Microsoft.Network/networkSecurity Groups/gravação	Sim	Não
Microsoft.Recursos/assinaturas/locais/leitura	Sim	Sim
Microsoft.Network/locais/resultados daoperação/leitura	Sim	Sim
Microsoft.Network/locais/operações/leitura	Sim	Sim
Microsoft.Network/redes virtuais/leitura	Sim	Sim
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/ler	Sim	Sim
Microsoft.Network/virtualNetworks/sub-redes/leitura	Sim	Sim
Microsoft.Network/virtualNetworks/sub-redes/virtualMachines/leitura	Sim	Sim
Microsoft.Network/redes virtuais/máquinas virtuais/leitura	Sim	Sim
Microsoft.Network/virtualNetworks/sub-redes/juntar/ação	Sim	Não
Microsoft.Network/virtualNetworks/sub-redes/gravação	Sim	Não
Microsoft.Network/routeTables/join/ação	Sim	Não
Microsoft.Recursos/implantações/operações/leitura	Sim	Sim
Microsoft.Recursos/implantações/leitura	Sim	Sim
Microsoft.Recursos/implantações/gravação	Sim	Não
Microsoft.Recursos/recursos/leitura	Sim	Sim
Microsoft.Recursos/assinaturas/resultados da operação/leitura	Sim	Sim
Microsoft.Recursos/assinaturas/grupos de recursos/excluir	Sim	Não
Microsoft.Recursos/assinaturas/grupos de recursos/leitura	Sim	Sim

Ação	Usado para configuração?	Usado para operações diárias?
Microsoft.Recursos/assinaturas/grupos de recursos/recursos/leitura	Sim	Sim
Microsoft.Recursos/assinaturas/grupos de recursos/gravação	Sim	Não

Cloud Volumes ONTAP

O agente faz as seguintes solicitações de API para implantar e gerenciar o Cloud Volumes ONTAP no Azure.

Propósito	Ação	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
Criar e gerenciar VMs	Microsoft.Compute/locais/operações/leitura	Sim	Sim	Não
	Microsoft.Compute/locais/tamanhos de vm/leitura	Sim	Sim	Não
	Microsoft.Recursos/assinaturas/locais/leitura	Sim	Não	Não
	Microsoft.Compute/operações/leitura	Sim	Sim	Não
	Microsoft.Compute/virtualMachines/instanceView/leitura	Sim	Sim	Não
	Microsoft.Compute/virtualMachines/powerOff/ação	Sim	Sim	Não
	Microsoft.Compute/máquinas virtuais/leitura	Sim	Sim	Não
	Microsoft.Compute/virtualMachines/reiniciar/ação	Sim	Sim	Não
	Microsoft.Compute/virtualMachines/iniciar/ação	Sim	Sim	Não
	Microsoft.Compute/virtualMachines/deallocate/ação	Não	Sim	Sim
	Microsoft.Compute/virtualMachines/vmSizes/leitura	Não	Sim	Não
	Microsoft.Compute/máquinasvirtuais/gravação	Sim	Sim	Não
	Microsoft.Compute/máquinasvirtuais/excluir	Sim	Sim	Sim
	Microsoft.Recursos/implantações/excluir	Sim	Não	Não

Propósito	Ação	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
Habilitar implantação de um VHD	Microsoft.Compute/imagens/leitura	Sim	Não	Não
	Microsoft.Compute/imagens/gravação	Sim	Não	Não
Crie e gerencie interfaces de rede na sub-rede de destino	Microsoft.Network/networkInterfaces/leitura	Sim	Sim	Não
	Microsoft.Network/networkInterfaces/escrever	Sim	Sim	Não
	Microsoft.Network/networkInterfaces/join/ação	Sim	Sim	Não
	Microsoft.Network/networkInterfaces/excluir	Sim	Sim	Não
Criar e gerenciar grupos de segurança de rede	Microsoft.Network/networkSecurityGroups/leitura	Sim	Sim	Não
	Microsoft.Network/networkSecurityGroups/gravação	Sim	Sim	Não
	Microsoft.Network/networkSecurityGroups/join/ação	Sim	Não	Não
	Microsoft.Network/networkSecurityGroups/excluir	Não	Sim	Sim

Propósito	Ação	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
Obtenha informações de rede sobre regiões, a VNet de destino e a sub-rede e adicione as VMs às VNets	Microsoft.Network/locais/resultadosdaoperação/leitura	Sim	Sim	Não
	Microsoft.Network/locais/operações/leitura	Sim	Sim	Não
	Microsoft.Network/redes virtuais/leitura	Sim	Não	Não
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/ler	Sim	Não	Não
	Microsoft.Network/virtualNetworks/sub-redes/leitura	Sim	Sim	Não
	Microsoft.Network/virtualNetworks/sub-redes/virtualMachines/leitura	Sim	Sim	Não
	Microsoft.Network/redes virtuais/máquinas virtuais/leitura	Sim	Sim	Não
	Microsoft.Network/virtualNetworks/sub-redes/juntar/ação	Sim	Sim	Não

Propósito	Ação	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
Criar e gerenciar grupos de recursos	Microsoft.Recursos/implantações/operações/leitura	Sim	Sim	Não
	Microsoft.Recursos/implantações/leitura	Sim	Sim	Não
	Microsoft.Recursos/implantações/gravação	Sim	Sim	Não
	Microsoft.Recursos/recursos/leitura	Sim	Sim	Não
	Microsoft.Recursos/assinaturas/resultados da operação/leitura	Sim	Sim	Não
	Microsoft.Recursos/assinaturas/grupos de recursos/excluir	Sim	Sim	Sim
	Microsoft.Recursos/assinaturas/grupos de recursos/leitura	Não	Sim	Não
	Microsoft.Recursos/assinaturas/grupos de recursos/recursos/leitura	Sim	Sim	Não
	Microsoft.Recursos/assinaturas/grupos de recursos/gravação	Sim	Sim	Não

Propósito	Ação	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
Gerenciar contas e discos de armazenamento do Azure	Microsoft.Compute/discos/leitura	Sim	Sim	Sim
	Microsoft.Compute/discos/gravação	Sim	Sim	Não
	Microsoft.Compute/discos/excluir	Sim	Sim	Sim
	Microsoft.Storage/checknameavailability/leitura	Sim	Sim	Não
	Microsoft.Armazenamento/operações/leitura	Sim	Sim	Não
	Microsoft.Storage/storageAccounts/listkeys/ação	Sim	Sim	Não
	Microsoft.Storage/storageAccounts/leitura	Sim	Sim	Não
	Microsoft.Storage/storageAccounts/delete	Não	Sim	Sim
	Microsoft.Storage/storageAccounts/write	Sim	Sim	Não
	Microsoft.Storage/usos/leitura	Não	Sim	Não
Habilitar backups para armazenamento de Blobs e criptografia de contas de armazenamento	Microsoft.Storage/storageAccounts/blobServices/containers/read	Sim	Sim	Não
	Microsoft.KeyVault/cofres/leitura	Sim	Sim	Não
	Microsoft.KeyVault/vaults/accessPolicies/gravação	Sim	Sim	Não
Habilitar pontos de extremidade de serviço VNet para camadas de dados	Microsoft.Network/virtualNetworks/sub-redes/gravação	Sim	Sim	Não
	Microsoft.Network/routeTables/join/ação	Sim	Sim	Não

Propósito	Ação	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
Criar e gerenciar snapshots gerenciados do Azure	Microsoft.Compute/instantâneos/gravação	Sim	Sim	Não
	Microsoft.Compute/instantâneos/leitura	Sim	Sim	Não
	Microsoft.Compute/instantâneos/excluir	Não	Sim	Sim
	Microsoft.Compute/discos/beginGetAccess/ação	Não	Sim	Não
Criar e gerenciar conjuntos de disponibilidade	Microsoft.Compute/availabilitySets/gravação	Sim	Não	Não
	Microsoft.Compute/availabilitySets/leitura	Sim	Não	Não
Habilitar implantações programáticas do marketplace	Microsoft.MarketplaceOrdering/tipos de oferta/editores/ofertas/planos/acordos/leitura	Sim	Não	Não
	Microsoft.MarketplaceOrdering/tipos de oferta/editores/ofertas/planos/acordos/escrever	Sim	Sim	Não

Propósito	Ação	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
Gerenciar um balanceador de carga para pares HA	Microsoft.Network/loadBalancers/leitura	Sim	Sim	Não
	Microsoft.Network/loadBalancers/gravação	Sim	Não	Não
	Microsoft.Network/loadBalancers/excluir	Não	Sim	Sim
	Microsoft.Network/loadBalancers/backendAddressPools/leitura	Sim	Não	Não
	Microsoft.Network/loadBalancers/backendAddressPools/junção/ação	Sim	Não	Não
	Microsoft.Network/loadBalancers/frontendIPConfigurations/leitura	Sim	Sim	Não
	Microsoft.Network/loadBalancers/regras de balanceamento de carga/leitura	Sim	Não	Não
	Microsoft.Network/loadBalancers/sondas/leitura	Sim	Não	Não
	Microsoft.Network/loadBalancers/probes/join/action	Sim	Não	Não
Habilitar o gerenciamento de bloqueios em discos do Azure	Microsoft.Autorização/bloqueios/*	Sim	Sim	Não

Propósito	Ação	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
Habilitar endpoints privados para pares HA quando não houver conectividade fora da sub-rede	Microsoft.Network/privateEndpoints/gravação	Sim	Sim	Não
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsAprovação/ação	Sim	Não	Não
	Microsoft.Storage/storageAccounts/privateEndpointConnections/leitura	Sim	Sim	Sim
	Microsoft.Network/privateEndpoints/leitura	Sim	Sim	Sim
	Microsoft.Network/privateDnsZones/gravação	Sim	Sim	Não
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/gravação	Sim	Sim	Não
	Microsoft.Network/virtualNetworks/join/ação	Sim	Sim	Não
	Microsoft.Network/privateDnsZones/A/gravação	Sim	Sim	Não
	Microsoft.Network/privateDnsZones/leitura	Sim	Sim	Não
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/leitura	Sim	Sim	Não
Necessário para algumas implantações de VM, dependendo do hardware físico subjacente	Microsoft.Recursos/implantações/Status de operação/leitura	Sim	Sim	Não

Propósito	Ação	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
Remover recursos de um grupo de recursos em caso de falha de implantação ou exclusão	Microsoft.Network/privateEndpoints/excluir	Sim	Sim	Não
	Microsoft.Compute/availabilitySets/excluir	Sim	Sim	Não
Habilitar o uso de chaves de criptografia gerenciadas pelo cliente ao usar a API	Microsoft.Compute/diskEncryptionSets/leitura	Sim	Sim	Sim
	Microsoft.Compute/diskEncryptionSets/gravação	Sim	Sim	Não
	Microsoft.KeyVault/cofres/implantar/ação	Sim	Não	Não
	Microsoft.Compute/diskEncryptionSets/excluir	Sim	Sim	Sim
Configurar um grupo de segurança de aplicativo para um par de HA para isolar a interconexão de HA e as NICs de rede do cluster	Microsoft.Network/applicationSecurityGroups/gravação	Não	Sim	Não
	Microsoft.Network/applicationSecurityGroups/leitura	Não	Sim	Não
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/ação	Não	Sim	Não
	Microsoft.Network/networkSecurityGroups/securityRules/write	Sim	Sim	Não
	Microsoft.Network/applicationSecurityGroups/excluir	Não	Sim	Sim
	Microsoft.Network/networkSecurityGroups/securityRules/excluir	Não	Sim	Sim
Ler, escrever e excluir tags associadas aos recursos do Cloud Volumes ONTAP	Microsoft.Recursos/tags/leitura	Não	Sim	Não
	Microsoft.Recursos/tags/gravação	Sim	Sim	Não
	Microsoft.Recursos/tags/excluir	Sim	Não	Não

Propósito	Ação	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
Criptografar contas de armazenamento durante a criação	Microsoft.ManagedIdentity/userAssignedIdentities/atribuir/ação	Sim	Sim	Não
Use conjuntos de dimensionamento de máquina virtual no modo de orquestração flexível para especificar zonas específicas para o Cloud Volumes ONTAP	Microsoft.Compute/virtualMachineScaleSets/gravação	Sim	Não	Não
	Microsoft.Compute/virtualMachineScaleSets/leitura	Sim	Não	Não
	Microsoft.Compute/virtualMachineScaleSets/excluir	Não	Não	Sim

Hierarquização

O agente faz as seguintes solicitações de API quando você configura o NetApp Cloud Tiering.

- Microsoft.Storage/storageAccounts/listkeys/ação
- Microsoft.Recursos/assinaturas/grupos de recursos/leitura
- Microsoft.Recursos/assinaturas/locais/leitura

O agente do Console faz as seguintes solicitações de API para operações diárias.

- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/managementPolicies/leitura
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Storage/storageAccounts/leitura

Registro de alterações

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

11 de novembro de 2025

Foi adicionada uma política JSON personalizada que reflete o mínimo de permissões possível e o escopo mais restrito possível.

As seguintes permissões foram adicionadas à lista mínima de permissões de backup e recuperação:

- Microsoft.Authorization/locks/write
- Microsoft.Authorization/locks/read

As seguintes permissões não são mais necessárias para Backup e Recuperação, a menos que você esteja usando a indexação legada:

- Microsoft.Synapse/espaços de trabalho/gravação

- Microsoft.Synapse/espaços de trabalho/leitura
- Microsoft.Synapse/espaços de trabalho/excluir
- Microsoft.Synapse/registro/ação
- Microsoft.Synapse/checkNameAvailability/ação
- Microsoft.Synapse/espaços de trabalho/status de operação/leitura
- Microsoft.Synapse/espaços de trabalho/regras de firewall/leitura
- Microsoft.Synapse/espaços de trabalho/replaceAllIpFirewallRules/ação
- Microsoft.Synapse/espaços de trabalho/resultadosdaoperação/leitura
- Microsoft.Synapse/workspaces/privateEndpointConnectionsAprovação/ação

As seguintes permissões foram movidas para a seção "Permissões adicionais de backup e recuperação" porque não são necessárias para uma configuração mínima:

- Microsoft.Storage/storageAccounts/listkeys/ação
- Microsoft.Storage/storageAccounts/leitura
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/ação
- Microsoft.Recursos/assinaturas/locais/leitura
- Microsoft.Recursos/assinaturas/grupos de recursos/leitura
- Microsoft.Recursos/assinaturas/grupos de recursos/recursos/leitura
- Microsoft.Recursos/assinaturas/grupos de recursos/gravação
- Microsoft.Storage/storageAccounts/managementPolicies/leitura
- Microsoft.Storage/storageAccounts/managementPolicies/write

9 de setembro de 2024

As seguintes permissões foram removidas da política JSON porque o Console não oferece mais suporte à descoberta e ao gerenciamento de clusters do Kubernetes:

- Microsoft.ContainerService/managedClusters/listClusterUserCredential/ação
- Microsoft.ContainerService/gerenciadosClusters/leitura

22 de agosto de 2024

As seguintes permissões foram adicionadas à política JSON porque são necessárias para o suporte do Cloud Volumes ONTAP aos conjuntos de dimensionamento de máquinas virtuais:

- Microsoft.Compute/virtualMachineScaleSets/gravação
- Microsoft.Compute/virtualMachineScaleSets/leitura
- Microsoft.Compute/virtualMachineScaleSets/excluir

5 de dezembro de 2023

As seguintes permissões não são mais necessárias para o NetApp Backup and Recovery ao fazer backup de dados de volume no armazenamento de Blobs do Azure:

- Microsoft.Compute/máquinas virtuais/leitura
- Microsoft.Compute/virtualMachines/iniciar/ação
- Microsoft.Compute/virtualMachines/deallocate/ação
- Microsoft.Compute/virtualMachines/extensões/excluir
- Microsoft.Compute/máquinasvirtuais/excluir

Essas permissões são necessárias para outros serviços de armazenamento do Console, portanto, elas permanecerão na função personalizada do agente se você estiver usando esses outros serviços de armazenamento.

12 de maio de 2023

As seguintes permissões foram adicionadas à política JSON porque são necessárias para o gerenciamento do Cloud Volumes ONTAP :

- Microsoft.Compute/imagens/gravação
- Microsoft.Network/loadBalancers/frontendIPConfigurations/leitura

As seguintes permissões foram removidas da política JSON porque não são mais necessárias:

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

23 de março de 2023

A permissão "Microsoft.Storage/storageAccounts/delete" não é mais necessária para a Classificação de Dados.

Essa permissão ainda é necessária para o Cloud Volumes ONTAP.

5 de janeiro de 2023

As seguintes permissões foram adicionadas à política JSON:

- Microsoft.Storage/storageAccounts/listAccountSas/ação
- Microsoft.Synapse/workspaces/privateEndpointConnectionsAprovação/ação

  Essas permissões são necessárias para o NetApp Backup and Recovery.

- Microsoft.Network/loadBalancers/backendAddressPools/junção/ação

  Essa permissão é necessária para a implantação do Cloud Volumes ONTAP .

Regras de grupo de segurança do agente de console no Azure

O grupo de segurança do Azure 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. Para outras opções de instalação, você precisa configurar esse grupo de segurança manualmente.

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 dos navegadores da Web do cliente à interface do usuário local e conexões da instância de NetApp Data Classification
TCP	3128	Fornece ao Cloud Volumes ONTAP acesso à Internet para enviar mensagens do AutoSupport ao Suporte da NetApp . Você deve abrir esta porta manualmente após a implantação. "Aprenda como o agente é usado como proxy para mensagens do AutoSupport"

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
Todos os UDP	Todos	Todo o tráfego de saída

Regras avançadas de saída

Se precisar de regras rígidas para o tráfego de saída, você pode 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 o Azure, para o ONTAP, para a NetApp Data Classification e envio de mensagens de AutoSupport para o NetApp
Chamadas de API	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

Permissões do Google Cloud e regras de firewall necessárias

Permissões do Google Cloud para o agente do Console

O agente do Console requer permissões para executar ações no Google Cloud. Essas permissões estão incluídas em uma função personalizada fornecida pela NetApp. Você deve entender o que o agente faz com essas permissões.

Permissões da conta de usuário do Google Cloud

A função personalizada abaixo concede a um usuário do Google Cloud as permissões necessárias para implantar um agente. Atribua essa função personalizada ao usuário que irá implantar o agente.

Exibir permissões da conta de usuário do Google Cloud

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- 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.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
```

```
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- 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
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

Permissões de conta de serviço

A função personalizada abaixo concede à conta de serviço do Google Cloud associada ao agente do Console as permissões necessárias para gerenciar recursos e processos em sua rede do Google Cloud.

Aplique essa função personalizada a uma conta de serviço associada à VM do agente do Console.

- "Configurar permissões do Google Cloud para o modo padrão"
- "Configurar permissões para o modo restrito"

Exibir permissões da conta de serviço do Google

Certifique-se de que a função esteja atualizada, pois novas permissões são adicionadas ou removidas em versões subsequentes. O registro de alterações lista todas as novas permissões necessárias."Consulte o registro de alterações de permissões do Google." "Veja como adicionar contas de serviço do Google Cloud."

```
title: NetApp Console agent
description: Permissions for the service account associated with the
Console agent.
stage: GA
includedPermissions:
- cloudbuild.builds.get
- cloudbuild.connections.list
- cloudbuild.repositories.accessReadToken
- cloudbuild.repositories.list
- cloudquotas.quotas.get
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
- config.artifacts.import
- config.deployments.create
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getLock
- config.deployments.getState
- config.deployments.update
- config.deployments.updateState
- config.previews.upload
- config.revisions.get
- config.revisions.getState
- config.deployments.getLock
- config.deployments.list
- config.deployments.lock
- config.operations.get
- config.previews.get
- config.previews.list
- config.resources.list
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.regionBackendServices.update
- compute.networks.updatePolicy
```

```
- compute.addresses.createInternal
- compute.addresses.deleteInternal
- compute.addresses.list
- compute.addresses.setLabels
- compute.addresses.useInternal
- compute.backendServices.create
- 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.forwardingRules.create
- compute.forwardingRules.delete
- compute.forwardingRules.get
- compute.forwardingRules.setLabels
- compute.globalOperations.get
- compute.healthChecks.create
- compute.healthChecks.delete
- compute.healthChecks.get
- compute.healthChecks.useReadOnly
- 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.instances.use
- compute.instanceGroups.create
- compute.instanceGroups.delete
- compute.instanceGroups.get
- compute.instanceGroups.update
- compute.instanceGroups.use
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.instances.setMinCpuPlatform
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.regionBackendServices.delete
- compute.regionBackendServices.use
- compute.resourcePolicies.create
- compute.resourcePolicies.delete
- compute.resourcePolicies.get
- 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
- logging.logEntries.create
- logging.logEntries.route
- monitoring.timeSeries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- storage.objects.create
- storage.objects.delete
- storage.objects.list
- storage.objects.update
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.get
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.objects.get
- storage.objects.list
- storage.buckets.getIamPolicy
```

Como as permissões do Google Cloud são usadas

O agente do Console usa as permissões na função personalizada para gerenciar recursos do Cloud Volumes ONTAP e processos de serviços de dados da NetApp em sua rede do Google Cloud. As seções a seguir descrevem como o agente utiliza essas permissões.

Permissões usadas para o Cloud Volumes ONTAP

O agente do Console usa as permissões da função personalizada para gerenciar recursos e processos do Cloud Volumes ONTAP na sua rede do Google Cloud. As seções a seguir descrevem como o agente utiliza essas permissões.

Permissões para Cloud Volumes ONTAP

Ações	Propósito	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
config.deployments.create	Para implantar a instância da máquina virtual Cloud Volumes ONTAP usando o Google Cloud Infrastructure Manager.	Sim	Não	Não
config.deployments.delete		Não	Não	Sim
config.deployments.deleteState		Não	Não	Sim
config.deployments.get		Não	Sim	Não
config.deployments.getLock		Não	Sim	Não
config.deployments.getState		Não	Sim	Não
config.deployments.list		Não	Sim	Não
config.deployments.lock		Não	Sim	Não
config.deployments.update		Não	Sim	Não
config.deployments.updateState		Não	Sim	Não
config.operações.obter		Não	Sim	Não
config.previews.get		Não	Sim	Não
config.previews.list		Não	Sim	Não
lista de recursos de configuração		Não	Sim	Não
config.revisions.get		Não	Sim	Não

Ações	Propósito	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
compute.disks.create	Para criar e gerenciar discos para Cloud Volumes ONTAP.	Sim	Sim	Não
compute.disks.createSnapshot		Não	Sim	Não
compute.disks.delete		Não	Sim	Sim
compute.disks.get		Não	Sim	Não
lista de discos de computação		Sim	Sim	Não
compute.disks.setLabels		Sim	Sim	Não
usar discos de computação		Não	Sim	Não
compute.firewalls.create	Para criar regras de firewall para o Cloud Volumes ONTAP.	Sim	Não	Não
compute.firewalls.delete		Não	Sim	Sim
compute.firewalls.get		Sim	Sim	Não
lista de firewalls de computação		Sim	Sim	Não
compute.forwardingRules.create	Crie regras de encaminhamento para o roteamento de tráfego para serviços de backend.	Não	Sim	Não
compute.forwardingRules.delete	Exclua as regras de encaminhamento existentes.	Não	Sim	Não
compute.forwardingRules.get	Recupere detalhes sobre as regras de encaminhamento existentes.	Não	Sim	Não
compute.forwardingRules.setLabels	Defina ou atualize os rótulos nas regras de encaminhamento da organização.	Não	Sim	Não
compute.globalOperations.get	Para obter o status das operações.	Sim	Sim	Não

Ações	Propósito	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
compute.healthChecks.create	Criar e gerenciar verificações de integridade para monitorar a saúde do serviço de backend.	Não	Sim	Não
compute.healthChecks.delete		Não	Sim	Não
compute.healthChecks.get		Não	Sim	Não
compute.healthChecks.useReadOnly		Não	Sim	Não
compute.images.get	Para obter imagens para instâncias de VM.	Sim	Não	Não
compute.images.getFromFamily		Sim	Não	Não
calcular.imagens.lista		Sim	Não	Não
compute.images.useReadOnly		Sim	Não	Não
compute.instances.attachDisk	Para anexar e desanexar discos ao Cloud Volumes ONTAP.	Sim	Sim	Não
compute.instances.detachDisk		Não	Sim	Sim
compute.instances.create	Para criar e excluir instâncias de VM do Cloud Volumes ONTAP .	Sim	Não	Não
compute.instances.delete		Não	Não	Sim
compute.instances.get	Para listar instâncias de VM.	Sim	Sim	Não
compute.instances.getSerialPortOutput	Para obter logs do console.	Sim	Sim	Não
lista de instâncias de computação	Para recuperar a lista de instâncias em uma zona.	Sim	Sim	Não
compute.instances.setDeletionProtection	Para definir a proteção contra exclusão na instância.	Sim	Não	Não
compute.instances.setLabels	Para adicionar rótulos.	Sim	Não	Não

Ações	Propósito	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
compute.instances.setMachineType	Para alterar o tipo de máquina do Cloud Volumes ONTAP.	Sim	Sim	Não
compute.instances.setMinCpuPlatform		Sim	Sim	Não
compute.instances.setMetadata	Para adicionar metadados.	Sim	Sim	Não
compute.instances.setTags	Para adicionar tags para regras de firewall.	Sim	Sim	Não
compute.instances.start	Para iniciar e parar o Cloud Volumes ONTAP.	Sim	Sim	Não
compute.instances.stop		Sim	Sim	Não
compute.instances.updateDisplayDevice		Sim	Sim	Não
instâncias de computação.	Utilizar instâncias de máquinas virtuais (operações de iniciar, parar e conectar).	Não	Sim	Não
compute.machineTypes.get	Para obter o número de núcleos e verificar as quotas.	Sim	Não	Não
compute.projects.get	Para dar suporte a multiprojetos.	Sim	Não	Não
compute.resourcePolicies.create	Crie e gerencie políticas de recursos para gerenciamento automatizado de recursos.	Não	Sim	Não
compute.resourcePolicies.delete		Não	Sim	Não
compute.resourcePolicies.get		Não	Sim	Não

Ações	Propósito	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
compute.snapshots.create	Para criar e gerenciar instantâneos de disco persistentes.	Sim	Sim	Não
compute.snapshots.delete		Não	Sim	Sim
compute.snapshots.get		Não	Sim	Não
compute.snapshots.list		Não	Sim	Não
compute.snapshots.setLabels		Sim	Sim	Não
compute.networks.get	Para obter as informações de rede necessárias para criar uma nova instância de máquina virtual do Cloud Volumes ONTAP .	Sim	Sim	Não
lista de redes computacionais		Sim	Sim	Não
compute.regions.get		Sim	Sim	Não
lista de regiões de computação		Sim	Sim	Não
compute.subnetworks.get		Sim	Sim	Não
lista de sub-redes de computação		Sim	Sim	Não
compute.zoneOperations.get		Sim	Sim	Não
compute.zones.get		Sim	Sim	Não
lista de zonas de computação		Sim	Sim	Não

Ações	Propósito	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
deploymentmanager.compositeTypes.get	Para implantar a instância da máquina virtual do Cloud Volumes ONTAP usando o Google Cloud Deployment Manager.	Sim	Não	Não
deploymentmanager.compositeTypes.list		Sim	Não	Não
deploymentmanager.deployments.create		Sim	Não	Não
deploymentmanager.deployments.delete		Sim	Não	Não
deploymentmanager.deployments.get		Sim	Não	Não
deploymentmanager.deployments.list		Sim	Não	Não
deploymentmanager.manifests.get		Sim	Não	Não
deploymentmanager.manifests.list		Sim	Não	Não
deploymentmanager.operations.get		Sim	Não	Não
lista de operações do gerenciador de implantação		Sim	Não	Não
deploymentmanager.resources.get		Sim	Não	Não
lista de recursos do gerenciador de implantação		Sim	Não	Não
deploymentmanager.typeProviders.get		Sim	Não	Não
deploymentmanager.typeProviders.list		Sim	Não	Não
deploymentmanager.types.get		Sim	Não	Não
lista de tipos do gerenciador de implantação		Sim	Não	Não

Ações	Propósito	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
logging.logEntries.list	Para obter unidades de log de pilha.	Sim	Sim	Não
logging.privateLogEntries.list		Sim	Sim	Não
logging.logEntries.create	Criar e encaminhar entradas de log para monitoramento, depuração e auditoria.	Sim	Sim	Não
logging.logEntries.route		Sim	Sim	Não
resourcemanager.projects.get	Para dar suporte a multiprojetos.	Sim	Sim	Não
armazenamento.buckets.create	Para criar e gerenciar um bucket do Google Cloud Storage para hierarquização de dados.	Sim	Sim	Não
storage.buckets.delete		Não	Sim	Sim
storage.buckets.get		Não	Sim	Não
lista de buckets de armazenamento		Não	Sim	Não
armazenamento.buckets.atualizar		Não	Sim	Não
cloudkms.cryptoKeyVersions.useToEncrypt	Para usar chaves de criptografia gerenciadas pelo cliente do Cloud Key Management Service com o Cloud Volumes ONTAP.	Sim	Sim	Não
cloudkms.cryptoKeys.get		Sim	Sim	Não
cloudkms.cryptoKeys.lista		Sim	Sim	Não
cloudkms.keyRings.lista		Sim	Sim	Não
cloudbuild.builds.get		Sim	Não	Não

Ações	Propósito	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
compute.instances.setServiceAccount	Para definir uma conta de serviço na instância do Cloud Volumes ONTAP . Esta conta de serviço fornece permissões para hierarquização de dados para um bucket do Google Cloud Storage.	Sim	Sim	Não
iam.serviceAccounts.actAs		Sim	Não	Não
iam.serviceAccounts.create		Sim	Não	Não
iam.serviceAccounts.getIamPolicy		Sim	Sim	Não
iam.serviceAccounts.list		Sim	Sim	Não
iam.serviceAccountKeys.create		Sim	Não	Não
armazenamento.objetos.criar	Crie e gerencie objetos (arquivos) em um bucket do Google Cloud Storage.	Sim	Sim	Não
storage.objects.delete		Não	Não	Sim
armazenamento.objetos.obter		Sim	Sim	Não
lista de objetos de armazenamento		Sim	Sim	Não
lista de endereços de computação	Para recuperar os endereços em uma região ao implantar um par HA.	Sim	Não	Não
compute.addresses.createInternal	Criar endereços IP internos dentro da rede VPC para alocação de recursos.	Não	Sim	Não
compute.addresses.deleteInternal	Exclua endereços IP internos para limpeza de recursos.	Não	Sim	Não
compute.addresses.setLabels	Atualizar rótulos no recurso Endereço.	Não	Sim	Não
compute.addresses.useInternal	Utilize endereços IP internos para comunicação em rede.	Não	Sim	Não

Ações	Propósito	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
compute.backendServices.create	Para configurar um serviço de backend para distribuir tráfego em um par HA.	Sim	Não	Não
compute.regionBackendServices.create	Criar e gerenciar serviços de backend para roteamento de tráfego.	Sim	Não	Não
compute.regionBackendServices.delete		Não	Sim	Não
compute.regionBackendServices.get		Sim	Não	Não
compute.regionBackendServices.update		Sim	Sim	Não
compute.regionBackendServices.list		Sim	Não	Não
compute.regionBackendServices.use		Não	Sim	Não
compute.networks.updatePolicy	Para aplicar regras de firewall nas VPCs e sub-redes para um par HA.	Sim	Não	Não
compute.instanceGroups.get	Para criar e gerenciar VMs de armazenamento em pares Cloud Volumes ONTAP HA.	Sim	Sim	Não
compute.addresses.get		Sim	Sim	Não
computar.instâncias.atualizarInterfaceDeRede		Sim	Sim	Não
compute.instanceGroups.create		Não	Sim	Não
compute.instanceGroups.delete		Não	Sim	Não
compute.instanceGroups.update		Não	Sim	Não
compute.instanceGroups.use		Não	Sim	Não

Ações	Propósito	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
monitoramento.séries.temporais.lista	Para descobrir informações sobre os buckets do Google Cloud Storage.	Sim	Sim	Não
storage.buckets.getIamPolicy		Sim	Sim	Não

Permissões usadas para o NetApp Backup and Recovery

O agente do Console usa as permissões da função personalizada para gerenciar os recursos e processos do NetApp Backup and Recovery em sua rede do Google Cloud. As seções a seguir descrevem como o agente utiliza essas permissões.

Exibir permissões para o NetApp Backup and Recovery.

Ações	Propósito	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
• cloudkms.cryptoKeys.get • cloudkms.cryptoKeys.getIamPolicy • cloudkms.cryptoKeys.lista • cloudkms.cryptoKeys.setIamPolicy • cloudkms.keyRings.obter • cloudkms.keyRings.getIamPolicy • cloudkms.keyRings.lista • cloudkms.keyRings.setIamPolicy	Para selecionar suas próprias chaves gerenciadas pelo cliente no assistente de ativação do NetApp Backup and Recovery em vez de usar as chaves de criptografia padrão gerenciadas pelo Google.	Sim	Sim	Não

Permissões usadas para a NetApp Data Classification

O agente do Console usa as permissões da função personalizada para gerenciar os recursos e processos do NetApp Data Classification na sua rede do Google Cloud. As seções a seguir descrevem como o agente utiliza essas permissões.

Exibir permissões para NetApp Data Classification

Ações	Propósito	Usado para implantação?	Usado para operações diárias?	Usado para exclusão?
• compute.subnetworks.use • compute.subnetworks.useExternalIp • compute.instances.addAccessConfig	Para habilitar a NetApp Data Classification.	Sim	Não	Não

Registro de alterações

As permissões adicionadas e removidas estão indicadas abaixo.

08 de dezembro de 2025

A NetApp está migrando do Google Cloud Deployment Manager para o Google Cloud Infrastructure Manager (IM) para implantar e executar o agente do Console no Google Cloud. As seguintes permissões foram adicionadas para dar suporte a essa alteração.

As seguintes permissões adicionais são necessárias para o usuário do Google Cloud que implanta o agente:

- armazenamento.buckets.create
- storage.buckets.get
- armazenamento.objetos.criar
- armazenamento.pastas.criar
- lista de objetos de armazenamento
- iam.serviceAccount.actAs
- config.deployments.create
- config.operações.obter

As seguintes permissões adicionais são necessárias para a conta de serviço no Google Cloud usada para as operações diárias:

- lista de conexões do cloudbuild
- cloudbuild.repositories.accessReadToken
- lista de repositórios cloudbuild.
- cotas.cotas.obter
- config.artefatos.importar

- config.deployments.deleteState
- config.deployments.getLock
- config.deployments.getState
- config.deployments.updateState
- config.previews.upload
- config.revisions.getState
- logging.logEntries.create
- armazenamento.objetos.criar
- storage.objects.delete
- armazenamento.objetos.atualizar
- iam.serviceAccounts.get

As seguintes permissões adicionais são necessárias para implantar o Cloud Volumes ONTAP:

- cloudbuild.builds.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- lista de recursos de configuração
- iam.serviceAccountKeys.create
- iam.serviceAccounts.create

As seguintes permissões adicionais são necessárias para a conta de serviço usada nas operações diárias do Cloud Volumes ONTAP.

- compute.addresses.createInternal
- compute.addresses.deleteInternal
- compute.addresses.setLabels
- compute.addresses.useInternal
- compute.forwardingRules.create
- compute.forwardingRules.delete
- compute.forwardingRules.get
- compute.forwardingRules.setLabels

- compute.healthChecks.create
- compute.healthChecks.delete
- compute.healthChecks.get
- compute.healthChecks.useReadOnly
- compute.instanceGroups.create
- compute.instanceGroups.delete
- compute.instanceGroups.update
- compute.instanceGroups.use
- instâncias de computação.
- compute.regionBackendServices.delete
- compute.regionBackendServices.update
- compute.regionBackendServices.use
- compute.resourcePolicies.create
- compute.resourcePolicies.delete
- compute.resourcePolicies.get
- logging.logEntries.route
- config.deployments.create
- config.deployments.delete
- config.deployments.get
- config.deployments.update
- config.revisions.get
- config.deployments.lock
- config.operações.obter

26 de novembro de 2025

As permissões foram atualizadas para maior clareza sobre seu uso, mas nenhuma permissão foi adicionada ou removida. Foram adicionadas três colunas para indicar se cada permissão é usada para implantação, operações diárias ou exclusão. Além disso, algumas permissões são segregadas com base em seu uso para NetApp Data Classification e NetApp Backup and Recovery.

06 de fevereiro de 2023

A seguinte permissão foi adicionada a esta política:

- computar.instâncias.atualizarInterface de Rede

Esta permissão é necessária para o Cloud Volumes ONTAP.

2023-01-27

As seguintes permissões foram adicionadas a esta política:

- cloudkms.cryptoKeys.getIamPolicy

- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.obter
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

Essas permissões são necessárias para o NetApp Backup and Recovery.

Regras de firewall do agente no Google Cloud

As regras de firewall do Google Cloud para o agente exigem 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. Para outras opções de instalação, você precisa configurar esse grupo de segurança manualmente.

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 dos navegadores da web do cliente para a interface do usuário local
TCP	3128	Fornece Cloud Volumes ONTAP com acesso à internet. Você deve abrir esta porta manualmente após a implantação.

Regras de saída

As regras de firewall predefinidas do agente abrem todo o tráfego de saída. Siga as regras básicas de saída, se aceitáveis, ou use regras avançadas de saída para requisitos mais rigorosos.

Regras básicas de saída

As regras de firewall predefinidas para o agente incluem as seguintes regras de saída.

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

Regras avançadas de saída

Se precisar de regras rígidas para o tráfego de saída, você pode 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 o Google Cloud, para o ONTAP, para a NetApp Data Classification e envio de mensagens de AutoSupport para a NetApp
Chamadas de API	TCP	8080	Classificação de Dados	Sondar a instância de classificação de dados durante a implantação
DNS	UDP	53	DNS	Usado para resolução de DNS por classificação de dados

Acesso de rede necessário para 3.9.55 e abaixo

O NetApp Console, o agente do NetApp Console e os serviços de dados do NetApp exigem acesso de saída à Internet para contatar os endpoints necessários.

Este tópico documenta o acesso à rede necessário para versões do modo padrão do NetApp Console 3.9.55 e anteriores. Para os endpoints necessários para 4.0.0 e superior, revise"os endpoints necessários para 4.0.0 e superior" .

Você precisa configurar o acesso à rede para o seguinte:

- Computadores que acessam o NetApp Console como software como serviço (SaaS)
- Agentes de console que você instala no local ou na nuvem.

Atualize sua lista de endpoints para a lista revisada para 4.0.0 e superior

A partir da versão 4.0.0, os agentes do Console exigem menos endpoints. Implantações existentes anteriores à versão 4.0.0 continuam com suporte. Após atualizar para a versão 4.0.0 ou posterior, você pode remover os endpoints antigos da sua lista de permissões quando for conveniente.

A NetApp recomenda atualizar as regras de firewall para usar a lista de endpoints revisada, que é menor, mais segura e mais fácil de gerenciar. A NetApp elimina a necessidade de entradas curinga, e os endpoints para atualizações de agentes oferecem suporte a todos os serviços de dados.

Endpoints para versões 3.9.55 e anteriores	Pontos finais para 4.0.0 e superiores	Propósito
• \ https://support.netapp.com • \ https://mysupport.netapp.com	• \ https://mysupport.netapp.com • \ https://signin.b2c.netapp.com • \ https://support.netapp.com	Para licenciamento e contato com o Suporte da NetApp .
• https://*.api.bluexp.netapp.com • \ https://api.bluexp.netapp.com • https://*.cloudmanager.cloud.netapp.com • \ https://cloudmanager.cloud.netapp.com • \ https://netapp-cloud-account.auth0.com • \ https://netapp-cloud-account.us.auth0.com • \ https://console.bluexp.netapp.com • https://*.console.bluexp.netapp.com	• \ https://api.bluexp.netapp.com • \ https://netapp-cloud-account.auth0.com • \ https://netapp-cloud-account.us.auth0.com • \ https://console.netapp.com • \ https://components.console.bluexp.netapp.com • \ https://cdn.auth0.com	Para operações do dia a dia.
• https://*.blob.core.windows.net • \ https://cloudmanagerinfraprod.azurecr.io	• \ https://bluexpinfraprod.eastus2.data.azurecr.io • \ https://bluexpinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console.

Passos

1. Verifique se a versão do seu agente é 4.0.0 ou superior."Ver versão do agente."
2. Coloque os endpoints na lista de permissões em"Pontos de extremidade suportados para 4.0.0 e superior" .
3. Reinicie o serviço do gerenciador de serviços 2 em cada agente executando o seguinte comando:

```
systemctl restart netapp-service-manager.service
```

4. Execute o seguinte comando e verifique se o status do agente é exibido como *ativo(em execução)*: _

```
systemctl status netapp-service-manager.service
```

5. Remova os endpoints antigos da lista de permissões do seu firewall.

Endpoints para NetApp Console e agentes de console para 3.9.55 e anteriores

Esses pontos de extremidade são usados para agentes do Console 3.9.55 e anteriores.

Pontos finais	Propósito
\ https://support.netapp.com \ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
https://*.api.bluexp.netapp.com \ https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com \ https://cloudmanager.cloud.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com	Para fornecer recursos e serviços no NetApp Console.
Escolha entre dois conjuntos de pontos de extremidade: • Opção 1 (recomendada) \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io • Opção 2 https://*.blob.core.windows.net \ https://cloudmanagerinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. A NetApp recomenda permitir endpoints da Opção 1 no seu firewall, pois eles são mais seguros, e não permitir endpoints da Opção 2, a menos que você esteja usando o Ransomware Resilience ou o Backup and Recovery. Observe o seguinte sobre esses pontos finais: • Os endpoints da Opção 1 são suportados em 3.9.47 e superiores. Versões anteriores à 3.9.47 não oferecem suporte à compatibilidade com versões anteriores. • O agente do Console inicia o contato com os endpoints na opção 2 primeiro. Se esses terminais não estiverem acessíveis, ele entrará em contato automaticamente com os terminais na opção 1. • Se você usar o agente do Console com o NetApp Backup and Recovery ou o Ransomware Resilience, o sistema não oferecerá suporte aos endpoints da Opção 1. Permitir pontos de extremidade da Opção 2 e não permitir a Opção 1.

Pontos de extremidade do provedor de nuvem contatados pelo agente do Console

Os agentes de console devem ter acesso a endpoints adicionais se estiverem implantados no seu provedor de nuvem.

Habilite o acesso aos endpoints do provedor de nuvem antes de instalar o agente do Console.

- "Configurar acesso à rede AWS para um agente do Console"
- "Configurar acesso à rede do Azure para um agente do Console"
- "Configurar o acesso à rede do Google Cloud para um agente do Console"

Os pontos de extremidade do provedor de nuvem são os mesmos para todas as versões.

Pontos de extremidade de serviços de dados contatados pelo agente do Console

O agente do Console requer acesso adicional à Internet de saída para dar suporte a alguns serviços de dados do NetApp e ao Cloud Volumes ONTAP.

Pontos de extremidade para Cloud Volumes ONTAP

- "Endpoints para Cloud Volumes ONTAP na AWS"
- "Pontos de extremidade para Cloud Volumes ONTAP no Azure"
- "Pontos de extremidade para Cloud Volumes ONTAP no Google Cloud"

Exigir o uso do IMDSv2 em instâncias do Amazon EC2

O NetApp Console oferece suporte ao Amazon EC2 Instance Metadata Service Versão 2 (IMDSv2) com o agente do Console e com o Cloud Volumes ONTAP (incluindo o mediador para implantações de HA). Na maioria dos casos, o IMDSv2 é configurado automaticamente em novas instâncias do EC2. O IMDSv1 foi habilitado antes de março de 2024. Se exigido por suas políticas de segurança, talvez seja necessário configurar manualmente o IMDSv2 em suas instâncias do EC2.

Antes de começar

- A versão do agente do Console deve ser 3.9.38 ou posterior.
- O Cloud Volumes ONTAP deve estar executando uma das seguintes versões:
  - 9.12.1 P2 (ou qualquer patch subsequente)
  - 9.13.0 P4 (ou qualquer patch subsequente)
  - 9.13.1 ou qualquer versão posterior a este lançamento
- Essa alteração exige que você reinicie as instâncias do Cloud Volumes ONTAP .
- Essas etapas exigem o uso da AWS CLI porque você deve alterar o limite de salto de resposta para 3.

Sobre esta tarefa

O IMDSv2 oferece proteção aprimorada contra vulnerabilidades. "Saiba mais sobre o IMDSv2 no blog de segurança da AWS"

O Serviço de Metadados de Instância (IMDS) é habilitado da seguinte maneira em instâncias do EC2:

- Para novas implantações de agentes do Console a partir do Console ou usando "Scripts do Terraform" O IMDSv2 é habilitado por padrão na instância do EC2.
- Se você iniciar uma nova instância do EC2 na AWS e depois instalar manualmente o software do agente do Console, o IMDSv2 também será habilitado por padrão.
- Se você iniciar o agente do Console no AWS Marketplace, o IMDSv1 será habilitado por padrão. Você pode configurar manualmente o IMDSv2 na instância do EC2.
- Para agentes de console existentes, o IMDSv1 ainda é suportado, mas você pode configurar manualmente o IMDSv2 na instância do EC2, se preferir.
- Para o Cloud Volumes ONTAP, o IMDSv1 é habilitado por padrão em instâncias novas e existentes. Você pode configurar manualmente o IMDSv2 nas instâncias do EC2, se preferir.

Passos

1. Exigir o uso do IMDSv2 na instância do agente do Console:

   a. Conecte-se à VM Linux para o agente do Console.

      Ao criar a instância do agente do Console na AWS, você forneceu uma chave de acesso e uma chave secreta da AWS. Você pode usar esse par de chaves para fazer SSH na instância. O nome de usuário para a instância do EC2 Linux é ubuntu (para agentes do Console criados antes de maio de 2023, o nome de usuário era ec2-user).

      "Documentação da AWS: Conecte-se à sua instância do Linux"

   b. Instale a AWS CLI.

      "Documentação da AWS: instalar ou atualizar para a versão mais recente da AWS CLI"

   c. Use o `aws ec2 modify-instance-metadata-options` comando para exigir o uso do IMDSv2 e alterar o limite de salto de resposta PUT para 3.

      Exemplo

```
aws ec2 modify-instance-metadata-options \
    --instance-id <instance-id> \
    --http-put-response-hop-limit 3 \
    --http-tokens required \
    --http-endpoint enabled
```

   +

   O `http-tokens` conjuntos de parâmetros IMDSv2 como obrigatórios. Quando `http-tokens` é necessário, você também deve definir `http-endpoint` para habilitado.

2. Exigir o uso do IMDSv2 em instâncias do Cloud Volumes ONTAP :

   a. Vá para o "Console Amazon EC2"

   b. No painel de navegação, selecione **Instâncias**.

   c. Selecione uma instância do Cloud Volumes ONTAP .

d. Selecione **Ações > Configurações da instância > Modificar opções de metadados da instância**.

e. Na caixa de diálogo **Modificar opções de metadados da instância**, selecione o seguinte:

- Para **Serviço de metadados de instância**, selecione **Ativar**.
- Para **IMDSv2**, selecione **Obrigatório**.
- Selecione **Salvar**.

f. Repita essas etapas para outras instâncias do Cloud Volumes ONTAP , incluindo o mediador HA.

g. "Pare e inicie as instâncias do Cloud Volumes ONTAP"

Resultado

A instância do agente do Console e as instâncias do Cloud Volumes ONTAP agora estão configuradas para usar o IMDSv2.

Configuração padrão para o agente do Console

Saiba mais sobre as configurações padrão do agente do Console para implantações padrão (com acesso à internet) na AWS, Azure e Google Cloud, bem como para implantações restritas (sem acesso à internet) em ambientes locais.

Configuração padrão com acesso à Internet

Os seguintes detalhes de configuração se aplicam se você implantou um agente do Console do NetApp Console, do marketplace do seu provedor de nuvem ou se instalou manualmente um agente do Console em um host Linux local com acesso à Internet.

Detalhes da VM do agente de console para AWS

Se você implantou um agente do Console a partir do Console ou do marketplace do provedor de nuvem, observe o seguinte:

- O tipo de instância EC2 é t3.2xlarge.
- O sistema operacional da imagem é o Ubuntu 22.04 LTS.

  O sistema operacional não inclui uma GUI. Você deve usar um terminal para acessar o sistema.

- A instalação inclui o Docker Engine, que é a ferramenta de orquestração de contêineres necessária.
- O nome de usuário para a instância do EC2 Linux é ubuntu (para agentes criados antes de maio de 2023, o nome de usuário é ec2-user).
- O disco padrão do sistema é um disco gp2 de 100 GiB.

Detalhes da VM do agente de console para o Azure

Se você implantou um agente do Console a partir do Console ou do marketplace do provedor de nuvem, observe o seguinte:

- O tipo de VM é Standard_D8s_v3.
- O sistema operacional da imagem é o Ubuntu 22.04 LTS.

  O sistema operacional não inclui uma GUI. Você deve usar um terminal para acessar o sistema.

- A instalação inclui o Docker Engine, que é a ferramenta de orquestração de contêineres necessária.
- O disco do sistema padrão é um disco SSD premium de 100 GiB.

Detalhes da VM do agente do console para o Google Cloud

Se você implantou um agente do Console a partir do Console, observe o seguinte:

- A instância da VM é n2-standard-8.
- O sistema operacional da imagem é o Ubuntu 22.04 LTS.

  O sistema operacional não inclui uma GUI. Você deve usar um terminal para acessar o sistema.

- A instalação inclui o Docker Engine, que é a ferramenta de orquestração de contêineres necessária.
- O disco do sistema padrão é um disco persistente SSD de 100 GiB.

Pasta de instalação

A pasta de instalação do agente está localizada no seguinte local:

`/opt/application/netapp/cloudmanager`

Arquivos de log

Os arquivos de log estão contidos nas seguintes pastas:

- `/opt/application/netapp/cloudmanager/log` ou
- `/opt/application/netapp/service-manager-2/logs` (a partir de novas instalações da versão 3.9.23)

  Os logs nessas pastas fornecem detalhes sobre o agente do Console.

- `/opt/application/netapp/cloudmanager/docker_occm/data/log`

  Os logs nesta pasta fornecem detalhes sobre os serviços de nuvem e o serviço do Console executado no agente do Console.

Serviço de agente de console

- O serviço do agente do Console é chamado occm.
- O serviço occm depende do serviço MySQL.

  Se o serviço MySQL estiver inativo, o serviço occm também estará.

Portos

O agente usa as seguintes portas no host Linux:

- 80 para acesso HTTP
- 443 para acesso HTTPS

Configuração padrão sem acesso à Internet

A configuração a seguir se aplica se você instalou manualmente o agente do Console em um host Linux local que não tem acesso à Internet. "Saiba mais sobre esta opção de instalação" .

- A pasta de instalação do agente está localizada no seguinte local:

  `/opt/application/netapp/ds`

- Os arquivos de log estão contidos nas seguintes pastas:

  `/var/lib/docker/volumes/ds_occmdata/_data/log`

  Os logs nesta pasta fornecem detalhes sobre o agente do Console e as imagens do Docker.

- Todos os serviços estão sendo executados dentro de contêineres docker

  Os serviços dependem do serviço de tempo de execução do Docker em execução

- O agente usa as seguintes portas no host Linux:
  - 80 para acesso HTTP
  - 443 para acesso HTTPS

Informações sobre direitos autorais

Informações sobre marcas comerciais