# Documentação de configuração e administração do BlueXP

BlueXP setup and administration

NetApp
December 11, 2024

# Índice

# Documentação de configuração e administração do BlueXP

# Notas de lançamento

## O que há de novo

Saiba o que há de novo com os recursos de administração do BlueXP : Gerenciamento de identidade e acesso (IAM), conetores, credenciais de provedor de nuvem e muito mais.

### 9 de dezembro de 2024

#### Conetor 3.9.47

Esta versão do conetor BlueXP  inclui correções de erros e uma alteração nos pontos finais contactados durante a instalação do conetor.

Neste momento, a versão 3.9.47 está disponível para o modo padrão e modo restrito.

#### Endpoint para entrar em Contato com o suporte do NetApp durante a instalação

Quando instala manualmente o conetor, o instalador deixa de entrar em contacto com a https://support.NetApp.com.

O instalador ainda entra em Contato com https://mysupport.NetApp.com.

#### Gerenciamento de identidade e acesso do BlueXP

A página conetores lista apenas os conetores atualmente disponíveis. Ele não exibe mais conetores que você removeu.

### 26 de novembro de 2024

#### Lançamento do modo privado (3,9.46)

Uma nova versão do modo privado está agora disponível para transferência a partir do "Site de suporte da NetApp"

A versão 3.9.46 inclui atualizações para os seguintes componentes e serviços do BlueXP .

| Componente ou serviço | Versão incluída nesta versão | Alterações desde a versão anterior do modo privado |
|---|---|---|
| Conetor | 3.9.46 | Pequenas melhorias de segurança e correções de bugs |
| Backup e recuperação | 22 de novembro de 2024 | Aceda ao "Novidades na página de backup e recuperação do BlueXP" e consulte as alterações incluídas na versão de Novembro de 2024 |
| Classificação | 4 de Novembro de 2024 (versão 1,37) | Aceda ao "Novidades na página de classificação do BlueXP" e consulte as alterações incluídas nas versões 1,32 a 1,37 |

| Componente ou serviço | Versão incluída nesta versão | Alterações desde a versão anterior do modo privado |
|---|---|---|
| Gerenciamento de Cloud Volumes ONTAP | 11 de novembro de 2024 | Acesse "Novidades na página de gerenciamento do Cloud Volumes ONTAP" e consulte as alterações incluídas nos lançamentos de outubro de 2024 e novembro de 2024 |
| Gerenciamento de clusters do ONTAP no local | 26 de novembro de 2024 | Aceda ao "Novidades na página de gerenciamento de clusters do ONTAP no local" e consulte as alterações incluídas na versão de Novembro de 2024 |

Embora a carteira digital BlueXP  e a replicação BlueXP  também estejam incluídas no modo privado, não há alterações na versão anterior do modo privado.

Para obter mais detalhes sobre o modo privado, incluindo como atualizar, consulte o seguinte:

- "Saiba mais sobre o modo privado"
- "Saiba como começar a usar o BlueXP  no modo privado"
- "Saiba como atualizar o conetor ao usar o modo privado"

## 11 de novembro de 2024

### Conetor 3.9.46

Esta versão do conetor BlueXP  inclui pequenas melhorias de segurança e correções de bugs.

Neste momento, a versão 3.9.46 está disponível para o modo padrão e modo restrito.

### ID para projetos IAM

Agora você pode exibir o ID de um projeto a partir do gerenciamento de identidade e acesso do BlueXP . Talvez seja necessário usar o ID ao fazer uma chamada à API.

"Saiba como obter o ID de um projeto".

## 10 de outubro de 2024

### Conetor 3.9.45 patch

Este patch inclui correções de bugs.

## 7 de outubro de 2024

### Gerenciamento de identidade e acesso do BlueXP

O BlueXP  Identity and Access Management (IAM) é um novo modelo de gerenciamento de recursos e acessos que substitui e aprimora a funcionalidade anterior fornecida pelas contas BlueXP  ao usar o BlueXP no modo padrão.

O BlueXP  IAM fornece gerenciamento mais granular de recursos e permissões:

- Uma *organização* de nível superior permite que você gerencie o acesso em seus vários *projetos*.
- *Pastas* permitem agrupar projetos relacionados.
- O gerenciamento de recursos aprimorado permite associar um recurso a uma ou mais pastas ou projetos.

  Por exemplo, você pode associar um sistema Cloud Volumes ONTAP a vários projetos.

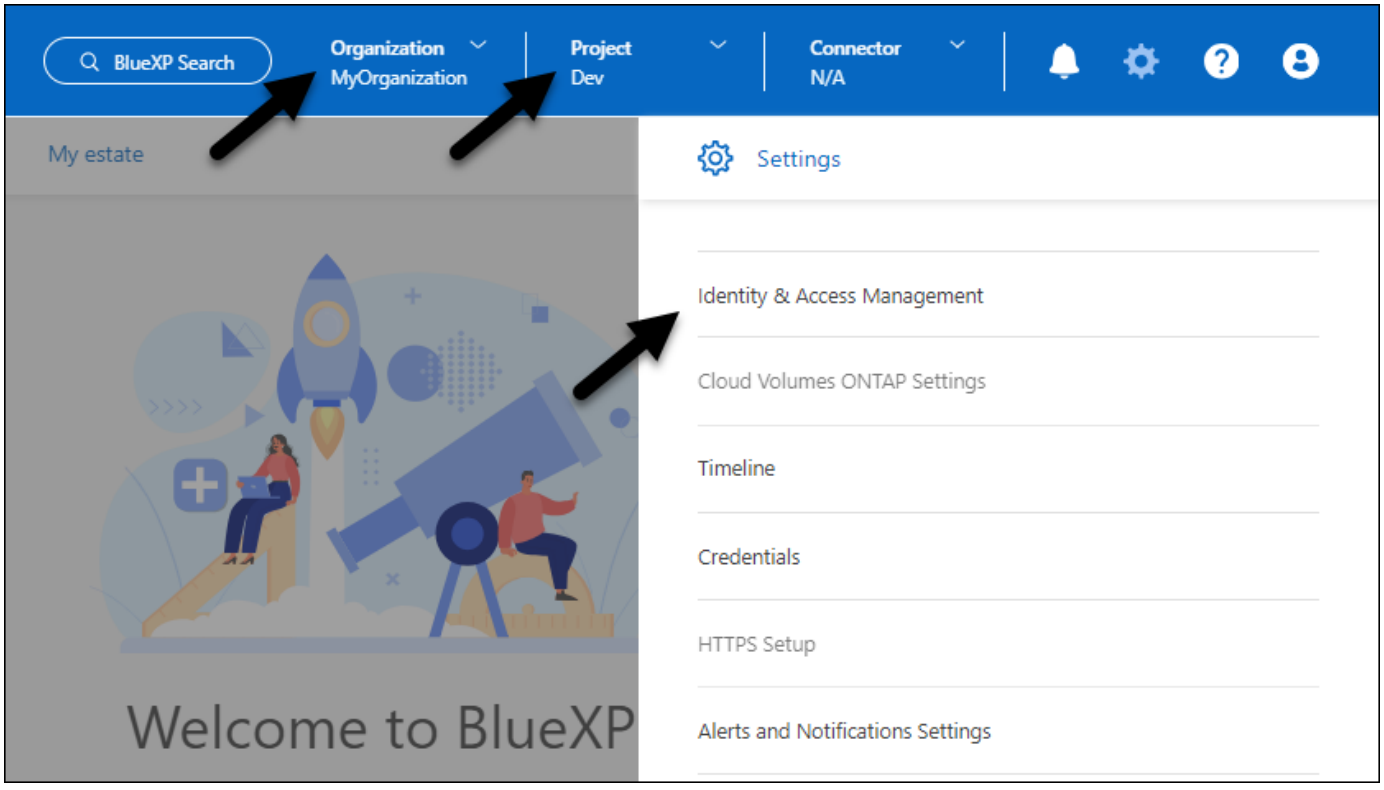
- O gerenciamento de acesso aprimorado permite que você atribua uma função a membros em diferentes níveis da hierarquia da organização.

Esses aprimoramentos fornecem melhor controle sobre as ações que os usuários podem executar e os recursos que podem acessar.

**Como o BlueXP  IAM afeta sua conta existente**

Ao fazer login no BlueXP , você notará estas alterações:

- Sua *conta* agora é chamada de *organização*
- Seus *workspaces* agora são chamados de *projects*
- Os nomes das funções de usuário mudaram:
  - *Account admin* é agora *Organization admin*
  - *Workspace admin* agora é *pasta ou projeto admin*
  - *Compliance Viewer* agora é *Classification Viewer*
- Em Configurações, você pode acessar o gerenciamento de identidade e acesso do BlueXP  para aproveitar esses aprimoramentos




Observe o seguinte:

- Não há alterações nos seus usuários ou ambientes de trabalho existentes.
- Embora os nomes das funções tenham mudado, não há diferenças em relação a uma perspetiva de permissões. Os usuários continuarão a ter acesso aos mesmos ambientes de trabalho que antes.
- Não há alterações na forma como inicia sessão no BlueXP . O BlueXP  IAM funciona com logins na nuvem do NetApp, credenciais do site de suporte da NetApp e conexões federadas, assim como as contas do BlueXP .
- Se você tivesse várias contas do BlueXP , agora você tem várias organizações do BlueXP .

**API para BlueXP  IAM**

Essa alteração introduz uma nova API para o BlueXP  IAM, mas é retrocompatível com a API de alocação anterior. "Saiba mais sobre a API para BlueXP  IAM"

**Modos de implantação suportados**

O BlueXP  IAM é suportado ao usar o BlueXP  no modo padrão. Se você estiver usando o BlueXP  no modo restrito ou privado, continuará usando uma conta *BlueXP*  para gerenciar espaços de trabalho, usuários e recursos.

**Onde ir a seguir**

- "Saiba mais sobre o BlueXP  IAM"
- "Comece a usar o BlueXP  IAM"

### Conetor 3.9.45

Esta versão inclui suporte expandido ao sistema operacional e correções de bugs.

A versão 3.9.45 está disponível para o modo padrão e modo restrito.

**Suporte para Ubuntu 24,04 LTS**

Começando com a versão 3.9.45, o BlueXP  agora suporta novas instalações do conetor em hosts Ubuntu 24,04 LTS quando usando BlueXP  em modo padrão ou modo restrito.

"Ver os requisitos do host do conetor".

### Suporte para SELinux com hosts RHEL

O BlueXP  agora suporta o conetor com hosts Red Hat Enterprise Linux que têm o SELinux habilitado em modo de imposição ou modo permissivo.

O suporte para SELinux começa com a versão 3.9.40 para o modo padrão e modo restrito e com a versão 3.9.42 para o modo privado.

Observe as seguintes limitações:

- O BlueXP  não suporta SELinux com hosts Ubuntu.
- Gerenciamento de sistemas Cloud Volumes ONTAP não é suportado por conetores que têm SELinux habilitado no sistema operacional.

"Saiba mais sobre o SELinux"

## 30 de setembro de 2024

### Lançamento do modo privado (3,9.44)

Uma nova versão do modo privado está agora disponível para download a partir do site de suporte da NetApp.

Esta versão inclui as seguintes versões dos componentes e serviços do BlueXP  compatíveis com o modo privado.

| Serviço | Versão incluída |
|---|---|
| Conetor | 3.9.44 |
| Backup e recuperação | 27 de setembro de 2024 |
| Classificação | 15 de Maio de 2024 (versão 1,31) |
| Gerenciamento de Cloud Volumes ONTAP | 9 de setembro de 2024 |
| Carteira digital | 30 de julho de 2023 |
| Gerenciamento de clusters do ONTAP no local | 22 de abril de 2024 |
| Replicação | 18 de setembro de 2022 |

Para o conetor, o lançamento do modo privado 3.9.44 inclui as atualizações introduzidas nas versões de agosto de 2024 e setembro de 2024. Mais notavelmente, o suporte para Red Hat Enterprise Linux 9,4.

Para saber mais sobre o que está incluído nas versões desses componentes e serviços do BlueXP , consulte as notas de versão de cada serviço do BlueXP :

- "Novidades na versão de setembro de 2024 do conetor"
- "Novidades na versão de agosto de 2024 do conetor"
- "Novidades com backup e recuperação do BlueXP"
- "Novidades com a classificação BlueXP"
- "O que há de novo com o gerenciamento de Cloud Volumes ONTAP no BlueXP"

Para obter mais detalhes sobre o modo privado, incluindo como atualizar, consulte o seguinte:

- "Saiba mais sobre o modo privado"
- "Saiba como começar a usar o BlueXP  no modo privado"
- "Saiba como atualizar o conetor ao usar o modo privado"

## 9 de setembro de 2024

### Conetor 3.9.44

Esta versão inclui suporte para Docker Engine 26, um aprimoramento para certificados SSL e correções de bugs.

A versão 3.9.44 está disponível para o modo padrão e modo restrito.

#### Suporte para Docker Engine 26 com novas instalações

Começando com a versão 3.9.44 do conetor, Docker Engine 26 agora é suportado com *new* Connector

installations em hosts Ubuntu.

Se você tiver um conetor existente criado antes da versão 3.9.44, então Docker Engine 25.0.5 ainda é a versão máxima suportada em hosts Ubuntu.

"Saiba mais sobre os requisitos do Docker Engine".

**Certificado SSL atualizado para acesso à IU local**

Quando você usa o BlueXP  no modo restrito ou no modo privado, a interface do usuário é acessível a partir da máquina virtual do conetor que é implantada na sua região de nuvem ou no local. Por padrão, o BlueXP usa um certificado SSL autoassinado para fornecer acesso HTTPS seguro ao console baseado na Web em execução no conetor.

Nesta versão, fizemos alterações no certificado SSL para conetores novos e existentes:

- O Nome Comum para o certificado agora corresponde ao nome curto do host
- O Nome alternativo do assunto do certificado é o nome de domínio totalmente qualificado (FQDN) da máquina host

### Suporte para RHEL 9,4

O BlueXP  agora suporta a instalação do conetor em um host Red Hat Enterprise Linux 9,4 ao usar o BlueXP no modo padrão ou no modo restrito.

O suporte para RHEL 9,4 começa com a liberação 3.9.40 do conetor.

A lista atualizada de versões RHEL compatíveis para o modo padrão e modo restrito agora inclui o seguinte:

- 8,6 a 8,10
- 9,1 a 9,4

"Saiba mais sobre o suporte para RHEL 8 e 9 com o conetor".

### Suporte para Podman 4.9.4 com todas as versões RHEL

O Podman 4.9.4 agora é compatível com todas as versões suportadas do Red Hat Enterprise Linux. A versão 4.9.4 foi anteriormente suportada com apenas RHEL 8,10.

A lista atualizada de versões suportadas do Podman inclui 4.6.1 e 4.9.4 com hosts Red Hat Enterprise Linux.

Podman é necessário para hosts RHEL começando com a versão 3.9.40 do conetor.

"Saiba mais sobre o suporte para RHEL 8 e 9 com o conetor".

### Permissões da AWS e do Azure atualizadas

Atualizamos as políticas da AWS e do Azure para que o conetor remova permissões que não são mais necessárias. As permissões estavam relacionadas ao armazenamento em cache na borda do BlueXP  e à descoberta e gerenciamento de clusters do Kubernetes, que não são mais compatíveis em agosto de 2024.

- "Saiba o que mudou na política da AWS".
- "Saiba o que mudou na política do Azure".

## 22 de agosto de 2024

### Conetor 3.9.43 patch

Atualizamos o conetor para suportar a versão Cloud Volumes ONTAP 9.15.1.

O suporte para esta versão inclui uma atualização da política de conetores para Azure. A política agora inclui as seguintes permissões:

```
"Microsoft.Compute/virtualMachineScaleSets/write",
"Microsoft.Compute/virtualMachineScaleSets/read",
"Microsoft.Compute/virtualMachineScaleSets/delete"
```

Essas permissões são necessárias para o suporte do Cloud Volumes ONTAP de conjuntos de escala de máquinas virtuais. Se você tiver conetores existentes e quiser usar esse novo recurso, será necessário adicionar essas permissões às funções personalizadas associadas às credenciais do Azure.

- "Saiba mais sobre o lançamento do Cloud Volumes ONTAP 9.15.1"
- "Ver permissões do Azure para o conetor".

## 8 de agosto de 2024

### Conetor 3.9.43

Esta versão inclui pequenas melhorias e correções de bugs.

A versão 3.9.43 está disponível para o modo padrão e modo restrito.

### Requisitos atualizados de CPU e RAM

Para fornecer maior confiabilidade e melhorar o desempenho do BlueXP  e do conetor, agora precisamos de CPU e RAM adicionais para a máquina virtual do conetor:

- CPU: 8 núcleos ou 8 vCPUs (o requisito anterior era 4)
- RAM: 32 GB (o requisito anterior era de 14 GB)

Como resultado dessa alteração, o tipo de instância de VM padrão ao implantar o conetor do BlueXP  ou do mercado do provedor de nuvem é o seguinte:

- AWS: t3,2xlarge
- Azure: Standard_D8s_v3
- Google Cloud: N2-standard-8

Os requisitos atualizados de CPU e RAM aplicam-se a todos os novos conetores. Para os conetores existentes, é recomendável aumentar a CPU e a RAM para fornecer melhor desempenho e confiabilidade.

### Suporte para Podman 4.9.4 com RHEL 8,10

O Podman versão 4.9.4 agora é suportado ao instalar o conetor em um host Red Hat Enterprise Linux 8,10.

### Validação de usuário para federação de identidade

Se você usar a federação de identidade com o BlueXP , cada usuário que fizer login no BlueXP  pela primeira vez precisará preencher um formulário rápido para validar sua identidade.

## 31 de julho de 2024

### Lançamento do modo privado (3,9.42)

Uma nova versão do modo privado está agora disponível para download a partir do site de suporte da NetApp.

#### Suporte para RHEL 8 e 9

Esta versão inclui suporte para instalar o conetor em um host Red Hat Enterprise Linux 8 ou 9 ao usar o BlueXP  em modo privado. As seguintes versões do RHEL são suportadas:

- 8,6 a 8,10
- 9,1 a 9,3

O Podman é necessário como a ferramenta de orquestração de contentores para esses sistemas operacionais.

Você deve estar ciente dos requisitos do Podman, limitações conhecidas, um resumo do suporte ao sistema operacional, o que fazer se você tiver um host RHEL 7, como começar e muito mais.

"Saiba mais sobre o suporte para RHEL 8 e 9 com o conetor".

#### Versões incluídas nesta versão

Esta versão inclui as seguintes versões dos serviços BlueXP  que são compatíveis com o modo privado.

| Serviço | Versão incluída |
|---|---|
| Conetor | 3.9.42 |
| Backup e recuperação | 18 de julho de 2024 |
| Classificação | 1 de Julho de 2024 (versão 1,33) |
| Gerenciamento de Cloud Volumes ONTAP | 10 de junho de 2024 |
| Carteira digital | 30 de julho de 2023 |
| Gerenciamento de clusters do ONTAP no local | 30 de julho de 2023 |
| Replicação | 18 de setembro de 2022 |

Para saber mais sobre o que está incluído nas versões desses serviços BlueXP , consulte as notas de versão de cada serviço BlueXP .

- "Saiba mais sobre o modo privado"
- "Saiba como começar a usar o BlueXP  no modo privado"
- "Saiba como atualizar o conetor ao usar o modo privado"
- "Saiba o que há de novo com backup e recuperação do BlueXP "
- "Saiba o que há de novo com a classificação BlueXP "
- "Saiba o que há de novo com o gerenciamento de Cloud Volumes ONTAP no BlueXP "

## 15 de julho de 2024

### Suporte para RHEL 8,10

O BlueXP  agora suporta a instalação do conetor em um host Red Hat Enterprise Linux 8,10 quando usa o modo padrão ou o modo restrito.

O suporte para RHEL 8,10 começa com a liberação 3.9.40 do conetor.

"Saiba mais sobre o suporte para RHEL 8 e 9 com o conetor".

## 8 de julho de 2024

### Conetor 3.9.42

Esta versão inclui pequenas melhorias, correções de bugs e suporte para o conetor na região AWS Canada West (Calgary).

A versão 3.9.42 está disponível para o modo padrão e modo restrito.

### Requisitos atualizados do Docker Engine

Quando o conetor é instalado em um host Ubuntu, a versão mínima suportada do Docker Engine é agora 23,0.6. Era anteriormente 19,3.1.

A versão máxima suportada ainda é 25,0.5.

"Ver os requisitos do host do conetor".

### A verificação de e-mail agora é necessária

Os novos usuários que se inscreverem no BlueXP  agora precisam verificar seu endereço de e-mail antes de poderem fazer login.

## 12 de junho de 2024

### Conetor 3.9.41

Esta versão do conetor BlueXP  inclui pequenas melhorias de segurança e correções de bugs.

A versão 3.9.41 está disponível para o modo padrão e modo restrito.

## 4 de junho de 2024

### Lançamento do modo privado (3,9.40)

Uma nova versão do modo privado está agora disponível para download a partir do site de suporte da NetApp. Esta versão inclui as seguintes versões dos serviços BlueXP  que são compatíveis com o modo privado.

Observe que essa versão de modo privado *não* inclui suporte para o conetor com Red Hat Enterprise Linux 8 e 9.

| Serviço | Versão incluída |
| --- | --- |
| Conetor | 3.9.40 |
| Backup e recuperação | 17 de maio de 2024 |
| Classificação | 15 de Maio de 2024 (versão 1,31) |
| Gerenciamento de Cloud Volumes ONTAP | 17 de maio de 2024 |
| Carteira digital | 30 de julho de 2023 |
| Gerenciamento de clusters do ONTAP no local | 30 de julho de 2023 |
| Replicação | 18 de setembro de 2022 |

Para saber mais sobre o que está incluído nas versões desses serviços BlueXP , consulte as notas de versão de cada serviço BlueXP .

- "Saiba mais sobre o modo privado"
- "Saiba como começar a usar o BlueXP  no modo privado"
- "Saiba como atualizar o conetor ao usar o modo privado"
- "Saiba o que há de novo com backup e recuperação do BlueXP "
- "Saiba o que há de novo com a classificação BlueXP "
- "Saiba o que há de novo com o gerenciamento de Cloud Volumes ONTAP no BlueXP "

## 17 de maio de 2024

### Conetor 3.9.40

Esta versão do conetor BlueXP  inclui suporte para sistemas operacionais adicionais, pequenas melhorias de segurança e correções de bugs.

Neste momento, a versão 3.9.40 está disponível para o modo padrão e modo restrito.

#### Suporte para RHEL 8 e 9

O conetor agora é suportado em hosts que executam as seguintes versões do Red Hat Enterprise Linux com instalações *new* Connector ao usar o BlueXP  no modo padrão ou no modo restrito:

- 8,6 a 8,9
- 9,1 a 9,3

O Podman é necessário como a ferramenta de orquestração de contentores para esses sistemas operacionais.

Você deve estar ciente dos requisitos do Podman, limitações conhecidas, um resumo do suporte ao sistema operacional, o que fazer se você tiver um host RHEL 7, como começar e muito mais.

"Saiba mais sobre o suporte para RHEL 8 e 9 com o conetor".

#### Fim do suporte para RHEL 7 e CentOS 7

Em 30 de junho de 2024, o RHEL 7 chegará ao fim da manutenção (EOM), enquanto o CentOS 7 chegará ao fim da vida útil (EOL). O NetApp continuará a suportar o conetor nessas distribuições Linux até 30 de junho de 2024.

"Saiba o que fazer se você tiver um conetor existente em execução no RHEL 7 ou no CentOS 7".

#### Atualização de permissões da AWS

Na versão 3.9.38, atualizamos a política de conetores para a AWS para incluir a permissão "EC2:DescribeAvailabilityZones". Essa permissão agora é necessária para oferecer suporte a zonas locais da AWS com o Cloud Volumes ONTAP.

- "Exibir permissões da AWS para o conetor".
- "Saiba mais sobre o suporte para zonas locais da AWS"

## 22 de abril de 2024

#### Conetor 3.9.39

Esta versão do conetor BlueXP  inclui pequenas melhorias de segurança e correções de bugs.

Neste momento, a versão 3.9.39 está disponível para o modo padrão e modo restrito.

#### Permissões da AWS para criar um conetor

Duas permissões adicionais agora são necessárias para criar um conetor na AWS a partir do BlueXP :

```
"ec2:DescribeLaunchTemplates",
"ec2:CreateLaunchTemplate",
```

Essas permissões são necessárias para habilitar o IMDSv2 na instância EC2 para o conetor.

Incluímos essas permissões na política exibida na interface de usuário do BlueXP  ao criar um conetor e na mesma política fornecida na documentação.

> Esta política contém apenas as permissões necessárias para iniciar a instância do Connector no AWS a partir do BlueXP . Não é a mesma política que é atribuída à instância do conetor.

"Saiba como configurar permissões da AWS para criar um conetor da AWS".

## 11 de abril de 2024

#### Atualização do Docker Engine

Atualizamos os requisitos do Docker Engine para especificar a versão máxima suportada no conetor, que é 25,0.5. A versão mínima suportada ainda é 19,3.1.

"Ver os requisitos do host do conetor".

## 26 de março de 2024

#### Lançamento do modo privado (3,9.38)

Uma nova versão do modo privado está agora disponível para o BlueXP . Esta versão inclui as seguintes versões dos serviços BlueXP  que são compatíveis com o modo privado.

| Serviço | Versão incluída |
| --- | --- |
| Conetor | 3.9.38 |
| Backup e recuperação | 12 de março de 2024 |
| Classificação | 4 de março de 2024 |
| Gerenciamento de Cloud Volumes ONTAP | 8 de março de 2024 |
| Carteira digital | 30 de julho de 2023 |
| Gerenciamento de clusters do ONTAP no local | 30 de julho de 2023 |
| Replicação | 18 de setembro de 2022 |

Esta nova versão está disponível para download no site de suporte da NetApp.

- "Saiba mais sobre o modo privado"
- "Saiba como começar a usar o BlueXP  no modo privado"
- "Saiba como atualizar o conetor ao usar o modo privado"

## 8 de março de 2024

### Conetor 3.9.38

Neste momento, a versão 3.9.38 está disponível para o modo padrão e modo restrito. Esta versão inclui suporte para IMDSv2 na AWS e uma atualização de permissões da AWS.

#### Suporte para IMDSv2

O BlueXP  agora oferece suporte ao serviço de metadados de instância do Amazon EC2 versão 2 (IMDSv2) com a instância do conetor e com instâncias do Cloud Volumes ONTAP. O IMDSv2 fornece proteção aprimorada contra vulnerabilidades. Apenas IMDSv1 foi anteriormente suportado.

"Saiba mais sobre o IMDSv2 no Blog de Segurança da AWS"

O Serviço de metadados de instância (IMDS) está habilitado da seguinte forma em instâncias EC2:

- Para novas implantações de conetores do BlueXP  ou usando "Scripts do Terraform"o , o IMDSv2 é habilitado por padrão na instância do EC2.
- Se você iniciar uma nova instância do EC2 na AWS e instalar manualmente o software Connector, o IMDSv2 também será habilitado por padrão.
- Se você iniciar o conetor no AWS Marketplace, o IMDSv1 será habilitado por padrão. Você pode configurar manualmente o IMDSv2 na instância do EC2.
- Para os conetores existentes, IMDSv1 ainda é suportado, mas você pode configurar manualmente IMDSv2 na instância 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.

"Saiba como configurar o IMDSv2 em instâncias existentes".

#### Atualização de permissões da AWS

Atualizamos a política de conetores para a AWS para incluir a permissão "EC2:DescribeAvailabilityZones". Esta permissão é necessária para uma próxima versão. Atualizaremos as notas de versão com mais detalhes

quando essa versão estiver disponível.

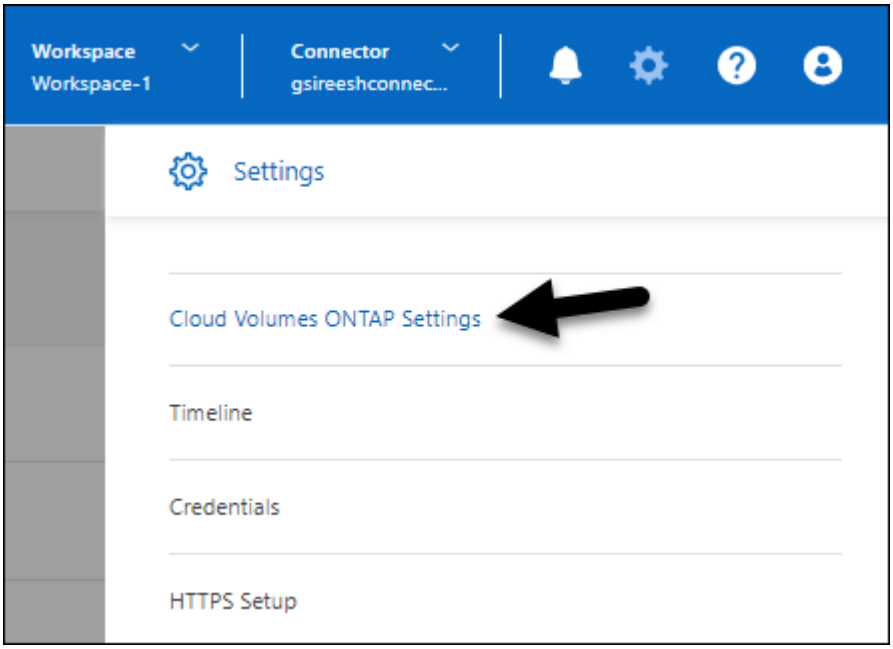
"Exibir permissões da AWS para o conetor".

### Configurações de proxy e configurações de Cloud Volumes ONTAP

As configurações do servidor proxy para o conetor estão agora disponíveis na página **Gerenciar conetores** (modo padrão) ou na página **Editar conetores** (modo restrito e modo privado).

"Saiba como configurar o conetor para usar um servidor proxy".

Além disso, renomeamos a página **Configurações do conetor** para **Configurações do Cloud Volumes ONTAP**.




## 15 de fevereiro de 2024

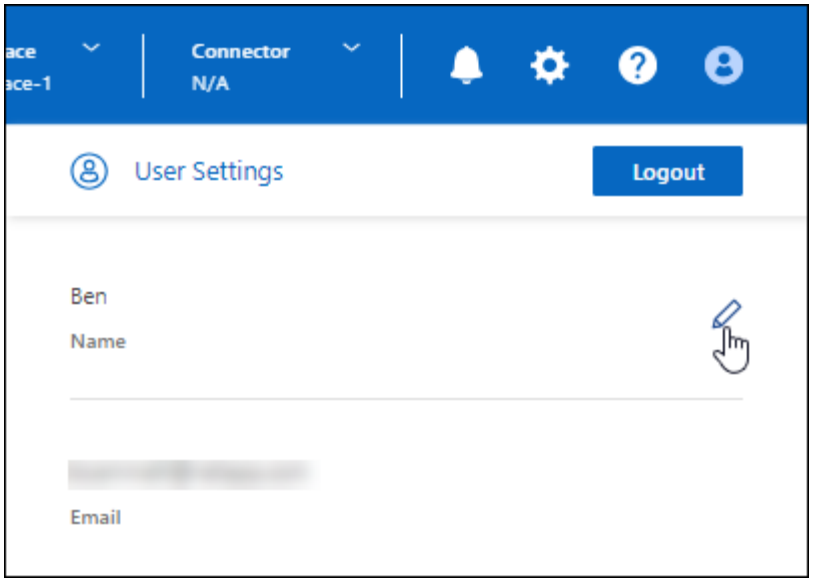
### Conetor 3.9.37

Esta versão do conetor BlueXP  inclui pequenas melhorias de segurança e correções de bugs.

Neste momento, a versão 3.9.37 está disponível para o modo padrão e modo restrito.

### Editar nome

Se você usar credenciais de nuvem do NetApp para fazer login no BlueXP , agora você pode editar seu nome em **Configurações do usuário**.




Editar seu nome não é suportado se você fizer login com uma conexão federada ou com sua conta do site de suporte da NetApp.

## 11 de janeiro de 2024

### Conetor 3.9.36

Esta versão inclui pequenas melhorias, correções de bugs e suporte para o conetor nas seguintes regiões de nuvem:

- A região de Israel (Tel Aviv) na AWS
- A região da Arábia Saudita no Google Cloud

## 5 de dezembro de 2023

### Lançamento do modo privado (3,9.35)

Uma nova versão do modo privado está agora disponível para o BlueXP . Esta versão inclui a versão 3.9.35 do conetor e versões dos serviços BlueXP  que são suportados com o modo privado a partir de outubro de 2023.

Esta nova versão está disponível para download no site de suporte da NetApp.

- "Saiba mais sobre os serviços BlueXP  que estão incluídos no modo privado"
- "Saiba como começar a usar o BlueXP  no modo privado"
- "Saiba como atualizar o conetor ao usar o modo privado"

## 8 de novembro de 2023

### Conetor 3.9.35

Esta versão contém pequenas melhorias de segurança e correções de bugs.

## 6 de outubro de 2023

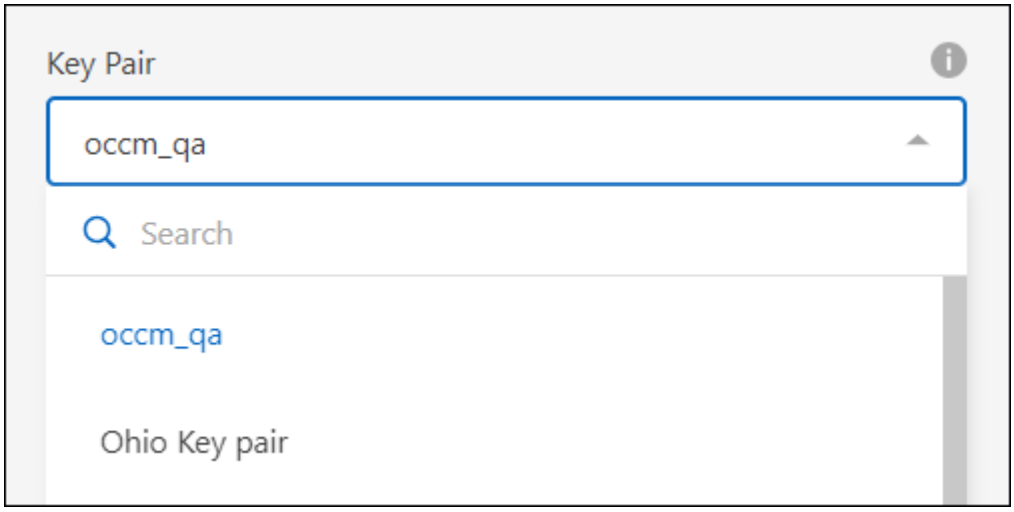
### Conetor 3.9.34

Esta versão contém pequenas melhorias e correções de bugs.

## 10 de setembro de 2023

### Conetor 3.9.33

- Quando você cria um conetor no AWS a partir do BlueXP , agora você pode pesquisar no campo par de chaves para encontrar mais facilmente o par de chaves que deseja usar com a instância do Connector.




- Esta atualização também inclui correções de bugs.

## 30 de julho de 2023

### Conetor 3.9.32

- Agora você pode usar a API de serviço de auditoria do BlueXP  para exportar logs de auditoria.

  O serviço de auditoria Registra informações sobre as operações realizadas pelos serviços BlueXP . Isso inclui espaços de trabalho, conetores usados e outros dados de telemetria. Você pode usar esses dados para determinar quais ações foram executadas, quem as executou e quando elas ocorreram.

  "Saiba mais sobre como usar a API de serviço de auditoria"

  Observe que esse link também é acessível a partir da interface de usuário do BlueXP  na página linha do tempo.

- Esta versão do conetor também inclui aprimoramentos do Cloud Volumes ONTAP e aprimoramentos de cluster do ONTAP no local.
  - "Saiba mais sobre os aprimoramentos do Cloud Volumes ONTAP"
  - "Saiba mais sobre os aprimoramentos de cluster no ONTAP on-premise"

## 2 de julho de 2023

### Conetor 3.9.31

- Agora você pode descobrir clusters ONTAP no local na guia **My ESTATE** (anteriormente **Minhas oportunidades**)

  "Saiba como descobrir clusters a partir da página My ESTATE".

- Se você estiver usando o conetor em uma região do Azure Government, certifique-se de que o conetor pode entrar em Contato com o seguinte endpoint:

  https://occmclientinfragov.azurecr.us

  Este endpoint é necessário para instalar manualmente o conetor e atualizar o conetor e seus componentes do Docker.

  Como resultado dessa alteração, um conetor em uma região do Azure Government não entra em Contato com o seguinte endpoint:

  https://cloudmanagerinfraprod.azurecr.io

  Observe que esse ponto final ainda é necessário para todas as outras configurações de modo restrito e para o modo padrão.

## 4 de junho de 2023

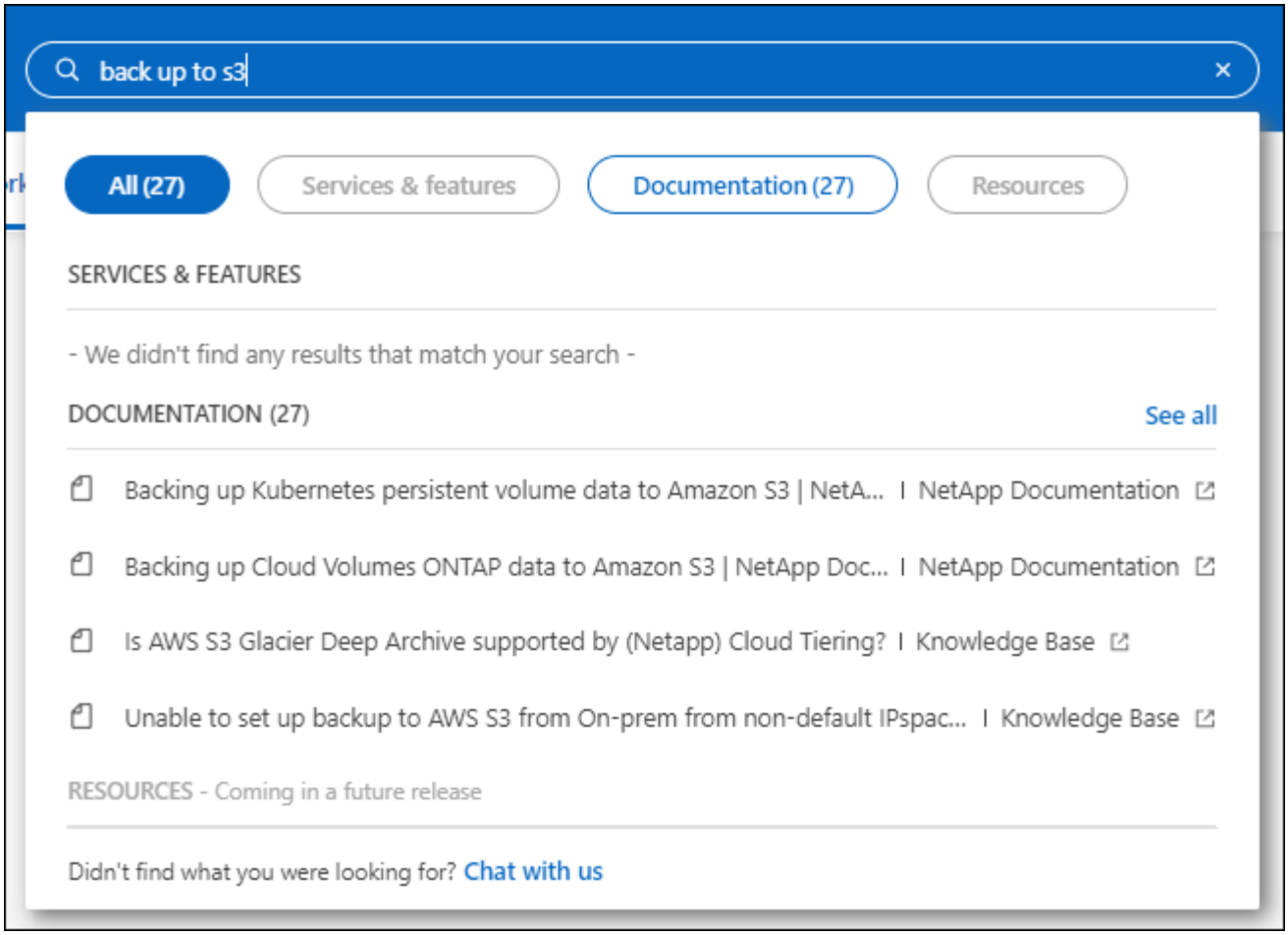
### Conetor 3.9.30

- Quando você abre um caso de suporte da NetApp no Painel de suporte, o BlueXP agora abre o caso usando a conta do site de suporte da NetApp associada ao login do BlueXP . A BlueXP usou anteriormente a conta do site de suporte da NetApp associada a toda a conta do BlueXP .

  Como parte dessa alteração, o Registro de suporte para uma conta do BlueXP agora é feito através da conta do site de suporte da NetApp associada ao login do BlueXP de um usuário. Anteriormente, o Registro de suporte foi feito através de uma conta NSS associada a toda a conta BlueXP . Como resultado, outros usuários do BlueXP não verão o mesmo status de Registro de suporte se não associarem uma conta do site de suporte da NetApp ao login do BlueXP . Se você já registrou sua conta do BlueXP para obter suporte, então seu status de Registro ainda é válido. Você só precisa adicionar uma conta NSS no nível do usuário para ver o status.

  - "Saiba como criar um caso com o suporte da NetApp"
  - "Saiba como gerenciar credenciais associadas ao seu login no BlueXP"
  - "Saiba como se inscrever para obter suporte"

- Agora você pode procurar documentação no BlueXP . Os resultados da pesquisa agora fornecem links para conteúdo em docs.NetApp.com e kb.NetApp.com, o que pode ajudar a responder a uma pergunta que você tem.




- O conetor agora permite adicionar e gerenciar contas de storage do Azure a partir do BlueXP .

  "Veja como adicionar novas contas de armazenamento do Azure em suas assinaturas do Azure do BlueXP ".

- O conetor agora é suportado nas seguintes regiões da AWS:
  - Hyderabad (ap-South-2)
  - Melbourne (ap-sudeste-4)
  - Espanha (ue-Sul-2)
  - EAU (me-central-1)
  - Zurique (eu-central-2)
- O conetor agora é suportado nas seguintes regiões do Azure:
  - Brasil Sul
  - França Sul
  - Rio de Janeiro Central
  - Rio de Janeiro West
  - Polónia Central
  - Qatar Central
- O conetor agora é compatível com as seguintes regiões do Google Cloud:

- Columbus (US-east5)
- Dallas (US-south1)

"Veja a lista completa de regiões suportadas"

## 7 de maio de 2023

### Conetor 3.9.29

- Ubuntu 22,04 é o novo sistema operacional para o conetor quando você implementa um conetor do BlueXP ou do mercado do seu provedor de nuvem.

  Você também tem a opção de instalar manualmente o conetor em seu próprio host Linux que está executando o Ubuntu 22,04.

- O Red Hat Enterprise Linux 8,6 e 8,7 não são mais compatíveis com novas implantações de conetores.

  Essas versões não são suportadas com novas implantações porque a Red Hat não suporta mais Docker, o que é necessário para o conetor. Se você tiver um conetor existente em execução no RHEL 8,6 ou 8,7, o NetApp continuará a suportar sua configuração.

  Red Hat 7,6, 7,7, 7,8 e 7,9 ainda são suportados com conetores novos e existentes.

- O conetor agora é suportado na região do Qatar no Google Cloud.
- O conetor também é suportado na região Central da Suécia no Microsoft Azure.

  "Veja a lista completa de regiões suportadas"

- Esta versão do conetor inclui melhorias no Cloud Volumes ONTAP.

  "Saiba mais sobre os aprimoramentos do Cloud Volumes ONTAP"

## 4 de abril de 2023

### Modos de implantação

BlueXP *modos de implantação* permitem que você use o BlueXP de uma forma que atenda aos requisitos de negócios e segurança. Você pode escolher entre três modos:

- Modo padrão
- Modo restrito
- Modo privado

"Saiba mais sobre esses modos de implantação".

A introdução do modo restrito substitui a opção de ativar ou desativar a plataforma SaaS. Você pode ativar o modo restrito no momento da criação da conta. Não pode ser ativado ou desativado mais tarde.

## 3 de abril de 2023

### Conetor 3.9.28

- As notificações por e-mail são agora suportadas com a carteira digital BlueXP .

  Se você configurar suas configurações de notificação, você poderá receber notificações por e-mail quando suas licenças BYOL estiverem prestes a expirar (uma notificação de "Aviso") ou se elas já tiverem expirado (uma notificação de "erro").

  "Saiba como configurar notificações por e-mail".

- O conetor agora é suportado na região do Google Cloud Turin.

  "Veja a lista completa de regiões suportadas"

- Agora você pode gerenciar as credenciais de usuário associadas ao login do BlueXP : Credenciais do ONTAP e credenciais do site de suporte da NetApp (NSS).

  Quando acede a **Definições > credenciais**, pode visualizar as credenciais, atualizar as credenciais e eliminá-las. Por exemplo, se você alterar a senha dessas credenciais, precisará atualizar a senha no BlueXP .

  "Saiba como gerenciar credenciais de usuário".

- Agora você pode fazer upload de anexos quando criar um caso de suporte ou quando atualizar as notas de caso para um caso de suporte existente.

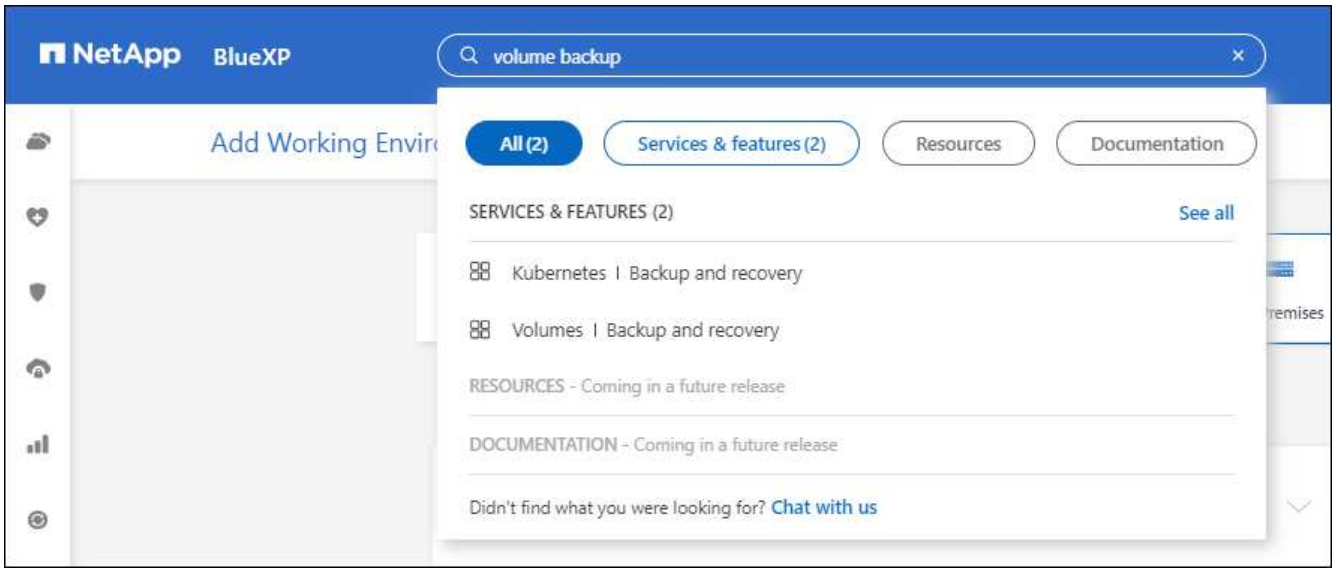
  "Saiba como criar e gerenciar casos de suporte".

- Esta versão do conetor também inclui aprimoramentos do Cloud Volumes ONTAP e aprimoramentos de cluster do ONTAP no local.
  - "Saiba mais sobre os aprimoramentos do Cloud Volumes ONTAP"
  - "Saiba mais sobre os aprimoramentos de cluster no ONTAP on-premise"

## 5 de março de 2023

### Conetor 3.9.27

- A pesquisa já está disponível no console do BlueXP . Neste momento, você pode usar a pesquisa para encontrar serviços e recursos do BlueXP .




- Você pode visualizar e gerenciar casos de suporte ativos e resolvidos diretamente do BlueXP . Você pode gerenciar os casos associados à sua conta NSS e à sua empresa.

  "Saiba como gerenciar seus casos de suporte".

- O conetor agora é suportado em qualquer ambiente de nuvem que tenha isolamento completo da Internet. Depois, use o console do BlueXP executado no conector para implantar o Cloud Volumes ONTAP no mesmo local e descobrir clusters ONTAP no local (se você tiver uma conexão do ambiente de nuvem para o ambiente no local). Você também pode usar o backup e a recuperação do BlueXP para fazer backup de volumes do Cloud Volumes ONTAP nas regiões comerciais da AWS e do Azure. Nenhum outro serviço BlueXP é suportado neste tipo de implantação, exceto para a carteira digital BlueXP .

  A região da nuvem pode ser uma região para agências seguras dos EUA, como AWS Top Secret Cloud, AWS Secret Cloud, Azure IL6 ou qualquer região comercial.

  Para começar, instale manualmente o software Connector, faça login no console BlueXP que está sendo executado no conetor, adicione sua licença BYOL à carteira digital BlueXP e, em seguida, implante o Cloud Volumes ONTAP.

  - "Instale o conetor num local sem acesso à Internet"
  - "Adicione uma licença não atribuída"
  - "Comece a usar o Cloud Volumes ONTAP"

- O conetor agora permite adicionar e gerenciar buckets do Amazon S3 no BlueXP .

  "Veja como adicionar novos buckets do Amazon S3 na sua conta da AWS a partir do BlueXP ".

- Esta versão do conetor inclui melhorias no Cloud Volumes ONTAP.

  "Saiba mais sobre os aprimoramentos do Cloud Volumes ONTAP"

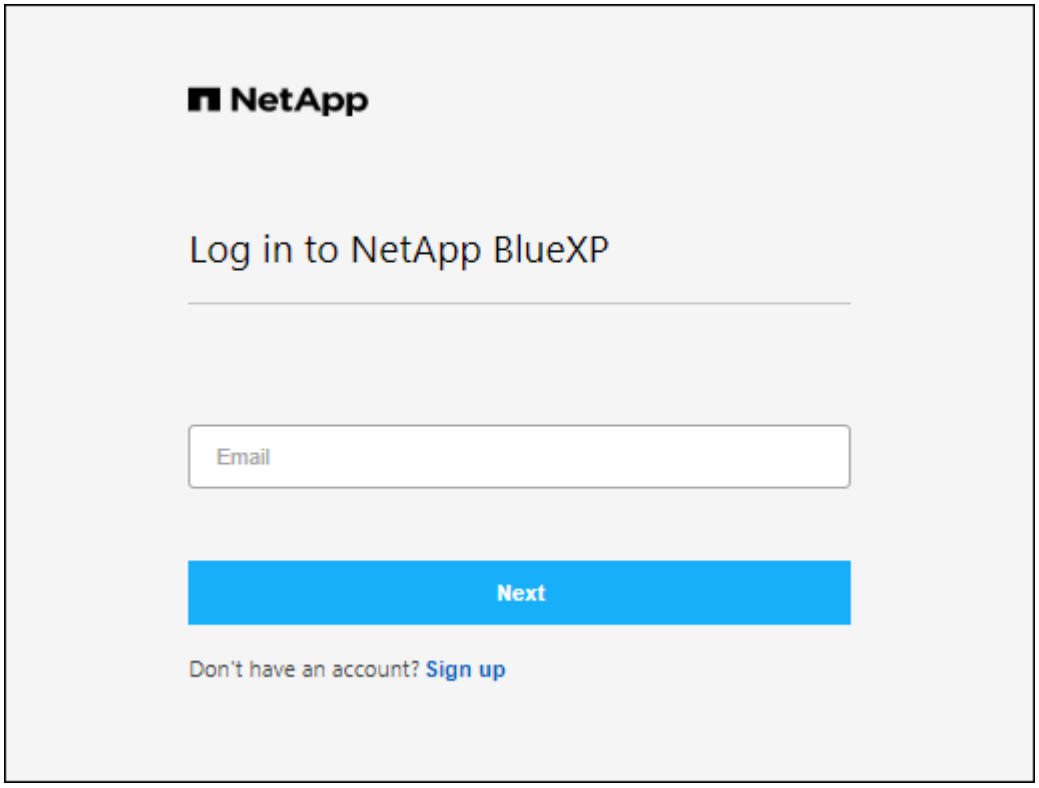
## 5 de fevereiro de 2023

### Conetor 3.9.26

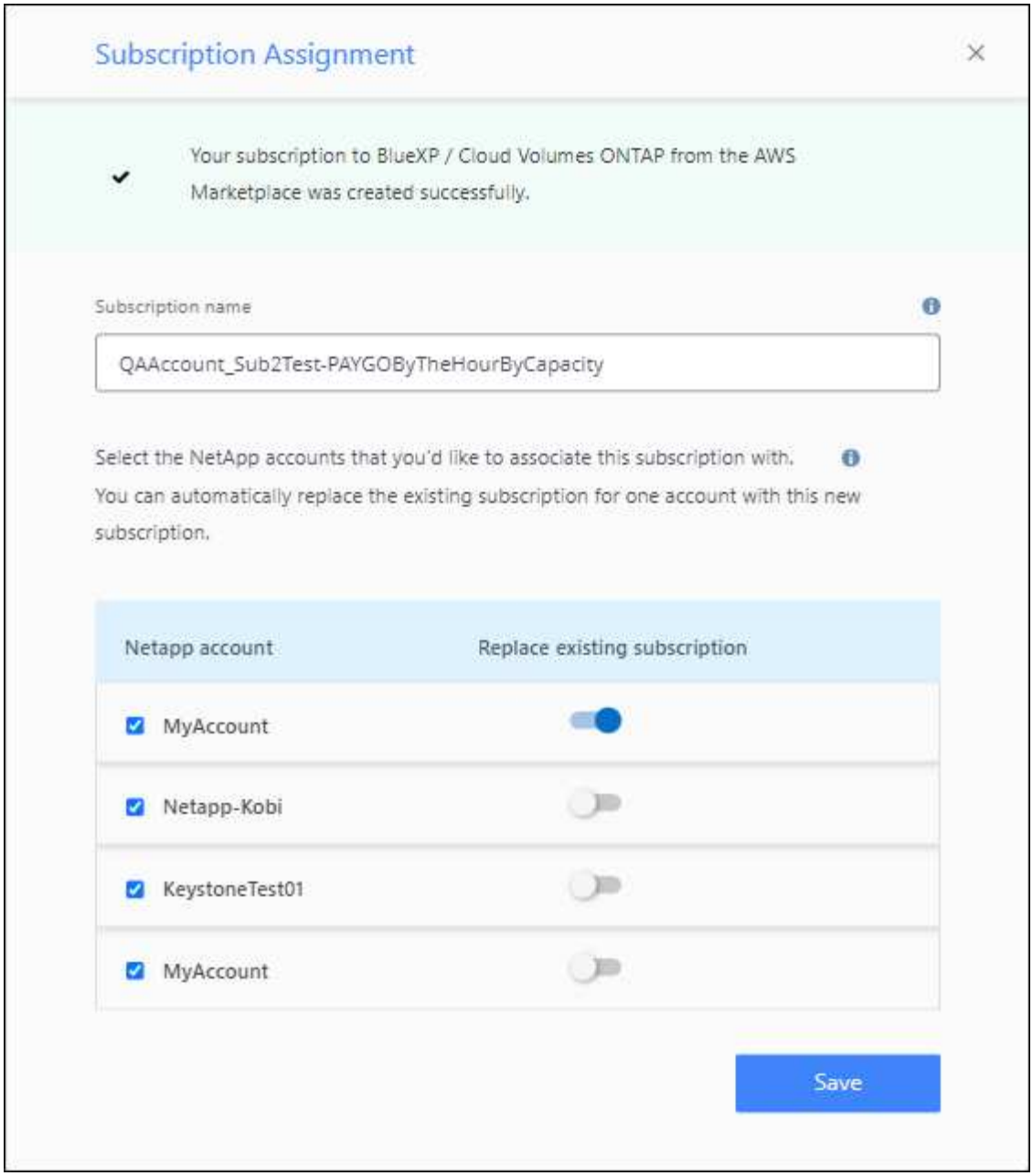
- Na página **Log in**, você será solicitado a inserir o endereço de e-mail associado ao seu login. Depois de

selecionar **seguinte**, o BlueXP  solicita que você se autentique usando o método de autenticação associado ao seu login:

- A senha para suas credenciais de nuvem do NetApp
- Suas credenciais de identidade federadas
- Suas credenciais do site de suporte da NetApp




- Se você é novo no BlueXP  e tem credenciais existentes do site de suporte da NetApp (NSS), então você pode pular a página de inscrição e inserir seu endereço de e-mail diretamente na página de login. O BlueXP  irá inscrevê-lo como parte deste início de sessão inicial.
- Ao assinar o BlueXP  no mercado do seu provedor de nuvem, agora você tem a opção de substituir a assinatura existente por uma conta pela nova assinatura.




  - "Saiba como associar uma assinatura da AWS"
  - "Saiba como associar uma assinatura do Azure"
  - "Saiba como associar uma assinatura do Google Cloud"

- A BlueXP  irá notificá-lo se o seu conetor foi desligado por 14 dias ou mais.
  - "Saiba mais sobre as notificações do BlueXP "
  - "Saiba por que os conetores devem permanecer em funcionamento"
- Atualizamos a política de conetor para o Google Cloud para incluir uma permissão necessária para criar e gerenciar VMs de storage em pares de HA do Cloud Volumes ONTAP:

  compute.instances.updateNetworkInterface

  "Veja as permissões do Google Cloud para o conetor".

- Esta versão do conetor inclui melhorias no Cloud Volumes ONTAP.

  "Saiba mais sobre os aprimoramentos do Cloud Volumes ONTAP"

## 1 de janeiro de 2023

### Conetor 3.9.25

Esta versão do conetor inclui melhorias no Cloud Volumes ONTAP e correções de bugs.

"Saiba mais sobre os aprimoramentos do Cloud Volumes ONTAP"

## 4 de dezembro de 2022

### Conetor 3.9.24

- Atualizamos o URL para o console do BlueXP  https://console.bluexp.netapp.com
- O conetor agora é suportado na região do Google Cloud Israel.
- Esta versão do conetor também inclui aprimoramentos do Cloud Volumes ONTAP e aprimoramentos de cluster do ONTAP no local.
  - "Saiba mais sobre os aprimoramentos do Cloud Volumes ONTAP"
  - "Saiba mais sobre os aprimoramentos de cluster no ONTAP on-premise"

## 6 de novembro de 2022

### Conetor 3.9.23

- As suas subscrições PAYGO e contratos anuais para a BlueXP  estão agora disponíveis para visualizar e gerir a partir da carteira digital.

  "Saiba como gerenciar suas assinaturas"

- Esta versão do conetor também inclui melhorias no Cloud Volumes ONTAP.

  "Saiba mais sobre os aprimoramentos do Cloud Volumes ONTAP"

## 1 de novembro de 2022

### Introdução do BlueXP

O NetApp BlueXP  estende e aprimora as funcionalidades fornecidas pelo Cloud Manager. O BlueXP  é um painel de controle unificado que oferece uma experiência multicloud híbrida para serviços de storage e dados em ambientes locais e de nuvem.

#### Experiência de gerenciamento unificado

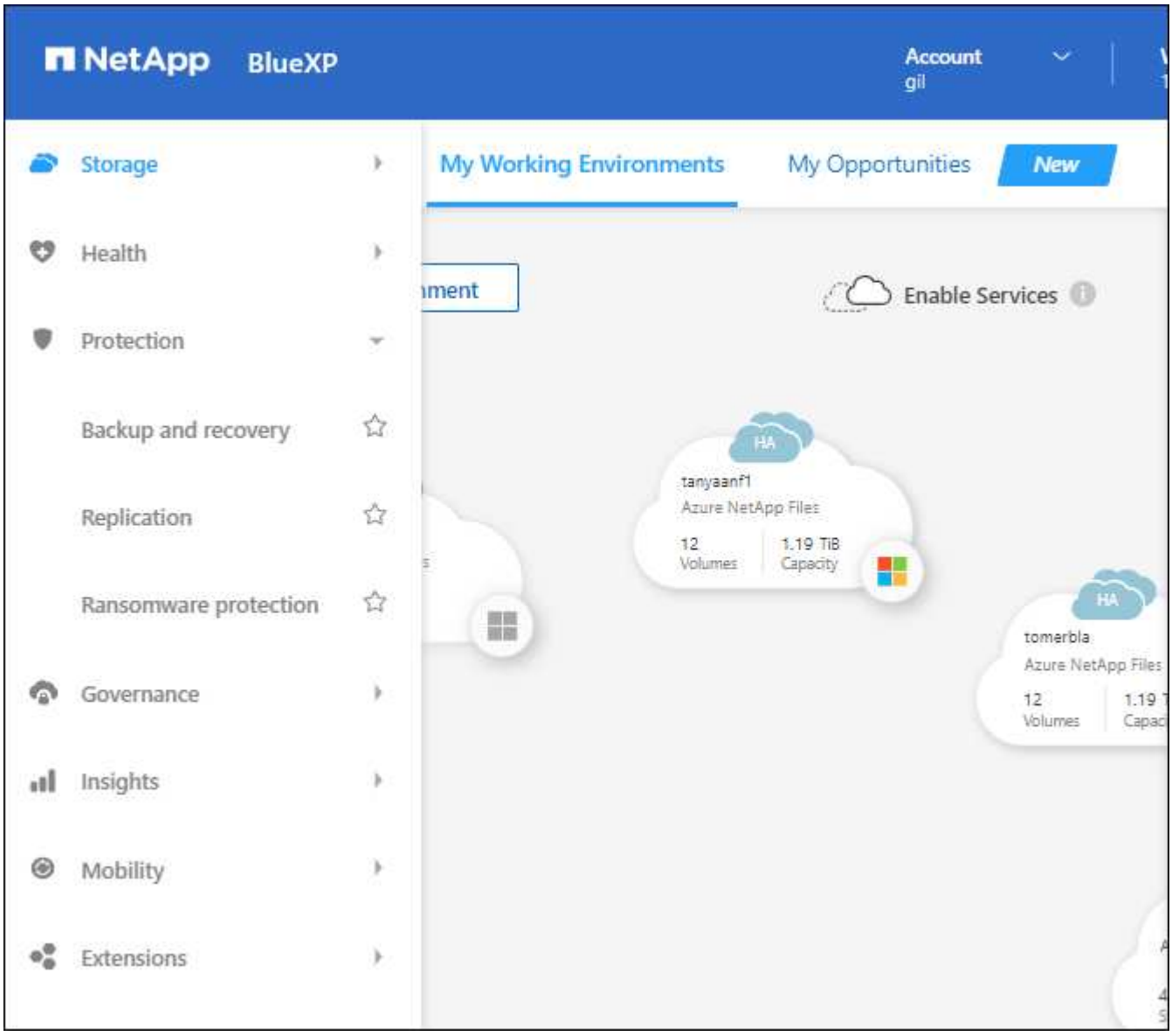
O BlueXP  permite gerenciar todos os ativos de storage e dados em uma única interface.

Use o BlueXP  para criar e administrar storage de nuvem (por exemplo, Cloud Volumes ONTAP e Azure NetApp Files), mover, proteger e analisar dados e controlar muitos dispositivos de storage no local e na borda.

"Saiba mais no site da BlueXP "

### Novo menu de navegação

No menu de navegação do BlueXP , os serviços são agora organizados por categorias e são nomeados de acordo com a sua funcionalidade. Por exemplo, você pode acessar o backup e a recuperação do BlueXP a partir da categoria **proteção**.




### Integrações de novos produtos

- Agora você pode gerenciar os buckets do Amazon S3 nas contas da AWS onde o conetor está instalado.
- Agora, você pode gerenciar mais sistemas de storage no local, como o e-Series e o StorageGRID.
- Agora você pode usar serviços de dados anteriormente disponíveis apenas como um serviço autônomo com uma interface de usuário separada, como o BlueXP  digital ADVISOR (Active IQ).

### Saiba mais

- "Gerenciar buckets do Amazon S3"
- "Gerenciar sistemas de storage e-Series"

- "Gerencie os sistemas de storage StorageGRID"
- "Saiba mais sobre a integração do Digital Advisor"

#### Solicitar a atualização das credenciais do NSS

O Cloud Manager agora solicita que você atualize as credenciais associadas às contas do site de suporte da NetApp quando o token de atualização associado à sua conta expirar após 3 meses. "Saiba como gerenciar contas NSS"

## 18 de setembro de 2022

#### Conetor 3.9.22

- Melhoramos o assistente de implantação do conetor adicionando um *guia no produto* que fornece etapas para atender aos requisitos mínimos para instalação do conetor: Permissões, autenticação e rede.
- Agora você pode criar um caso de suporte do NetApp diretamente do Cloud Manager no **Painel de suporte**.

  "Saiba como criar um caso".

- Esta versão do conetor também inclui melhorias no Cloud Volumes ONTAP.

  "Saiba mais sobre os aprimoramentos do Cloud Volumes ONTAP"

## 31 de julho de 2022

#### Conetor 3.9.21

- Apresentamos uma nova maneira de descobrir os recursos de nuvem que você ainda não está gerenciando no Cloud Manager.

  No Canvas, a guia **Minhas oportunidades** fornece um local centralizado para descobrir os recursos existentes que você pode adicionar ao Cloud Manager para serviços e operações de dados consistentes em sua multicloud híbrida.

  Nesta versão inicial, My Opportunities permite que você descubra os sistemas de arquivos FSX for ONTAP existentes em sua conta da AWS.

  "Saiba como descobrir o FSX for ONTAP usando Minhas oportunidades"

- Esta versão do conetor também inclui melhorias no Cloud Volumes ONTAP.

  "Saiba mais sobre os aprimoramentos do Cloud Volumes ONTAP"

## 15 de julho de 2022

#### Mudanças de política

Atualizamos a documentação adicionando as políticas do Cloud Manager diretamente dentro dos documentos. Isso significa que agora você pode visualizar as permissões necessárias para o conetor e o Cloud Volumes ONTAP ao lado das etapas que descrevem como configurá-los. Essas políticas eram anteriormente acessíveis a partir de uma página no site de suporte da NetApp.

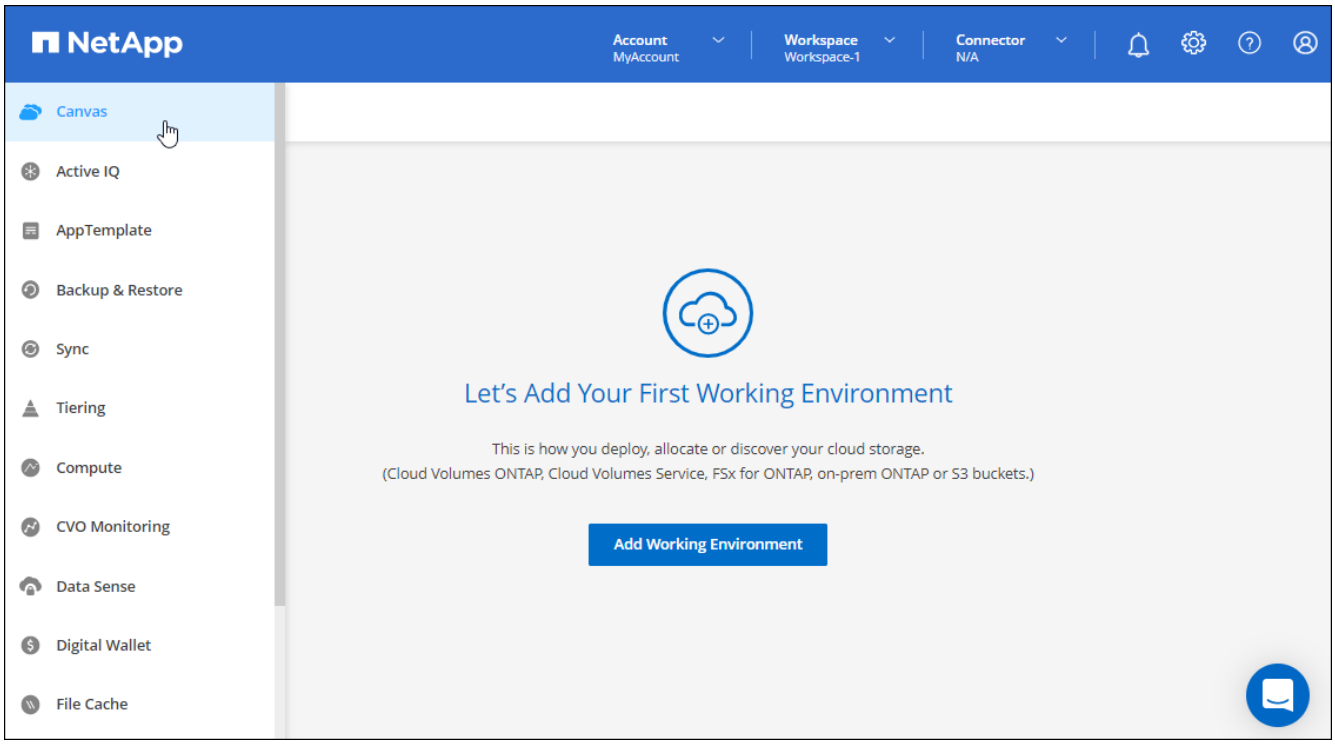
"Aqui está um exemplo que mostra as permissões de função do AWS IAM usadas para criar um conetor".

Também criamos uma página que fornece links para cada uma das políticas. "Veja o resumo das permissões do Cloud Manager".

## 3 de julho de 2022

### Conetor 3.9.20

- Introduzimos uma nova maneira de navegar para a crescente lista de recursos na interface do Cloud Manager. Todos os recursos familiares do Cloud Manager agora podem ser encontrados facilmente, passando o Mouse sobre o painel esquerdo.



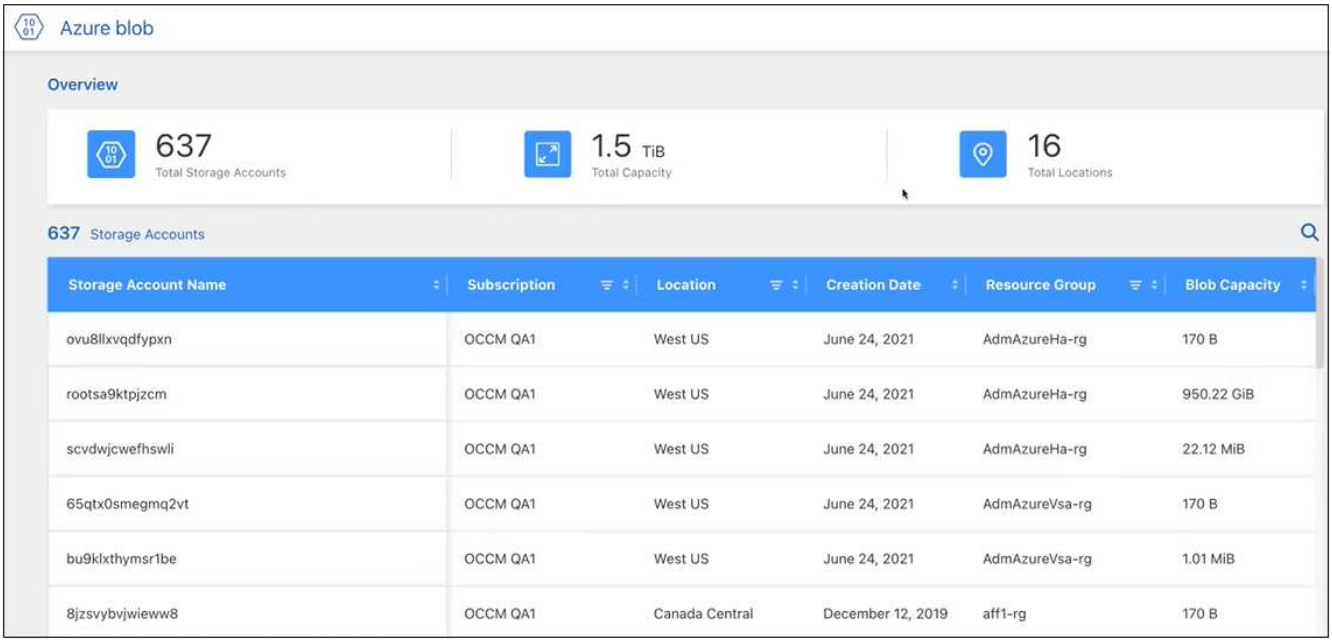

- Agora você pode configurar o Cloud Manager para enviar notificações por e-mail para que você possa ser informado sobre atividades importantes do sistema, mesmo quando não estiver conetado ao sistema.

  "Saiba mais sobre operações de monitoramento em sua conta".

- Agora, o Cloud Manager oferece suporte ao storage Azure Blob e ao Google Cloud Storage como ambientes de trabalho, semelhante ao suporte do Amazon S3.

  Depois de instalar um conector no Azure ou no Google Cloud, o Cloud Manager agora descobre automaticamente informações sobre o storage do Azure Blob na sua assinatura do Azure ou do Google Cloud Storage no projeto em que o conector é instalado. O Cloud Manager exibe o storage de objetos como um ambiente de trabalho que pode ser aberto para exibir informações mais detalhadas.

  Veja um exemplo de um ambiente de trabalho do Blob do Azure:




- Redesenhamos a página recursos para um ambiente de trabalho do Amazon S3 fornecendo informações mais detalhadas sobre buckets do S3, como capacidade, detalhes de criptografia e muito mais.
- O conetor agora é compatível com as seguintes regiões do Google Cloud:
  - Madrid (Europa-southwest1)
  - Paris (Europa-west9)
  - Varsóvia (Europa-central2)
- O conetor agora é suportado na região do Azure West US 3.

  "Veja a lista completa de regiões suportadas"

- Esta versão do conetor também inclui melhorias no Cloud Volumes ONTAP.

  "Saiba mais sobre os aprimoramentos do Cloud Volumes ONTAP"

## 28 de junho de 2022

### Faça login com credenciais NetApp

Quando novos usuários se inscrevem no Cloud Central, eles agora podem selecionar a opção **entrar com o NetApp** para fazer login com suas credenciais do site de suporte da NetApp. Esta é uma alternativa para inserir um endereço de e-mail e uma senha.

Os logins existentes que usam um endereço de e-mail e senha precisam continuar usando esse método de login. A opção entrar com NetApp está disponível para novos usuários que se inscreverem.

## 7 de junho de 2022

### Conetor 3.9.19

- O conetor agora é suportado na região AWS Jakarta (ap-sudeste-3).

- O conetor agora é suportado na região Sudeste do Azure Brasil.

  "Veja a lista completa de regiões suportadas"

- Esta versão do conetor também inclui aprimoramentos do Cloud Volumes ONTAP e aprimoramentos de cluster do ONTAP no local.
  - "Saiba mais sobre os aprimoramentos do Cloud Volumes ONTAP"
  - "Saiba mais sobre os aprimoramentos de cluster no ONTAP on-premise"

## 12 de maio de 2022

### Conetor 3.9.18 patch

Atualizamos o conetor para introduzir correções de bugs. A correção mais notável é um problema que afeta a implantação do Cloud Volumes ONTAP no Google Cloud quando o conetor está em uma VPC compartilhada.

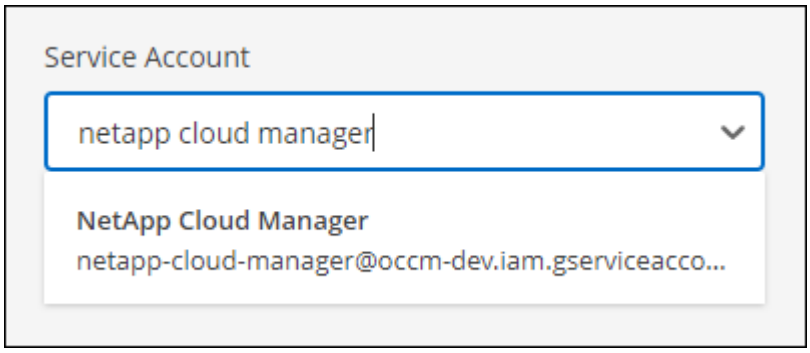
## 2 de maio de 2022

### Conetor 3.9.18

- O conetor agora é compatível com as seguintes regiões do Google Cloud:
  - Delhi (Ásia-south2)
  - Melbourne (austrália-southeast2)
  - Milão (Europa-west8)
  - Santiago (américa do sul-west1)

  "Veja a lista completa de regiões suportadas"

- Quando você seleciona a conta de serviço do Google Cloud a ser usada com o conetor, o Cloud Manager agora exibe o endereço de e-mail associado a cada conta de serviço. A exibição do endereço de e-mail pode facilitar a distinção entre contas de serviço que compartilham o mesmo nome.




- Certificamos o conetor no Google Cloud em uma instância de VM com um sistema operacional compatível "Recursos de VM blindados"
- Esta versão do conetor também inclui melhorias no Cloud Volumes ONTAP. "Saiba mais sobre esses aprimoramentos"
- Novas permissões da AWS são necessárias para que o conetor implante o Cloud Volumes ONTAP.

  As permissões a seguir agora são necessárias para criar um grupo de posicionamento de spread da AWS

ao implantar um par de HA em uma única zona de disponibilidade (AZ):

```
"ec2:DescribePlacementGroups",
"iam:GetRolePolicy",
```

Essas permissões agora são necessárias para otimizar a forma como o Cloud Manager cria o grupo de posicionamento.

Certifique-se de fornecer essas permissões a cada conjunto de credenciais da AWS que você adicionou ao Cloud Manager. "Veja a política do IAM mais recente para o conetor".

## 3 de abril de 2022

### Conetor 3.9.17

- Agora você pode criar um conetor deixando o Cloud Manager assumir uma função do IAM configurada no seu ambiente. Esse método de autenticação é mais seguro do que compartilhar uma chave de acesso da AWS e uma chave secreta.

  "Saiba como criar um conetor usando uma função do IAM".

- Esta versão do conetor também inclui melhorias no Cloud Volumes ONTAP. "Saiba mais sobre esses aprimoramentos"

## 27 de fevereiro de 2022

### Conetor 3.9.16

- Quando você cria um novo conetor no Google Cloud, o Cloud Manager agora exibirá todas as políticas de firewall existentes. Anteriormente, o Cloud Manager não exibiria nenhuma política que não tivesse uma tag de destino.
- Esta versão do conetor também inclui melhorias no Cloud Volumes ONTAP. "Saiba mais sobre esses aprimoramentos"

## 30 de janeiro de 2022

### Conetor 3.9.15

Esta versão do conetor inclui melhorias no Cloud Volumes ONTAP. "Saiba mais sobre esses aprimoramentos"

## 2 de janeiro de 2022

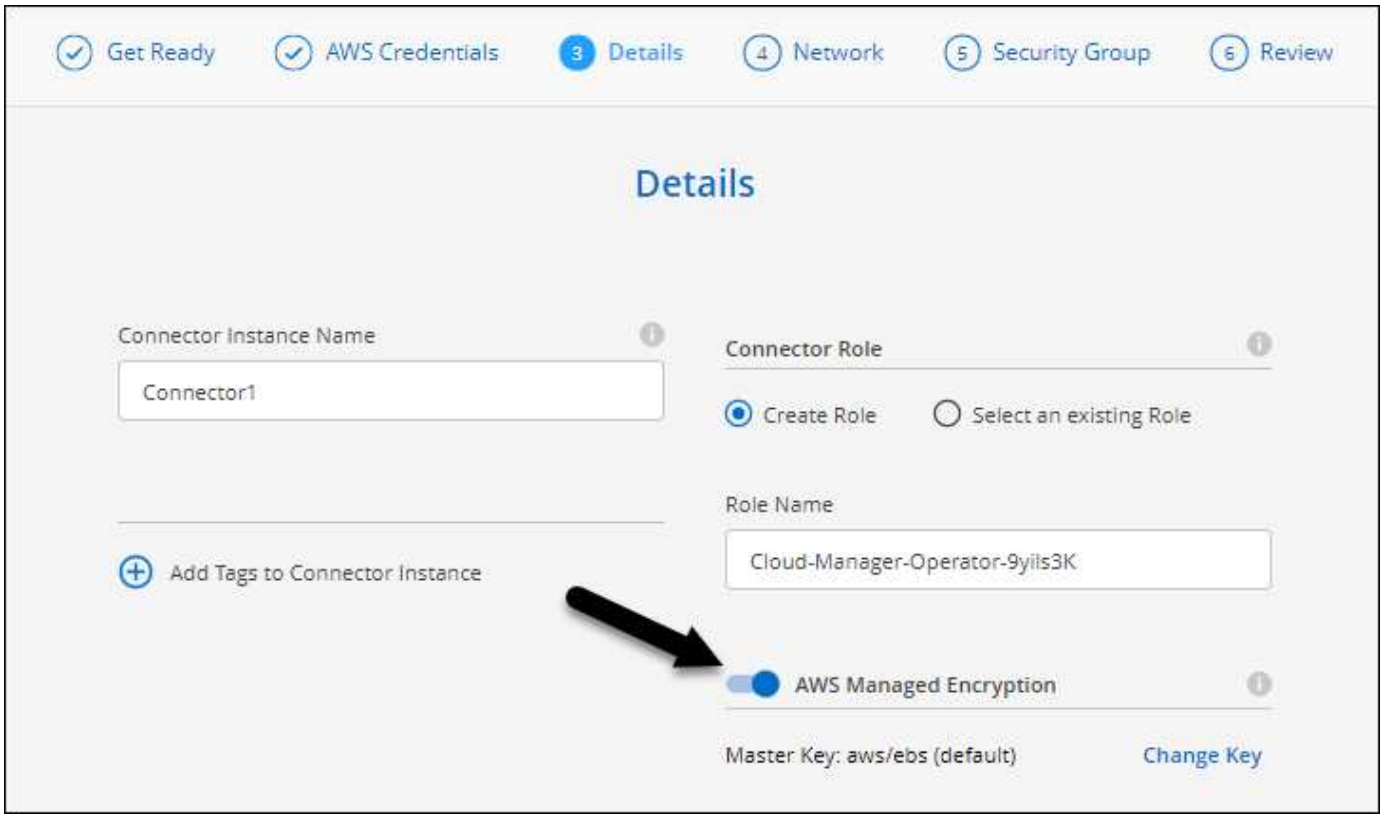
### Pontos finais reduzidos para o conetor

Reduzimos o número de endpoints que um conetor precisa entrar em Contato para gerenciar recursos e processos em seu ambiente de nuvem pública.

"Veja a lista de endpoints necessários"

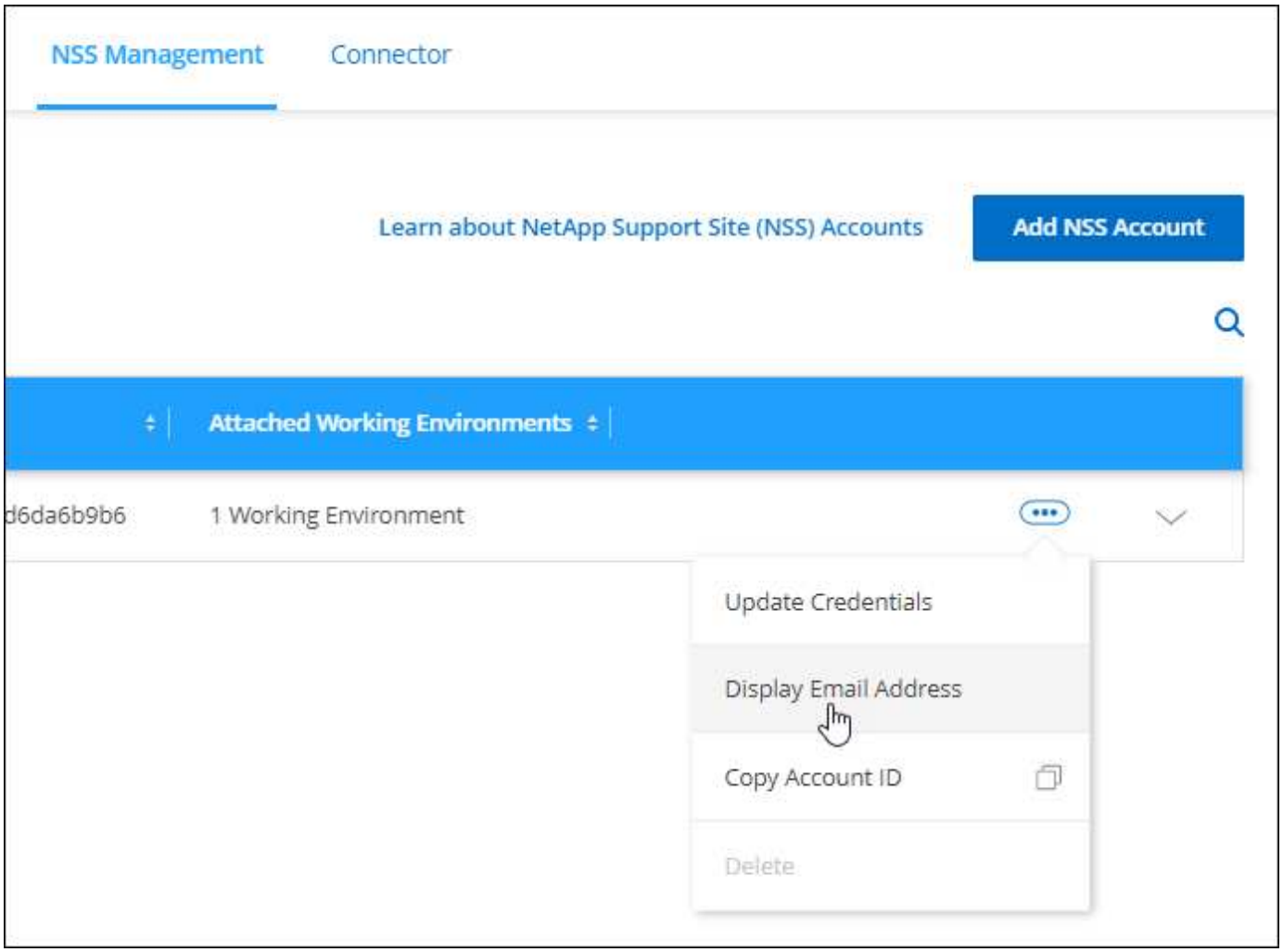
### Encriptação do disco EBS para o conetor

Ao implantar um novo conetor no AWS a partir do Cloud Manager, agora você pode optar por criptografar os discos EBS do conetor usando a chave mestra padrão ou uma chave gerenciada.




### Endereço de e-mail para contas NSS

Agora, o Cloud Manager pode exibir o endereço de e-mail associado a uma conta do site de suporte da NetApp.




## 28 de novembro de 2021

**Atualização necessária para contas do site de suporte da NetApp**

A partir de dezembro de 2021, o NetApp agora usa o Microsoft Azure ative Directory como provedor de identidade para serviços de autenticação específicos para suporte e licenciamento. Como resultado desta atualização, o Cloud Manager solicitará que você atualize as credenciais de quaisquer contas existentes do site de suporte da NetApp que você adicionou anteriormente.

Se você ainda não migrou sua conta NSS para IDaaS, primeiro você precisa migrar a conta e, em seguida, atualizar suas credenciais no Cloud Manager.

"Saiba mais sobre o uso do ative Directory do NetApp para gerenciamento de identidades"

**Alterar contas NSS para Cloud Volumes ONTAP**

Se a sua organização tiver várias contas do site de suporte da NetApp, agora você pode alterar qual conta está associada a um sistema Cloud Volumes ONTAP.

"Saiba como anexar um ambiente de trabalho a uma conta NSS diferente".

## 4 de novembro de 2021

### Certificação SOC 2 tipo 2

Uma empresa de contabilidade pública e um auditor de serviços certificado independente examinou o Cloud Manager, o Cloud Sync, o Cloud Tiering, o Cloud Data Sense e o Cloud Backup (plataforma Cloud Manager) e afirmou que eles alcançaram relatórios SOC 2 tipo 2 com base nos critérios de Serviços de confiança aplicáveis.

"Veja os relatórios SOC 2 da NetApp".

### O conetor não é mais suportado como proxy

Você não pode mais usar o Cloud Manager Connector como um servidor proxy para enviar mensagens AutoSupport do Cloud Volumes ONTAP. Esta funcionalidade foi removida e já não é suportada. Você precisará fornecer conetividade AutoSupport por meio de uma instância NAT ou dos serviços proxy do seu ambiente.

"Saiba mais sobre como verificar o AutoSupport com o Cloud Volumes ONTAP"

## 31 de outubro de 2021

### Autenticação com o responsável pelo serviço

Quando você cria um novo conetor no Microsoft Azure, agora você pode autenticar com um responsável de serviço do Azure, em vez de com as credenciais da conta do Azure.

"Saiba como autenticar com um diretor de serviço do Azure".

### Aprimoramento de credenciais

Redesenhamos a página credenciais para facilitar o uso e corresponder à aparência atual da interface do Cloud Manager.

## 2 de setembro de 2021

### Foi adicionado um novo Serviço de notificação

O serviço de notificação foi introduzido para que você possa visualizar o status das operações do Cloud Manager iniciadas durante a sessão de login atual. Você pode verificar se a operação foi bem-sucedida ou se ela falhou. "Veja como monitorar operações em sua conta".

## 7 de julho de 2021

### Melhorias no assistente Adicionar conetor

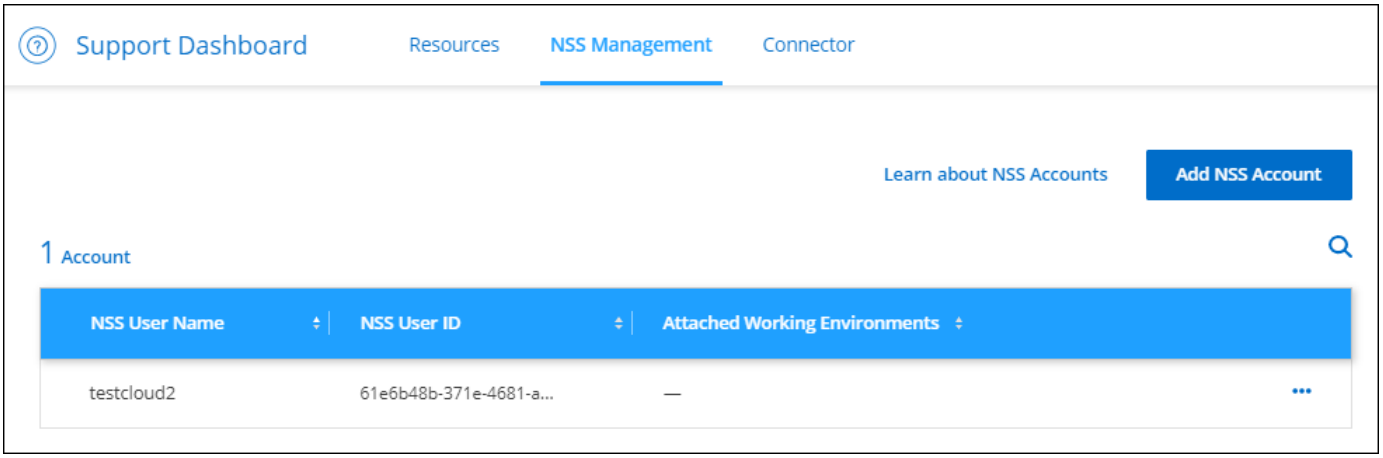
Redesenhamos o assistente **Add Connector** para adicionar novas opções e facilitar o uso. Agora você pode adicionar tags, especificar uma função (para AWS ou Azure), carregar um certificado raiz para um servidor proxy, exibir código para automação do Terraform, exibir detalhes de progresso e muito mais.

- "Crie um conetor na AWS"
- "Crie um conetor no Azure"
- "Crie um conetor no Google Cloud"

### Gerenciamento de contas NSS no Painel de suporte

As contas do site de suporte da NetApp (NSS) agora são gerenciadas a partir do painel de suporte, em vez do menu Configurações. Essa alteração facilita a localização e o gerenciamento de todas as informações relacionadas ao suporte a partir de um único local.

"Saiba como gerenciar contas NSS".




## 5 de maio de 2021

### Contas na linha do tempo

A linha do tempo no Cloud Manager agora mostra ações e eventos relacionados ao gerenciamento de contas. As ações incluem coisas como associar usuários, criar espaços de trabalho e criar conetores. Verificar a linha do tempo pode ser útil se você precisar identificar quem executou uma ação específica ou se precisar identificar o status de uma ação.

"Saiba como filtrar a linha do tempo para o serviço de alocação".

## 11 de abril de 2021

### A API chama diretamente para o Cloud Manager

Se você configurou um servidor proxy, agora você pode habilitar uma opção para enviar chamadas de API diretamente para o Cloud Manager sem passar pelo proxy. Essa opção é compatível com conetores executados na AWS ou no Google Cloud.

"Saiba mais sobre esta definição".

### Usuários de conta de serviço

Agora você pode criar um usuário de conta de serviço.

Uma conta de serviço atua como um "usuário" que pode fazer chamadas de API autorizadas para o Cloud Manager para fins de automação. Isso torna mais fácil gerenciar a automação porque você não precisa criar scripts de automação com base na conta de usuário de uma pessoa real que pode sair da empresa a qualquer momento. E se você estiver usando federação, você pode criar um token sem gerar um token de atualização a partir da nuvem.

"Saiba mais sobre como usar contas de serviço".

### Pré-visualizações privadas

Agora você pode permitir que visualizações privadas em sua conta tenham acesso a novos serviços de nuvem do NetApp, já que eles são disponibilizados como uma prévia no Cloud Manager.

"Saiba mais sobre esta opção".

### Serviços de terceiros

Você também pode permitir que serviços de terceiros em sua conta tenham acesso a serviços de terceiros que estão disponíveis no Cloud Manager.

"Saiba mais sobre esta opção".

## 8 de março de 2021

Esta atualização inclui melhorias para vários recursos e serviços.

### Melhorias no Cloud Volumes ONTAP

Esta versão do Cloud Manager inclui melhorias no gerenciamento do Cloud Volumes ONTAP.

#### Aprimoramento disponível em todos os provedores de nuvem

O Cloud Manager agora pode implantar e gerenciar o Cloud Volumes ONTAP 9,9.0.

"Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP".

#### Aprimoramentos disponíveis na AWS

- Agora você pode implantar o Cloud Volumes ONTAP 9,8 no ambiente de Serviços de nuvem comerciais da AWS (C2S).

  "Saiba como começar em C2S"

- O Cloud Manager sempre permitiu que você criptografasse dados do Cloud Volumes ONTAP usando o AWS Key Management Service (KMS). A partir do Cloud Volumes ONTAP 9,9.0, os dados em discos EBS e dados dispostos em camadas em S3 são criptografados se você selecionar um CMK gerenciado pelo cliente. Anteriormente, apenas os dados do EBS seriam criptografados.

  Observe que você precisará fornecer à função Cloud Volumes ONTAP IAM acesso para usar o CMK.

  "Saiba mais sobre como configurar o AWS KMS com o Cloud Volumes ONTAP"

#### Aprimoramento disponível no Azure

Agora você pode implantar o Cloud Volumes ONTAP 9,8 no nível de impacto do Departamento de Defesa do Azure (DoD) 6 (IL6).

#### Melhorias disponíveis no Google Cloud

- Reduzimos o número de endereços IP necessários para o Cloud Volumes ONTAP 9,8 e posterior no Google Cloud. Por padrão, um endereço IP a menos é necessário (nós unificamos o LIF entre clusters com o LIF de gerenciamento de nós). Você também tem a opção de ignorar a criação do LIF de gerenciamento de SVM ao usar a API, o que reduziria a necessidade de um endereço IP adicional.

  "Saiba mais sobre os requisitos de endereço IP no Google Cloud"

- Ao implantar um par de HA do Cloud Volumes ONTAP no Google Cloud, você pode escolher VPCs compartilhados para VPC-1, VPC-2 e VPC-3. Anteriormente, apenas a VPC-0 poderia ser uma VPC compartilhada. Esta alteração é suportada com o Cloud Volumes ONTAP 9,8 e posterior.

  "Saiba mais sobre os requisitos de rede do Google Cloud"

### Melhorias no conetor

- O Cloud Manager agora notifica os usuários Admin por meio de um e-mail quando um conetor não está sendo executado.

  Manter seus conetores ativos e em funcionamento ajuda a garantir o melhor gerenciamento do Cloud Volumes ONTAP e de outros serviços de nuvem da NetApp.

- O Cloud Manager agora exibe uma notificação se você precisar alterar o tipo de instância do seu conetor.

  Alterar o tipo de instância garante que você possa usar os novos recursos e recursos que você está faltando no momento.

### Melhorias no Cloud Sync

- O Cloud Sync agora suporta relações de sincronização entre o armazenamento ONTAP S3 e os servidores SMB:
  - Armazenamento ONTAP S3 para um servidor SMB
  - Um servidor SMB para o armazenamento ONTAP S3

    "Exibir relacionamentos de sincronização suportados"

- O Cloud Sync agora permite unificar a configuração de um grupo de corretores de dados diretamente da interface do usuário.

  Não recomendamos alterar a configuração por conta própria. Você deve consultar o NetApp para entender quando alterar a configuração e como alterá-la.

  "Saiba mais sobre como definir uma configuração unificada"

### Melhorias no Cloud Tiering

- Ao dispor em camadas no Google Cloud Storage, você pode aplicar uma regra de ciclo de vida para que os dados em camadas façam a transição da classe de storage padrão para o storage Nearline, Coldline ou Archive de baixo custo após 30 dias.
- A disposição em camadas na nuvem agora é exibida se você tiver clusters ONTAP no local não descobertos para que você possa adicioná-los ao Cloud Manager para habilitar a disposição em categorias ou outros serviços nesses clusters.

  "Saiba como descobrir esses clusters adicionais"

### Melhorias no Azure NetApp Files

Agora você pode alterar dinamicamente o nível de serviço de um volume para atender às necessidades de workload e otimizar seus custos. O volume é movido para o outro pool de capacidade sem afetar o volume. "Saiba mais"

## 9 de fevereiro de 2021

### Melhorias no painel de suporte

Atualizamos o Painel de suporte permitindo que você adicione suas credenciais do site de suporte da NetApp, que o Registra para obter suporte. Você também pode iniciar um caso de suporte da NetApp diretamente no painel. Basta clicar no ícone Ajuda e, em seguida, **suporte**.

# Limitações conhecidas

As limitações conhecidas identificam plataformas, dispositivos ou funções que não são suportadas por esta versão do produto ou que não interoperam corretamente com ele. Revise essas limitações com cuidado.

Essas limitações são específicas para a configuração e administração do BlueXP : O conetor, a plataforma de software como serviço (SaaS) e muito mais.

## Limitações do conetor

### Servidores proxy transparentes não são suportados

O BlueXP  não suporta servidores proxy transparentes com o conetor.

"Saiba mais sobre como usar um servidor proxy com o conetor".

### Possível conflito com endereços IP no intervalo 172

O BlueXP  implanta o conetor com duas interfaces que têm endereços IP nos intervalos 172.17.0.0/16 e 172.18.0.0/16.

Se a rede tiver uma sub-rede configurada com qualquer um desses intervalos, poderá ocorrer falhas de conetividade do BlueXP . Por exemplo, a descoberta de clusters ONTAP no local no BlueXP  pode falhar.

Consulte o artigo da base de dados de Conhecimento "Conflito de IP do conetor BlueXP  com a rede existente"para obter instruções sobre como alterar o endereço IP das interfaces do conetor.

### A descriptografia SSL não é suportada

O BlueXP  não suporta configurações de firewall que tenham a descriptografia SSL ativada. Se a descriptografia SSL estiver ativada, as mensagens de erro aparecerão no BlueXP  e a instância do conetor será exibida como inativa.

Para uma segurança melhorada, tem a opção de "Instalar um certificado HTTPS assinado por uma autoridade de certificação (CA)".

### Página em branco ao carregar a IU local

Se você carregar o console baseado na Web que está sendo executado em um conetor, a interface pode não ser exibida às vezes, e você apenas obtém uma página em branco.

Este problema está relacionado a um problema de armazenamento em cache. A solução alternativa é usar uma sessão anônima ou privada do navegador da Web.

**Hosts Linux compartilhados não são suportados**

O conetor não é suportado em uma VM compartilhada com outros aplicativos. A VM deve ser dedicada ao software do conetor.

**agentes e extensões de 3rd partes**

Agentes de 3rd partes ou extensões de VM não são suportados na VM do conetor.

# Alterações nos sistemas operacionais Linux suportados

À medida que adicionamos e removemos suporte para o conetor em sistemas operacionais Linux específicos, você pode ter dúvidas sobre como esse suporte afeta suas implantações de conetores existentes.

## Sistemas operacionais suportados

O conetor BlueXP  é compatível com os seguintes sistemas operacionais Linux.

**Modo padrão**

**Instalação manual**

- Ubuntu 24,04 LTS
- Ubuntu 22,04 LTS
- Red Hat Enterprise Linux
  - 8,6 a 8,10
  - 9,1 a 9,4

**Implantação da BlueXP**

Ubuntu 22,04 LTS

**Implantação no AWS Marketplace**

Ubuntu 22,04 LTS

**Implantação a partir do Azure Marketplace**

Ubuntu 22,04 LTS

**Modo restrito**

**Instalação manual**

- Ubuntu 24,04 LTS
- Ubuntu 22,04 LTS
- Red Hat Enterprise Linux
  - 8,6 a 8,10
  - 9,1 a 9,4

**Implantação no AWS Marketplace**

Ubuntu 22,04 LTS

**Implantação a partir do Azure Marketplace**

Ubuntu 22,04 LTS

**Modo privado**

**Instalação manual**

- Ubuntu 22,04 LTS
- Red Hat Enterprise Linux
  - 8,6 a 8,10
  - 9,1 a 9,4

## Suporte para RHEL 8 e 9

Observe o seguinte sobre o suporte para RHEL 8 e 9:

**Limitações**

- Quando o conetor é instalado em um host RHEL 8 ou 9, o backup e a recuperação do BlueXP  têm limitações relacionadas à restauração de um único arquivo e à verificação de ransomware. Para obter

mais informações, consulte "Limitações conhecidas para backup e recuperação do BlueXP "

- A classificação BlueXP  é suportada se você instalar o conetor em um host RHEL 8 ou 9 que reside no local. Não será compatível se o host RHEL 8 ou 9 residir na AWS, Azure ou Google Cloud.

**Ferramenta de orquestração de contêineres**

O Podman é necessário como a ferramenta de orquestração de contentores quando você instala o conetor em um host RHEL 8 ou 9. O Docker Engine não é compatível com RHEL 8 e 9.

**Modo de implantação**

RHEL 8 e 9 são suportados quando se usa BlueXP  no modo padrão, modo restrito e modo privado.

**Versões de conetor suportadas**

RHEL 8 e 9 são suportados a partir das seguintes versões do conetor:

- 3.9.40 ao utilizar o BlueXP  no modo padrão ou no modo restrito
- 3.9.42 ao usar o BlueXP  no modo privado

**Apenas novas instalações manuais**

RHEL 8 e 9 são suportados com instalações *new* Connector ao instalar manualmente o conetor em hosts executados em suas instalações ou na nuvem.

**Atualizações RHEL**

Se você tiver um conetor existente em execução em um host RHEL 7, não suportaremos a atualização do sistema operacional RHEL 7 para RHEL 8 ou 9. Saiba mais sobre os conetores existentes no RHEL 7 ou CentOS 7.

## Fim do suporte para RHEL 7 e CentOS 7

Em 30 de junho de 2024, o RHEL 7 chegou ao fim da manutenção (MOE), enquanto o CentOS 7 chegou ao fim da vida útil (EOL). O NetApp parou de suportar o conetor nessas distribuições Linux em 30 de junho de 2024.

"Red Hat: O que saber sobre o fim da manutenção do Red Hat Enterprise Linux 7"

### Conetores existentes no RHEL 7 ou CentOS 7

Se você tiver um conetor existente em execução no RHEL 7 ou CentOS 7, não suportaremos a atualização ou conversão do sistema operacional para RHEL 8 ou 9. Para começar a executar um conetor em um host RHEL 8 ou 9, você precisa fazer o seguinte:

1. Configure um host RHEL 8 ou 9.
2. Instale o Podman.
3. Execute uma instalação do conetor *new*.
4. Configure o conetor para descobrir os ambientes de trabalho que o conetor antigo gerenciava.

## Links relacionados

### Como começar a usar o RHEL 8 e 9

Consulte as páginas a seguir para obter detalhes sobre os requisitos do host, os requisitos do Podman e as etapas para instalar o Podman e o conetor:

**Modo padrão**

- "Instale e configure um conetor no local"
- "Instale manualmente o conetor na AWS"
- "Instale manualmente o conetor no Azure"
- "Instale manualmente o conetor no Google Cloud"

**Modo restrito**

"Prepare-se para a implantação no modo restrito"

**Modo privado**

"Prepare-se para a implantação no modo privado"

### Como redescobrir seus ambientes de trabalho

Consulte as páginas a seguir para redescobrir seus ambientes de trabalho após uma nova implantação do conetor.

- "Adicione sistemas Cloud Volumes ONTAP existentes ao BlueXP "
- "Descubra clusters ONTAP no local"
- "Crie ou descubra um ambiente de trabalho do FSX for ONTAP"
- "Crie um ambiente de trabalho Azure NetApp Files"
- "Descubra os sistemas e-Series"
- "Descubra os sistemas StorageGRID"

# Comece agora

## Aprenda o básico

### Saiba mais sobre o BlueXP

O NetApp BlueXP  oferece à sua organização um único painel de controle que ajuda a criar, proteger e governar os dados em ambientes locais e de nuvem. A plataforma software como serviço (SaaS) da BlueXP  inclui serviços que fornecem gerenciamento de storage, mobilidade de dados, proteção de dados e análise e controle. Os recursos de gerenciamento são fornecidos por meio de um console e APIs baseados na Web.

#### Caraterísticas

O BlueXP  fornece controle unificado do storage na multicloud híbrida e nos serviços de dados integrados para proteger, proteger e otimizar os dados.

##### Controle unificado do armazenamento a partir da tela BlueXP

A tela *BlueXP*  permite que você descubra, implante, otimize e gerencie o armazenamento na nuvem e no local. A tela fornece um único local para todo o gerenciamento de armazenamento.

#### Storage de nuvem e no local compatível

O BlueXP  permite gerenciar os seguintes tipos de storage a partir da tela BlueXP :

**Soluções de storage em nuvem**

- Amazon FSX para NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP

**Storage de objetos e flash no local**

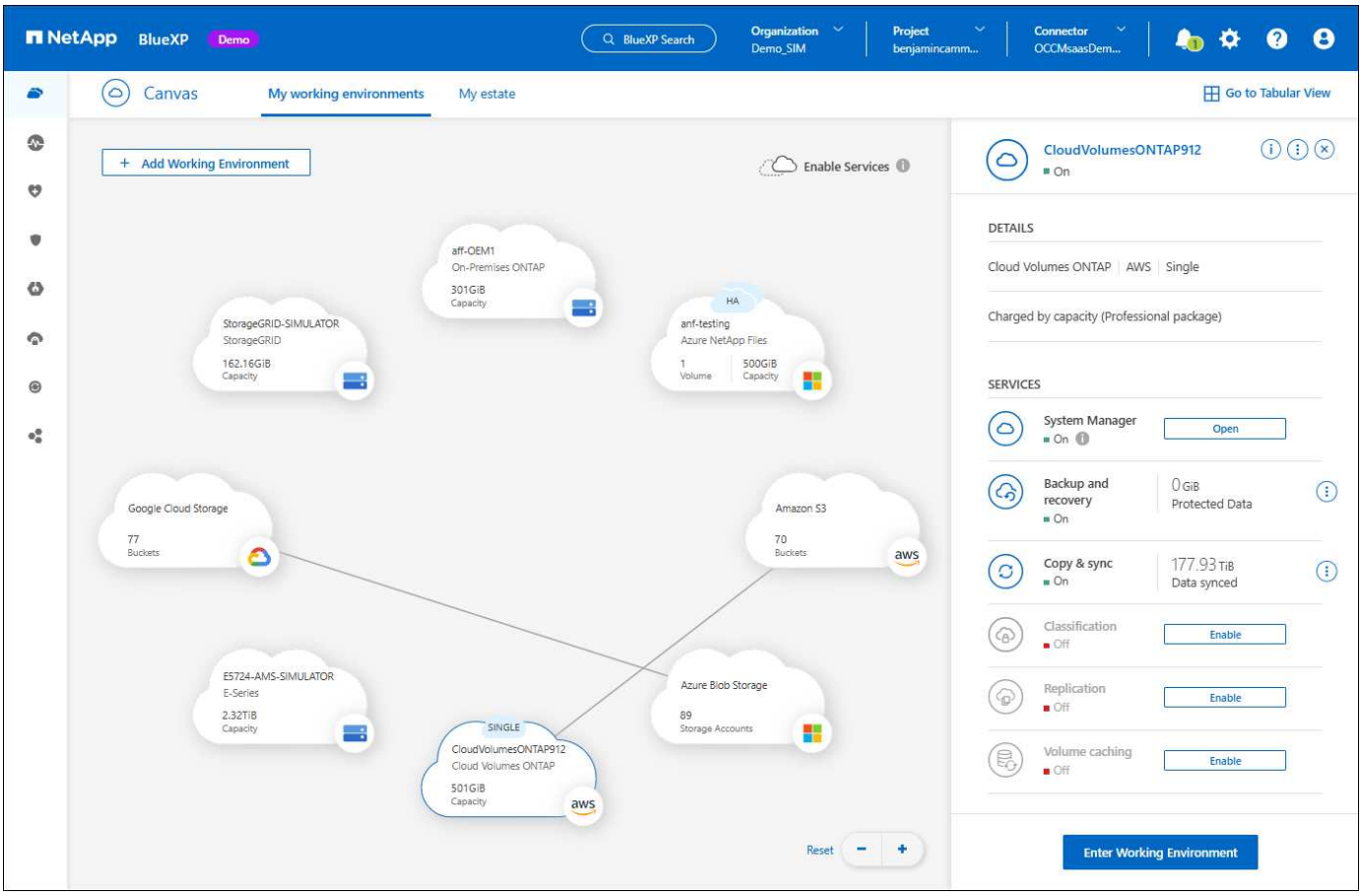
- Sistemas e-Series
- Clusters de ONTAP
- Sistemas StorageGRID

**Storage de objetos na nuvem**

- Storage Amazon S3
- Storage Azure Blob
- Google Cloud Storage

#### Gerenciamento de storage a partir de ambientes de trabalho

Na tela do BlueXP , *ambientes de trabalho* representam o storage de nuvem e no local que você descobriu ou implantou. Você pode selecionar um ambiente de trabalho e integrá-lo aos serviços de dados do BlueXP  ou entrar no ambiente de trabalho para concluir ações de gerenciamento de storage, como a adição de volumes.




**Serviços integrados para proteger, proteger e otimizar dados**

O BlueXP  inclui um pacote abrangente de serviços de dados integrados para ajudar você a manter a segurança, integridade e disponibilidade dos dados em ambientes de storage de nuvem e no local.

### Alertas do BlueXP

Veja problemas relacionados à capacidade, disponibilidade, performance, proteção e segurança no seu ambiente ONTAP.

### Catálogo de automação da BlueXP

Use soluções com script para automatizar a implantação e a integração de produtos e serviços da NetApp.

### Backup e recuperação do BlueXP

Faça backup e restauração de dados na nuvem e no local.

### Classificação BlueXP

Prepare sua privacidade nos ambientes de nuvem e dados de aplicações.

### Operações de nuvem da BlueXP

Obtenha visibilidade dos gastos da computação em nuvem e identifique possíveis economias.

### Cópia e sincronização do BlueXP

Sincronize dados entre armazenamentos de dados no local e na nuvem.

**Consultor digital da BlueXP**

Use análises preditivas e suporte proativo para otimizar a infraestrutura de dados.

**Carteira digital BlueXP**

Gerencie e monitore suas licenças e assinaturas.

**Recuperação de desastres da BlueXP**

Proteja workloads da VMware no local usando o VMware Cloud no Amazon FSX for ONTAP como um site de recuperação de desastres.

**Eficiência econômica da BlueXP**

Identificar clusters com baixa capacidade atual ou prevista e implementar categorias de dados ou recomendações de capacidade adicional.

**Resiliência operacional da BlueXP**

Implemente correções automatizadas de risco de configuração de software e firmware para manter a integridade dos clusters do ONTAP.

**Proteção contra ransomware da BlueXP**

Detectar anomalias que possam resultar em ataques de ransomware. Proteja e recupere workloads.

**Replicação BlueXP**

Replique dados entre sistemas de storage para dar suporte a backup e recuperação de desastres.

**Atualizações de software BlueXP**

Automatize a avaliação, o Planejamento e a execução de atualizações do ONTAP.

**Painel de sustentabilidade do BlueXP**

Analise a sustentabilidade dos seus sistemas de storage.

**Disposição em camadas do BlueXP**

Estenda seu storage ONTAP no local para a nuvem.

**Armazenamento em cache de volume BlueXP**

Crie um volume de cache gravável para acelerar o acesso aos dados ou descarregar o tráfego de volumes acessados com muita facilidade.

**Carga de trabalho de fábrica da BlueXP**

Crie, configure e opere as principais cargas de trabalho usando o Amazon FSX for NetApp ONTAP.

"Saiba mais sobre o BlueXP  e os serviços de dados disponíveis"

### Fornecedores de nuvem compatíveis

O BlueXP  permite que você gerencie o storage de nuvem e use serviços de nuvem no Amazon Web Services, no Microsoft Azure e no Google Cloud.

### Custo

O preço do BlueXP  depende dos serviços que você planeja usar. "Saiba mais sobre os preços do BlueXP "

## Como o BlueXP  funciona

O BlueXP  inclui um console baseado na Web fornecido pela camada SaaS, um sistema de gerenciamento de recursos e acessos, conetores que gerenciam ambientes de trabalho e habilitam serviços em nuvem da BlueXP  e diferentes modos de implantação para atender aos requisitos de negócios.

#### Software como serviço

O BlueXP  é acessível por meio de APIs a "console baseado na web" e. Essa experiência SaaS permite que você acesse automaticamente os recursos mais recentes à medida que são lançados e alterne facilmente entre suas organizações, projetos e conetores BlueXP .

#### Gerenciamento de identidade e acesso do BlueXP  (IAM)

O BlueXP  Identity and Access Management (IAM) é um modelo de gerenciamento de recursos e acessos que fornece gerenciamento granular de recursos e permissões:

- Uma *organização* de nível superior permite que você gerencie o acesso em seus vários *projetos*
- *Pastas* permitem agrupar projetos relacionados
- O gerenciamento de recursos permite associar um recurso a uma ou mais pastas ou projetos
- O gerenciamento de acesso permite que você atribua uma função a membros em diferentes níveis da hierarquia da organização

O BlueXP  IAM é suportado ao usar o BlueXP  no modo padrão. Se você estiver usando o BlueXP  no modo restrito ou privado, use uma conta *BlueXP*  para gerenciar espaços de trabalho, usuários e recursos.

- "Saiba mais sobre o BlueXP  IAM"
- "Saiba mais sobre as contas do BlueXP "

#### Conetores

Você não precisa de um conetor para começar a usar o BlueXP , mas precisará criar um conetor para desbloquear todos os recursos e serviços do BlueXP . Um conetor permite o gerenciamento de recursos e processos em ambientes locais e de nuvem. É necessário gerenciar ambientes de trabalho (por exemplo, Cloud Volumes ONTAP) e usar muitos serviços BlueXP .

"Saiba mais sobre conetores".

#### Modos de implantação

O BlueXP  oferece três modos de implantação. *Modo padrão* utiliza a camada de software como serviço (SaaS) da BlueXP  para fornecer funcionalidade completa. Se o seu ambiente tiver restrições de segurança e conetividade, o *modo restrito* e o *modo privado* limitam a conetividade de saída à camada SaaS do BlueXP .

"Saiba mais sobre os modos de implantação do BlueXP".

## Certificação SOC 2 tipo 2

Uma empresa de contabilidade pública certificada independente e auditor de serviços examinou a BlueXP  e afirmou que alcançou relatórios SOC 2 tipo 2 com base nos critérios de Serviços de confiança aplicáveis.

"Veja os relatórios SOC 2 da NetApp"

## Saiba mais sobre conetores

Um *Connector* é um software NetApp executado em sua rede na nuvem ou na rede local. Ele executa as ações que o BlueXP  precisa executar para gerenciar sua infraestrutura de dados. O conetor constantemente pesquisa a camada de software como serviço (SaaS) da BlueXP  para qualquer ação que precise ser executada. Você não precisa de um conetor para começar a usar o BlueXP , mas precisará criar um conetor para desbloquear todos os recursos e serviços do BlueXP .

### O que você pode fazer sem um conetor

Não é necessário um conetor para começar a usar o BlueXP . Você pode usar vários recursos e serviços no BlueXP  sem nunca criar um conetor.

Você pode usar os seguintes recursos e serviços do BlueXP  sem um conetor:

- Amazon FSX para NetApp ONTAP

  Algumas ações exigem um conetor ou um link de fábrica da carga de trabalho do BlueXP . "Saiba quais ações exigem um conetor ou link"

- Catálogo de automação
- Azure NetApp Files

  Embora um conetor não seja necessário para configurar e gerenciar Azure NetApp Files, um conetor é necessário se você quiser usar a classificação BlueXP  para digitalizar dados Azure NetApp Files.

- Cloud Volumes Service para Google Cloud
- Copiar e sincronizar
- Consultor digital
- Carteira digital

  Em quase todos os casos, você pode adicionar uma licença à carteira digital sem um conetor.

  A única vez que um conetor é necessário para adicionar uma licença à carteira digital é para licenças Cloud Volumes ONTAP *node-based*. Neste caso, é necessário um conetor porque os dados são retirados das licenças instaladas em sistemas Cloud Volumes ONTAP.

- Detecção direta de clusters ONTAP no local

  Embora um conetor não seja necessário para a descoberta direta de um cluster ONTAP no local, um conetor é necessário se você quiser aproveitar os recursos adicionais do BlueXP .

  "Saiba mais sobre as opções de descoberta e gerenciamento para clusters ONTAP no local"

- Atualizações de software
- Sustentabilidade
- Fábrica de carga de trabalho

### Quando é necessário um conetor

Quando você usa o BlueXP  no modo padrão, um conetor é necessário para os seguintes recursos e serviços no BlueXP :

- Alertas
- Recursos de gerenciamento do Amazon FSX for ONTAP
- Storage Amazon S3
- Storage Azure Blob
- Backup e recuperação
- Classificação
- Cloud Volumes ONTAP
- Recuperação de desastres
- Sistemas e-Series
- Eficiência econômica 1
- Buckets do Google Cloud Storage
- Integração de clusters ONTAP no local com serviços de dados BlueXP
- Resiliência operacional 1
- Proteção contra ransomware
- Sistemas StorageGRID
- Disposição em camadas
- Armazenamento em cache de volume

1 enquanto você pode acessar esses serviços sem um conetor, um conetor é necessário para iniciar ações a partir dos serviços.

É necessário um conetor para utilizar o BlueXP  no modo restrito ou no modo privado.

### Os conetores devem estar sempre operacionais

Os conetores são uma parte fundamental da arquitetura de serviços do BlueXP . É da sua responsabilidade garantir que os conetores relevantes estejam sempre ativos, operacionais e acessíveis. Embora o serviço seja projetado para superar interrupções curtas da disponibilidade do conetor, você precisa tomar medidas imediatas quando necessário para solucionar falhas de infraestrutura.

Esta documentação é regida pelo EULA. Se o produto não for operado de acordo com a documentação, a funcionalidade e o funcionamento do produto, bem como os seus direitos ao abrigo do EULA, podem ser afetados negativamente.

#### Impacto no Cloud Volumes ONTAP

Um conetor é um componente chave na integridade e funcionamento do Cloud Volumes ONTAP. Se um conetor for desligado, os sistemas Cloud Volumes ONTAP PAYGO e os sistemas BYOL baseados em capacidade serão desligados após perder a comunicação com um conetor por mais de 14 dias. Isso acontece porque o conetor atualiza o licenciamento no sistema todos os dias.

Se o seu sistema Cloud Volumes ONTAP tiver uma licença BYOL baseada em nós, o sistema permanecerá em execução após 14 dias porque a licença é instalada no sistema Cloud Volumes ONTAP.

### Locais suportados

Um conetor é suportado nos seguintes locais:

- Amazon Web Services
- Microsoft Azure

  Um conetor no Azure deve ser implantado na mesma região do Azure que os sistemas Cloud Volumes ONTAP que gerencia, ou no "Par de regiões do Azure" para os sistemas Cloud Volumes ONTAP. Esse requisito garante que uma conexão com o Azure Private Link seja usada entre o Cloud Volumes ONTAP e suas contas de armazenamento associadas. "Saiba como o Cloud Volumes ONTAP usa um link privado do Azure"

- Google Cloud

  Se você quiser usar os serviços do BlueXP  com o Google Cloud, use um conetor em execução no Google Cloud.

- No local

### Comunicação com fornecedores de nuvem

O conetor usa o TLS 1,2 para todas as comunicações com a AWS, o Azure e o Google Cloud.

### Modo restrito e modo privado

Para usar o BlueXP  no modo restrito ou no modo privado, você começa a usar o BlueXP  instalando o conetor e acessando a interface do usuário que está sendo executada localmente no conetor.

"Saiba mais sobre os modos de implantação do BlueXP".

### Como criar um conetor

Você pode criar um conetor diretamente do BlueXP , a partir do mercado do seu provedor de nuvem ou instalando manualmente o software em seu próprio host Linux. A forma como começar depende se está a utilizar o BlueXP  no modo padrão, no modo restrito ou no modo privado.

- "Saiba mais sobre os modos de implantação do BlueXP"
- "Comece a usar o BlueXP  no modo padrão"
- "Comece a usar o BlueXP  no modo restrito"
- "Comece a usar BlueXP  no modo privado"

### Permissões

Permissões específicas são necessárias para criar o conetor diretamente do BlueXP  e outro conjunto de permissões é necessário para a própria instância do conetor. Se você criar o conetor na AWS ou no Azure diretamente do BlueXP , o BlueXP  criará o conetor com as permissões de que ele precisa.

Ao usar o BlueXP  no modo padrão, a forma como você fornece permissões depende de como você planeja criar o conetor.

Para saber como configurar permissões, consulte o seguinte:

- Modo padrão
  - "Opções de instalação do conetor na AWS"
  - "Opções de instalação do conetor no Azure"
  - "Opções de instalação do conetor no Google Cloud"
  - "Configurar permissões de nuvem para implantações locais"
- "Configurar permissões para o modo restrito"
- "Configurar permissões para o modo privado"

Para ver as permissões exatas que o conetor precisa para operações diárias, consulte as seguintes páginas:

- "Saiba como o conetor usa permissões da AWS"
- "Saiba como o conetor usa permissões do Azure"
- "Saiba como o conetor usa as permissões do Google Cloud"

É da sua responsabilidade atualizar as políticas do conetor à medida que novas permissões são adicionadas nas versões subsequentes. Se novas permissões forem necessárias, elas serão listadas nas notas de versão.

**Atualizações do conetor**

Normalmente, atualizamos o software Connector a cada mês para introduzir novos recursos e fornecer melhorias de estabilidade. Embora a maioria dos serviços e recursos na plataforma BlueXP  sejam oferecidos por software baseado em SaaS, alguns recursos dependem da versão do conetor. Isso inclui gerenciamento de Cloud Volumes ONTAP, gerenciamento de cluster do ONTAP no local, configurações e ajuda.

Quando você usa o BlueXP  no modo padrão ou no modo restrito, o conetor atualiza automaticamente seu software para a versão mais recente, desde que tenha acesso de saída à Internet para obter a atualização de software. Se você estiver usando o BlueXP  no modo privado, precisará atualizar manualmente o conetor.

"Saiba como atualizar manualmente o software do conetor ao usar o modo privado".

**Manutenção do sistema operacional e VM**

Manter o sistema operacional no host do conetor é sua responsabilidade. Por exemplo, você deve aplicar atualizações de segurança ao sistema operacional no host do conetor seguindo os procedimentos padrão da sua empresa para distribuição do sistema operacional.

Observe que você não precisa interromper nenhum serviço no host do conetor ao aplicar pequenas atualizações de segurança.

Se você precisar parar e, em seguida, iniciar a VM do conetor, você deve fazê-lo a partir do console do seu provedor de nuvem ou usando os procedimentos padrão para gerenciamento no local.

Tenha em atenção que o conetor deve estar sempre operacional.

**Vários ambientes de trabalho e conetores**

Um conetor pode gerenciar vários ambientes de trabalho no BlueXP . O número máximo de ambientes de trabalho que um único conetor deve gerenciar varia. Depende do tipo de ambiente de trabalho, do número de volumes, da capacidade que está sendo gerenciada e do número de usuários.

Se você tiver uma implantação em grande escala, trabalhe com seu representante da NetApp para

dimensionar o ambiente. Se você tiver algum problema ao longo do caminho, entre em Contato conosco usando o bate-papo no produto.

Em alguns casos, você pode precisar apenas de um conetor, mas você pode encontrar-se precisando de dois ou mais conetores.

Aqui estão alguns exemplos:

- Você tem um ambiente multicloud (por exemplo, AWS e Azure) e prefere ter um conetor na AWS e outro no Azure. Cada um gerencia os sistemas Cloud Volumes ONTAP executados nesses ambientes.
- Um provedor de serviços pode usar uma organização da BlueXP para fornecer serviços para seus clientes, enquanto usa outra organização para fornecer recuperação de desastres para uma de suas unidades de negócios. Cada organização teria conetores separados.

## Saiba mais sobre os modos de implantação do BlueXP

O BlueXP oferece vários *modos de implantação* que permitem que você use o BlueXP de uma forma que atenda aos requisitos de negócios e segurança. O *modo padrão* aproveita a camada de software como serviço (SaaS) do BlueXP para fornecer funcionalidade completa, enquanto o *modo restrito* e o *modo privado* estão disponíveis para organizações que têm restrições de conetividade.

Embora o BlueXP iniba o fluxo de tráfego, comunicação e dados ao usar o modo restrito ou o modo privado, é sua responsabilidade garantir que seu ambiente (no local e na nuvem) esteja em conformidade com os regulamentos exigidos.

### Visão geral

O BlueXP oferece três modos de implantação. Cada modo difere em termos de requisitos de conetividade de saída, localização de implementação, processo de instalação, método de autenticação, serviços de dados e armazenamento disponíveis e métodos de carregamento.

**Modo padrão**

O BlueXP é acessível aos usuários como um serviço de nuvem a partir do console baseado na Web. Dependendo dos serviços do BlueXP que você planeja usar, um administrador do BlueXP cria um ou mais conetores para gerenciar dados em seu ambiente de nuvem híbrida.

Este modo utiliza a transmissão de dados encriptados através da Internet pública.

**Modo restrito**

Um conetor BlueXP é instalado na nuvem (em uma região do governo, região de nuvem soberana ou região comercial) e tem conetividade de saída limitada à camada BlueXP SaaS. Os usuários acessam o BlueXP localmente a partir do console baseado na Web que está disponível no conetor, não na camada SaaS.

Este modo é normalmente usado por governos estaduais e locais e empresas regulamentadas.

Saiba mais sobre a conetividade de saída à camada SaaS.

**Modo privado**

Um conetor BlueXP é instalado no local ou na nuvem (em uma região segura, região de nuvem soberana ou região comercial) e tem *no* conetividade à camada SaaS do BlueXP . Os usuários acessam o BlueXP localmente a partir do console baseado na Web que está disponível no conetor, não na camada SaaS.

Uma região segura inclui "Nuvem secreta da AWS", "Nuvem secreta principal da AWS" e "Azure IL6"

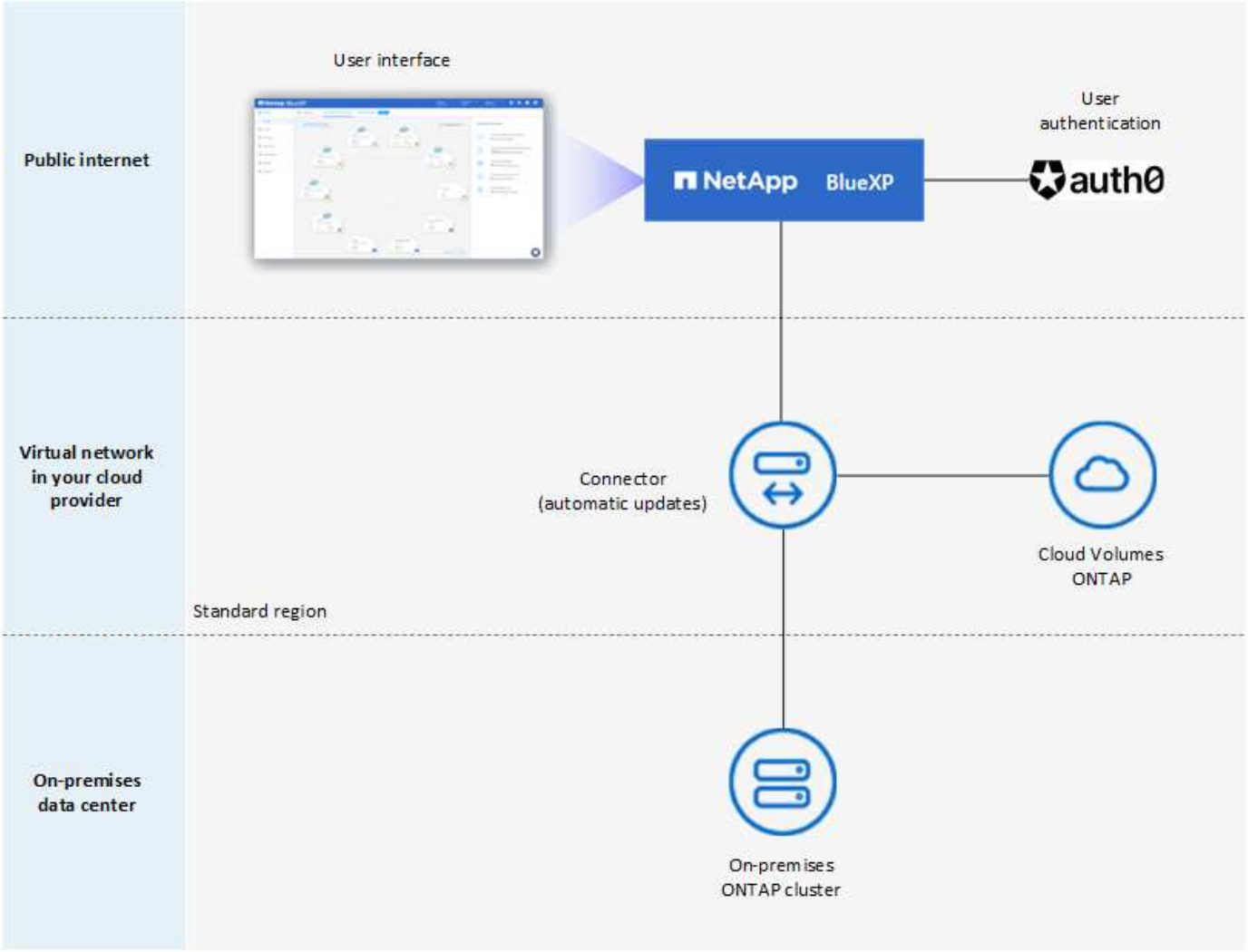
A tabela a seguir fornece uma comparação desses modos.

| | Modo padrão | Modo restrito | Modo privado |
|---|---|---|---|
| **Conexão necessária à camada BlueXP  SaaS?** | Sim | Apenas saída | Não |
| **Conexão necessária ao seu provedor de nuvem?** | Sim | Sim, dentro da região | Sim, dentro da região (se estiver usando Cloud Volumes ONTAP) |
| **Instalação do conetor** | Do BlueXP , mercado de nuvem ou instalação manual | Mercado da nuvem ou instalação manual | Instalação manual |
| **Atualizações do conetor** | Atualizações automáticas do software NetApp Connector | Atualizações automáticas do software NetApp Connector | Atualização manual necessária |
| **Acesso da IU** | Da camada SaaS da BlueXP | Localmente a partir do conetor VM | Localmente a partir do conetor VM |
| **Endpoint da API** | A camada SaaS do BlueXP | A ficha | A ficha |
| **Autenticação** | Por meio de SaaS usando auth0, login NSS ou federação de identidade | Por meio de SaaS usando auth0 ou federação de identidade | Autenticação de usuário local |
| **Serviços de storage e dados** | Todos são suportados | Muitos são suportados | Vários são suportados |
| **Opções de licenciamento** | Assinaturas de mercado e BYOL | Assinaturas de mercado e BYOL | BYOL |

Leia as seções a seguir para saber mais sobre esses modos, incluindo quais recursos e serviços do BlueXP são suportados.

### Modo padrão

A imagem a seguir é um exemplo de implantação de modo padrão.




O BlueXP  funciona da seguinte forma no modo padrão:

**Comunicação de saída**

A conectividade é necessária do conetor à camada SaaS do BlueXP , aos recursos disponíveis publicamente do seu fornecedor de nuvem e a outros componentes essenciais para operações diárias.

- "Endpoints que o conetor entra em Contato na AWS"
- "Endpoints que o conetor entra em Contato no Azure"
- "Endpoints que o conetor entra em Contato no Google Cloud"

**Localização suportada para o conetor**

No modo padrão, o conetor é compatível com a nuvem ou no local.

**Instalação do conetor**

A instalação do conetor é possível a partir de um assistente de configuração no BlueXP , no AWS ou no Azure Marketplace, ou usando um instalador para instalar manualmente o conetor no seu próprio host Linux no data center ou na nuvem.

**Atualizações do conetor**

Atualizações automatizadas do software Connector estão disponíveis no BlueXP  com atualizações mensais.

**Acesso à interface do utilizador**

A interface do usuário é acessível a partir do console baseado na Web que é fornecido através da camada SaaS.

**Endpoint da API**

As chamadas de API são feitas para o seguinte endpoint: https://cloudmanager.cloud.NetApp.com

**Autenticação**

A autenticação é fornecida por meio do serviço de nuvem da BlueXP  usando auth0 ou por meio de logins do site de suporte da NetApp (NSS). A federação de identidade está disponível.

**Serviços BlueXP  compatíveis**

Todos os serviços BlueXP  estão disponíveis para os usuários.

**Opções de licenciamento suportadas**

As assinaturas do Marketplace e o BYOL são compatíveis com o modo padrão; no entanto, as opções de licenciamento suportadas dependem do serviço BlueXP  que você está usando. Revise a documentação de cada serviço para saber mais sobre as opções de licenciamento disponíveis.

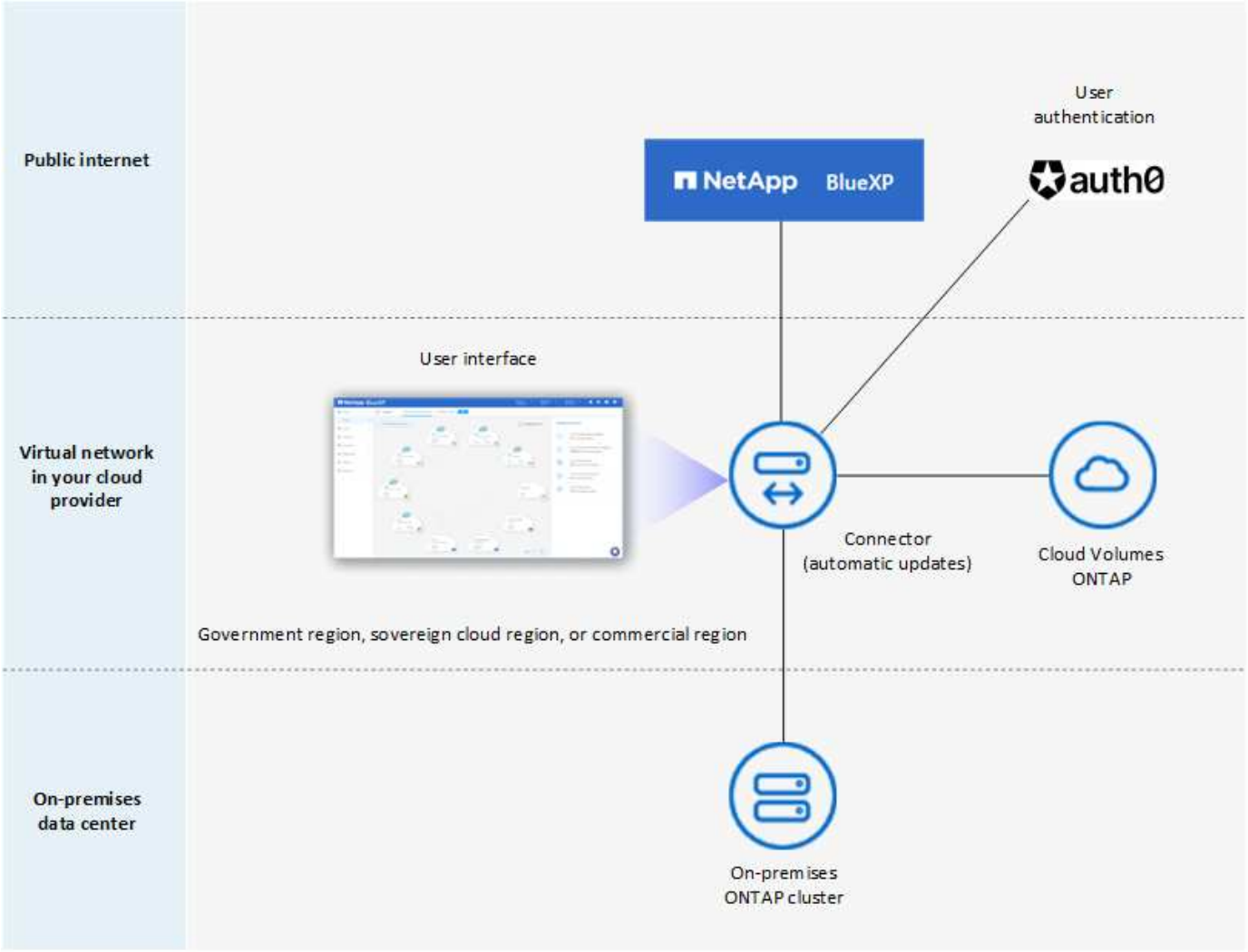
**Como começar com o modo padrão**

Vá para o "Console baseado na Web do BlueXP " e inscreva-se.

"Saiba como começar a usar o modo padrão".

**Modo restrito**

A imagem a seguir é um exemplo de implantação de modo restrito.




O BlueXP  funciona da seguinte forma no modo restrito:

**Comunicação de saída**

A conectividade de saída é necessária do conetor à camada SaaS do BlueXP  para usar os serviços de dados do BlueXP , para habilitar atualizações automáticas de software do conetor, usar autenticação baseada em auth0 e enviar metadados para carregamento (nome da VM de storage, capacidade alocada e UID de volume, tipo e IOPS).

A camada SaaS do BlueXP  não inicia a comunicação com o conetor. Toda a comunicação é iniciada pelo conetor, que pode extrair ou enviar dados da camada SaaS ou para a camada SaaS, conforme necessário.

Uma conexão também é necessária para os recursos do provedor de nuvem de dentro da região.

**Localização suportada para o conetor**

No modo restrito, o conetor é suportado na nuvem: Em uma região governamental, região soberana ou região comercial.

**Instalação do conetor**

A instalação do conetor é possível a partir do AWS ou do Azure Marketplace ou de uma instalação manual em seu próprio host Linux.

**Atualizações do conetor**

Atualizações automatizadas do software Connector estão disponíveis no BlueXP  com atualizações mensais.

**Acesso à interface do utilizador**

A interface do usuário é acessível a partir da máquina virtual Connector que é implantada em sua região de nuvem.

**Endpoint da API**

As chamadas de API são feitas para a máquina virtual do conetor.

**Autenticação**

A autenticação é fornecida através do serviço de nuvem da BlueXP  usando o auth0. A federação de identidade também está disponível.

**Serviços BlueXP  compatíveis**

O BlueXP  oferece suporte aos seguintes serviços de armazenamento e dados com modo restrito:

| Serviços compatíveis | Notas |
|---|---|
| Azure NetApp Files | Suporte completo |
| Backup e recuperação | Suportado em regiões governamentais e regiões comerciais com modo restrito. Não suportado em regiões soberanas com modo restrito. No modo restrito, o backup e a recuperação do BlueXP  são compatíveis apenas com backup e restauração de dados de volume do ONTAP. "Veja a lista de destinos de backup suportados para dados do ONTAP" Não há suporte para backup e restauração de dados de aplicativos e dados de máquina virtual. |
| Classificação | Suportado em regiões governamentais com modo restrito. Não suportado em regiões comerciais ou em regiões soberanas com modo restrito. |
| Cloud Volumes ONTAP | Suporte completo |
| Carteira digital | Pode utilizar a carteira digital com as opções de licenciamento suportadas listadas abaixo para o modo restrito. |
| Clusters ONTAP on-premises | A descoberta com um conetor e descoberta sem um conetor (descoberta direta) são suportadas. Quando você descobre um cluster no local com um conetor, a visualização avançada (System Manager) não é suportada. |
| Replicação | Suportado em regiões governamentais com modo restrito. Não suportado em regiões comerciais ou em regiões soberanas com modo restrito. |

**Opções de licenciamento suportadas**

As seguintes opções de licenciamento são suportadas com o modo restrito:

- Assinaturas de mercado (contratos por hora e anuais)

  Observe o seguinte:

  - Para o Cloud Volumes ONTAP, somente o licenciamento baseado em capacidade é suportado.
  - No Azure, os contratos anuais não são compatíveis com regiões governamentais.
- BYOL

  Para o Cloud Volumes ONTAP, o licenciamento baseado em capacidade e o licenciamento baseado em nós são compatíveis com o BYOL.

**Como começar com o modo restrito**

Você precisa ativar o modo restrito ao criar sua conta do BlueXP .

Se ainda não tiver uma conta, ser-lhe-á pedido que crie a sua conta e ative o modo restrito quando iniciar sessão no BlueXP  pela primeira vez a partir de um conetor que instalou manualmente ou que criou a partir do mercado do seu fornecedor de nuvem.

Se você já tem uma conta e deseja criar outra, então você precisa usar a API do Tenancy.

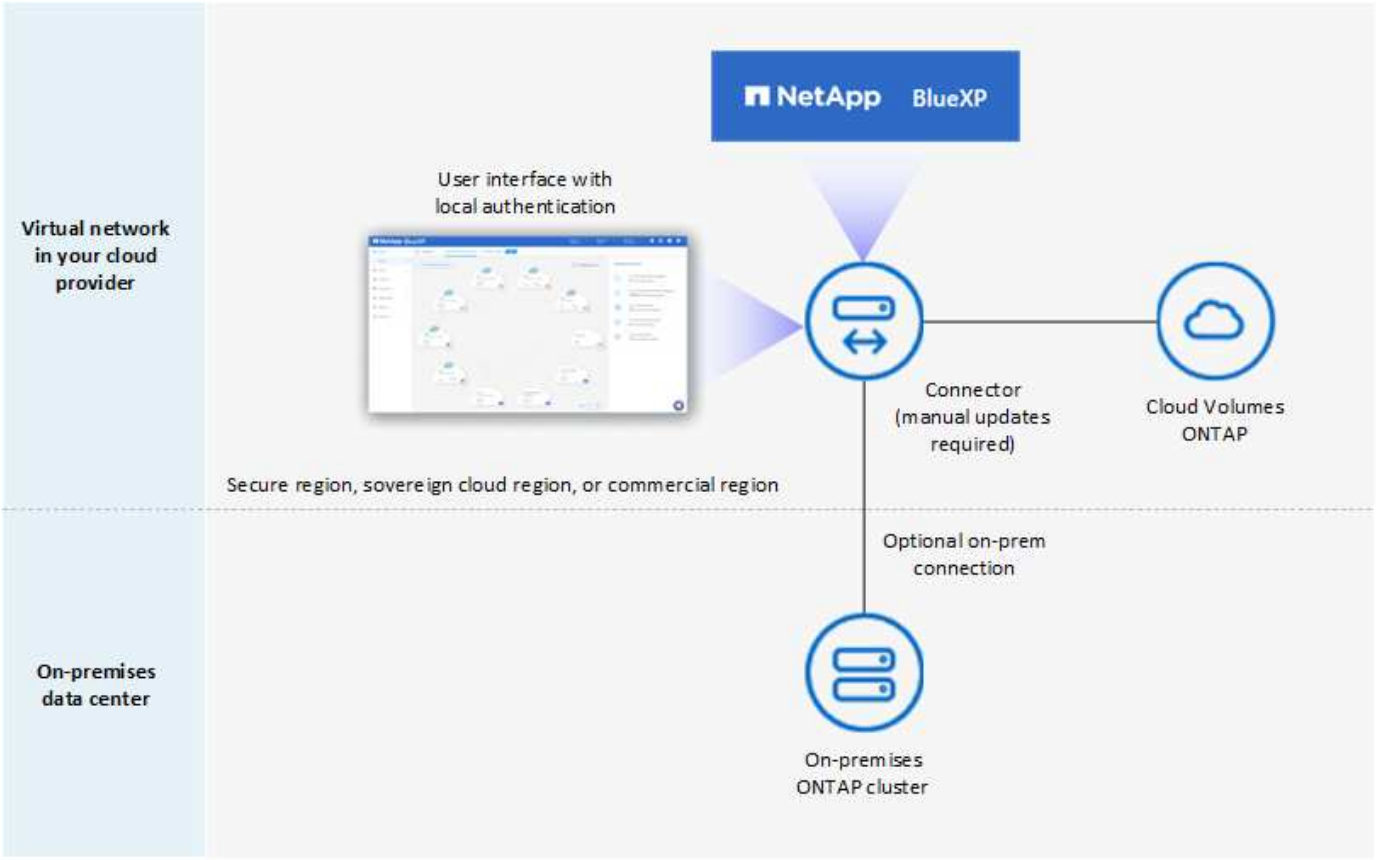
Observe que você não pode alterar a configuração do modo restrito depois que o BlueXP  criar a conta. Não é possível ativar o modo restrito mais tarde e não é possível desativá-lo mais tarde. Ele deve ser definido no momento da criação da conta.

- "Saiba como começar com o modo restrito".
- "Saiba como criar uma conta BlueXP  adicional".

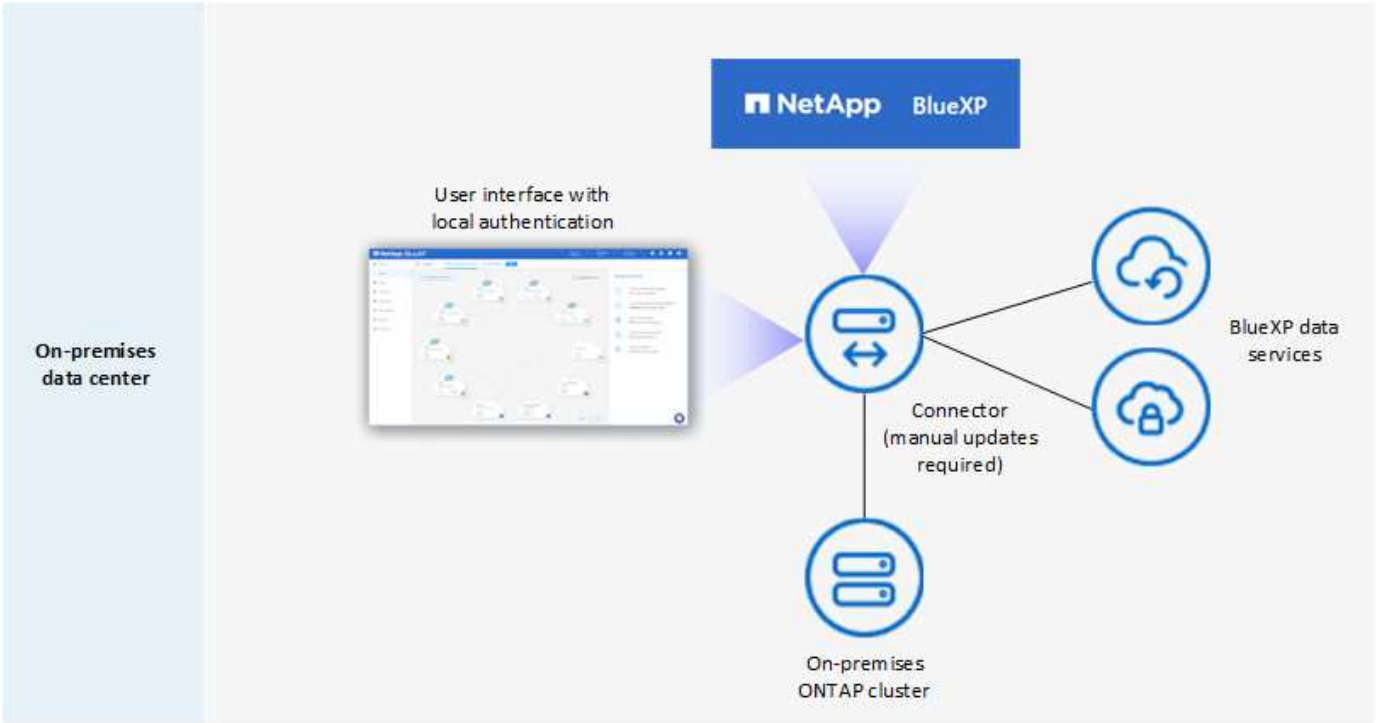
**Modo privado**

No modo privado, você pode instalar um conector no local ou na nuvem e usar o BlueXP  para gerenciar dados na nuvem híbrida. Não há conetividade com a camada SaaS do BlueXP .

A imagem a seguir mostra um exemplo de implantação de modo privado em que o conetor é instalado na nuvem e gerencia o Cloud Volumes ONTAP e um cluster ONTAP no local.




Enquanto isso, a segunda imagem mostra um exemplo de implantação de modo privado em que o conetor é instalado no local, gerencia um cluster ONTAP no local e fornece acesso a serviços de dados BlueXP compatíveis.




O BlueXP  funciona da seguinte forma no modo privado:

**Comunicação de saída**

Nenhuma conectividade de saída é necessária para a camada SaaS do BlueXP . Todos os pacotes, dependências e componentes essenciais são empacotados com o conetor e servidos a partir da máquina local. A conetividade com os recursos disponíveis publicamente do seu provedor de nuvem é necessária somente se você estiver implantando o Cloud Volumes ONTAP.

**Localização suportada para o conetor**

No modo privado, o conetor é suportado na nuvem ou no local.

**Instalação do conetor**

As instalações manuais do conetor são suportadas no seu próprio host Linux na nuvem ou no local.

**Atualizações do conetor**

Você precisa atualizar o software do conetor manualmente. O software Connector é publicado no site de suporte da NetApp em intervalos indefinidos.

**Acesso à interface do utilizador**

A interface do usuário é acessível a partir do conetor que é implantado na sua região de nuvem ou no local.

**Endpoint da API**

As chamadas de API são feitas para a máquina virtual do conetor.

**Autenticação**

A autenticação é fornecida através do gerenciamento e acesso de usuários locais. A autenticação não é fornecida através do serviço de nuvem da BlueXP .

**Serviços BlueXP  compatíveis em implantações de nuvem**

O BlueXP  oferece suporte aos seguintes serviços de armazenamento e dados com modo privado quando o conetor é instalado na nuvem:

| Serviços compatíveis | Notas |
|---|---|
| Backup e recuperação | Compatível com regiões comerciais da AWS e do Azure. Não é compatível com o Google Cloud ou no "Nuvem secreta da AWS" "Nuvem secreta principal da AWS" , ou "Azure IL6" no modo privado, o backup e a recuperação do BlueXP  são compatíveis apenas com backup e restauração de dados de volume do ONTAP. "Veja a lista de destinos de backup suportados para dados do ONTAP" Não há suporte para backup e restauração de dados de aplicativos e dados de máquina virtual. |
| Cloud Volumes ONTAP | Como não há acesso à Internet, os seguintes recursos não estão disponíveis: Atualizações de software automatizadas e AutoSupport. |
| Carteira digital | Você pode usar a carteira digital com as opções de licenciamento suportadas listadas abaixo para o modo privado. |

| Serviços compatíveis | Notas |
| --- | --- |
| Clusters ONTAP on-premises | Requer conectividade da nuvem (onde o conetor está instalado) para o ambiente local. A descoberta sem um conetor (descoberta direta) não é suportada. |

### Serviços BlueXP  compatíveis em implantações locais

O BlueXP  dá suporte aos seguintes serviços de storage e dados com modo privado quando o conetor é instalado em suas instalações:

| Serviços compatíveis | Notas |
| --- | --- |
| Backup e recuperação | No modo privado, o backup e a recuperação do BlueXP  são compatíveis apenas com backup e restauração de dados de volume do ONTAP. "Veja a lista de destinos de backup suportados para dados de volume do ONTAP"<br><br>Não há suporte para backup e restauração de dados de aplicativos e dados de máquina virtual. |
| Classificação | • As únicas fontes de dados suportadas são as que você pode descobrir localmente.<br><br>"Veja as fontes que você pode descobrir localmente"<br><br>• Os recursos que exigem acesso de saída à Internet não são suportados.<br><br>"Veja as limitações de recursos" |
| Carteira digital | Você pode usar a carteira digital com as opções de licenciamento suportadas listadas abaixo para o modo privado. |
| Clusters ONTAP on-premises | A descoberta sem um conetor (descoberta direta) não é suportada. |
| Replicação | Suporte completo |

### Opções de licenciamento suportadas

Apenas o BYOL é suportado com o modo privado.

Para o Cloud Volumes ONTAP BYOL, apenas o licenciamento baseado em nós é suportado. O licenciamento baseado em capacidade não é suportado. Como uma conexão de saída à Internet não está disponível, você precisará fazer o upload manual do arquivo de licenciamento do Cloud Volumes ONTAP na carteira digital do BlueXP .

"Saiba como adicionar licenças à carteira digital BlueXP "

### Como começar com o modo privado

O modo privado está disponível baixando o instalador "offline" do site de suporte da NetApp.

"Saiba como começar a usar o modo privado".

Se quiser usar o BlueXP no "Nuvem secreta da AWS" ou no "Nuvem secreta principal da AWS", siga instruções separadas para começar nesses ambientes. "Saiba como começar a usar o Cloud Volumes ONTAP na nuvem secreta da AWS ou na nuvem secreta principal"

### Comparação de serviços e funcionalidades

A tabela a seguir pode ajudá-lo a identificar rapidamente quais serviços e recursos do BlueXP são suportados com modo restrito e modo privado.

Observe que alguns serviços podem ser suportados com limitações. Para obter mais detalhes sobre como esses serviços são suportados com modo restrito e modo privado, consulte as seções acima.

| Área do produto | Serviço ou recurso do BlueXP | Modo restrito | Modo privado |
|---|---|---|---|
| **Ambientes de trabalho** esta parte da tabela lista o suporte para o gerenciamento do ambiente de trabalho a partir da tela BlueXP . Ele não indica os destinos de backup suportados para backup e recuperação do BlueXP . | Amazon FSX para ONTAP | Não | Não |
| | Amazon S3 | Não | Não |
| | Blob do Azure | Não | Não |
| | Azure NetApp Files | Sim | Não |
| | Cloud Volumes ONTAP | Sim | Sim |
| | Cloud Volumes Service para Google Cloud | Não | Não |
| | Google Cloud Storage | Não | Não |
| | Clusters ONTAP no local | Sim | Sim |
| | E-Series | Não | Não |
| | StorageGRID | Não | Não |

| Área do produto | Serviço ou recurso do BlueXP | Modo restrito | Modo privado |
|---|---|---|---|
| **Serviços** | Alertas | Não | Não |
| | Backup e recuperação | Sim "Veja a lista de destinos de backup suportados para dados de volume do ONTAP" | Sim "Veja a lista de destinos de backup suportados para dados de volume do ONTAP" |
| | Classificação | Sim | Sim |
| | Operações da nuvem | Não | Não |
| | Copiar e sincronizar | Não | Não |
| | Consultor digital | Não | Não |
| | Carteira digital | Sim | Sim |
| | Recuperação de desastres | Não | Não |
| | Eficiência económica | Não | Não |
| | Resiliência operacional | Não | Não |
| | Proteção contra ransomware | Não | Não |
| | Replicação | Sim | Sim |
| | Atualizações de software | Não | Não |
| | Sustentabilidade | Não | Não |
| | Disposição em camadas | Não | Não |
| | Armazenamento em cache de volume | Não | Não |
| | Fábrica de carga de trabalho | Não | Não |
| **Caraterísticas** | Gerenciamento de identidade e acesso do BlueXP | Não | Não |
| | Contas BlueXP | Sim | Sim |
| | Credenciais | Sim | Sim |
| | Contas NSS | Sim | Não |
| | Notificações | Sim | Não |
| | Pesquisa | Sim | Não |
| | Linha do tempo | Sim | Sim |

# Comece com o modo padrão

## Fluxo de trabalho de introdução (modo padrão)

Comece a usar o BlueXP  no modo padrão, preparando a rede para o console BlueXP , inscrevendo-se e criando uma conta, criando opcionalmente um conetor e assinando o BlueXP .

No modo padrão, o BlueXP  é acessível aos usuários como um serviço de nuvem a partir do console baseado na Web. Antes de começar, você deve ter uma compreensão de "modos de implantação" e "Conetores".

1 **"Prepare a rede para usar o console BlueXP"**

Os computadores que acessam o console BlueXP  devem ter conexões com endpoints específicos para concluir algumas tarefas administrativas. Se a rede restringir o acesso de saída, você deve garantir que esses endpoints sejam permitidos.

2 **"Inscreva-se e crie uma organização"**

Vá para o "Consola BlueXP" e inscreva-se. Você terá a opção de criar uma organização do BlueXP , mas poderá pular essa etapa se estiver sendo convidado para uma organização existente.

Neste ponto, você está logado e pode começar a usar vários serviços do BlueXP , como Consultor Digital, Amazon FSX for ONTAP, Azure NetApp Files e muito mais. "Saiba o que você pode fazer sem um conetor".

3 **Crie um conetor**

Você não precisa de um conetor para começar a usar o BlueXP , mas pode criar um conetor para desbloquear todos os recursos e serviços do BlueXP . O Connector é o software NetApp que permite ao BlueXP  gerenciar recursos e processos em seu ambiente de nuvem híbrida.

Você pode criar um conetor na nuvem ou na rede local.

- "Saiba mais sobre quando os conetores são necessários e como funcionam"
- "Saiba como criar um conetor na AWS"
- "Saiba como criar um conetor no Azure"
- "Saiba como criar um conetor no Google Cloud"
- "Saiba como criar um conetor no local"

Observe que, se você quiser usar os serviços do BlueXP  para gerenciar storage e dados no Google Cloud, o conetor deve estar em execução no Google Cloud.

4 **"Inscreva-se no BlueXP "**

Inscreva-se no BlueXP  no mercado do seu fornecedor de nuvem para pagar os serviços da BlueXP  a uma taxa por hora (PAYGO) ou por meio de um contrato anual.

## Prepare a rede para o console BlueXP

Quando você faz login e usa o console baseado na Web do BlueXP , o BlueXP  entra em

Contato com vários endpoints para concluir as ações iniciadas. Os computadores que acessam o console BlueXP  devem ter conexões com esses endpoints.

Esses endpoints são contatados em dois cenários:

- A partir do computador de um usuário ao concluir ações específicas do "Console baseado na Web do BlueXP " que está disponível como software como serviço (SaaS).
- No computador de um usuário ao abrir um navegador da Web, insira o endereço IP do host do conetor e, em seguida, efetue login e configure o conetor. Estes passos são necessários se instalar manualmente o conetor.

| Endpoints | Finalidade |
|---|---|
| https://console.BlueXP .NetApp.com<br>https://*.console.BlueXP .NetApp.com | Este é o ponto de extremidade que você insere no navegador da Web para usar o console baseado na Web do BlueXP . |
| https://api.BlueXP .NetApp.com | O console baseado na Web do BlueXP  entra em Contato com esse endpoint para interagir com a API do BlueXP  para ações relacionadas a autorização, licenciamento, assinaturas, credenciais, notificações e muito mais. |
| https://aiq.NetApp.com | Necessário para acessar o consultor digital da BlueXP . |
| Serviços da AWS (amazonaws.com):<br>• CloudFormation<br>• Nuvem de computação elástica (EC2)<br>• Key Management Service (KMS)<br>• Serviço de token de segurança (STS)<br>• Serviço de armazenamento simples (S3) | Necessário para implantar um conetor da BlueXP  na AWS. O ponto final exato depende da região em que você implementa o conetor. "Consulte a documentação da AWS para obter detalhes." |
| https://management.azure.com<br>https://login.microsoftonline.com | Necessário para implantar um conetor da BlueXP  na maioria das regiões do Azure. |
| https://management.microsoftazure.de<br>https://login.microsoftonline.de | Necessário para implantar um conetor da BlueXP  nas regiões do Azure Alemanha. |
| https://management.usgovcloudapi.net<br>https://login.microsoftonline.com | Necessário para implantar um conetor da BlueXP  nas regiões do Azure US Gov. |
| https://www.googleapis.com | Necessário para implantar um conetor do BlueXP  no Google Cloud. |
| https://signin.b2c.NetApp.com | Necessário para atualizar as credenciais do site de suporte da NetApp (NSS) ou para adicionar novas credenciais NSS ao BlueXP . |
| https://NetApp-cloud-account.auth0.com<br>https://cdn.auth0.com<br>https://services.cloud.NetApp.com | Seu navegador da Web se coneta a esses endpoints para autenticação de usuário centralizada por meio do BlueXP . |

| Endpoints | Finalidade |
| --- | --- |
| https://widget.intercom.io | Para um bate-papo no produto que permite conversar com especialistas em nuvem da NetApp. |

Além desses endpoints, você também precisa garantir que o conetor tenha acesso de saída à Internet para contatar endpoints específicos para operações diárias. Você pode encontrar a lista desses endpoints seguindo os links na próxima seção abaixo.

**Informações relacionadas**

- Prepare a rede para o conetor
  - "Configurar a rede AWS"
  - "Configurar a rede do Azure"
  - "Configurar a rede do Google Cloud"
  - "Configurar redes locais"
- Prepare a rede para os serviços BlueXP

  Consulte a documentação de cada serviço BlueXP .

  "Documentação do BlueXP"

## Inscreva-se ou faça login no BlueXP

O BlueXP é acessível a partir de um console baseado na Web. Quando você começar a usar o BlueXP , seu primeiro passo é se inscrever ou fazer login usando suas credenciais do site de suporte da NetApp ou credenciais SSO do diretório corporativo.

**Sobre esta tarefa**

Quando você acessa o BlueXP pela primeira vez, o BlueXP permite que você se inscreva ou faça login usando uma das seguintes opções:

**Login BlueXP**

Você pode se inscrever criando um login no BlueXP . Este método de autenticação requer que você especifique seu endereço de e-mail e uma senha. Depois de verificar seu endereço de e-mail, você pode fazer login e criar uma organização do BlueXP , se você ainda não pertence a uma.

**Credenciais do site de suporte da NetApp (NSS)**

Se você tiver credenciais do site de suporte da NetApp, não precisará se inscrever no BlueXP . Você faz login usando suas credenciais NSS e, em seguida, o BlueXP solicita que você crie uma organização do BlueXP , se você ainda não pertence a uma.

Observe que a experiência de senha padrão é uma senha de uso único (OTP) para o endereço de e-mail registrado. Uma nova OTP é gerada a cada tentativa de login.

**Ligação federada**

Você pode usar o logon único para fazer login usando credenciais de seu diretório corporativo (identidade federada). O primeiro usuário na conta da sua organização deve se inscrever no BlueXP ou fazer login usando credenciais NSS e, em seguida, configurar a federação de identidade. Depois disso, você pode adicionar membros da sua identidade corporativa à sua organização. Esses usuários podem então fazer login usando suas credenciais SSO.

"Saiba como usar a federação de identidade com o BlueXP ".

**Passos**

1. Abra um navegador da Web e aceda ao "Consola BlueXP"
2. Se você tiver uma conta do site de suporte da NetApp ou já tiver configurado uma federação de identidade, insira o endereço de e-mail associado à sua conta diretamente na página **entrar**.

   Em ambos os casos, o BlueXP irá inscrevê-lo como parte deste início de sessão inicial.

3. Se você quiser se inscrever criando um login no BlueXP , selecione **Inscrever-se**.
   a. Na página **Inscrever-se**, insira as informações necessárias e selecione **seguinte**.

      Observe que somente carateres em inglês são permitidos no formulário de inscrição.

   b. Verifique se há um e-mail do NetApp na sua caixa de entrada que inclua instruções para verificar o seu endereço de e-mail.

      Este passo é necessário antes de poder iniciar sessão no BlueXP .

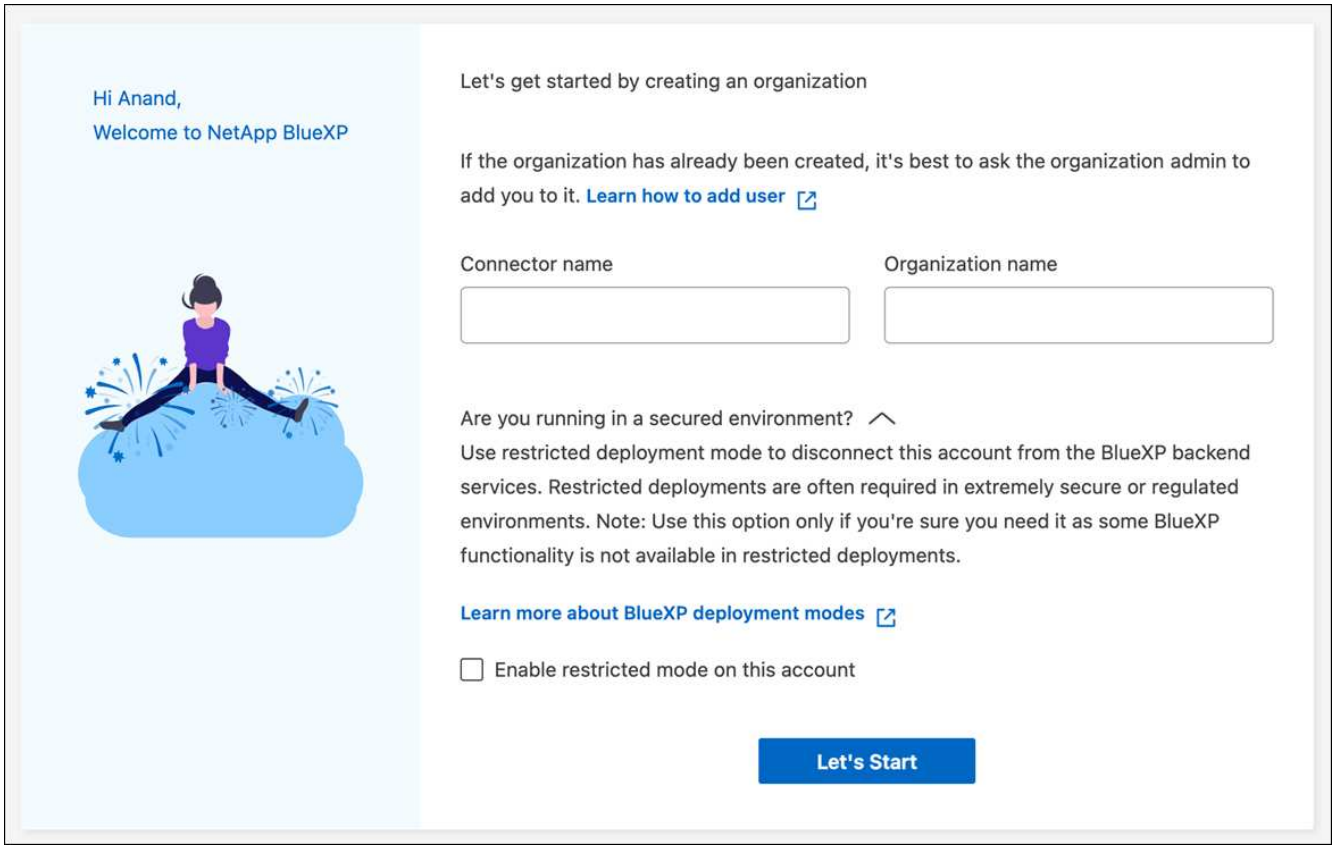
4. Depois de iniciar sessão, reveja o Contrato de Licença de Utilizador final e aceite os termos.

   Se sua conta de usuário ainda não pertencer a uma organização do BlueXP , você será solicitado a criar uma.

5. Na página **bem-vindo**, insira um nome para sua organização do BlueXP .

   Uma organização é o elemento de alto nível no gerenciamento de identidade e acesso (IAM) do BlueXP . "Saiba mais sobre o BlueXP IAM".

   Se sua empresa já tem uma organização BlueXP e você deseja ingressar nela, você deve fechar o BlueXP e pedir ao proprietário para associá-lo à organização. Depois que o proprietário adicionar você, você pode fazer login e terá acesso à conta. "Saiba como adicionar membros a uma organização existente".




6. Selecione **vamos começar**.

**Resultado**

Agora você tem um login no BlueXP  e uma organização. Na maioria dos casos, a próxima etapa é criar um conetor, que conecta os serviços da BlueXP  ao seu ambiente de nuvem híbrida.

## Crie um conetor

### AWS

#### Opções de instalação do conetor na AWS

Existem algumas maneiras diferentes de criar um conetor na AWS. Diretamente de BlueXP  é a maneira mais comum.

Estão disponíveis as seguintes opções de instalação:

- "Crie o conetor diretamente do BlueXP " (esta é a opção padrão)

  Essa ação lança uma instância do EC2 executando o Linux e o software Connector em uma VPC de sua escolha.

- "Crie um conetor no AWS Marketplace"

  Essa ação também lança uma instância do EC2 executando o Linux e o software Connector, mas a implantação é iniciada diretamente do AWS Marketplace, em vez do BlueXP .

- "Baixe e instale manualmente o software em seu próprio host Linux"

A opção de instalação que você escolher afeta a forma como você se prepara para a instalação. Isso inclui como você fornece ao BlueXP  as permissões necessárias que ele precisa para autenticar e gerenciar recursos na AWS.

#### Crie um conetor na AWS a partir do BlueXP

# Um conetor é o software NetApp executado em sua rede na nuvem ou na rede local que permite usar todos os recursos e serviços do BlueXP . Uma das opções de instalação disponíveis é criar um conetor na AWS diretamente do BlueXP . Para criar um conetor na AWS a partir do BlueXP , você precisa configurar sua rede, preparar permissões da AWS e criar o conetor.

### Antes de começar

- Você deve ter um "Compreensão dos conetores".
- Você deve rever "Limitações do conetor".

### Passo 1: Configurar a rede

Certifique-se de que a localização da rede onde pretende instalar o conetor suporta os seguintes requisitos. Atender a esses requisitos permite que o conetor gerencie recursos e processos em seu ambiente de nuvem híbrida.

#### VPC e sub-rede

Ao criar o conetor, você precisa especificar a VPC e a sub-rede onde o conetor deve residir.

#### Conexões com redes de destino

Um conetor requer uma conexão de rede com o local onde você está planejando criar e gerenciar ambientes de trabalho. Por exemplo, a rede em que você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de storage em seu ambiente local.

#### Acesso de saída à Internet

O local de rede onde você implantar o conetor deve ter uma conexão de saída de Internet para contatar pontos de extremidade específicos.

#### Terminais contactados a partir do conetor

O conetor requer acesso de saída à Internet para entrar em Contato com os seguintes endpoints, a fim de gerenciar recursos e processos em seu ambiente de nuvem pública para operações diárias.

Observe que os endpoints listados abaixo são todas as entradas CNAME.

| Endpoints | Finalidade |
| --- | --- |
| Serviços da AWS (amazonaws.com):<br>• CloudFormation<br>• Nuvem de computação elástica (EC2)<br>• Gerenciamento de identidade e acesso (IAM)<br>• Key Management Service (KMS)<br>• Serviço de token de segurança (STS)<br>• Serviço de armazenamento simples (S3) | Para gerenciar recursos na AWS. O endpoint exato depende da região da AWS que você está usando. "Consulte a documentação da AWS para obter detalhes" |
| https://support.NetApp.com https://mysupport.NetApp.com | Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte do NetApp. |
| https://*.api.BlueXP .NetApp.com<br>https://api.BlueXP .NetApp.com<br>https://*.cloudmanager.cloud.NetApp.com<br>https://cloudmanager.cloud.NetApp.com<br>https://NetApp-cloud-account.auth0.com | Para fornecer recursos e serviços SaaS no BlueXP .<br>Observe que o conetor está entrando em Contato atualmente com "cloudmanager.cloud.NetApp.com", mas começará a entrar em Contato com "API.BlueXP .NetApp.com" em uma próxima versão. |
| https://*.blob.core.windows.net<br>https://cloudmanagerinfraprod.azurecr.io | Para atualizar o conetor e seus componentes do Docker. |

**Terminais contactados a partir da consola BlueXP**

À medida que você usa o console baseado na Web do BlueXP  fornecido pela camada SaaS, ele entra em Contato com vários endpoints para concluir as tarefas de gerenciamento de dados. Isso inclui endpoints que são contatados para implantar o conetor a partir do console BlueXP .

"Veja a lista de endpoints contactados a partir da consola BlueXP ".

**Servidor proxy**

Se a sua empresa exigir a implantação de um servidor proxy para todo o tráfego de saída da Internet, obtenha as seguintes informações sobre o proxy HTTP ou HTTPS. Você precisará fornecer essas informações durante a instalação. Observe que o BlueXP  não oferece suporte a servidores proxy transparentes.

- Endereço IP
- Credenciais
- Certificado HTTPS

**Portas**

Não há tráfego de entrada para o conetor, a menos que você o inicie ou se o conetor for usado como um proxy para enviar mensagens AutoSupport do Cloud Volumes ONTAP para o suporte da NetApp.

- HTTP (80) e HTTPS (443) fornecem acesso à IU local, que você usará em circunstâncias raras.
- SSH (22) só é necessário se você precisar se conetar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 são necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída à Internet não está disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída à Internet para enviar mensagens AutoSupport, o BlueXP configura automaticamente esses sistemas para usar um servidor proxy incluído no conetor. O único requisito é garantir que o grupo de segurança do conetor permita conexões de entrada pela porta 3128. Você precisará abrir essa porta depois de implantar o conetor.

**Ativar NTP**

Se estiver a planear utilizar a classificação BlueXP para analisar as suas fontes de dados empresariais, deve ativar um serviço de Protocolo de tempo de rede (NTP) no sistema de conetores BlueXP e no sistema de classificação BlueXP para que o tempo seja sincronizado entre os sistemas. "Saiba mais sobre a classificação BlueXP"

Você precisará implementar esse requisito de rede depois de criar o conetor.

**Etapa 2: Configurar permissões da AWS**

O BlueXP precisa se autenticar com a AWS antes de implantar a instância do Connector na VPC. Você pode escolher um destes métodos de autenticação:

- Deixe o BlueXP assumir uma função do IAM que tenha as permissões necessárias
- Forneça uma chave de acesso da AWS e uma chave secreta para um usuário do IAM que tenha as permissões necessárias

Com qualquer uma das opções, o primeiro passo é criar uma política do IAM. Esta política contém apenas as permissões necessárias para iniciar a instância do Connector no AWS a partir do BlueXP .

Se necessário, você pode restringir a política do IAM usando o elemento IAM `Condition`. "Documentação da AWS: Elemento condição"

**Passos**

1. Vá para o console do AWS IAM.
2. Selecione **políticas > criar política**.
3. Selecione **JSON**.
4. Copie e cole a seguinte política:

   Esta política contém apenas as permissões necessárias para iniciar a instância do Connector no AWS a partir do BlueXP . Quando o BlueXP cria o conetor, ele aplica um novo conjunto de permissões à instância do conetor que permite que o conetor gerencie recursos da AWS. "Exibir permissões necessárias para a própria instância do conetor".

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "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:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
```

```
            "ec2:DisassociateIamInstanceProfile",
            "iam:GetRole",
            "iam:TagRole",
            "kms:ListAliases",
            "cloudformation:ListStacks"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:TerminateInstances"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/OCCMInstance": "*"
            }
        },
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ]
    }
  ]
}
```

5. Selecione **Next** e adicione tags, se necessário.
6. Selecione **seguinte** e introduza um nome e uma descrição.
7. Selecione **criar política**.
8. Anexe a política a uma função do IAM que o BlueXP pode assumir ou a um usuário do IAM para que você possa fornecer chaves de acesso ao BlueXP :
   - (Opção 1) Configurar uma função do IAM que o BlueXP pode assumir:
     i. Vá para o console do AWS IAM na conta de destino.
     ii. Em Gerenciamento de Acesso, selecione **funções > criar função** e siga as etapas para criar a função.
     iii. Em **tipo de entidade confiável**, selecione **conta AWS**.
     iv. Selecione **outra conta AWS** e insira o ID da conta SaaS do BlueXP : 952013314444
     v. Selecione a política que você criou na seção anterior.
     vi. Depois de criar a função, copie a função ARN para que possa colá-la no BlueXP quando criar o conetor.
   - (Opção 2) Configurar permissões para um usuário do IAM para que você possa fornecer chaves de acesso ao BlueXP :
     i. No console do AWS IAM, selecione **Users** e, em seguida, selecione o nome de usuário.
     ii. Selecione **Adicionar permissões > Anexar políticas existentes diretamente**.

iii. Selecione a política criada.

iv. Selecione **seguinte** e, em seguida, selecione **Adicionar permissões**.

v. Certifique-se de que tem a chave de acesso e a chave secreta para o utilizador do IAM.

**Resultado**

Agora você deve ter uma função do IAM que tenha as permissões necessárias ou um usuário do IAM que tenha as permissões necessárias. Ao criar o conetor a partir do BlueXP , você pode fornecer informações sobre a função ou as chaves de acesso.

### Passo 3: Crie o conetor

Crie o conetor diretamente do console baseado na Web do BlueXP .

**Sobre esta tarefa**

- A criação do conetor do BlueXP  implanta uma instância do EC2 na AWS usando uma configuração padrão. Depois de criar o conetor, você não deve mudar para um tipo de instância EC2 menor que tenha menos CPU ou RAM. "Saiba mais sobre a configuração padrão do conetor".
- Quando o BlueXP  cria o conetor, ele cria uma função do IAM e um perfil de instância para a instância. Essa função inclui permissões que permitem que o conetor gerencie recursos da AWS. Você precisa garantir que a função seja mantida atualizada à medida que novas permissões são adicionadas em versões subsequentes. "Saiba mais sobre a política do IAM para o conetor".

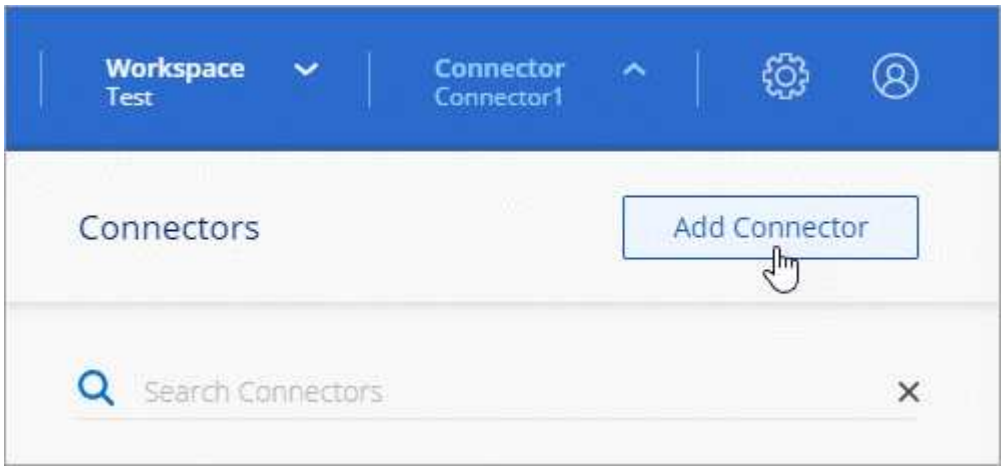
**Antes de começar**

Você deve ter o seguinte:

- Um método de autenticação da AWS: Uma função do IAM ou chaves de acesso para um usuário do IAM com as permissões necessárias.
- VPC e sub-rede que atendem aos requisitos de rede.
- Um par de chaves para a instância EC2.
- Detalhes sobre um servidor proxy, se for necessário um proxy para acesso à Internet a partir do conetor.

**Passos**

1. Selecione a lista suspensa **Connector** e selecione **Add Connector**.




2. Escolha **Amazon Web Services** como seu provedor de nuvem e selecione **continuar**.
3. Na página **implantando um conetor**, revise os detalhes sobre o que você precisará. Você tem duas

opções:

a. Selecione **continuar** para se preparar para a implantação usando o guia do produto. Cada etapa do guia do produto inclui as informações contidas nesta página da documentação.

b. Selecione **Skip to Deployment** se você já tiver preparado seguindo as etapas desta página.

4. Siga as etapas no assistente para criar o conetor:

   - **Get Ready**: Revise o que você vai precisar.
   - **Credenciais da AWS**: Especifique sua região da AWS e escolha um método de autenticação, que é uma função do IAM que o BlueXP pode assumir ou uma chave de acesso e chave secreta da AWS.

     Se você escolher **assumir função**, você poderá criar o primeiro conjunto de credenciais a partir do assistente de implantação do conetor. Qualquer conjunto adicional de credenciais deve ser criado a partir da página credenciais. Eles estarão disponíveis no assistente em uma lista suspensa. "Saiba como adicionar credenciais adicionais".

   - * Detalhes *: Fornecer detalhes sobre o conetor.
     - Insira um nome para a instância.
     - Adicione tags personalizadas (metadados) à instância.
     - Escolha se deseja que o BlueXP crie uma nova função que tenha as permissões necessárias ou se deseja selecionar uma função existente configurada com "as permissões necessárias"o .
     - Escolha se pretende encriptar os discos EBS do conetor. Você tem a opção de usar a chave de criptografia padrão ou usar uma chave personalizada.
   - **Rede**: Especifique uma VPC, sub-rede e par de chaves para a instância, escolha se deseja ativar um endereço IP público e, opcionalmente, especifique uma configuração de proxy.

     Certifique-se de que tem o par de chaves correto a utilizar com o conetor. Sem um par de chaves, você não será capaz de acessar a máquina virtual do conetor.

   - **Grupo de segurança**: Escolha se deseja criar um novo grupo de segurança ou se deseja selecionar um grupo de segurança existente que permita as regras de entrada e saída necessárias.

     "Veja as regras do grupo de segurança da AWS".

   - **Revisão**: Revise suas seleções para verificar se a configuração está correta.

5. Selecione **Adicionar**.

   A instância deve estar pronta em cerca de 7 minutos. Você deve permanecer na página até que o processo esteja concluído.

**Resultado**

Após o processo ser concluído, o conetor está disponível para uso no BlueXP .

Se você tiver buckets do Amazon S3 na mesma conta da AWS onde criou o conetor, verá um ambiente de trabalho do Amazon S3 aparecer automaticamente na tela do BlueXP . "Saiba como gerenciar buckets do S3 no BlueXP "

#### Crie um conetor no AWS Marketplace

Um conetor é o software NetApp executado em sua rede na nuvem ou na rede local que

permite usar todos os recursos e serviços do BlueXP . Uma das opções de instalação disponíveis é criar um conetor na AWS diretamente do AWS Marketplace. Para criar um conetor no AWS Marketplace, você precisa configurar sua rede, preparar permissões da AWS, analisar os requisitos de instância e criar o conetor.

**Antes de começar**

- Você deve ter um "Compreensão dos conetores".
- Você deve rever "Limitações do conetor".

### Passo 1: Configurar a rede

Certifique-se de que a localização da rede onde pretende instalar o conetor suporta os seguintes requisitos. Atender a esses requisitos permite que o conetor gerencie recursos e processos em seu ambiente de nuvem híbrida.

**VPC e sub-rede**

Ao criar o conetor, você precisa especificar a VPC e a sub-rede onde o conetor deve residir.

**Conexões com redes de destino**

Um conetor requer uma conexão de rede com o local onde você está planejando criar e gerenciar ambientes de trabalho. Por exemplo, a rede em que você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de storage em seu ambiente local.

**Acesso de saída à Internet**

O local de rede onde você implantar o conetor deve ter uma conexão de saída de Internet para contatar pontos de extremidade específicos.

**Terminais contactados a partir do conetor**

O conetor requer acesso de saída à Internet para entrar em Contato com os seguintes endpoints, a fim de gerenciar recursos e processos em seu ambiente de nuvem pública para operações diárias.

Observe que os endpoints listados abaixo são todas as entradas CNAME.

| Endpoints | Finalidade |
|---|---|
| Serviços da AWS (amazonaws.com):<br>• CloudFormation<br>• Nuvem de computação elástica (EC2)<br>• Gerenciamento de identidade e acesso (IAM)<br>• Key Management Service (KMS)<br>• Serviço de token de segurança (STS)<br>• Serviço de armazenamento simples (S3) | Para gerenciar recursos na AWS. O endpoint exato depende da região da AWS que você está usando. "Consulte a documentação da AWS para obter detalhes" |
| https://support.NetApp.com https://mysupport.NetApp.com | Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte do NetApp. |

| Endpoints | Finalidade |
| --- | --- |
| https://*.api.BlueXP .NetApp.com<br><br>https://api.BlueXP .NetApp.com<br><br>https://*.cloudmanager.cloud.NetApp.com<br><br>https://cloudmanager.cloud.NetApp.com<br><br>https://NetApp-cloud-account.auth0.com | Para fornecer recursos e serviços SaaS no BlueXP .<br><br>Observe que o conetor está entrando em Contato atualmente com "cloudmanager.cloud.NetApp.com ", mas começará a entrar em Contato com "API.BlueXP .NetApp.com" em uma próxima versão. |
| https://*.blob.core.windows.net<br><br>https://cloudmanagerinfraprod.azurecr.io | Para atualizar o conetor e seus componentes do Docker. |

**Servidor proxy**

Se a sua empresa exigir a implantação de um servidor proxy para todo o tráfego de saída da Internet, obtenha as seguintes informações sobre o proxy HTTP ou HTTPS. Você precisará fornecer essas informações durante a instalação. Observe que o BlueXP não oferece suporte a servidores proxy transparentes.

- Endereço IP
- Credenciais
- Certificado HTTPS

**Portas**

Não há tráfego de entrada para o conetor, a menos que você o inicie ou se o conetor for usado como um proxy para enviar mensagens AutoSupport do Cloud Volumes ONTAP para o suporte da NetApp.

- HTTP (80) e HTTPS (443) fornecem acesso à IU local, que você usará em circunstâncias raras.
- SSH (22) só é necessário se você precisar se conetar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 são necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída à Internet não está disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída à Internet para enviar mensagens AutoSupport, o BlueXP configura automaticamente esses sistemas para usar um servidor proxy incluído no conetor. O único requisito é garantir que o grupo de segurança do conetor permita conexões de entrada pela porta 3128. Você precisará abrir essa porta depois de implantar o conetor.

**Ativar NTP**

Se estiver a planear utilizar a classificação BlueXP para analisar as suas fontes de dados empresariais, deve ativar um serviço de Protocolo de tempo de rede (NTP) no sistema de conetores BlueXP e no sistema de classificação BlueXP para que o tempo seja sincronizado entre os sistemas. "Saiba mais sobre a classificação BlueXP"

Você precisará implementar esse requisito de rede depois de criar o conetor.

### Etapa 2: Configurar permissões da AWS

Para se preparar para uma implantação de mercado, crie políticas do IAM na AWS e anexe-as a uma função do IAM. Ao criar o conetor no AWS Marketplace, você será solicitado a selecionar essa função do IAM.

#### Passos

1. Faça login no console da AWS e navegue até o serviço do IAM.
2. Criar uma política:
   a. Selecione **políticas > criar política**.
   b. Selecione **JSON** e copie e cole o conteúdo do "Política do IAM para o conetor".
   c. Conclua as etapas restantes para criar a política.

      Dependendo dos serviços do BlueXP que você está planejando usar, talvez seja necessário criar uma segunda política. Para regiões padrão, as permissões são distribuídas em duas políticas. Duas políticas são necessárias devido a um limite máximo de tamanho de caractere para políticas gerenciadas na AWS. "Saiba mais sobre as políticas do IAM para o conetor".
3. Crie uma função do IAM:
   a. Selecione **funções > criar função**.
   b. Selecione **AWS Service > EC2**.
   c. Adicione permissões anexando a política que você acabou de criar.
   d. Conclua as etapas restantes para criar a função.

#### Resultado

Agora você tem uma função do IAM que pode associar à instância do EC2 durante a implantação no AWS Marketplace.

### Etapa 3: Revise os requisitos da instância

Ao criar o conetor, você precisa escolher um tipo de instância EC2 que atenda aos seguintes requisitos.

**CPU**
8 núcleos ou 8 vCPUs

**RAM**
32 GB

**Tipo de instância do AWS EC2**
Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos t3,2xlarge.

### Passo 4: Crie o conetor

Crie o conetor diretamente do AWS Marketplace.

#### Sobre esta tarefa

A criação do conetor no AWS Marketplace implanta uma instância do EC2 na AWS usando uma configuração padrão. "Saiba mais sobre a configuração padrão do conetor".

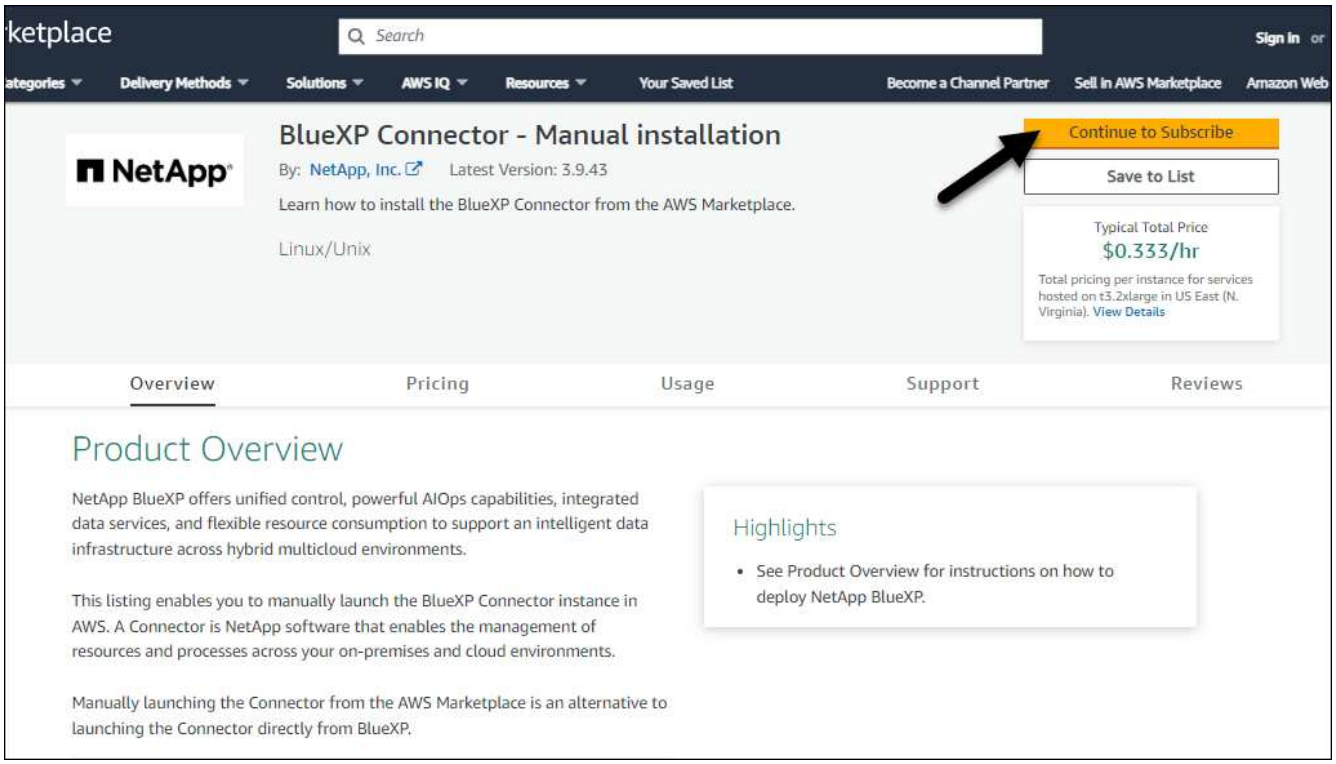
#### Antes de começar

Você deve ter o seguinte:

- VPC e sub-rede que atendem aos requisitos de rede.
- Uma função do IAM com uma política anexada que inclui as permissões necessárias para o conetor.
- Permissões para se inscrever e cancelar a assinatura do AWS Marketplace para seu usuário do IAM.
- Uma compreensão dos requisitos de CPU e RAM para a instância.
- Um par de chaves para a instância EC2.

**Passos**

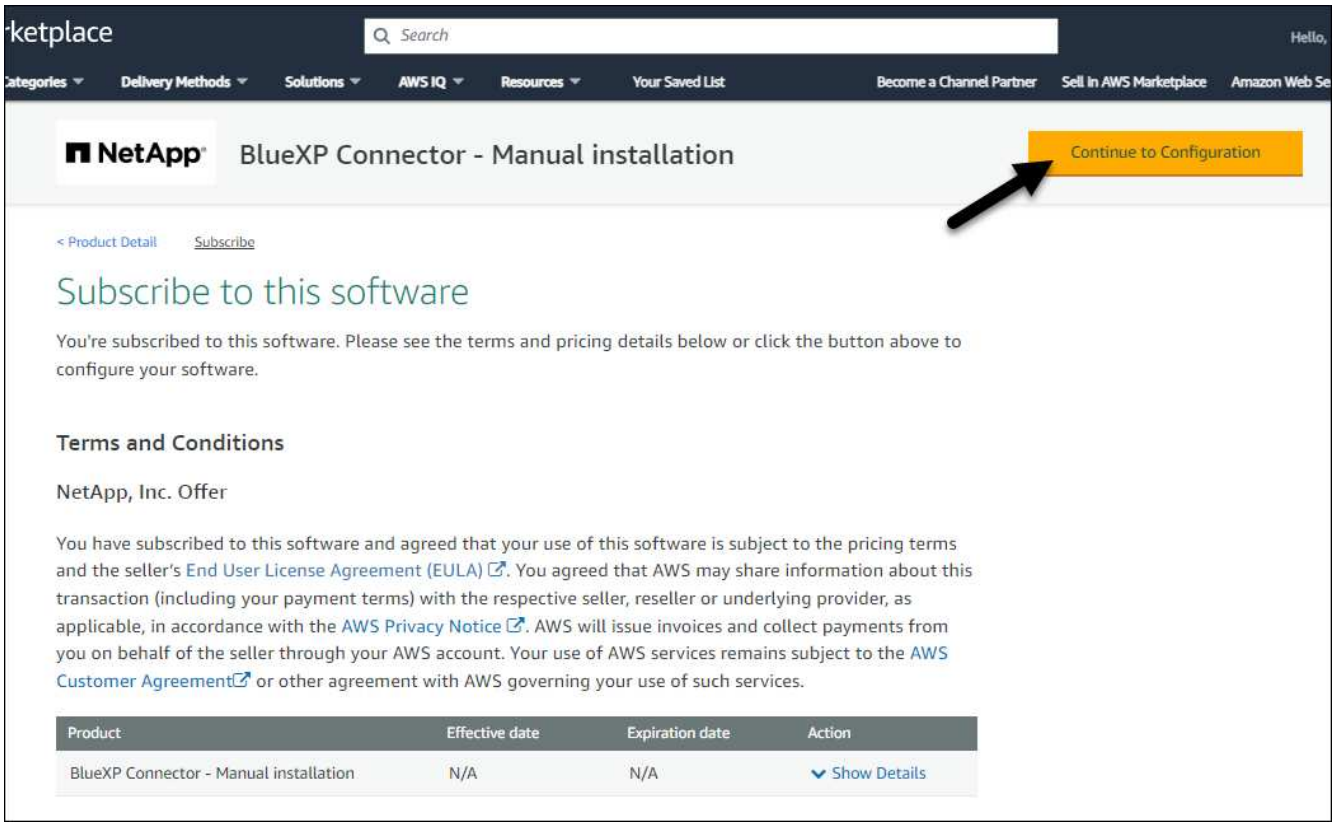
1. Vá para "Listagem do BlueXP  Connector no AWS Marketplace"
2. Na página Marketplace, selecione **Continue to Subscribe**.




3. Para assinar o software, selecione **aceitar termos**.

   O processo de assinatura pode levar alguns minutos.

4. Depois que o processo de assinatura estiver concluído, selecione **Continue to Configuration**.




5. Na página **Configure this software**, certifique-se de que selecionou a região correta e selecione **Continue to Launch**.
6. Na página **Launch this software**, em **Choose Action**, selecione **Launch through EC2** e, em seguida, selecione **Launch**.

   Estas etapas descrevem como iniciar a instância a partir do Console EC2 porque o console permite que você anexe uma função do IAM à instância do conetor. Isso não é possível usando a ação **Launch from Website**.

7. Siga as instruções para configurar e implantar a instância:

   - **Nome e tags**: Insira um nome e tags para a instância.
   - **Imagens de aplicativos e SO**: Pule esta seção. O AMI do conetor já está selecionado.
   - **Tipo de instância**: Dependendo da disponibilidade da região, escolha um tipo de instância que atenda aos requisitos de RAM e CPU (t3,2xlarge é pré-selecionado e recomendado).
   - **Par de chaves (login)**: Selecione o par de chaves que você deseja usar para se conetar com segurança à instância.
   - **Configurações de rede**: Edite as configurações de rede conforme necessário:
     - Escolha a VPC e a sub-rede desejadas.
     - Especifique se a instância deve ter um endereço IP público.
     - Especifique as configurações do grupo de segurança que ativam os métodos de conexão necessários para a instância do conetor: SSH, HTTP e HTTPS.

       "Veja as regras do grupo de segurança da AWS".
   - **Configurar armazenamento**: Mantenha o tamanho padrão e o tipo de disco para o volume raiz.

Se você quiser ativar a criptografia do Amazon EBS no volume raiz, selecione **Avançado**, expanda **volume 1**, selecione **criptografado** e escolha uma chave KMS.

- **Detalhes avançados**: Em **Perfil de instância do IAM**, escolha a função do IAM que inclui as permissões necessárias para o conetor.
- **Summary**: Revise o resumo e selecione **Launch instance**.

A AWS inicia o software com as configurações especificadas. A instância do conetor e o software devem estar sendo executados em aproximadamente cinco minutos.

8. Abra um navegador da Web a partir de um host que tenha uma conexão com a máquina virtual do conetor e insira o seguinte URL:

   <a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

9. Depois de iniciar sessão, configure o conetor:
   a. Especifique a organização BlueXP  a associar ao conetor.
   b. Introduza um nome para o sistema.
   c. Em **você está executando em um ambiente seguro?** mantenha o modo restrito desativado.

      Você deve manter o modo restrito desativado porque estas etapas descrevem como usar o BlueXP  no modo padrão. Você deve habilitar o modo restrito somente se tiver um ambiente seguro e quiser desconetar essa conta dos serviços de back-end do BlueXP . Se for esse o caso"Siga os passos para começar a utilizar o BlueXP  no modo restrito", .

   d. Selecione **vamos começar**.

**Resultado**

O conetor está agora instalado e configurado com a sua organização BlueXP .

Abra um navegador da Web e vá para a "Consola BlueXP" para começar a usar o conetor com o BlueXP .

Se você tiver buckets do Amazon S3 na mesma conta da AWS onde criou o conetor, verá um ambiente de trabalho do Amazon S3 aparecer automaticamente na tela do BlueXP . "Saiba como gerenciar buckets do S3 no BlueXP "

#### Instale manualmente o conetor na AWS

Um conetor é o software NetApp executado em sua rede na nuvem ou na rede local que permite usar todos os recursos e serviços do BlueXP . Uma das opções de instalação disponíveis é instalar manualmente o software Connector em um host Linux executado na AWS. Para instalar manualmente o conetor em seu próprio host Linux, você precisa analisar os requisitos de host, configurar sua rede, preparar permissões da AWS, instalar o conetor e fornecer as permissões que você preparou.

**Antes de começar**

- Você deve ter um "Compreensão dos conetores".
- Você deve rever "Limitações do conetor".

### Etapa 1: Revise os requisitos do host

O software do conetor deve ser executado em um host que atenda a requisitos específicos do sistema operacional, requisitos de RAM, requisitos de porta, etc.

#### Host dedicado

O conetor não é suportado em um host que é compartilhado com outros aplicativos. O host deve ser um host dedicado.

#### Hipervisor

É necessário um hypervisor bare metal ou hospedado certificado para executar um sistema operacional suportado.

#### requisitos de sistema operacional e contentor

O BlueXP  suporta o conetor com os seguintes sistemas operacionais ao usar o BlueXP  no modo padrão ou no modo restrito. Uma ferramenta de orquestração de contêineres é necessária antes de instalar o conetor.

| Sistema operacional | Versões de OS compatíveis | Versões de conetor suportadas | Ferramenta de recipiente necessária | SELinux |
|---|---|---|---|---|
| Red Hat Enterprise Linux | 9,1 a 9,4<br><br>8,6 a 8,10 | 3.9.40 ou posterior com BlueXP  no modo padrão ou modo restrito | Podman versão 4.6.1 ou 4.9.4<br><br>Veja os requisitos de configuração do Podman. | Suporte no modo de execução ou modo permissivo 1 |
| Ubuntu | 24,04 LTS | 3.9.45 ou posterior com BlueXP  no modo padrão ou modo restrito | Docker Engine 26.0.0 | Não suportado |

Notas:

1. O gerenciamento de sistemas Cloud Volumes ONTAP não é suportado por conetores que tenham o SELinux habilitado no sistema operacional.
2. O conetor é suportado em versões em inglês destes sistemas operativos.
3. Para o RHEL, o host deve estar registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar repositórios para atualizar o software necessário de 3rd partes durante a instalação do conetor.

#### CPU

8 núcleos ou 8 vCPUs

#### RAM

32 GB

#### Tipo de instância do AWS EC2

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos t3,2xlarge.

**Par de chaves**

Ao criar o conetor, você precisará selecionar um par de chaves EC2 para usar com a instância.

**COLOQUE limite de salto de resposta ao usar IMDSv2**

Se IMDSv2 estiver habilitado na instância EC2 (essa é a configuração padrão para novas instâncias EC2), você deverá alterar o limite de salto de resposta PUT na instância para 3. Se você não alterar o limite na instância do EC2, receberá um erro de inicialização da IU quando tentar configurar o conetor.

- "Exigir o uso do IMDSv2 em instâncias do Amazon EC2"
- "Documentação da AWS: Altere o limite de saltos de resposta PUT"

**Espaço em disco em /opt**

100 GiB de espaço deve estar disponível

O BlueXP usa `/opt` para instalar o `/opt/application/netapp` diretório e seu conteúdo.

**Espaço em disco em /var**

20 GiB de espaço deve estar disponível

O BlueXP requer esse espaço `/var` porque o Docker ou o Podman são arquitetados para criar os contentores dentro desse diretório. Especificamente, eles irão criar contentores no `/var/lib/containers/storage` diretório. Montagens externas ou links simbólicos não funcionam para este espaço.

### Passo 2: Instale o Podman ou Docker Engine

Dependendo do seu sistema operacional, o Podman ou o Docker Engine são necessários antes de instalar o conetor.

- O Podman é necessário para o Red Hat Enterprise Linux 8 e 9.

  Veja as versões do Podman suportadas pelo BlueXP .

- Docker Engine é necessário para o Ubuntu.

  Veja as versões do Docker Engine que o BlueXP suporta.

**Exemplo 1. Passos**

**Podman**

Siga estas etapas para instalar o Podman e configurá-lo para atender aos seguintes requisitos:

- O serviço podman.socket deve ser ativado e iniciado
- python3 deve ser instalado
- O pacote podman-compose versão 1.0.6 deve ser instalado
- Podman-compose deve ser adicionado à variável de ambiente PATH

**Passos**

1. Remova o pacote podman-docker se ele estiver instalado no host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Instale o Podman.

   O Podman está disponível nos repositórios oficiais do Red Hat Enterprise Linux.

   Para Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

   Onde o <version> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas pelo BlueXP .

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

   Onde o <version> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas pelo BlueXP .

3. Ative e inicie o serviço podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Instale o python3.

```
sudo dnf install python3
```

5. Instale o pacote do repositório EPEL se ainda não estiver disponível no seu sistema.

Esta etapa é necessária porque o podman-compose está disponível no repositório extra Packages for Enterprise Linux (EPEL).

Para Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

Para Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Instale o pacote podman-compose 1,0.6.

```
sudo dnf install podman-compose-1.0.6
```

> Usar o `dnf install` comando atende ao requisito para adicionar podman-compose à variável de ambiente PATH. O comando installation adiciona podman-compose ao /usr/bin, que já está incluído na `secure_path` opção no host.

**Docker Engine**

Siga a documentação do Docker para instalar o Docker Engine.

**Passos**

1. "Veja as instruções de instalação do Docker"

   Certifique-se de seguir as etapas para instalar uma versão específica do Docker Engine. Instalar a versão mais recente irá instalar uma versão do Docker que o BlueXP  não suporta.

2. Verifique se o Docker está ativado e em execução.

```
sudo systemctl enable docker && sudo systemctl start docker
```

### Passo 3: Configurar a rede

Certifique-se de que a localização da rede onde pretende instalar o conetor suporta os seguintes requisitos. Atender a esses requisitos permite que o conetor gerencie recursos e processos em seu ambiente de nuvem híbrida.

**Conexões com redes de destino**

Um conetor requer uma conexão de rede com o local onde você está planejando criar e gerenciar ambientes de trabalho. Por exemplo, a rede em que você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de storage em seu ambiente local.

### Acesso de saída à Internet

O local de rede onde você implantar o conetor deve ter uma conexão de saída de Internet para contatar pontos de extremidade específicos.

### Endpoints contatados de computadores ao usar o console baseado na Web do BlueXP

Os computadores que acessam o console BlueXP  a partir de um navegador da Web devem ter a capacidade de entrar em Contato com vários endpoints. Você precisará usar o console BlueXP  para configurar o conetor e para uso diário do BlueXP .

"Prepare a rede para o console BlueXP ".

### Terminais contactados durante a instalação manual

Quando você instala manualmente o conetor em seu próprio host Linux, o instalador do conetor requer acesso aos seguintes URLs durante o processo de instalação:

- https://mysupport.NetApp.com
- https://signin.b2c.NetApp.com (este endpoint é o URL CNAME para https://mysupport.NetApp.com)
- https://cloudmanager.cloud.NetApp.com/locação
- https://stream.cloudmanager.cloud.NetApp.com
- https://production-artifacts.cloudmanager.cloud.NetApp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  O host pode tentar atualizar os pacotes do sistema operacional durante a instalação. O host pode entrar em Contato com diferentes sites de espelhamento para esses pacotes do sistema operacional.

### Terminais contactados a partir do conetor

O conetor requer acesso de saída à Internet para entrar em Contato com os seguintes endpoints, a fim de gerenciar recursos e processos em seu ambiente de nuvem pública para operações diárias.

Observe que os endpoints listados abaixo são todas as entradas CNAME.

| Endpoints | Finalidade |
|---|---|
| Serviços da AWS (amazonaws.com):<br>• CloudFormation<br>• Nuvem de computação elástica (EC2)<br>• Gerenciamento de identidade e acesso (IAM)<br>• Key Management Service (KMS)<br>• Serviço de token de segurança (STS)<br>• Serviço de armazenamento simples (S3) | Para gerenciar recursos na AWS. O endpoint exato depende da região da AWS que você está usando. "Consulte a documentação da AWS para obter detalhes" |
| https://support.NetApp.com https://mysupport.NetApp.com | Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte do NetApp. |

| Endpoints | Finalidade |
| --- | --- |
| https://*.api.BlueXP .NetApp.com<br><br>https://api.BlueXP .NetApp.com<br><br>https://*.cloudmanager.cloud.NetApp.com<br><br>https://cloudmanager.cloud.NetApp.com<br><br>https://NetApp-cloud-account.auth0.com | Para fornecer recursos e serviços SaaS no BlueXP .<br><br>Observe que o conetor está entrando em Contato atualmente com "cloudmanager.cloud.NetApp.com ", mas começará a entrar em Contato com "API.BlueXP .NetApp.com" em uma próxima versão. |
| https://*.blob.core.windows.net<br><br>https://cloudmanagerinfraprod.azurecr.io | Para atualizar o conetor e seus componentes do Docker. |

**Servidor proxy**

Se a sua empresa exigir a implantação de um servidor proxy para todo o tráfego de saída da Internet, obtenha as seguintes informações sobre o proxy HTTP ou HTTPS. Você precisará fornecer essas informações durante a instalação. Observe que o BlueXP não oferece suporte a servidores proxy transparentes.

- Endereço IP
- Credenciais
- Certificado HTTPS

**Portas**

Não há tráfego de entrada para o conetor, a menos que você o inicie ou se o conetor for usado como um proxy para enviar mensagens AutoSupport do Cloud Volumes ONTAP para o suporte da NetApp.

- HTTP (80) e HTTPS (443) fornecem acesso à IU local, que você usará em circunstâncias raras.
- SSH (22) só é necessário se você precisar se conetar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 são necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída à Internet não está disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída à Internet para enviar mensagens AutoSupport, o BlueXP configura automaticamente esses sistemas para usar um servidor proxy incluído no conetor. O único requisito é garantir que o grupo de segurança do conetor permita conexões de entrada pela porta 3128. Você precisará abrir essa porta depois de implantar o conetor.

**Ativar NTP**

Se estiver a planear utilizar a classificação BlueXP para analisar as suas fontes de dados empresariais, deve ativar um serviço de Protocolo de tempo de rede (NTP) no sistema de conetores BlueXP e no sistema de classificação BlueXP para que o tempo seja sincronizado entre os sistemas. "Saiba mais sobre a classificação BlueXP"

### Passo 4: Configurar permissões

Você precisa fornecer permissões da AWS ao BlueXP  usando uma das seguintes opções:

- Opção 1: Crie políticas do IAM e anexe as políticas a uma função do IAM que você pode associar à instância do EC2.
- Opção 2: Forneça ao BlueXP  a chave de acesso da AWS para um usuário do IAM que tenha as permissões necessárias.

Siga as etapas para preparar permissões para o BlueXP .

**Função do IAM**

**Passos**

1. Faça login no console da AWS e navegue até o serviço do IAM.
2. Criar uma política:
   a. Selecione **políticas > criar política**.
   b. Selecione **JSON** e copie e cole o conteúdo do "Política do IAM para o conetor".
   c. Conclua as etapas restantes para criar a política.

      Dependendo dos serviços do BlueXP que você está planejando usar, talvez seja necessário criar uma segunda política. Para regiões padrão, as permissões são distribuídas em duas políticas. Duas políticas são necessárias devido a um limite máximo de tamanho de caractere para políticas gerenciadas na AWS. "Saiba mais sobre as políticas do IAM para o conetor".
3. Crie uma função do IAM:
   a. Selecione **funções > criar função**.
   b. Selecione **AWS Service > EC2**.
   c. Adicione permissões anexando a política que você acabou de criar.
   d. Conclua as etapas restantes para criar a função.

**Resultado**

Agora você tem uma função do IAM que pode associar à instância do EC2 depois de instalar o conetor.

**Chave de acesso da AWS**

**Passos**

1. Faça login no console da AWS e navegue até o serviço do IAM.
2. Criar uma política:
   a. Selecione **políticas > criar política**.
   b. Selecione **JSON** e copie e cole o conteúdo do "Política do IAM para o conetor".
   c. Conclua as etapas restantes para criar a política.

      Dependendo dos serviços do BlueXP que você está planejando usar, talvez seja necessário criar uma segunda política.

   Para regiões padrão, as permissões são distribuídas em duas políticas. Duas políticas são necessárias devido a um limite máximo de tamanho de caractere para políticas gerenciadas na AWS. "Saiba mais sobre as políticas do IAM para o conetor".
3. Anexe as políticas a um usuário do IAM.
   - "Documentação da AWS: Criando funções do IAM"
   - "Documentação da AWS: Adicionando e removendo políticas do IAM"
4. Certifique-se de que o utilizador tem uma chave de acesso que pode adicionar ao BlueXP depois de instalar o conetor.

**Resultado**

Agora você tem um usuário do IAM com as permissões necessárias e uma chave de acesso que pode

fornecer ao BlueXP .

### Passo 5: Instale o conetor

Após a conclusão dos pré-requisitos, você pode instalar manualmente o software em seu próprio host Linux.

**Antes de começar**

Você deve ter o seguinte:

- Root Privileges para instalar o conetor.
- Detalhes sobre um servidor proxy, se for necessário um proxy para acesso à Internet a partir do conetor.

  Você tem a opção de configurar um servidor proxy após a instalação, mas isso requer a reinicialização do conetor.

  Observe que o BlueXP  não oferece suporte a servidores proxy transparentes.

- Um certificado assinado pela CA, se o servidor proxy usar HTTPS ou se o proxy for um proxy intercetor.

**Sobre esta tarefa**

O instalador disponível no site de suporte da NetApp pode ser uma versão anterior. Após a instalação, o conetor se atualiza automaticamente se uma nova versão estiver disponível.

**Passos**

1. Se as variáveis de sistema *http_proxy* ou *https_proxy* estiverem definidas no host, remova-as:

   ```
   unset http_proxy
   unset https_proxy
   ```

   Se você não remover essas variáveis do sistema, a instalação falhará.

2. Faça o download do software Connector do "Site de suporte da NetApp"e copie-o para o host Linux.

   Você deve baixar o instalador do conetor "online" destinado a ser usado em sua rede ou na nuvem. Um instalador "offline" separado está disponível para o conetor, mas só é suportado com implantações de modo privado.

3. Atribua permissões para executar o script.

   ```
   chmod +x BlueXP-Connector-Cloud-<version>
   ```

   Onde <version> é a versão do conetor que você baixou.

4. Execute o script de instalação.

   ```
    ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
   --cacert <path and file name of a CA-signed certificate>
   ```

Os parâmetros --proxy e --cacert são opcionais. Se você tiver um servidor proxy, será necessário inserir os parâmetros como mostrado. O instalador não solicita que você forneça informações sobre um proxy.

Aqui está um exemplo do comando usando ambos os parâmetros opcionais:

```
 ./BlueXP-Connector-Cloud-v3.9.40--proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

--proxy configura o conetor para usar um servidor proxy HTTP ou HTTPS usando um dos seguintes formatos:

- http://address:port
- http://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Observe o seguinte:

  - O usuário pode ser um usuário local ou usuário de domínio.
  - Para um usuário de domínio, você deve usar o código ASCII para a como mostrado acima.
  - O BlueXP  não suporta nomes de usuário ou senhas que incluem o caractere A.
  - Se a senha incluir qualquer um dos seguintes carateres especiais, você deve escapar desse caractere especial, prependendo-o com uma barra invertida: & Ou !

    Por exemplo:

  http://bxpproxyuser:netapp1\!@address:3128

--cacert especifica um certificado assinado pela CA a ser usado para acesso HTTPS entre o conetor e o servidor proxy. Este parâmetro só é necessário se especificar um servidor proxy HTTPS ou se o proxy for um proxy intercetor.

5. Aguarde até que a instalação seja concluída.

   No final da instalação, o serviço de conetor (occm) será reiniciado duas vezes se você tiver especificado um servidor proxy.

6. Abra um navegador da Web a partir de um host que tenha uma conexão com a máquina virtual do conetor e insira o seguinte URL:

   <a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

7. Depois de iniciar sessão, configure o conetor:
   a. Especifique a organização BlueXP  a associar ao conetor.
   b. Introduza um nome para o sistema.

c. Em **você está executando em um ambiente seguro?** mantenha o modo restrito desativado.

   Você deve manter o modo restrito desativado porque estas etapas descrevem como usar o BlueXP no modo padrão. Você deve habilitar o modo restrito somente se tiver um ambiente seguro e quiser desconetar essa conta dos serviços de back-end do BlueXP . Se for esse o caso"Siga os passos para começar a utilizar o BlueXP no modo restrito", .

d. Selecione **vamos começar**.

**Resultado**

O conetor está agora instalado e está configurado com a sua organização BlueXP .

Se você tiver buckets do Amazon S3 na mesma conta da AWS onde criou o conetor, verá um ambiente de trabalho do Amazon S3 aparecer automaticamente na tela do BlueXP . "Saiba como gerenciar buckets do S3 no BlueXP "

### Passo 6: Forneça permissões para o BlueXP

Agora que você instalou o conetor, você precisa fornecer ao BlueXP as permissões da AWS que você configurou anteriormente. O fornecimento de permissões permite que o BlueXP gerencie sua infraestrutura de dados e storage na AWS.

**Função do IAM**

Anexe a função do IAM que você criou anteriormente à instância do Connector EC2.

**Passos**

1. Vá para o console do Amazon EC2.
2. Selecione **instâncias**.
3. Selecione a instância do conetor.
4. Selecione **ações > Segurança > Modificar função do IAM**.
5. Selecione a função do IAM e selecione **Atualizar função do IAM**.

**Resultado**

O BlueXP  agora tem as permissões necessárias para executar ações na AWS em seu nome.

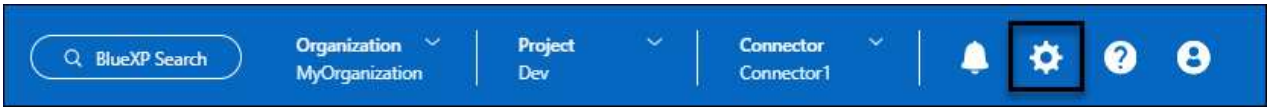
Passe à "Consola BlueXP" para começar a utilizar o conetor com o BlueXP .

**Chave de acesso da AWS**

Forneça ao BlueXP  a chave de acesso da AWS para um usuário do IAM que tenha as permissões necessárias.

**Passos**

1. Certifique-se de que o conetor correto está atualmente selecionado no BlueXP .
2. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.




3. Selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Localização das credenciais**: Selecione **Amazon Web Services > Connector**.
   b. **Definir credenciais**: Insira uma chave de acesso da AWS e uma chave secreta.
   c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.
   d. **Revisão**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

**Resultado**

O BlueXP  agora tem as permissões necessárias para executar ações na AWS em seu nome.

Passe à "Consola BlueXP" para começar a utilizar o conetor com o BlueXP .

## Azure

### Opções de instalação do conetor no Azure

Existem algumas maneiras diferentes de criar um conetor no Azure. Diretamente de BlueXP  é a maneira mais comum.

Estão disponíveis as seguintes opções de instalação:

- "Crie um conetor diretamente do BlueXP " (esta é a opção padrão)

  Esta ação lança uma VM executando Linux e o software Connector em um VNet de sua escolha.

- "Crie um conetor a partir do Azure Marketplace"

  Essa ação também lança uma VM executando o Linux e o software Connector, mas a implantação é iniciada diretamente do Azure Marketplace, em vez do BlueXP .

- "Baixe e instale manualmente o software em seu próprio host Linux"

A opção de instalação que você escolher afeta a forma como você se prepara para a instalação. Isso inclui como você fornece ao BlueXP  as permissões necessárias que ele precisa para autenticar e gerenciar recursos no Azure.

#### Crie um conetor no Azure a partir do BlueXP

Um conetor é o software NetApp executado em sua rede na nuvem ou na rede local que permite usar todos os recursos e serviços do BlueXP . Uma das opções de instalação disponíveis é criar um conetor no Azure diretamente a partir do BlueXP . Para criar um conetor no Azure a partir do BlueXP , você precisa configurar sua rede, preparar permissões do Azure e, em seguida, criar o conetor.

**Antes de começar**

- Você deve ter um "Compreensão dos conetores".
- Você deve rever "Limitações do conetor".

**Passo 1: Configurar a rede**

Certifique-se de que a localização da rede onde pretende instalar o conetor suporta os seguintes requisitos. Atender a esses requisitos permite que o conetor gerencie recursos e processos em seu ambiente de nuvem híbrida.

**Região do Azure**

Se você usar o Cloud Volumes ONTAP, o conetor deve ser implantado na mesma região do Azure que os sistemas Cloud Volumes ONTAP gerenciados ou no "Par de regiões do Azure" para os sistemas Cloud Volumes ONTAP. Esse requisito garante que uma conexão com o Azure Private Link seja usada entre o Cloud Volumes ONTAP e suas contas de armazenamento associadas.

"Saiba como o Cloud Volumes ONTAP usa um link privado do Azure"

**VNet e sub-rede**

Ao criar o conetor, você precisa especificar a VNet e a sub-rede onde o conetor deve residir.

**Conexões com redes de destino**

Um conetor requer uma conexão de rede com o local onde você está planejando criar e gerenciar ambientes de trabalho. Por exemplo, a rede em que você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de storage em seu ambiente local.

### Acesso de saída à Internet

O local de rede onde você implantar o conetor deve ter uma conexão de saída de Internet para contatar pontos de extremidade específicos.

### Terminais contactados a partir do conetor

O conetor requer acesso de saída à Internet para entrar em Contato com os seguintes endpoints, a fim de gerenciar recursos e processos em seu ambiente de nuvem pública para operações diárias.

Observe que os endpoints listados abaixo são todas as entradas CNAME.

| Endpoints | Finalidade |
|---|---|
| https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net | Para gerenciar recursos em regiões públicas do Azure. |
| https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn | Para gerenciar recursos nas regiões do Azure China. |
| https://support.NetApp.com https://mysupport.NetApp.com | Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte do NetApp. |
| https://*.api.BlueXP .NetApp.com<br><br>https://api.BlueXP .NetApp.com<br><br>https://*.cloudmanager.cloud.NetApp.com<br><br>https://cloudmanager.cloud.NetApp.com<br><br>https://NetApp-cloud-account.auth0.com | Para fornecer recursos e serviços SaaS no BlueXP .<br><br>Observe que o conetor está entrando em Contato atualmente com "cloudmanager.cloud.NetApp.com ", mas começará a entrar em Contato com "API.BlueXP .NetApp.com" em uma próxima versão. |
| https://*.blob.core.windows.net<br><br>https://cloudmanagerinfraprod.azurecr.io | Para atualizar o conetor e seus componentes do Docker. |

### Terminais contactados a partir da consola BlueXP

À medida que você usa o console baseado na Web do BlueXP  fornecido pela camada SaaS, ele entra em Contato com vários endpoints para concluir as tarefas de gerenciamento de dados. Isso inclui endpoints que são contatados para implantar o conetor a partir do console BlueXP .

"Veja a lista de endpoints contactados a partir da consola BlueXP ".

### Servidor proxy

Se a sua empresa exigir a implantação de um servidor proxy para todo o tráfego de saída da Internet, obtenha as seguintes informações sobre o proxy HTTP ou HTTPS. Você precisará fornecer essas informações durante a instalação. Observe que o BlueXP  não oferece suporte a servidores proxy transparentes.

- Endereço IP
- Credenciais
- Certificado HTTPS

**Portas**

Não há tráfego de entrada para o conetor, a menos que você o inicie ou se o conetor for usado como um proxy para enviar mensagens AutoSupport do Cloud Volumes ONTAP para o suporte da NetApp.

- HTTP (80) e HTTPS (443) fornecem acesso à IU local, que você usará em circunstâncias raras.
- SSH (22) só é necessário se você precisar se conetar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 são necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída à Internet não está disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída à Internet para enviar mensagens AutoSupport, o BlueXP configura automaticamente esses sistemas para usar um servidor proxy incluído no conetor. O único requisito é garantir que o grupo de segurança do conetor permita conexões de entrada pela porta 3128. Você precisará abrir essa porta depois de implantar o conetor.

**Ativar NTP**

Se estiver a planear utilizar a classificação BlueXP para analisar as suas fontes de dados empresariais, deve ativar um serviço de Protocolo de tempo de rede (NTP) no sistema de conetores BlueXP e no sistema de classificação BlueXP para que o tempo seja sincronizado entre os sistemas. "Saiba mais sobre a classificação BlueXP"

Você precisará implementar esse requisito de rede depois de criar o conetor.

### Passo 2: Crie uma função personalizada

Crie uma função personalizada do Azure que você pode atribuir à sua conta do Azure ou a um diretor de serviço do Microsoft Entra. O BlueXP se autentica com o Azure e usa essas permissões para criar a instância do Connector em seu nome.

Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se você preferir usar um método diferente, consulte "Documentação do Azure"

**Passos**

1. Copie as permissões necessárias para uma nova função personalizada no Azure e salve-as em um arquivo JSON.

   Esta função personalizada contém apenas as permissões necessárias para iniciar a VM Connector no Azure a partir do BlueXP . Não use esta política para outras situações. Quando o BlueXP cria o conetor, ele aplica um novo conjunto de permissões à VM do conetor que permite que o conetor gerencie recursos do Azure.

```
{
    "Name": "Azure SetupAsService",
    "Actions": [
        "Microsoft.Compute/disks/delete",
        "Microsoft.Compute/disks/read",
```

```
        "Microsoft.Compute/disks/write",
        "Microsoft.Compute/locations/operations/read",
        "Microsoft.Compute/operations/read",
        "Microsoft.Compute/virtualMachines/instanceView/read",
        "Microsoft.Compute/virtualMachines/read",
        "Microsoft.Compute/virtualMachines/write",
        "Microsoft.Compute/virtualMachines/delete",
        "Microsoft.Compute/virtualMachines/extensions/write",
        "Microsoft.Compute/virtualMachines/extensions/read",
        "Microsoft.Compute/availabilitySets/read",
        "Microsoft.Network/locations/operationResults/read",
        "Microsoft.Network/locations/operations/read",
        "Microsoft.Network/networkInterfaces/join/action",
        "Microsoft.Network/networkInterfaces/read",
        "Microsoft.Network/networkInterfaces/write",
        "Microsoft.Network/networkInterfaces/delete",
        "Microsoft.Network/networkSecurityGroups/join/action",
        "Microsoft.Network/networkSecurityGroups/read",
        "Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/virtualNetworks/subnets/join/action",
        "Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
        "Microsoft.Network/virtualNetworks/virtualMachines/read",
        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/publicIPAddresses/delete",
        "Microsoft.Network/networkSecurityGroups/securityRules/read",
        "Microsoft.Network/networkSecurityGroups/securityRules/write",
        "Microsoft.Network/networkSecurityGroups/securityRules/delete",
        "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
d",
        "Microsoft.Network/networkInterfaces/ipConfigurations/read",
        "Microsoft.Resources/deployments/operations/read",
        "Microsoft.Resources/deployments/read",
        "Microsoft.Resources/deployments/delete",
        "Microsoft.Resources/deployments/cancel/action",
        "Microsoft.Resources/deployments/validate/action",
        "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.Authorization/roleDefinitions/write",
        "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
        "Microsoft.Network/networkSecurityGroups/delete",
        "Microsoft.Storage/storageAccounts/delete",
        "Microsoft.Storage/storageAccounts/write",
        "Microsoft.Resources/deployments/write",
        "Microsoft.Resources/deployments/operationStatuses/read",
        "Microsoft.Authorization/roleAssignments/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure SetupAsService",
    "IsCustom": "true"
}
```

2. Modifique o JSON adicionando seu ID de assinatura do Azure ao escopo atribuível.

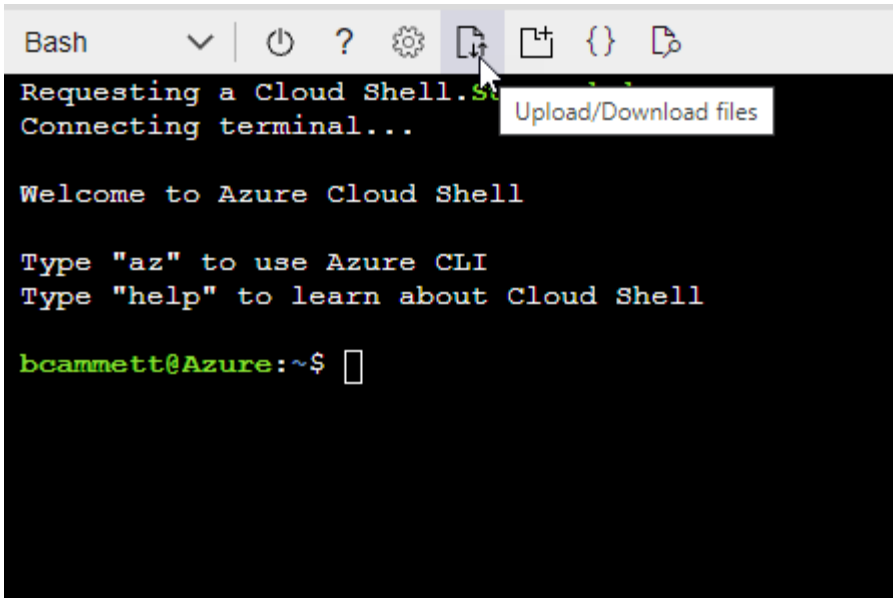
   **Exemplo**

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],
```

3. Use o arquivo JSON para criar uma função personalizada no Azure.

   As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

   a. Comece "Azure Cloud Shell" e escolha o ambiente Bash.
   b. Carregue o arquivo JSON.




c. Digite o seguinte comando CLI do Azure:

```
az role definition create --role-definition
Policy_for_Setup_As_Service_Azure.json
```

Agora você deve ter uma função personalizada chamada *Azure SetupAsService*. Agora você pode aplicar essa função personalizada à sua conta de usuário ou a um responsável de serviço.

**Passo 3: Configurar a autenticação**

Ao criar o conetor do BlueXP , você precisa fornecer um login que permita que o BlueXP se autentique com o Azure e implante a VM. Você tem duas opções:

1. Inicie sessão com a sua conta Azure quando solicitado. Essa conta deve ter permissões específicas do Azure. Esta é a opção padrão.
2. Fornecer detalhes sobre um responsável de serviço Microsoft Entra. Este princípio de serviço também requer permissões específicas.

Siga as etapas para preparar um desses métodos de autenticação para uso com o BlueXP .

**Conta Azure**

Atribua a função personalizada ao usuário que implantará o conetor do BlueXP .

**Passos**

1. No portal do Azure, abra o serviço **Subscrições** e selecione a assinatura do usuário.
2. Clique em **Access Control (IAM)**.
3. Clique em **Adicionar** > **Adicionar atribuição de função** e, em seguida, adicione as permissões:
   a. Selecione a função **Azure SetupAsService** e clique em **Next**.

      Azure SetupAsService é o nome padrão fornecido na política de implantação do conetor para o Azure. Se você escolher um nome diferente para a função, selecione esse nome em vez disso.

   b. Mantenha **Usuário, grupo ou responsável do serviço** selecionado.
   c. Clique em **Selecionar membros**, escolha sua conta de usuário e clique em **Selecionar**.
   d. Clique em **seguinte**.
   e. Clique em **Rever e atribuir**.

**Resultado**

O usuário do Azure agora tem as permissões necessárias para implantar o conetor do BlueXP .

**Serviço principal**

Em vez de iniciar sessão com a sua conta Azure, pode fornecer à BlueXP  as credenciais de um responsável de serviço do Azure que tem as permissões necessárias.

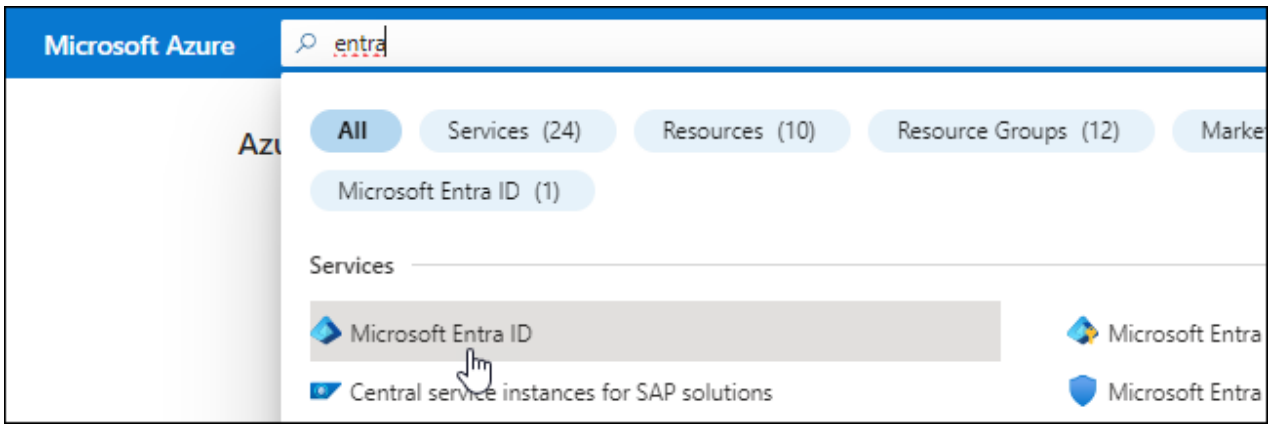
Crie e configure um princípio de serviço no Microsoft Entra ID e obtenha as credenciais do Azure de que o BlueXP  precisa.

**Crie um aplicativo Microsoft Entra para controle de acesso baseado em funções**

1. Certifique-se de ter permissões no Azure para criar um aplicativo do ative Directory e atribuir o aplicativo a uma função.

   Para obter mais informações, consulte "Documentação do Microsoft Azure: Permissões necessárias"

2. No portal do Azure, abra o serviço **Microsoft Entra ID**.



3. No menu, selecione **inscrições de aplicativos**.
4. Selecione **novo registo**.
5. Especifique detalhes sobre o aplicativo:
   - **Nome**: Insira um nome para o aplicativo.
   - **Tipo de conta**: Selecione um tipo de conta (qualquer funcionará com o BlueXP ).
   - * URI de redirecionamento*: Você pode deixar este campo em branco.
6. Selecione **Registe-se**.

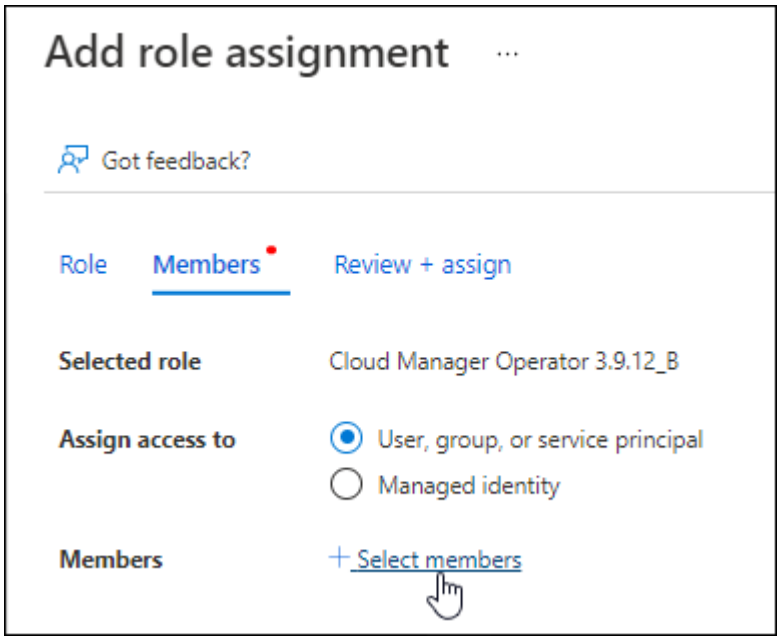
   Você criou o aplicativo AD e o principal de serviço.

**Atribua a função personalizada ao aplicativo**

1. No portal do Azure, abra o serviço **Subscrições**.
2. Selecione a subscrição.
3. Clique em **Access control (IAM) > Add > Add Role assignment** (Adicionar > Adicionar atribuição de função*).
4. Na guia **Role**, selecione a função **Operador BlueXP** e clique em **Avançar**.
5. Na guia **Membros**, execute as seguintes etapas:

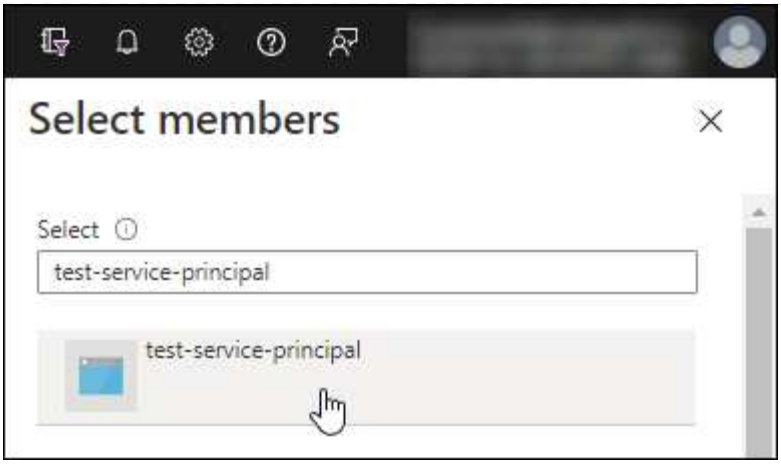
   a. Mantenha **Usuário, grupo ou responsável do serviço** selecionado.

   b. Clique em **Selecionar membros**.




   c. Procure o nome da aplicação.

   Aqui está um exemplo:




a. Selecione a aplicação e clique em **Select**.

b. Clique em **seguinte**.

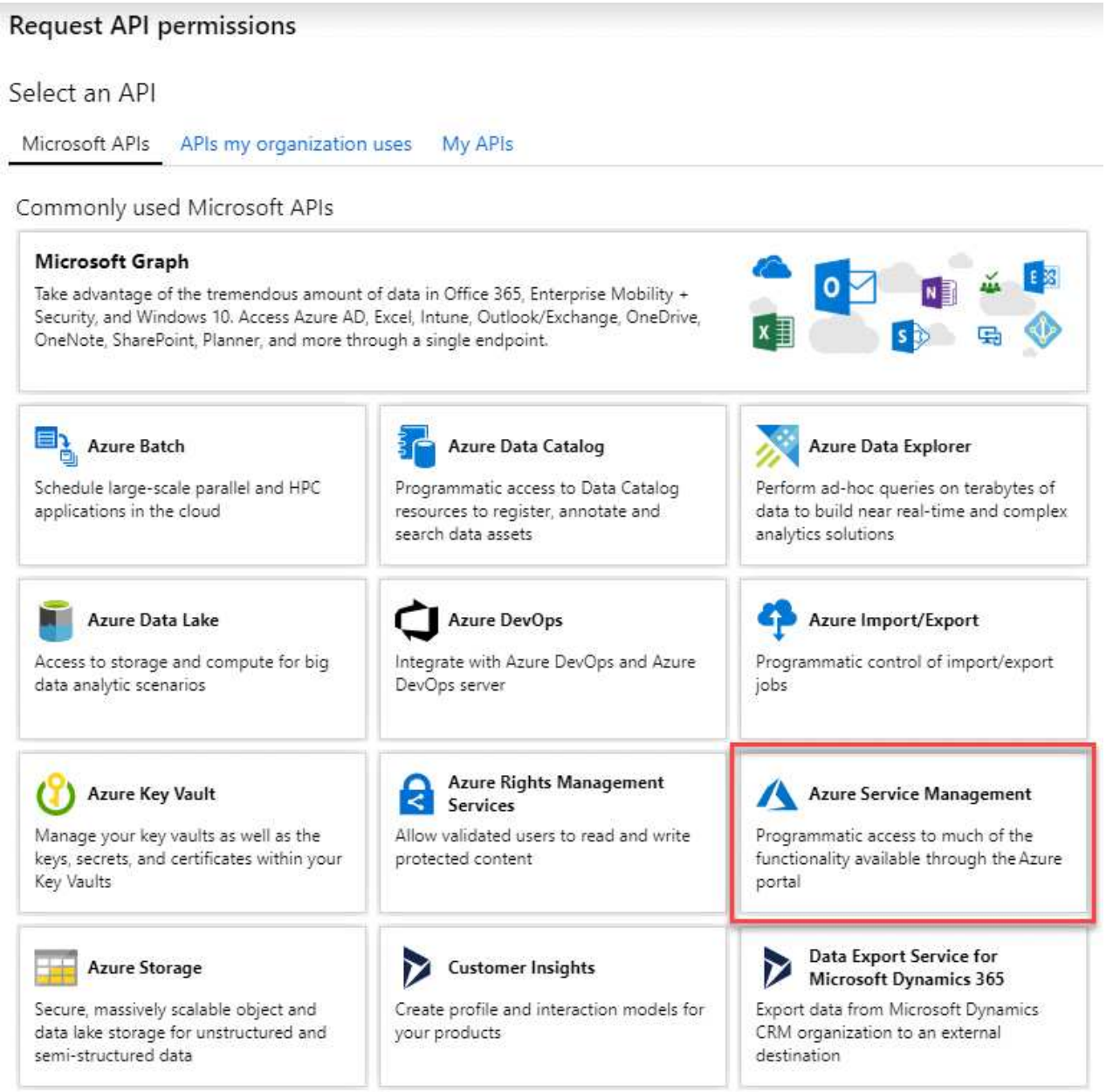
6. Clique em **Rever e atribuir**.

   O principal de serviço agora tem as permissões necessárias do Azure para implantar o conetor.

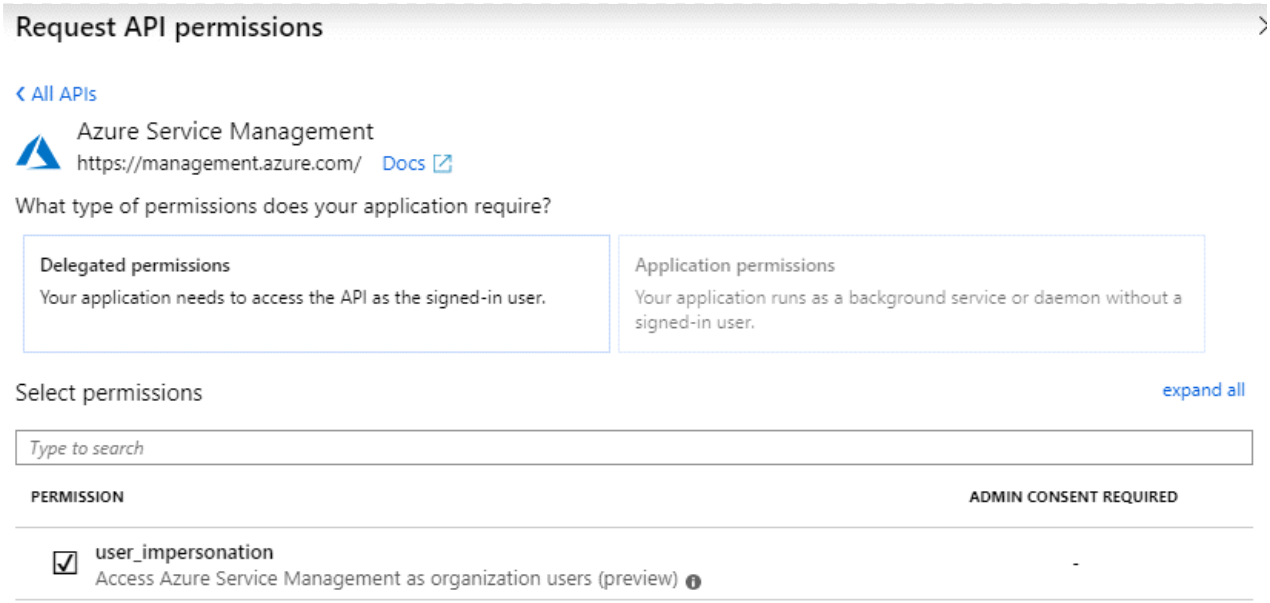
   Se você quiser gerenciar recursos em várias assinaturas do Azure, então você deve vincular o principal de serviço a cada uma dessas assinaturas. Por exemplo, o BlueXP  permite que você selecione a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

**Adicione permissões da API de Gerenciamento de Serviços do Windows Azure**

1. No serviço **Microsoft Entra ID**, selecione **inscrições de aplicativos** e selecione o aplicativo.
2. Selecione **permissões de API > Adicionar uma permissão**.
3. Em **Microsoft APIs**, selecione **Azure Service Management**.

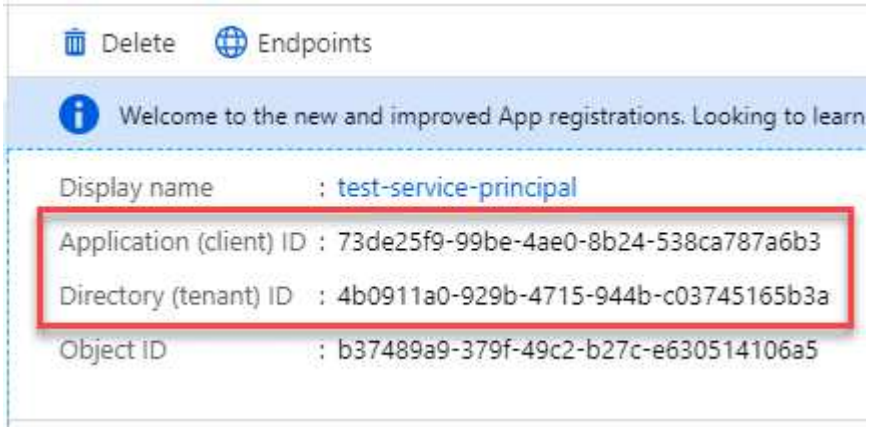



4. Selecione **Acesse o Gerenciamento de Serviços do Azure como usuários da organização** e selecione **Adicionar permissões**.




**Obtenha o ID do aplicativo e o ID do diretório para o aplicativo**

1. No serviço **Microsoft Entra ID**, selecione **inscrições de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.




Quando você adiciona a conta do Azure ao BlueXP , você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O BlueXP  usa os IDs para fazer login programaticamente.

**Crie um segredo de cliente**

1. Abra o serviço **Microsoft Entra ID**.
2. Selecione **inscrições de aplicativos** e selecione sua inscrição.
3. Selecione **certificados e segredos > segredo de novo cliente**.
4. Forneça uma descrição do segredo e uma duração.
5. Selecione **Adicionar**.
6. Copie o valor do segredo do cliente.


Agora você tem um segredo de cliente que o BlueXP pode usá-lo para autenticar com o Microsoft Entra ID.

**Resultado**

Seu responsável de serviço está configurado e você deve ter copiado o ID do aplicativo (cliente), o ID do diretório (locatário) e o valor do segredo do cliente. Você precisa inserir essas informações no BlueXP quando você criar o conetor.

### Passo 4: Crie o conetor

Crie o conetor diretamente do console baseado na Web do BlueXP .

**Sobre esta tarefa**

- A criação do conetor do BlueXP implanta uma máquina virtual no Azure usando uma configuração padrão. Depois de criar o conetor, você não deve mudar para um tipo de VM menor que tenha menos CPU ou RAM. "Saiba mais sobre a configuração padrão do conetor".
- Quando o BlueXP implanta o conetor, ele cria uma função personalizada e o atribui à VM do conetor. Essa função inclui permissões que permitem que o conetor gerencie recursos do Azure. Você precisa garantir que a função seja mantida atualizada à medida que novas permissões são adicionadas em versões subsequentes. "Saiba mais sobre a função personalizada para o conetor".

**Antes de começar**

Você deve ter o seguinte:

- Uma subscrição do Azure.
- Uma VNet e uma sub-rede na sua região do Azure escolhida.
- Detalhes sobre um servidor proxy, se a sua organização exigir um proxy para todo o tráfego de saída da Internet:
  - Endereço IP
  - Credenciais
  - Certificado HTTPS
- Uma chave pública SSH, se você quiser usar esse método de autenticação para a máquina virtual do conetor. A outra opção para o método de autenticação é usar uma senha.

  "Saiba mais sobre como conetar-se a uma VM Linux no Azure"

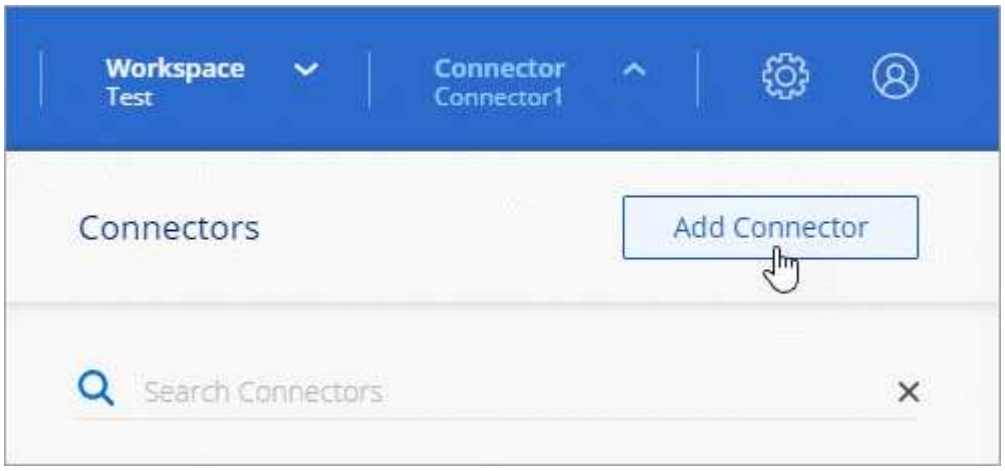
- Se você não quiser que o BlueXP crie automaticamente uma função do Azure para o conetor, precisará criar o seu próprio "uso da política nesta página".

  Essas permissões são para a própria instância do conetor. É um conjunto diferente de permissões do que

você configurou anteriormente para implantar a VM Connector.

**Passos**

1. Selecione a lista suspensa **Connector** e selecione **Add Connector**.




2. Escolha **Microsoft Azure** como seu provedor de nuvem.
3. Na página **Implantando um conetor**:

   a. Em **Autenticação**, selecione a opção de autenticação que corresponde à configuração das permissões do Azure:

      - Selecione **conta de utilizador do Azure** para iniciar sessão na sua conta Microsoft, que deve ter as permissões necessárias.

        O formulário é de propriedade e hospedado pela Microsoft. Suas credenciais não são fornecidas ao NetApp.

        Se você já estiver conetado a uma conta do Azure, o BlueXP usará essa conta automaticamente. Se você tiver várias contas, talvez seja necessário fazer logout primeiro para garantir que esteja usando a conta certa.

      - Selecione **Principal de serviço do ative Directory** para inserir informações sobre o principal de serviço do Microsoft Entra que concede as permissões necessárias:
        - ID da aplicação (cliente)
        - ID do diretório (locatário)
        - Segredo Cliente

   Saiba como obter esses valores para um responsável de serviço.

4. Siga as etapas no assistente para criar o conetor:

   ◦ **Autenticação da VM**: Escolha uma assinatura do Azure, um local, um novo grupo de recursos ou um grupo de recursos existente e, em seguida, escolha um método de autenticação para a máquina virtual do conetor que você está criando.

   O método de autenticação para a máquina virtual pode ser uma senha ou uma chave pública SSH.

   "Saiba mais sobre como conetar-se a uma VM Linux no Azure"

- **Detalhes**: Insira um nome para a instância, especifique tags e escolha se deseja que o BlueXP crie uma nova função que tenha as permissões necessárias ou se deseja selecionar uma função existente configurada com "as permissões necessárias"o .

  Observe que você pode escolher as assinaturas do Azure associadas a essa função. Cada assinatura escolhida fornece as permissões do conetor para gerenciar recursos nessa assinatura (por exemplo, Cloud Volumes ONTAP).

- **Rede**: Escolha uma VNet e uma sub-rede, se deseja ativar um endereço IP público e, opcionalmente, especifique uma configuração de proxy.
- **Grupo de segurança**: Escolha se deseja criar um novo grupo de segurança ou se deseja selecionar um grupo de segurança existente que permita as regras de entrada e saída necessárias.

  "Veja as regras do grupo de segurança para o Azure".

- **Revisão**: Revise suas seleções para verificar se a configuração está correta.

5. Clique em **Add**.

   A máquina virtual deve estar pronta em cerca de 7 minutos. Você deve permanecer na página até que o processo esteja concluído.

#### Resultado

Após o processo ser concluído, o conetor está disponível para uso no BlueXP .

Se você tiver o armazenamento de Blobs do Azure na mesma assinatura do Azure em que criou o conetor, verá um ambiente de trabalho de armazenamento de Blobs do Azure aparecer automaticamente na tela do BlueXP . "Saiba como gerenciar o armazenamento de Blobs do Azure a partir do BlueXP "

##### Crie um conetor a partir do Azure Marketplace

Um conetor é o software NetApp executado em sua rede na nuvem ou na rede local que permite usar todos os recursos e serviços do BlueXP . Uma das opções de instalação disponíveis é criar um conetor no Azure diretamente a partir do Azure Marketplace. Para criar um conetor a partir do Azure Marketplace, você precisa configurar sua rede, preparar permissões do Azure, analisar os requisitos de instância e criar o conetor.

#### Antes de começar

- Você deve ter um "Compreensão dos conetores".
- Você deve rever "Limitações do conetor".

#### Passo 1: Configurar a rede

Certifique-se de que a localização da rede onde pretende instalar o conetor suporta os seguintes requisitos. Atender a esses requisitos permite que o conetor gerencie recursos e processos em seu ambiente de nuvem híbrida.

#### Região do Azure

Se você usar o Cloud Volumes ONTAP, o conetor deve ser implantado na mesma região do Azure que os sistemas Cloud Volumes ONTAP gerenciados ou no "Par de regiões do Azure" para os sistemas Cloud Volumes ONTAP. Esse requisito garante que uma conexão com o Azure Private Link seja usada entre o Cloud Volumes ONTAP e suas contas de armazenamento associadas.

"Saiba como o Cloud Volumes ONTAP usa um link privado do Azure"

**VNet e sub-rede**

Ao criar o conetor, você precisa especificar a VNet e a sub-rede onde o conetor deve residir.

**Conexões com redes de destino**

Um conetor requer uma conexão de rede com o local onde você está planejando criar e gerenciar ambientes de trabalho. Por exemplo, a rede em que você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de storage em seu ambiente local.

**Acesso de saída à Internet**

O local de rede onde você implantar o conetor deve ter uma conexão de saída de Internet para contatar pontos de extremidade específicos.

**Terminais contactados a partir do conetor**

O conetor requer acesso de saída à Internet para entrar em Contato com os seguintes endpoints, a fim de gerenciar recursos e processos em seu ambiente de nuvem pública para operações diárias.

Observe que os endpoints listados abaixo são todas as entradas CNAME.

| Endpoints | Finalidade |
|---|---|
| https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net | Para gerenciar recursos em regiões públicas do Azure. |
| https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn | Para gerenciar recursos nas regiões do Azure China. |
| https://support.NetApp.com https://mysupport.NetApp.com | Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte do NetApp. |
| https://*.api.BlueXP .NetApp.com<br><br>https://api.BlueXP .NetApp.com<br><br>https://*.cloudmanager.cloud.NetApp.com<br><br>https://cloudmanager.cloud.NetApp.com<br><br>https://NetApp-cloud-account.auth0.com | Para fornecer recursos e serviços SaaS no BlueXP .<br><br>Observe que o conetor está entrando em Contato atualmente com "cloudmanager.cloud.NetApp.com ", mas começará a entrar em Contato com "API.BlueXP .NetApp.com" em uma próxima versão. |
| https://*.blob.core.windows.net<br><br>https://cloudmanagerinfraprod.azurecr.io | Para atualizar o conetor e seus componentes do Docker. |

**Servidor proxy**

Se a sua empresa exigir a implantação de um servidor proxy para todo o tráfego de saída da Internet,

obtenha as seguintes informações sobre o proxy HTTP ou HTTPS. Você precisará fornecer essas informações durante a instalação. Observe que o BlueXP  não oferece suporte a servidores proxy transparentes.

- Endereço IP
- Credenciais
- Certificado HTTPS

**Portas**

Não há tráfego de entrada para o conetor, a menos que você o inicie ou se o conetor for usado como um proxy para enviar mensagens AutoSupport do Cloud Volumes ONTAP para o suporte da NetApp.

- HTTP (80) e HTTPS (443) fornecem acesso à IU local, que você usará em circunstâncias raras.
- SSH (22) só é necessário se você precisar se conetar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 são necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída à Internet não está disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída à Internet para enviar mensagens AutoSupport, o BlueXP  configura automaticamente esses sistemas para usar um servidor proxy incluído no conetor. O único requisito é garantir que o grupo de segurança do conetor permita conexões de entrada pela porta 3128. Você precisará abrir essa porta depois de implantar o conetor.

**Ativar NTP**

Se estiver a planear utilizar a classificação BlueXP  para analisar as suas fontes de dados empresariais, deve ativar um serviço de Protocolo de tempo de rede (NTP) no sistema de conetores BlueXP  e no sistema de classificação BlueXP  para que o tempo seja sincronizado entre os sistemas. "Saiba mais sobre a classificação BlueXP"

Você precisará implementar esse requisito de rede depois de criar o conetor.

### Etapa 2: Revise os requisitos da VM

Ao criar o conetor, você precisa escolher um tipo de máquina virtual que atenda aos seguintes requisitos.

**CPU**

8 núcleos ou 8 vCPUs

**RAM**

32 GB

**Tamanho da VM do Azure**

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos Standard_D8s_v3.

### Passo 3: Configurar permissões

Você pode fornecer permissões das seguintes maneiras:

- Opção 1: Atribua uma função personalizada à VM do Azure usando uma identidade gerenciada atribuída ao sistema.
- Opção 2: Forneça ao BlueXP  as credenciais de um responsável de serviço do Azure que tenha as permissões necessárias.

Siga estas etapas para configurar permissões para o BlueXP .

**Função personalizada**

Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se você preferir usar um método diferente, consulte "Documentação do Azure"

**Passos**

1. Se você estiver planejando instalar manualmente o software em seu próprio host, habilite uma identidade gerenciada atribuída ao sistema na VM para que você possa fornecer as permissões necessárias do Azure por meio de uma função personalizada.

   "Documentação do Microsoft Azure: Configure identidades gerenciadas para recursos do Azure em uma VM usando o portal do Azure"

2. Copie o conteúdo do "Permissões de função personalizadas para o conetor" e salve-o em um arquivo JSON.
3. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

   Você deve adicionar o ID para cada assinatura do Azure que deseja usar com o BlueXP .

   **Exemplo**

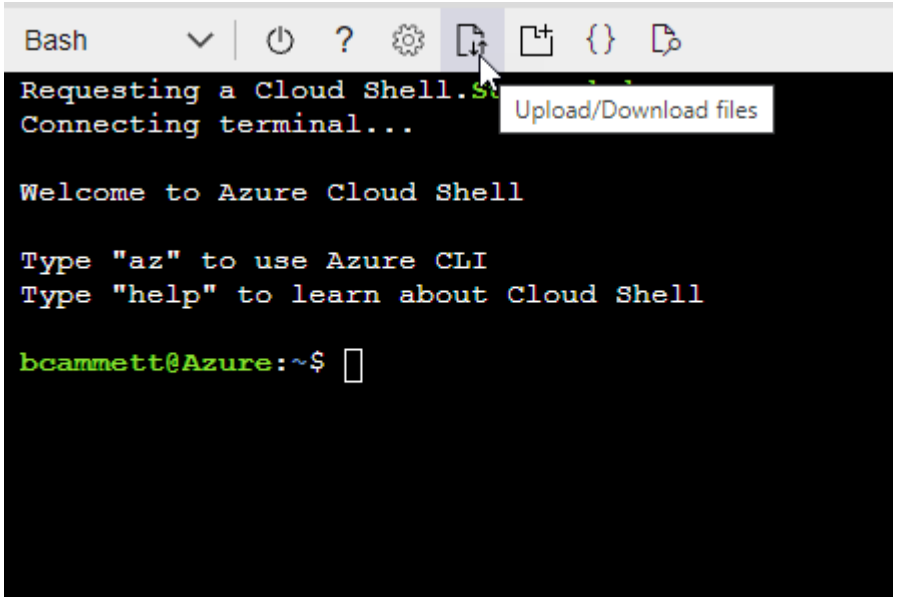
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

4. Use o arquivo JSON para criar uma função personalizada no Azure.

   As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

   a. Comece "Azure Cloud Shell" e escolha o ambiente Bash.

   b. Carregue o arquivo JSON.



c. Use a CLI do Azure para criar a função personalizada:

```
az role definition create --role-definition Connector_Policy.json
```

**Resultado**

Agora você deve ter uma função personalizada chamada Operador BlueXP  que você pode atribuir à máquina virtual do conetor.

**Serviço principal**

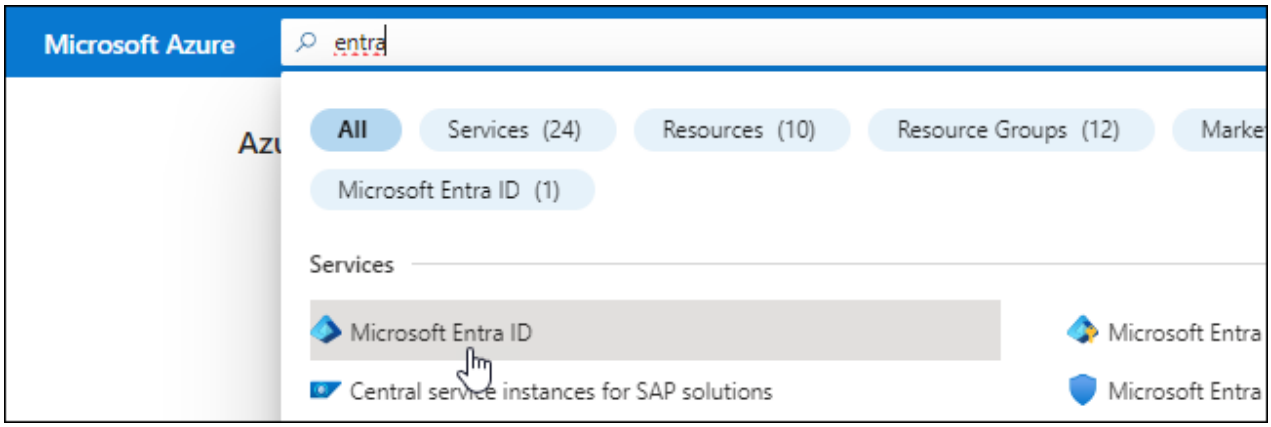
Crie e configure um princípio de serviço no Microsoft Entra ID e obtenha as credenciais do Azure de que o BlueXP  precisa.

**Crie um aplicativo Microsoft Entra para controle de acesso baseado em funções**

1. Certifique-se de ter permissões no Azure para criar um aplicativo do ative Directory e atribuir o aplicativo a uma função.

   Para obter mais informações, consulte "Documentação do Microsoft Azure: Permissões necessárias"

2. No portal do Azure, abra o serviço **Microsoft Entra ID**.




3. No menu, selecione **inscrições de aplicativos**.
4. Selecione **novo registo**.
5. Especifique detalhes sobre o aplicativo:
   - **Nome**: Insira um nome para o aplicativo.
   - **Tipo de conta**: Selecione um tipo de conta (qualquer funcionará com o BlueXP ).
   - * URI de redirecionamento*: Você pode deixar este campo em branco.
6. Selecione **Registe-se**.

   Você criou o aplicativo AD e o principal de serviço.

**Atribua a aplicação a uma função**

1. Crie uma função personalizada:

   Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando

a CLI do Azure. Se você preferir usar um método diferente, consulte "Documentação do Azure"

a. Copie o conteúdo do "Permissões de função personalizadas para o conetor" e salve-o em um arquivo JSON.

b. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

   Você deve adicionar o ID para cada assinatura do Azure a partir da qual os usuários criarão sistemas Cloud Volumes ONTAP.

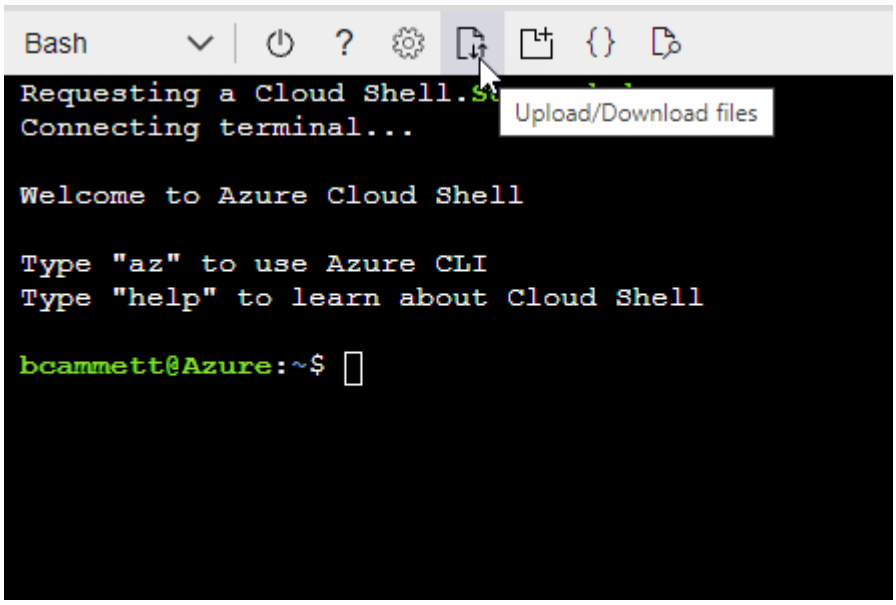
   **Exemplo**

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

c. Use o arquivo JSON para criar uma função personalizada no Azure.

   As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

   - Comece "Azure Cloud Shell" e escolha o ambiente Bash.
   - Carregue o arquivo JSON.




   - Use a CLI do Azure para criar a função personalizada:

```
az role definition create --role-definition
Connector_Policy.json
```

   Agora você deve ter uma função personalizada chamada Operador BlueXP  que você pode atribuir à máquina virtual do conetor.

2. Atribua o aplicativo à função:

    a. No portal do Azure, abra o serviço **Subscrições**.

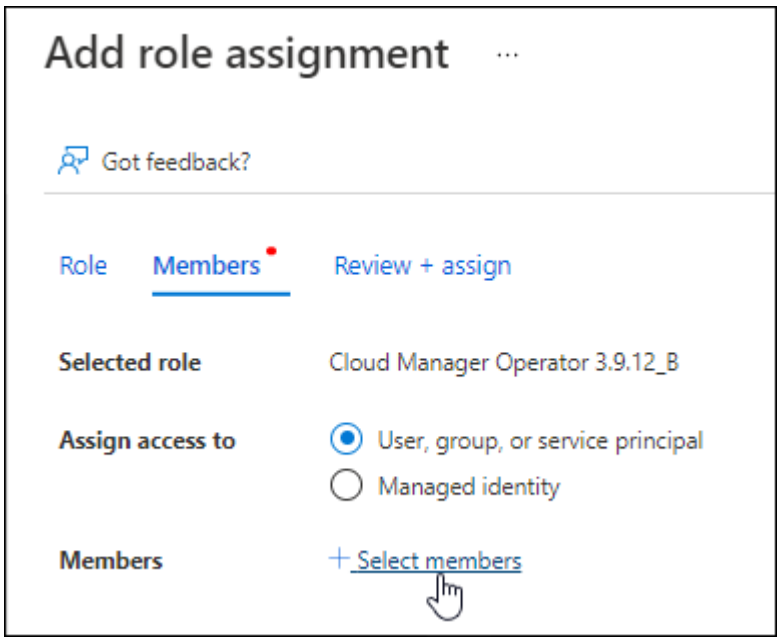
    b. Selecione a subscrição.

    c. Selecione **Access Control (IAM) > Add > Add > Add Role assignment** (Adicionar controlo de acesso).

    d. Na guia **função**, selecione a função **Operador BlueXP** e selecione **seguinte**.

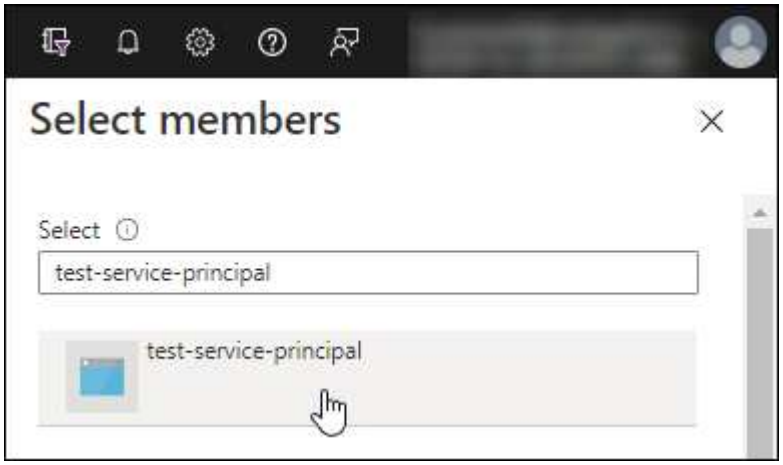
    e. Na guia **Membros**, execute as seguintes etapas:

    - Mantenha **Usuário, grupo ou responsável do serviço** selecionado.
    - Selecione **Selecionar membros**.




    - Procure o nome da aplicação.

      Aqui está um exemplo:




    - Selecione a aplicação e selecione **Select**.
    - Selecione **seguinte**.

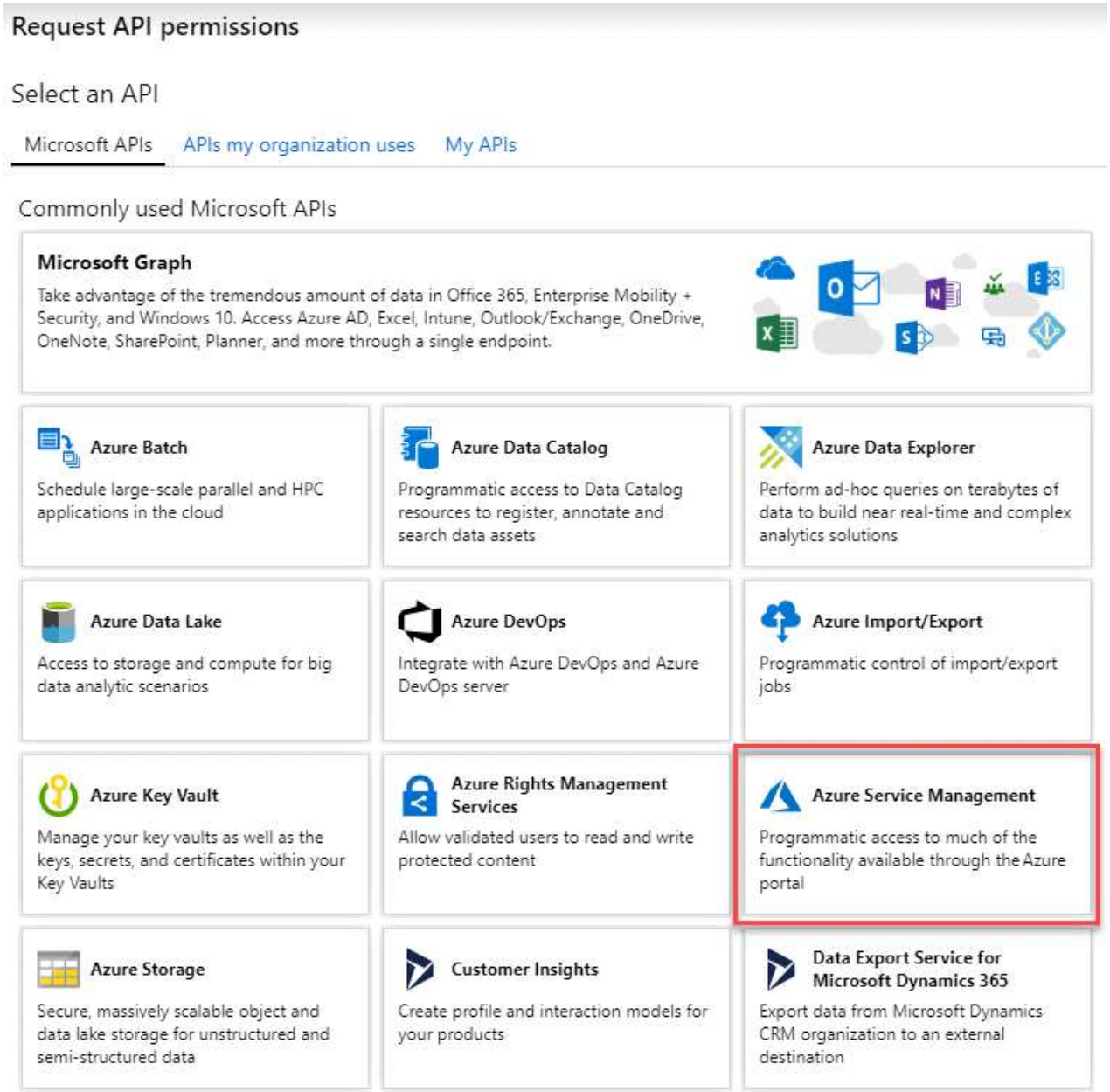
f. Selecione **Rever e atribuir**.

O principal de serviço agora tem as permissões necessárias do Azure para implantar o conetor.

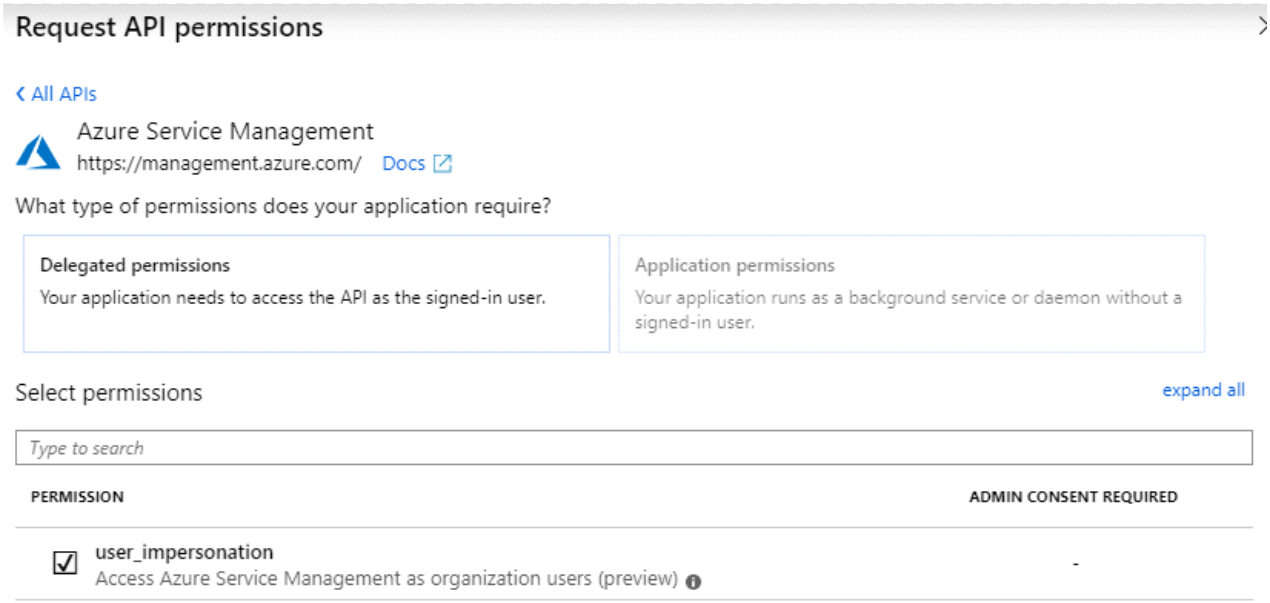
Se você quiser implantar o Cloud Volumes ONTAP a partir de várias assinaturas do Azure, então você deve vincular o principal de serviço a cada uma dessas assinaturas. O BlueXP  permite que você selecione a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

**Adicione permissões da API de Gerenciamento de Serviços do Windows Azure**

1. No serviço **Microsoft Entra ID**, selecione **inscrições de aplicativos** e selecione o aplicativo.
2. Selecione **permissões de API > Adicionar uma permissão**.
3. Em **Microsoft APIs**, selecione **Azure Service Management**.

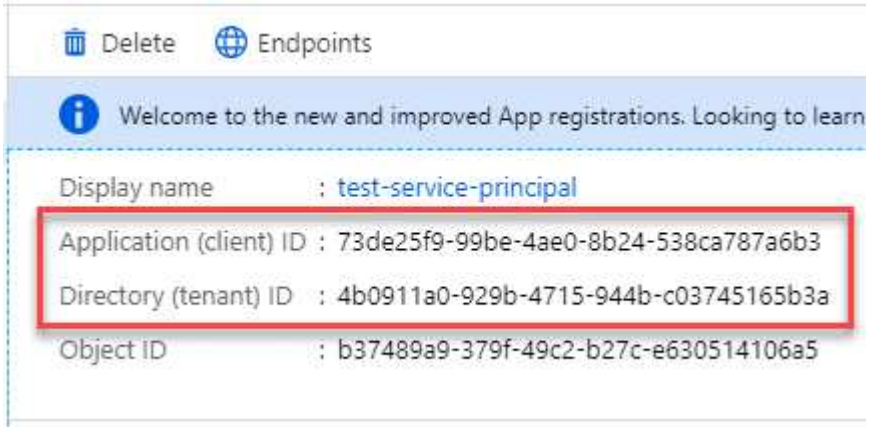



4. Selecione **Acesse o Gerenciamento de Serviços do Azure como usuários da organização** e selecione **Adicionar permissões**.




**Obtenha o ID do aplicativo e o ID do diretório para o aplicativo**

1. No serviço **Microsoft Entra ID**, selecione **inscrições de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.




Quando você adiciona a conta do Azure ao BlueXP , você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O BlueXP  usa os IDs para fazer login programaticamente.

**Crie um segredo de cliente**

1. Abra o serviço **Microsoft Entra ID**.
2. Selecione **inscrições de aplicativos** e selecione sua inscrição.
3. Selecione **certificados e segredos > segredo de novo cliente**.
4. Forneça uma descrição do segredo e uma duração.
5. Selecione **Adicionar**.
6. Copie o valor do segredo do cliente.


Agora você tem um segredo de cliente que o BlueXP pode usá-lo para autenticar com o Microsoft Entra ID.

**Resultado**

Seu responsável de serviço está configurado e você deve ter copiado o ID do aplicativo (cliente), o ID do diretório (locatário) e o valor do segredo do cliente. Você precisa inserir essas informações no BlueXP ao adicionar uma conta do Azure.

### Passo 4: Crie o conetor

Inicie o conetor diretamente do Azure Marketplace.

**Sobre esta tarefa**

A criação do conetor no Azure Marketplace implanta uma máquina virtual no Azure usando uma configuração padrão. "Saiba mais sobre a configuração padrão do conetor".

**Antes de começar**

Você deve ter o seguinte:

- Uma subscrição do Azure.
- Uma VNet e uma sub-rede na sua região do Azure escolhida.
- Detalhes sobre um servidor proxy, se a sua organização exigir um proxy para todo o tráfego de saída da Internet:
  - Endereço IP
  - Credenciais
  - Certificado HTTPS
- Uma chave pública SSH, se você quiser usar esse método de autenticação para a máquina virtual do conetor. A outra opção para o método de autenticação é usar uma senha.

  "Saiba mais sobre como conetar-se a uma VM Linux no Azure"

- Se você não quiser que o BlueXP crie automaticamente uma função do Azure para o conetor, precisará criar o seu próprio "uso da política nesta página".

  Essas permissões são para a própria instância do conetor. É um conjunto diferente de permissões do que você configurou anteriormente para implantar a VM Connector.

**Passos**

1. Vá para a página VM do NetApp Connector no Azure Marketplace.

"Página do Azure Marketplace para regiões comerciais"

2. Selecione **Obtenha agora** e, em seguida, selecione **continuar**.
3. No portal do Azure, selecione **criar** e siga as etapas para configurar a máquina virtual.

   Observe o seguinte ao configurar a VM:

   - **Tamanho da VM**: Escolha um tamanho de VM que atenda aos requisitos de CPU e RAM. Recomendamos Standard_D8s_v3.
   - **Disks**: O conetor pode funcionar de forma ideal com discos HDD ou SSD.
   - **Grupo de segurança de rede**: O conetor requer conexões de entrada usando SSH, HTTP e HTTPS.

     "Veja as regras do grupo de segurança para o Azure".

   - **Identidade**: Em **Gerenciamento**, selecione **Ativar identidade gerenciada atribuída ao sistema**.

     Essa configuração é importante porque uma identidade gerenciada permite que a máquina virtual do conetor se identifique com o Microsoft Entra ID sem fornecer credenciais. "Saiba mais sobre identidades gerenciadas para recursos do Azure".

4. Na página **Revisão e criação**, revise suas seleções e selecione **criar** para iniciar a implantação.

   O Azure implanta a máquina virtual com as configurações especificadas. A máquina virtual e o software do conetor devem estar funcionando em aproximadamente cinco minutos.

5. Abra um navegador da Web a partir de um host que tenha uma conexão com a máquina virtual do conetor e insira o seguinte URL:

   <a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

6. Depois de iniciar sessão, configure o conetor:
   a. Especifique a organização BlueXP  a associar ao conetor.
   b. Introduza um nome para o sistema.
   c. Em **você está executando em um ambiente seguro?** mantenha o modo restrito desativado.

      Você deve manter o modo restrito desativado porque estas etapas descrevem como usar o BlueXP  no modo padrão. Você deve habilitar o modo restrito somente se tiver um ambiente seguro e quiser desconetar essa conta dos serviços de back-end do BlueXP . Se for esse o caso"Siga os passos para começar a utilizar o BlueXP  no modo restrito", .

   d. Selecione **vamos começar**.

**Resultado**

O conetor está agora instalado e está configurado com a sua organização BlueXP .

Se você tiver o armazenamento de Blobs do Azure na mesma assinatura do Azure em que criou o conetor, verá um ambiente de trabalho de armazenamento de Blobs do Azure aparecer automaticamente na tela do BlueXP . "Saiba como gerenciar o armazenamento de Blobs do Azure a partir do BlueXP "

### Passo 5: Forneça permissões para o BlueXP

Agora que você criou o conetor, você precisa fornecer ao BlueXP  as permissões que você configurou anteriormente. Com o fornecimento de permissões, o BlueXP  pode gerenciar sua infraestrutura de dados e

storage no Azure.

**Função personalizada**

Vá para o portal do Azure e atribua a função personalizada do Azure à máquina virtual Connector para uma ou mais subscrições.

**Passos**

1. No Portal do Azure, abra o serviço **Subscrições** e selecione a sua subscrição.

   É importante atribuir a função do serviço **Subscrições** porque especifica o escopo da atribuição de função no nível da assinatura. O *scope* define o conjunto de recursos aos quais o acesso se aplica. Se você especificar um escopo em um nível diferente (por exemplo, no nível da máquina virtual), sua capacidade de concluir ações de dentro do BlueXP  será afetada.

   "Documentação do Microsoft Azure: Entenda o escopo do Azure RBAC"

2. Selecione **Access control (IAM)** > **Add** > **Add** > **Add role assignment**.
3. Na guia **função**, selecione a função **Operador BlueXP**  e selecione **seguinte**.

   Operador BlueXP  é o nome padrão fornecido na política BlueXP . Se você escolher um nome diferente para a função, selecione esse nome em vez disso.

4. Na guia **Membros**, execute as seguintes etapas:
   a. Atribua acesso a uma **identidade gerenciada**.
   b. Selecione **Selecionar membros**, selecione a assinatura na qual a máquina virtual do conetor foi criada, em **identidade gerenciada**, escolha **Máquina Virtual** e, em seguida, selecione a máquina virtual do conetor.
   c. Selecione **Selecionar**.
   d. Selecione **seguinte**.
   e. Selecione **Rever e atribuir**.
   f. Se você quiser gerenciar recursos em assinaturas adicionais do Azure, mude para essa assinatura e repita essas etapas.

**Resultado**

O BlueXP  agora tem as permissões necessárias para executar ações no Azure em seu nome.

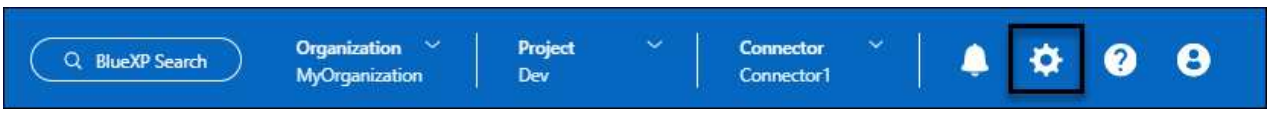
**O que se segue?**

Passe à "Consola BlueXP" para começar a utilizar o conetor com o BlueXP .

**Serviço principal**

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.




2. Selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Credentials Location**: Selecione **Microsoft Azure > Connector**.

b. **Definir credenciais**: Insira informações sobre o responsável do serviço Microsoft Entra que concede as permissões necessárias:
   - ID da aplicação (cliente)
   - ID do diretório (locatário)
   - Segredo Cliente
c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.
d. **Revisão**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

**Resultado**

O BlueXP agora tem as permissões necessárias para executar ações no Azure em seu nome.

#### Instale manualmente o conetor no Azure

Um conetor é o software NetApp executado em sua rede na nuvem ou na rede local que permite usar todos os recursos e serviços do BlueXP . Uma das opções de instalação disponíveis é instalar manualmente o software Connector em um host Linux em execução no Azure. Para instalar manualmente o conetor em seu próprio host Linux, você precisa revisar os requisitos de host, configurar sua rede, preparar permissões do Azure, instalar o conetor e, em seguida, fornecer as permissões que você preparou.

**Antes de começar**

- Você deve ter um "Compreensão dos conetores".
- Você deve rever "Limitações do conetor".

**Etapa 1: Revise os requisitos do host**

O software do conetor deve ser executado em um host que atenda a requisitos específicos do sistema operacional, requisitos de RAM, requisitos de porta, etc.

**Host dedicado**

O conetor não é suportado em um host que é compartilhado com outros aplicativos. O host deve ser um host dedicado.

**Hipervisor**

É necessário um hypervisor bare metal ou hospedado certificado para executar um sistema operacional suportado.

**requisitos de sistema operacional e contentor**

O BlueXP suporta o conetor com os seguintes sistemas operacionais ao usar o BlueXP no modo padrão ou no modo restrito. Uma ferramenta de orquestração de contêineres é necessária antes de instalar o conetor.

| Sistema operacional | Versões de OS compatíveis | Versões de conetor suportadas | Ferramenta de recipiente necessária | SELinux |
|---|---|---|---|---|
| Red Hat Enterprise Linux | 9,1 a 9,4<br><br>8,6 a 8,10 | 3.9.40 ou posterior com BlueXP no modo padrão ou modo restrito | Podman versão 4.6.1 ou 4.9.4<br><br>Veja os requisitos de configuração do Podman. | Suporte no modo de execução ou modo permissivo 1 |
| Ubuntu | 24,04 LTS | 3.9.45 ou posterior com BlueXP no modo padrão ou modo restrito | Docker Engine 26.0.0 | Não suportado |

Notas:

1. O gerenciamento de sistemas Cloud Volumes ONTAP não é suportado por conetores que tenham o SELinux habilitado no sistema operacional.
2. O conetor é suportado em versões em inglês destes sistemas operativos.
3. Para o RHEL, o host deve estar registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar repositórios para atualizar o software necessário de 3rd partes durante a instalação do conetor.

**CPU**

8 núcleos ou 8 vCPUs

**RAM**

32 GB

**Tamanho da VM do Azure**

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos Standard_D8s_v3.

**Espaço em disco em /opt**

100 GiB de espaço deve estar disponível

O BlueXP usa `/opt` para instalar o `/opt/application/netapp` diretório e seu conteúdo.

**Espaço em disco em /var**

20 GiB de espaço deve estar disponível

O BlueXP requer esse espaço `/var` porque o Docker ou o Podman são arquitetados para criar os contentores dentro desse diretório. Especificamente, eles irão criar contentores no `/var/lib/containers/storage` diretório. Montagens externas ou links simbólicos não funcionam para este espaço.

### Passo 2: Instale o Podman ou Docker Engine

Dependendo do seu sistema operacional, o Podman ou o Docker Engine são necessários antes de instalar o conetor.

- O Podman é necessário para o Red Hat Enterprise Linux 8 e 9.

  Veja as versões do Podman suportadas pelo BlueXP .

- Docker Engine é necessário para o Ubuntu.

  Veja as versões do Docker Engine que o BlueXP  suporta.

**Exemplo 2. Passos**

**Podman**

Siga estas etapas para instalar o Podman e configurá-lo para atender aos seguintes requisitos:

- O serviço podman.socket deve ser ativado e iniciado
- python3 deve ser instalado
- O pacote podman-compose versão 1.0.6 deve ser instalado
- Podman-compose deve ser adicionado à variável de ambiente PATH

**Passos**

1. Remova o pacote podman-docker se ele estiver instalado no host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Instale o Podman.

   O Podman está disponível nos repositórios oficiais do Red Hat Enterprise Linux.

   Para Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

   Onde o <version> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas pelo BlueXP .

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

   Onde o <version> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas pelo BlueXP .

3. Ative e inicie o serviço podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Instale o python3.

```
sudo dnf install python3
```

5. Instale o pacote do repositório EPEL se ainda não estiver disponível no seu sistema.

Esta etapa é necessária porque o podman-compose está disponível no repositório extra Packages for Enterprise Linux (EPEL).

Para Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

Para Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Instale o pacote podman-compose 1,0.6.

```
sudo dnf install podman-compose-1.0.6
```

> Usar o `dnf install` comando atende ao requisito para adicionar podman-compose à variável de ambiente PATH. O comando installation adiciona podman-compose ao /usr/bin, que já está incluído na `secure_path` opção no host.

**Docker Engine**

Siga a documentação do Docker para instalar o Docker Engine.

**Passos**

1. "Veja as instruções de instalação do Docker"

   Certifique-se de seguir as etapas para instalar uma versão específica do Docker Engine. Instalar a versão mais recente irá instalar uma versão do Docker que o BlueXP  não suporta.

2. Verifique se o Docker está ativado e em execução.

```
sudo systemctl enable docker && sudo systemctl start docker
```

### Passo 3: Configurar a rede

Certifique-se de que a localização da rede onde pretende instalar o conetor suporta os seguintes requisitos. Atender a esses requisitos permite que o conetor gerencie recursos e processos em seu ambiente de nuvem híbrida.

**Região do Azure**

Se você usar o Cloud Volumes ONTAP, o conetor deve ser implantado na mesma região do Azure que os sistemas Cloud Volumes ONTAP gerenciados ou no "Par de regiões do Azure" para os sistemas Cloud Volumes ONTAP. Esse requisito garante que uma conexão com o Azure Private Link seja usada entre o

Cloud Volumes ONTAP e suas contas de armazenamento associadas.

"Saiba como o Cloud Volumes ONTAP usa um link privado do Azure"

**Conexões com redes de destino**

Um conetor requer uma conexão de rede com o local onde você está planejando criar e gerenciar ambientes de trabalho. Por exemplo, a rede em que você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de storage em seu ambiente local.

**Acesso de saída à Internet**

O local de rede onde você implantar o conetor deve ter uma conexão de saída de Internet para contatar pontos de extremidade específicos.

**Endpoints contatados de computadores ao usar o console baseado na Web do BlueXP**

Os computadores que acessam o console BlueXP  a partir de um navegador da Web devem ter a capacidade de entrar em Contato com vários endpoints. Você precisará usar o console BlueXP  para configurar o conetor e para uso diário do BlueXP .

"Prepare a rede para o console BlueXP ".

**Terminais contactados durante a instalação manual**

Quando você instala manualmente o conetor em seu próprio host Linux, o instalador do conetor requer acesso aos seguintes URLs durante o processo de instalação:

- https://mysupport.NetApp.com
- https://signin.b2c.NetApp.com (este endpoint é o URL CNAME para https://mysupport.NetApp.com)
- https://cloudmanager.cloud.NetApp.com/locação
- https://stream.cloudmanager.cloud.NetApp.com
- https://production-artifacts.cloudmanager.cloud.NetApp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  O host pode tentar atualizar os pacotes do sistema operacional durante a instalação. O host pode entrar em Contato com diferentes sites de espelhamento para esses pacotes do sistema operacional.

**Terminais contactados a partir do conetor**

O conetor requer acesso de saída à Internet para entrar em Contato com os seguintes endpoints, a fim de gerenciar recursos e processos em seu ambiente de nuvem pública para operações diárias.

Observe que os endpoints listados abaixo são todas as entradas CNAME.

| Endpoints | Finalidade |
|---|---|
| https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net | Para gerenciar recursos em regiões públicas do Azure. |
| https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn | Para gerenciar recursos nas regiões do Azure China. |

| Endpoints | Finalidade |
| --- | --- |
| https://support.NetApp.com https://mysupport.NetApp.com | Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte do NetApp. |
| https://*.api.BlueXP .NetApp.com<br><br>https://api.BlueXP .NetApp.com<br><br>https://*.cloudmanager.cloud.NetApp.com<br><br>https://cloudmanager.cloud.NetApp.com<br><br>https://NetApp-cloud-account.auth0.com | Para fornecer recursos e serviços SaaS no BlueXP .<br><br>Observe que o conetor está entrando em Contato atualmente com "cloudmanager.cloud.NetApp.com ", mas começará a entrar em Contato com "API.BlueXP .NetApp.com" em uma próxima versão. |
| https://*.blob.core.windows.net<br><br>https://cloudmanagerinfraprod.azurecr.io | Para atualizar o conetor e seus componentes do Docker. |

**Servidor proxy**

Se a sua empresa exigir a implantação de um servidor proxy para todo o tráfego de saída da Internet, obtenha as seguintes informações sobre o proxy HTTP ou HTTPS. Você precisará fornecer essas informações durante a instalação. Observe que o BlueXP  não oferece suporte a servidores proxy transparentes.

- Endereço IP
- Credenciais
- Certificado HTTPS

**Portas**

Não há tráfego de entrada para o conetor, a menos que você o inicie ou se o conetor for usado como um proxy para enviar mensagens AutoSupport do Cloud Volumes ONTAP para o suporte da NetApp.

- HTTP (80) e HTTPS (443) fornecem acesso à IU local, que você usará em circunstâncias raras.
- SSH (22) só é necessário se você precisar se conetar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 são necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída à Internet não está disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída à Internet para enviar mensagens AutoSupport, o BlueXP  configura automaticamente esses sistemas para usar um servidor proxy incluído no conetor. O único requisito é garantir que o grupo de segurança do conetor permita conexões de entrada pela porta 3128. Você precisará abrir essa porta depois de implantar o conetor.

**Ativar NTP**

Se estiver a planear utilizar a classificação BlueXP  para analisar as suas fontes de dados empresariais, deve ativar um serviço de Protocolo de tempo de rede (NTP) no sistema de conetores BlueXP  e no

sistema de classificação BlueXP  para que o tempo seja sincronizado entre os sistemas. "Saiba mais sobre a classificação BlueXP"

**Passo 4: Configurar permissões**

Você precisa fornecer permissões do Azure ao BlueXP  usando uma das seguintes opções:

- Opção 1: Atribua uma função personalizada à VM do Azure usando uma identidade gerenciada atribuída ao sistema.
- Opção 2: Forneça ao BlueXP  as credenciais de um responsável de serviço do Azure que tenha as permissões necessárias.

Siga as etapas para preparar permissões para o BlueXP .

**Função personalizada**

Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se você preferir usar um método diferente, consulte "Documentação do Azure"

**Passos**

1. Se você estiver planejando instalar manualmente o software em seu próprio host, habilite uma identidade gerenciada atribuída ao sistema na VM para que você possa fornecer as permissões necessárias do Azure por meio de uma função personalizada.

   "Documentação do Microsoft Azure: Configure identidades gerenciadas para recursos do Azure em uma VM usando o portal do Azure"

2. Copie o conteúdo do "Permissões de função personalizadas para o conetor" e salve-o em um arquivo JSON.
3. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

   Você deve adicionar o ID para cada assinatura do Azure que deseja usar com o BlueXP .

   **Exemplo**

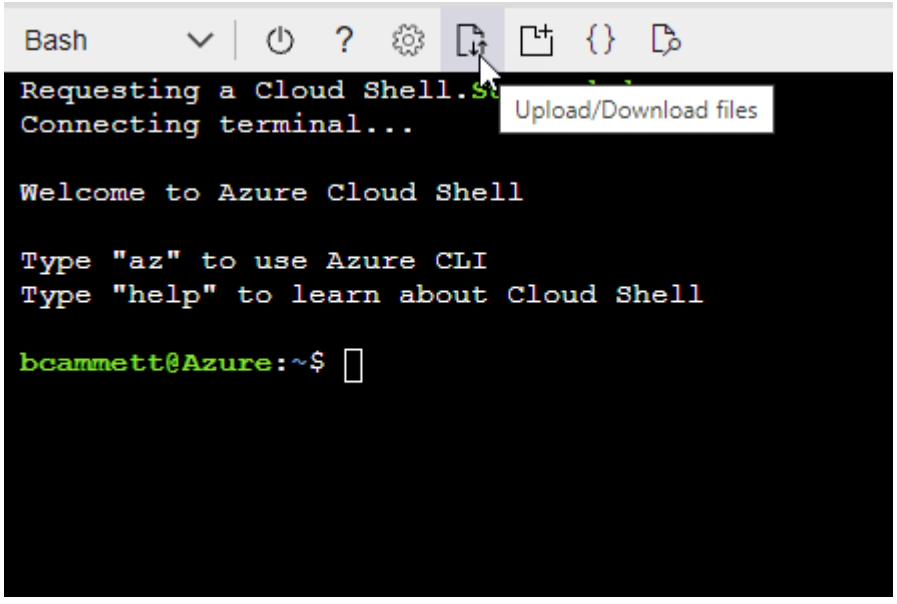
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

4. Use o arquivo JSON para criar uma função personalizada no Azure.

   As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

   a. Comece "Azure Cloud Shell" e escolha o ambiente Bash.

   b. Carregue o arquivo JSON.



c. Use a CLI do Azure para criar a função personalizada:

```
az role definition create --role-definition Connector_Policy.json
```

**Resultado**

Agora você deve ter uma função personalizada chamada Operador BlueXP  que você pode atribuir à máquina virtual do conetor.

**Serviço principal**

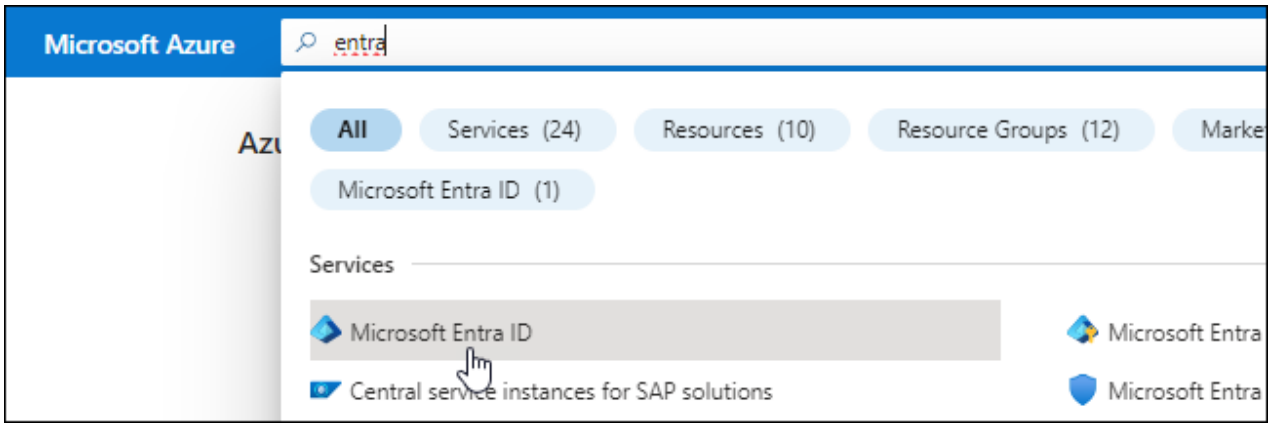
Crie e configure um princípio de serviço no Microsoft Entra ID e obtenha as credenciais do Azure de que o BlueXP  precisa.

**Crie um aplicativo Microsoft Entra para controle de acesso baseado em funções**

1. Certifique-se de ter permissões no Azure para criar um aplicativo do ative Directory e atribuir o aplicativo a uma função.

   Para obter mais informações, consulte "Documentação do Microsoft Azure: Permissões necessárias"

2. No portal do Azure, abra o serviço **Microsoft Entra ID**.




3. No menu, selecione **inscrições de aplicativos**.
4. Selecione **novo registo**.
5. Especifique detalhes sobre o aplicativo:
   - **Nome**: Insira um nome para o aplicativo.
   - **Tipo de conta**: Selecione um tipo de conta (qualquer funcionará com o BlueXP ).
   - * URI de redirecionamento*: Você pode deixar este campo em branco.
6. Selecione **Registe-se**.

   Você criou o aplicativo AD e o principal de serviço.

**Atribua a aplicação a uma função**

1. Crie uma função personalizada:

   Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando

a CLI do Azure. Se você preferir usar um método diferente, consulte "Documentação do Azure"

a. Copie o conteúdo do "Permissões de função personalizadas para o conetor" e salve-o em um arquivo JSON.

b. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

   Você deve adicionar o ID para cada assinatura do Azure a partir da qual os usuários criarão sistemas Cloud Volumes ONTAP.

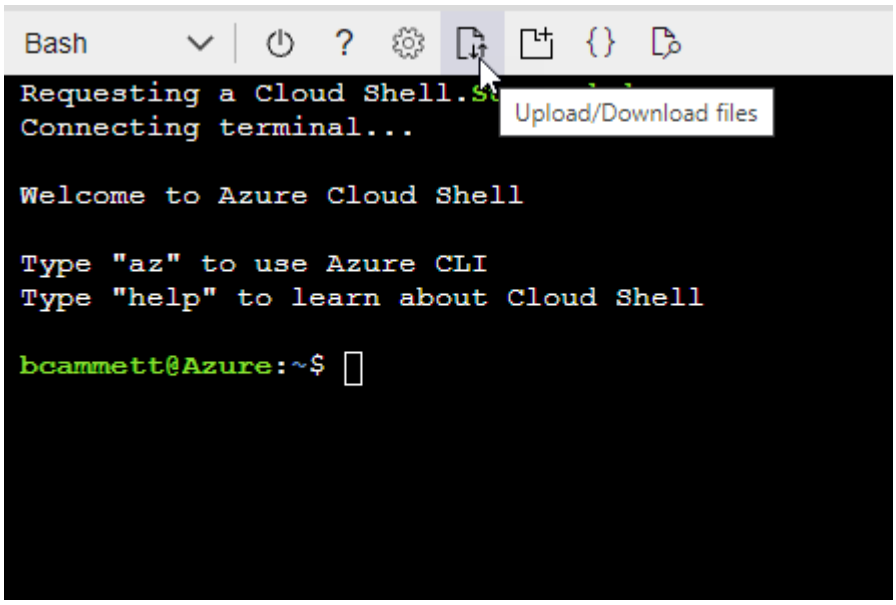
   **Exemplo**

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

c. Use o arquivo JSON para criar uma função personalizada no Azure.

   As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

   - Comece "Azure Cloud Shell" e escolha o ambiente Bash.
   - Carregue o arquivo JSON.




   - Use a CLI do Azure para criar a função personalizada:

```
az role definition create --role-definition
Connector_Policy.json
```

   Agora você deve ter uma função personalizada chamada Operador BlueXP  que você pode atribuir à máquina virtual do conetor.

2. Atribua o aplicativo à função:

    a. No portal do Azure, abra o serviço **Subscrições**.

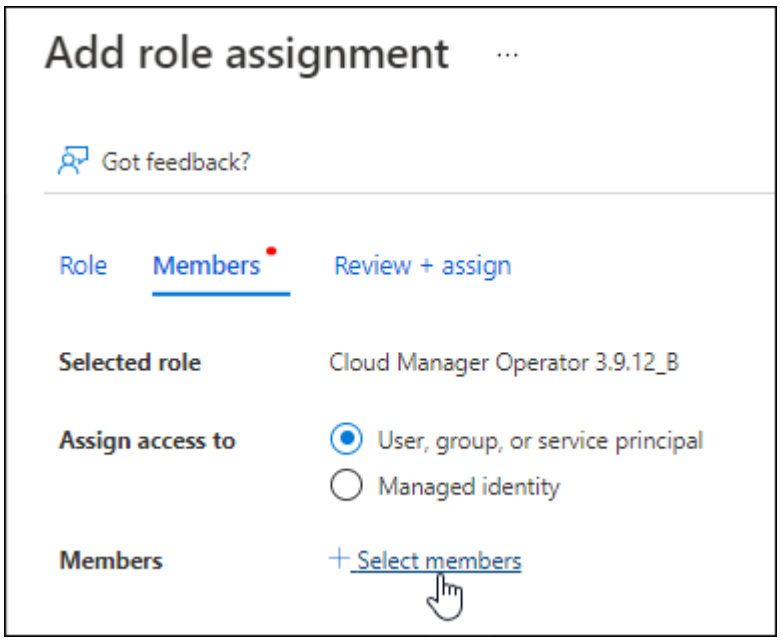
    b. Selecione a subscrição.

    c. Selecione **Access Control (IAM) > Add > Add > Add Role assignment** (Adicionar controlo de acesso).

    d. Na guia **função**, selecione a função **Operador BlueXP** e selecione **seguinte**.

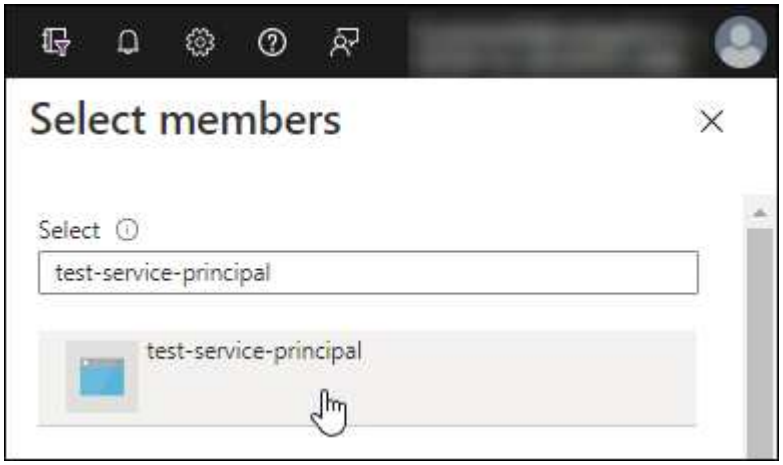
    e. Na guia **Membros**, execute as seguintes etapas:

    - Mantenha **Usuário, grupo ou responsável do serviço** selecionado.
    - Selecione **Selecionar membros**.




    - Procure o nome da aplicação.

      Aqui está um exemplo:




    - Selecione a aplicação e selecione **Select**.
    - Selecione **seguinte**.

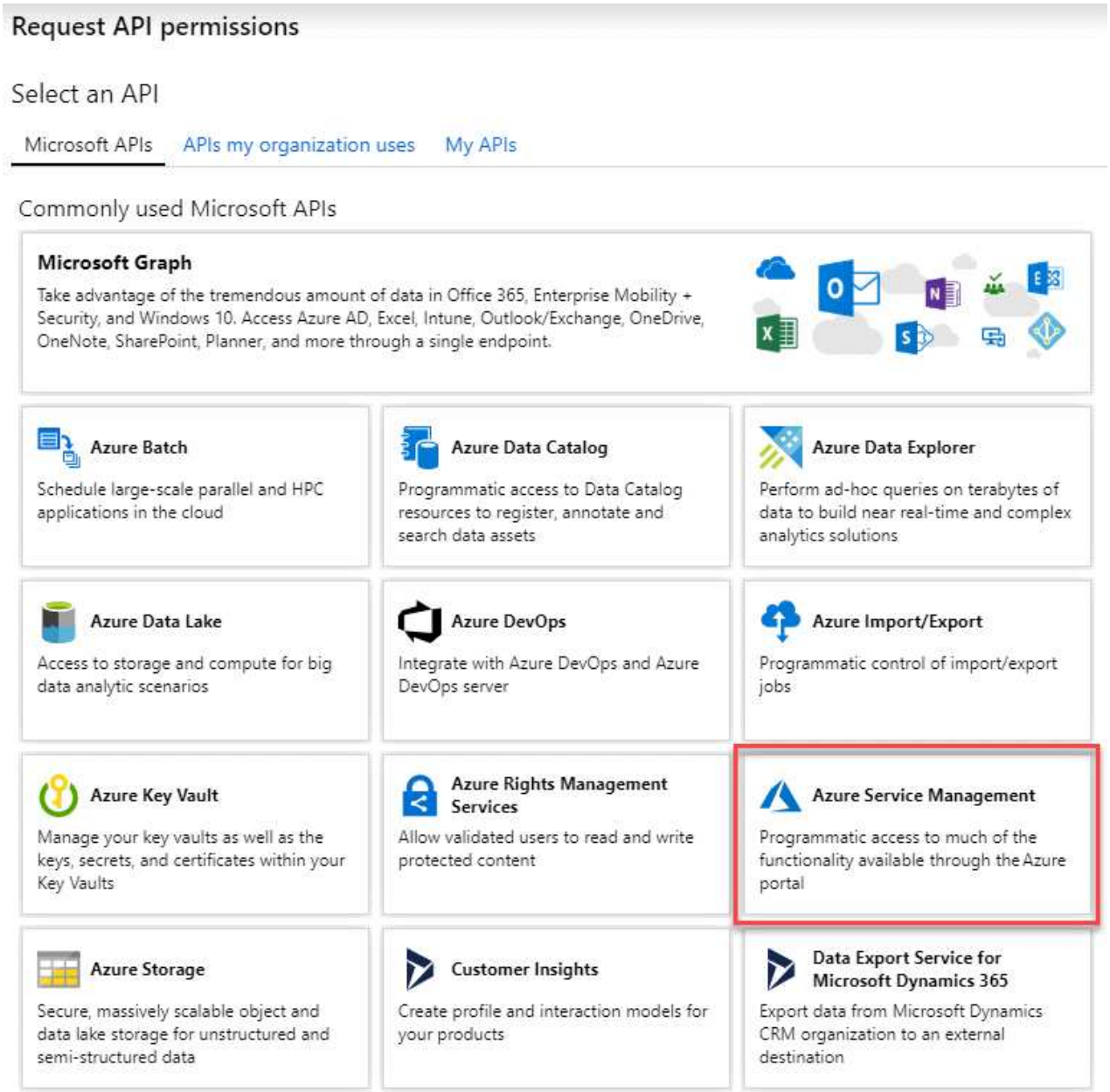
f. Selecione **Rever e atribuir**.

O principal de serviço agora tem as permissões necessárias do Azure para implantar o conetor.

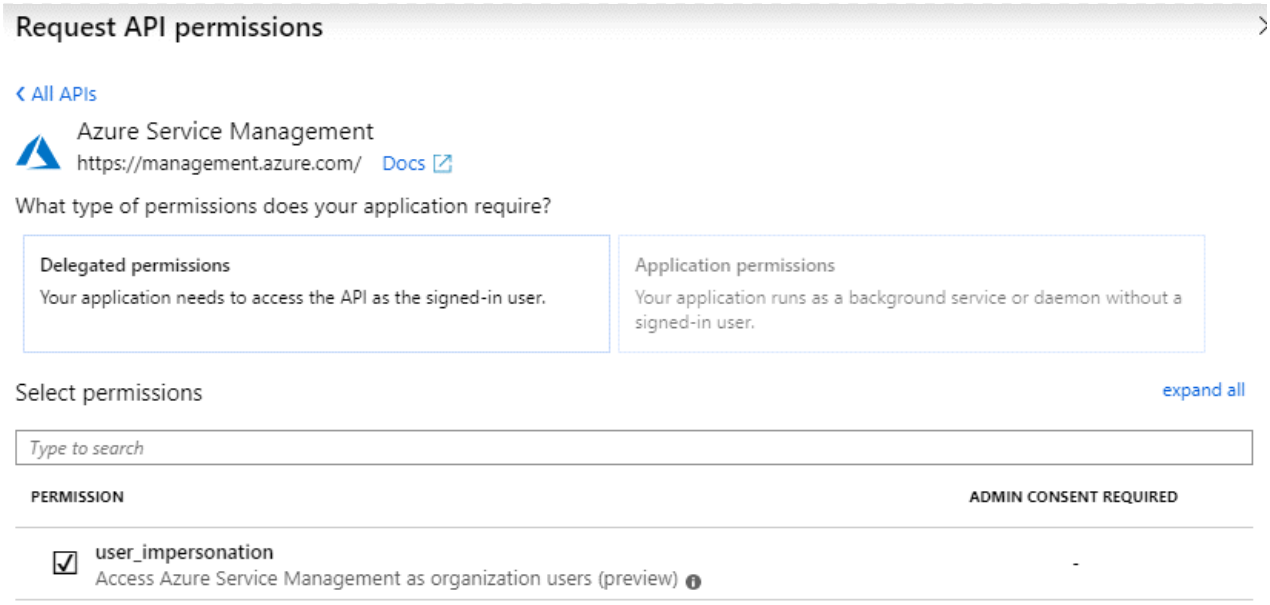
Se você quiser implantar o Cloud Volumes ONTAP a partir de várias assinaturas do Azure, então você deve vincular o principal de serviço a cada uma dessas assinaturas. O BlueXP  permite que você selecione a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

**Adicione permissões da API de Gerenciamento de Serviços do Windows Azure**

1. No serviço **Microsoft Entra ID**, selecione **inscrições de aplicativos** e selecione o aplicativo.
2. Selecione **permissões de API > Adicionar uma permissão**.
3. Em **Microsoft APIs**, selecione **Azure Service Management**.

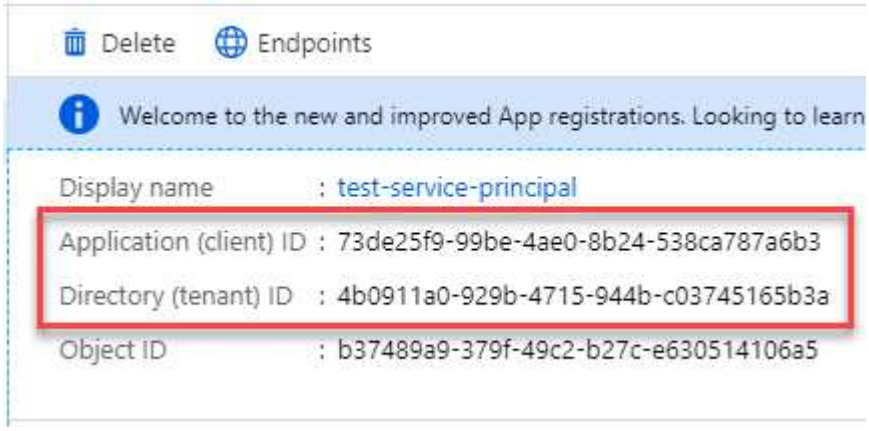



4. Selecione **Acesse o Gerenciamento de Serviços do Azure como usuários da organização** e selecione **Adicionar permissões**.




**Obtenha o ID do aplicativo e o ID do diretório para o aplicativo**

1. No serviço **Microsoft Entra ID**, selecione **inscrições de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.




Quando você adiciona a conta do Azure ao BlueXP , você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O BlueXP  usa os IDs para fazer login programaticamente.

**Crie um segredo de cliente**

1. Abra o serviço **Microsoft Entra ID**.
2. Selecione **inscrições de aplicativos** e selecione sua inscrição.
3. Selecione **certificados e segredos > segredo de novo cliente**.
4. Forneça uma descrição do segredo e uma duração.
5. Selecione **Adicionar**.
6. Copie o valor do segredo do cliente.


Agora você tem um segredo de cliente que o BlueXP pode usá-lo para autenticar com o Microsoft Entra ID.

**Resultado**

Seu responsável de serviço está configurado e você deve ter copiado o ID do aplicativo (cliente), o ID do diretório (locatário) e o valor do segredo do cliente. Você precisa inserir essas informações no BlueXP ao adicionar uma conta do Azure.

### Passo 5: Instale o conetor

Após a conclusão dos pré-requisitos, você pode instalar manualmente o software em seu próprio host Linux.

**Antes de começar**

Você deve ter o seguinte:

- Root Privileges para instalar o conetor.
- Detalhes sobre um servidor proxy, se for necessário um proxy para acesso à Internet a partir do conetor.

  Você tem a opção de configurar um servidor proxy após a instalação, mas isso requer a reinicialização do conetor.

  Observe que o BlueXP não oferece suporte a servidores proxy transparentes.

- Um certificado assinado pela CA, se o servidor proxy usar HTTPS ou se o proxy for um proxy intercetor.
- Uma identidade gerenciada habilitada na VM no Azure para que você possa fornecer as permissões necessárias do Azure por meio de uma função personalizada.

  "Documentação do Microsoft Azure: Configure identidades gerenciadas para recursos do Azure em uma VM usando o portal do Azure"

**Sobre esta tarefa**

O instalador disponível no site de suporte da NetApp pode ser uma versão anterior. Após a instalação, o conetor se atualiza automaticamente se uma nova versão estiver disponível.

**Passos**

1. Se as variáveis de sistema *http_proxy* ou *https_proxy* estiverem definidas no host, remova-as:

```
unset http_proxy
unset https_proxy
```

Se você não remover essas variáveis do sistema, a instalação falhará.

2. Faça o download do software Connector do "Site de suporte da NetApp"e copie-o para o host Linux.

   Você deve baixar o instalador do conetor "online" destinado a ser usado em sua rede ou na nuvem. Um instalador "offline" separado está disponível para o conetor, mas só é suportado com implantações de modo privado.

3. Atribua permissões para executar o script.

   ```
   chmod +x BlueXP-Connector-Cloud-<version>
   ```

   Onde <version> é a versão do conetor que você baixou.

4. Execute o script de instalação.

   ```
    ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
   --cacert <path and file name of a CA-signed certificate>
   ```

   Os parâmetros --proxy e --cacert são opcionais. Se você tiver um servidor proxy, será necessário inserir os parâmetros como mostrado. O instalador não solicita que você forneça informações sobre um proxy.

   Aqui está um exemplo do comando usando ambos os parâmetros opcionais:

   ```
    ./BlueXP-Connector-Cloud-v3.9.40--proxy
   https://user:password@10.0.0.30:8080/ --cacert
   /tmp/cacert/certificate.cer
   ```

   --proxy configura o conetor para usar um servidor proxy HTTP ou HTTPS usando um dos seguintes formatos:

   - http://address:port
   - http://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port
   - https://user-name:password@address:port
   - https://domain-name%92user-name:password@address:port

     Observe o seguinte:

     - O usuário pode ser um usuário local ou usuário de domínio.
     - Para um usuário de domínio, você deve usar o código ASCII para a como mostrado acima.
     - O BlueXP  não suporta nomes de usuário ou senhas que incluem o caractere A.
     - Se a senha incluir qualquer um dos seguintes carateres especiais, você deve escapar desse caractere especial, prependendo-o com uma barra invertida: & Ou !

Por exemplo:

http://bxpproxyuser:netapp1\!@address:3128

--cacert especifica um certificado assinado pela CA a ser usado para acesso HTTPS entre o conetor e o servidor proxy. Este parâmetro só é necessário se especificar um servidor proxy HTTPS ou se o proxy for um proxy intercetor.

5. Aguarde até que a instalação seja concluída.

   No final da instalação, o serviço de conetor (occm) será reiniciado duas vezes se você tiver especificado um servidor proxy.

6. Abra um navegador da Web a partir de um host que tenha uma conexão com a máquina virtual do conetor e insira o seguinte URL:

   <a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

7. Depois de iniciar sessão, configure o conetor:
   a. Especifique a organização BlueXP  a associar ao conetor.
   b. Introduza um nome para o sistema.
   c. Em **você está executando em um ambiente seguro?** mantenha o modo restrito desativado.

      Você deve manter o modo restrito desativado porque estas etapas descrevem como usar o BlueXP  no modo padrão. Você deve habilitar o modo restrito somente se tiver um ambiente seguro e quiser desconetar essa conta dos serviços de back-end do BlueXP . Se for esse o caso"Siga os passos para começar a utilizar o BlueXP  no modo restrito", .

   d. Selecione **vamos começar**.

**Resultado**

O conetor está agora instalado e está configurado com a sua organização BlueXP .

Se você tiver o armazenamento de Blobs do Azure na mesma assinatura do Azure em que criou o conetor, verá um ambiente de trabalho de armazenamento de Blobs do Azure aparecer automaticamente na tela do BlueXP . "Saiba como gerenciar o armazenamento de Blobs do Azure a partir do BlueXP "

### Passo 6: Forneça permissões para o BlueXP

Agora que você instalou o conetor, você precisa fornecer ao BlueXP  as permissões do Azure que você configurou anteriormente. Com o fornecimento de permissões, o BlueXP  pode gerenciar sua infraestrutura de dados e storage no Azure.

**Função personalizada**

Vá para o portal do Azure e atribua a função personalizada do Azure à máquina virtual Connector para uma ou mais subscrições.

**Passos**

1. No Portal do Azure, abra o serviço **Subscrições** e selecione a sua subscrição.

   É importante atribuir a função do serviço **Subscrições** porque especifica o escopo da atribuição de função no nível da assinatura. O *scope* define o conjunto de recursos aos quais o acesso se aplica. Se você especificar um escopo em um nível diferente (por exemplo, no nível da máquina virtual), sua capacidade de concluir ações de dentro do BlueXP  será afetada.

   "Documentação do Microsoft Azure: Entenda o escopo do Azure RBAC"

2. Selecione **Access control (IAM)** > **Add** > **Add** > **Add role assignment**.
3. Na guia **função**, selecione a função **Operador BlueXP**  e selecione **seguinte**.

   Operador BlueXP  é o nome padrão fornecido na política BlueXP . Se você escolher um nome diferente para a função, selecione esse nome em vez disso.

4. Na guia **Membros**, execute as seguintes etapas:
   a. Atribua acesso a uma **identidade gerenciada**.
   b. Selecione **Selecionar membros**, selecione a assinatura na qual a máquina virtual do conetor foi criada, em **identidade gerenciada**, escolha **Máquina Virtual** e, em seguida, selecione a máquina virtual do conetor.
   c. Selecione **Selecionar**.
   d. Selecione **seguinte**.
   e. Selecione **Rever e atribuir**.
   f. Se você quiser gerenciar recursos em assinaturas adicionais do Azure, mude para essa assinatura e repita essas etapas.

**Resultado**

O BlueXP  agora tem as permissões necessárias para executar ações no Azure em seu nome.

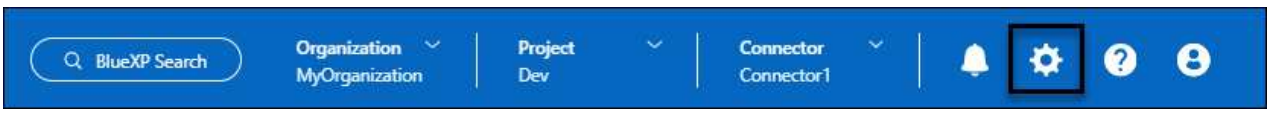
**O que se segue?**

Passe à "Consola BlueXP" para começar a utilizar o conetor com o BlueXP .

**Serviço principal**

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.




2. Selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Credentials Location**: Selecione **Microsoft Azure > Connector**.

b. **Definir credenciais**: Insira informações sobre o responsável do serviço Microsoft Entra que concede as permissões necessárias:
   - ID da aplicação (cliente)
   - ID do diretório (locatário)
   - Segredo Cliente
c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.
d. **Revisão**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

**Resultado**

O BlueXP agora tem as permissões necessárias para executar ações no Azure em seu nome.

## Google Cloud

### Opções de instalação do conetor no Google Cloud

Existem algumas maneiras diferentes de criar um conetor no Google Cloud. Diretamente de BlueXP é a maneira mais comum.

Estão disponíveis as seguintes opções de instalação:

- "Crie o conetor diretamente do BlueXP " (esta é a opção padrão)

  Essa ação inicia uma instância de VM executando o Linux e o software Connector em uma VPC de sua escolha.

- "Crie o conetor usando o gcloud"

  Essa ação também inicia uma instância de VM executando o Linux e o software Connector, mas a implantação é iniciada diretamente do Google Cloud, em vez do BlueXP .

- "Baixe e instale manualmente o software em seu próprio host Linux"

A opção de instalação que você escolher afeta a forma como você se prepara para a instalação. Isso inclui como você fornece ao BlueXP as permissões necessárias que ele precisa para autenticar e gerenciar recursos no Google Cloud.

### Crie um conetor no Google Cloud a partir do BlueXP ou do gcloud

Um conetor é o software NetApp executado em sua rede na nuvem ou na rede local que permite usar todos os recursos e serviços do BlueXP . As opções de instalação disponíveis incluem a criação do conetor na AWS diretamente do BlueXP ou usando o gcloud. Para criar um conetor no Google Cloud a partir do BlueXP ou usando o gcloud, você precisa configurar sua rede, preparar permissões do Google Cloud, ativar as APIs do Google Cloud e, em seguida, criar o conetor.

**Antes de começar**

- Você deve ter um "Compreensão dos conetores".
- Você deve rever "Limitações do conetor".

### Passo 1: Configurar a rede

Configure sua rede para que o conetor possa gerenciar recursos e processos em seu ambiente de nuvem híbrida. Por exemplo, você precisa garantir que as conexões estejam disponíveis para redes de destino e que o acesso de saída à Internet esteja disponível.

#### VPC e sub-rede

Ao criar o conetor, você precisa especificar a VPC e a sub-rede onde o conetor deve residir.

#### Conexões com redes de destino

Um conetor requer uma conexão de rede com o local onde você está planejando criar e gerenciar ambientes de trabalho. Por exemplo, a rede em que você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de storage em seu ambiente local.

#### Acesso de saída à Internet

O local de rede onde você implantar o conetor deve ter uma conexão de saída de Internet para contatar pontos de extremidade específicos.

#### Terminais contactados a partir do conetor

O conetor requer acesso de saída à Internet para entrar em Contato com os seguintes endpoints, a fim de gerenciar recursos e processos em seu ambiente de nuvem pública para operações diárias.

Observe que os endpoints listados abaixo são todas as entradas CNAME.

| Endpoints | Finalidade |
| --- | --- |
| https://www.googleapis.com/compute/v1/<br>https://compute.googleapis.com/compute/v1<br>https://cloudresourcemanager.googleapis.com/v1/projects<br>https://www.googleapis.com/compute/beta<br>https://storage.googleapis.com/storage/v1<br>https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1<br>https://cloudkms.googleapis.com/v1<br>https://www.googleapis.com/deploymentmanager/v2/projects | Para gerenciar recursos no Google Cloud. |
| https://support.NetApp.com https://mysupport.NetApp.com | Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte do NetApp. |
| https://*.api.BlueXP .NetApp.com<br><br>https://api.BlueXP .NetApp.com<br><br>https://*.cloudmanager.cloud.NetApp.com<br><br>https://cloudmanager.cloud.NetApp.com<br><br>https://NetApp-cloud-account.auth0.com | Para fornecer recursos e serviços SaaS no BlueXP .<br><br>Observe que o conetor está entrando em Contato atualmente com "cloudmanager.cloud.NetApp.com", mas começará a entrar em Contato com "API.BlueXP .NetApp.com" em uma próxima versão. |

| Endpoints | Finalidade |
| --- | --- |
| https://*.blob.core.windows.net<br><br>https://cloudmanagerinfraprod.azurecr.io | Para atualizar o conetor e seus componentes do Docker. |

**Terminais contactados a partir da consola BlueXP**

À medida que você usa o console baseado na Web do BlueXP fornecido pela camada SaaS, ele entra em Contato com vários endpoints para concluir as tarefas de gerenciamento de dados. Isso inclui endpoints que são contatados para implantar o conetor a partir do console BlueXP .

"Veja a lista de endpoints contactados a partir da consola BlueXP ".

**Servidor proxy**

Se a sua empresa exigir a implantação de um servidor proxy para todo o tráfego de saída da Internet, obtenha as seguintes informações sobre o proxy HTTP ou HTTPS. Você precisará fornecer essas informações durante a instalação. Observe que o BlueXP não oferece suporte a servidores proxy transparentes.

- Endereço IP
- Credenciais
- Certificado HTTPS

**Portas**

Não há tráfego de entrada para o conetor, a menos que você o inicie ou se o conetor for usado como um proxy para enviar mensagens AutoSupport do Cloud Volumes ONTAP para o suporte da NetApp.

- HTTP (80) e HTTPS (443) fornecem acesso à IU local, que você usará em circunstâncias raras.
- SSH (22) só é necessário se você precisar se conetar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 são necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída à Internet não está disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída à Internet para enviar mensagens AutoSupport, o BlueXP configura automaticamente esses sistemas para usar um servidor proxy incluído no conetor. O único requisito é garantir que o grupo de segurança do conetor permita conexões de entrada pela porta 3128. Você precisará abrir essa porta depois de implantar o conetor.

**Ativar NTP**

Se estiver a planear utilizar a classificação BlueXP para analisar as suas fontes de dados empresariais, deve ativar um serviço de Protocolo de tempo de rede (NTP) no sistema de conetores BlueXP e no sistema de classificação BlueXP para que o tempo seja sincronizado entre os sistemas. "Saiba mais sobre a classificação BlueXP"

Você precisará implementar esse requisito de rede depois de criar o conetor.

### Passo 2: Configurar permissões para criar o conetor

Antes de implantar um conetor do BlueXP ou usando o gcloud, você precisa configurar permissões para o usuário do Google Cloud que implantará a VM do Connector.

**Passos**

1. Crie uma função personalizada no Google Cloud:

   a. Crie um arquivo YAML que inclua as seguintes permissões:

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
BlueXP
stage: GA
includedPermissions:
- 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
```

```
- 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.list
```

b. No Google Cloud, ative o shell da nuvem.

c. Carregue o arquivo YAML que inclui as permissões necessárias.

d. Crie uma função personalizada usando o `gcloud iam roles create` comando.

O exemplo a seguir cria uma função chamada "connectorDeployment" no nível do projeto:

As funções do gcloud iam criam connectorDeployment --project-file-deployment.yaml

"Google Cloud docs: Criando e gerenciando funções personalizadas"

2. Atribua essa função personalizada ao usuário que implantará o conetor do BlueXP ou usando o gcloud.

"Google Cloud docs: Conceda uma única função"

**Resultado**

O usuário do Google Cloud agora tem as permissões necessárias para criar o conetor.

### Passo 3: Configurar permissões para o conetor

Uma conta de serviço do Google Cloud é necessária para fornecer ao conetor as permissões que o BlueXP precisa para gerenciar recursos no Google Cloud. Ao criar o conetor, você precisará associar essa conta de serviço à VM do conetor.

É sua responsabilidade atualizar a função personalizada à medida que novas permissões são adicionadas em versões subsequentes. Se novas permissões forem necessárias, elas serão listadas nas notas de versão.

**Passos**

1. Crie uma função personalizada no Google Cloud:

a. Crie um arquivo YAML que inclua o conteúdo do "Permissões de conta de serviço para o conetor".
b. No Google Cloud, ative o shell da nuvem.
c. Carregue o arquivo YAML que inclui as permissões necessárias.
d. Crie uma função personalizada usando o `gcloud iam roles create` comando.

O exemplo a seguir cria uma função chamada "Connector" no nível do projeto:

```
gcloud iam roles create connector --project=myproject --file=connector.yaml
```

"Google Cloud docs: Criando e gerenciando funções personalizadas"

2. Crie uma conta de serviço no Google Cloud e atribua a função à conta de serviço:
   a. No serviço IAM e Admin, selecione **Contas de serviço > criar conta de serviço**.
   b. Insira os detalhes da conta de serviço e selecione **criar e continuar**.
   c. Selecione a função que você acabou de criar.
   d. Conclua as etapas restantes para criar a função.

   "Google Cloud docs: Criando uma conta de serviço"

3. Se você planeja implantar sistemas Cloud Volumes ONTAP em projetos diferentes do projeto em que o conetor reside, precisará fornecer à conta de serviço do conetor acesso a esses projetos.

   Por exemplo, digamos que o conetor está no projeto 1 e você deseja criar sistemas Cloud Volumes ONTAP no projeto 2. Você precisará conceder acesso à conta de serviço no projeto 2.

   a. No serviço IAM e Admin, selecione o projeto Google Cloud onde você deseja criar sistemas Cloud Volumes ONTAP.
   b. Na página **IAM**, selecione **Grant Access** e forneça os detalhes necessários.
      - Introduza o e-mail da conta de serviço do conetor.
      - Selecione a função personalizada do conetor.
      - Selecione **Guardar**.

   Para obter mais detalhes, consulte "Documentação do Google Cloud"

**Resultado**

A conta de serviço da VM Connector é configurada.

### Etapa 4: Configurar permissões de VPC compartilhadas

Se você estiver usando uma VPC compartilhada para implantar recursos em um projeto de serviço, precisará preparar suas permissões.

Essa tabela é para referência e seu ambiente deve refletir a tabela de permissões quando a configuração do IAM estiver concluída.

**Exibir permissões de VPC compartilhadas**

| Identidade | Criador | Hospedado em | Permissões do projeto de serviço | Permissões do projeto de host | Finalidade |
|---|---|---|---|---|---|
| Conta Google para implantar o conetor | Personalizado | Projeto de Serviço | "Política de implantação do conetor" | compute.networkUser | Implantando o conetor no projeto de serviço |
| Conta de serviço do conetor | Personalizado | Projeto de serviço | "Política de conta de serviço do conetor" | compute.networkUser deploymentmanager.editor | Implantação e manutenção de Cloud Volumes ONTAP e serviços no projeto de serviço |
| Conta de serviço Cloud Volumes ONTAP | Personalizado | Projeto de serviço | Membro Storage.admin: Conta de serviço BlueXP como serviceAccount.user | N/A. | (Opcional) para disposição de dados em categorias e backup e recuperação do BlueXP |
| Agente de serviços de APIs do Google | Google Cloud | Projeto de serviço | (Predefinição) Editor | compute.networkUser | Interage com as APIs do Google Cloud em nome da implantação. Permite que o BlueXP utilize a rede partilhada. |
| Conta de serviço padrão do Google Compute Engine | Google Cloud | Projeto de serviço | (Predefinição) Editor | compute.networkUser | Implanta instâncias do Google Cloud e infraestrutura de computação em nome da implantação. Permite que o BlueXP utilize a rede partilhada. |

Notas:

1. Deploymentmanager.editor só é necessário no projeto host se você não estiver passando regras de firewall para a implantação e estiver escolhendo permitir que o BlueXP as crie para você. O BlueXP criará uma implantação no projeto host que contém a regra de firewall VPC0 se nenhuma regra for especificada.
2. Firewall.create e firewall.delete só são necessários se você não estiver passando regras de firewall para a implantação e estiver escolhendo permitir que o BlueXP as crie para você. Essas permissões residem no arquivo .yaml da conta do BlueXP . Se você estiver implantando um par de HA usando uma VPC compartilhada, essas permissões serão usadas para criar as regras de firewall para VPC1, 2 e 3. Para todas as outras implantações, essas permissões também serão usadas para criar regras para VPC0.
3. Para categorização de dados, a conta de serviço de disposição em categorias precisa ter a função serviceAccount.user na conta de serviço, não apenas no nível do projeto. Atualmente, se você atribuir serviceAccount.user no nível do projeto, as permissões não serão exibidas quando você consultar a conta de serviço com getIAMPolicy.

### Etapa 5: Habilite as APIs do Google Cloud

Várias APIs do Google Cloud devem estar ativadas antes de implantar o Connector e o Cloud Volumes ONTAP no Google Cloud.

**Passo**

1. Ative as seguintes APIs do Google Cloud em seu projeto:
    - API do Cloud Deployment Manager V2
    - API Cloud Logging
    - API do Cloud Resource Manager
    - API do mecanismo de computação
    - API de gerenciamento de identidade e acesso (IAM)
    - API do Cloud Key Management Service (KMS)

      (Necessário somente se você estiver planejando usar o backup e a recuperação do BlueXP com chaves de criptografia gerenciadas pelo cliente (CMEK))

"Documentação do Google Cloud: Habilitando APIs"

### Passo 6: Crie o conetor

Crie um conetor diretamente do console baseado na Web do BlueXP ou usando o gcloud.

**Sobre esta tarefa**

A criação do conetor implanta uma instância de máquina virtual no Google Cloud usando uma configuração padrão. Depois de criar o conetor, você não deve mudar para uma instância de VM menor que tenha menos CPU ou RAM. "Saiba mais sobre a configuração padrão do conetor".

**BlueXP**

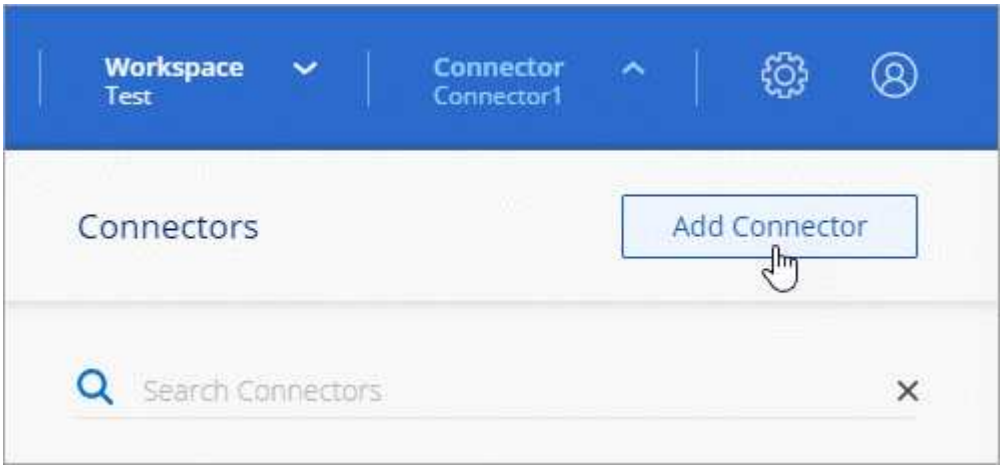
**Antes de começar**

Você deve ter o seguinte:

- As permissões necessárias do Google Cloud para criar o conetor e uma conta de serviço para a VM do conetor.
- VPC e sub-rede que atendem aos requisitos de rede.
- Detalhes sobre um servidor proxy, se for necessário um proxy para acesso à Internet a partir do conetor.

**Passos**

1. Selecione a lista suspensa **Connector** e selecione **Add Connector**.




2. Escolha **Google Cloud Platform** como seu provedor de nuvem.
3. Na página **implantando um conetor**, revise os detalhes sobre o que você precisará. Você tem duas opções:
   a. Selecione **continuar** para se preparar para a implantação usando o guia do produto. Cada etapa do guia do produto inclui as informações contidas nesta página da documentação.
   b. Selecione **Skip to Deployment** se você já tiver preparado seguindo as etapas desta página.
4. Siga as etapas no assistente para criar o conetor:
   - Se você for solicitado, faça login na sua conta do Google, que deve ter as permissões necessárias para criar a instância da máquina virtual.

     O formulário é de propriedade e hospedado pelo Google. Suas credenciais não são fornecidas ao NetApp.

   - **Detalhes**: Insira um nome para a instância da máquina virtual, especifique tags, selecione um projeto e, em seguida, selecione a conta de serviço que tem as permissões necessárias (consulte a seção acima para obter detalhes).
   - **Localização**: Especifique uma região, zona, VPC e sub-rede para a instância.
   - **Rede**: Escolha se deseja ativar um endereço IP público e, opcionalmente, especificar uma configuração de proxy.
   - **Política de firewall**: Escolha se deseja criar uma nova política de firewall ou se deseja selecionar uma política de firewall existente que permita as regras de entrada e saída necessárias.

"Regras de firewall no Google Cloud"

- **Revisão**: Revise suas seleções para verificar se a configuração está correta.

5. Selecione **Adicionar**.

   A instância deve estar pronta em cerca de 7 minutos. Você deve permanecer na página até que o processo esteja concluído.

**Resultado**

Após o processo ser concluído, o conetor está disponível para uso no BlueXP .

Se você tiver buckets do Google Cloud Storage na mesma conta do Google Cloud onde criou o conetor, verá um ambiente de trabalho do Google Cloud Storage aparecer automaticamente na tela do BlueXP . "Saiba como gerenciar o Google Cloud Storage da BlueXP "

**nuvem**

**Antes de começar**

Você deve ter o seguinte:

- As permissões necessárias do Google Cloud para criar o conetor e uma conta de serviço para a VM do conetor.
- VPC e sub-rede que atendem aos requisitos de rede.
- Uma compreensão dos requisitos de instância de VM.
  - * CPU*: 8 núcleos ou 8 vCPUs
  - **RAM**: 32 GB
  - * Tipo de máquina*: Recomendamos n2-standard-8.

    O conetor é compatível com o Google Cloud em uma instância de VM com um sistema operacional que suporta recursos de VM blindados.

**Passos**

1. Faça login no SDK do gcloud usando sua metodologia preferida.

   Em nossos exemplos, usaremos um shell local com o gcloud SDK instalado, mas você pode usar o Google Cloud Shell nativo no console do Google Cloud.

   Para obter mais informações sobre o SDK do Google Cloud, visite o "Página de documentação do Google Cloud SDK".

2. Verifique se você está conetado como um usuário que tem as permissões necessárias definidas na seção acima:

   ```
   gcloud auth list
   ```

   A saída deve mostrar o seguinte em que a conta de utilizador * é a conta de utilizador pretendida para iniciar sessão como:

```
Credentialed Accounts
ACTIVE  ACCOUNT
     some_user_account@domain.com
*    desired_user_account@domain.com
To set the active account, run:
 $ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install
them,
please run:
$ gcloud components update
```

3. Execute o `gcloud compute instances create` comando:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-8
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

**nome da instância**
: O nome da instância desejada para a instância da VM.

**projeto**
: (Opcional) o projeto onde você deseja implantar a VM.

**conta de serviço**
: A conta de serviço especificada na saída do passo 2.

**zona**
: A zona em que você deseja implantar a VM

**sem endereço**
: (Opcional) nenhum endereço IP externo é usado (você precisa de um NAT ou proxy na nuvem para rotear o tráfego para a Internet pública)

**etiqueta de rede**
: (Opcional) Adicione tags de rede para vincular uma regra de firewall usando tags à instância do conetor

**caminho de rede**

(Opcional) Adicione o nome da rede para implantar o conetor (para uma VPC compartilhada, você precisa do caminho completo)

**caminho de sub-rede**

(Opcional) Adicione o nome da sub-rede para implantar o conetor (para uma VPC compartilhada, você precisa do caminho completo)

**kms-chave-caminho**

(Opcional) Adicionar uma chave KMS para criptografar os discos do conetor (as permissões do IAM também precisam ser aplicadas)

Para obter mais informações sobre essas bandeiras, visite o "Documentação do SDK de computação do Google Cloud".

+
Executar o comando implanta o conetor usando a imagem dourada do NetApp. A instância do conetor e o software devem estar sendo executados em aproximadamente cinco minutos.

1. Abra um navegador da Web a partir de um host que tenha uma conexão com a instância do conetor e insira o seguinte URL:

   <a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

2. Depois de iniciar sessão, configure o conetor:
   a. Especifique a organização BlueXP  a associar ao conetor.

      "Saiba mais sobre o gerenciamento de identidades e acesso do BlueXP ".

   b. Introduza um nome para o sistema.

**Resultado**

O conetor está agora instalado e configurado com a sua organização BlueXP .

Abra um navegador da Web e vá para a "Consola BlueXP" para começar a usar o conetor com o BlueXP .

#### Instale manualmente o conetor no Google Cloud

Um conetor é o software NetApp executado em sua rede na nuvem ou na rede local que permite usar todos os recursos e serviços do BlueXP . Uma das opções de instalação disponíveis é instalar manualmente o software Connector em um host Linux executado no Google Cloud. Para instalar manualmente o conetor em seu próprio host Linux, você precisa analisar os requisitos de host, configurar sua rede, preparar permissões do Google Cloud, ativar APIs, instalar o conetor e, em seguida, fornecer as permissões que você preparou.

**Antes de começar**

- Você deve ter um "Compreensão dos conetores".
- Você deve rever "Limitações do conetor".

### Etapa 1: Revise os requisitos do host

O software do conetor deve ser executado em um host que atenda a requisitos específicos do sistema operacional, requisitos de RAM, requisitos de porta, etc.

#### Host dedicado

O conetor não é suportado em um host que é compartilhado com outros aplicativos. O host deve ser um host dedicado.

#### Hipervisor

É necessário um hypervisor bare metal ou hospedado certificado para executar um sistema operacional suportado.

#### requisitos de sistema operacional e contentor

O BlueXP  suporta o conetor com os seguintes sistemas operacionais ao usar o BlueXP  no modo padrão ou no modo restrito. Uma ferramenta de orquestração de contêineres é necessária antes de instalar o conetor.

| Sistema operacional | Versões de OS compatíveis | Versões de conetor suportadas | Ferramenta de recipiente necessária | SELinux |
|---|---|---|---|---|
| Red Hat Enterprise Linux | 9,1 a 9,4<br><br>8,6 a 8,10 | 3.9.40 ou posterior com BlueXP  no modo padrão ou modo restrito | Podman versão 4.6.1 ou 4.9.4<br><br>Veja os requisitos de configuração do Podman. | Suporte no modo de execução ou modo permissivo 1 |
| Ubuntu | 24,04 LTS | 3.9.45 ou posterior com BlueXP  no modo padrão ou modo restrito | Docker Engine 26.0.0 | Não suportado |

Notas:

1. O gerenciamento de sistemas Cloud Volumes ONTAP não é suportado por conetores que tenham o SELinux habilitado no sistema operacional.
2. O conetor é suportado em versões em inglês destes sistemas operativos.
3. Para o RHEL, o host deve estar registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar repositórios para atualizar o software necessário de 3rd partes durante a instalação do conetor.

#### CPU

8 núcleos ou 8 vCPUs

#### RAM

32 GB

#### Tipo de máquina Google Cloud

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos n2-standard-8.

O conetor é compatível com o Google Cloud em uma instância de VM com um sistema operacional compatível "Recursos de VM blindados"

**Espaço em disco em /opt**

100 GiB de espaço deve estar disponível

O BlueXP usa `/opt` para instalar o `/opt/application/netapp` diretório e seu conteúdo.

**Espaço em disco em /var**

20 GiB de espaço deve estar disponível

O BlueXP requer esse espaço `/var` porque o Docker ou o Podman são arquitetados para criar os contentores dentro desse diretório. Especificamente, eles irão criar contentores no `/var/lib/containers/storage` diretório. Montagens externas ou links simbólicos não funcionam para este espaço.

### Passo 2: Instale o Podman ou Docker Engine

Dependendo do seu sistema operacional, o Podman ou o Docker Engine são necessários antes de instalar o conetor.

- O Podman é necessário para o Red Hat Enterprise Linux 8 e 9.

  Veja as versões do Podman suportadas pelo BlueXP .

- Docker Engine é necessário para o Ubuntu.

  Veja as versões do Docker Engine que o BlueXP suporta.

**Exemplo 3. Passos**

**Podman**

Siga estas etapas para instalar o Podman e configurá-lo para atender aos seguintes requisitos:

- O serviço podman.socket deve ser ativado e iniciado
- python3 deve ser instalado
- O pacote podman-compose versão 1.0.6 deve ser instalado
- Podman-compose deve ser adicionado à variável de ambiente PATH

**Passos**

1. Remova o pacote podman-docker se ele estiver instalado no host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Instale o Podman.

   O Podman está disponível nos repositórios oficiais do Red Hat Enterprise Linux.

   Para Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

   Onde o <version> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas pelo BlueXP .

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

   Onde o <version> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas pelo BlueXP .

3. Ative e inicie o serviço podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Instale o python3.

```
sudo dnf install python3
```

5. Instale o pacote do repositório EPEL se ainda não estiver disponível no seu sistema.

Esta etapa é necessária porque o podman-compose está disponível no repositório extra Packages for Enterprise Linux (EPEL).

Para Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

Para Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Instale o pacote podman-compose 1,0.6.

```
sudo dnf install podman-compose-1.0.6
```

> Usar o `dnf install` comando atende ao requisito para adicionar podman-compose à variável de ambiente PATH. O comando installation adiciona podman-compose ao /usr/bin, que já está incluído na `secure_path` opção no host.

**Docker Engine**

Siga a documentação do Docker para instalar o Docker Engine.

**Passos**

1. "Veja as instruções de instalação do Docker"

   Certifique-se de seguir as etapas para instalar uma versão específica do Docker Engine. Instalar a versão mais recente irá instalar uma versão do Docker que o BlueXP  não suporta.

2. Verifique se o Docker está ativado e em execução.

```
sudo systemctl enable docker && sudo systemctl start docker
```

### Passo 3: Configurar a rede

Configure sua rede para que o conetor possa gerenciar recursos e processos em seu ambiente de nuvem híbrida. Por exemplo, você precisa garantir que as conexões estejam disponíveis para redes de destino e que o acesso de saída à Internet esteja disponível.

**Conexões com redes de destino**

Um conetor requer uma conexão de rede com o local onde você está planejando criar e gerenciar ambientes de trabalho. Por exemplo, a rede em que você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de storage em seu ambiente local.

### Acesso de saída à Internet

O local de rede onde você implantar o conetor deve ter uma conexão de saída de Internet para contatar pontos de extremidade específicos.

### Endpoints contatados de computadores ao usar o console baseado na Web do BlueXP

Os computadores que acessam o console BlueXP  a partir de um navegador da Web devem ter a capacidade de entrar em Contato com vários endpoints. Você precisará usar o console BlueXP  para configurar o conetor e para uso diário do BlueXP .

"Prepare a rede para o console BlueXP ".

### Terminais contactados durante a instalação manual

Quando você instala manualmente o conetor em seu próprio host Linux, o instalador do conetor requer acesso aos seguintes URLs durante o processo de instalação:

- https://mysupport.NetApp.com
- https://signin.b2c.NetApp.com (este endpoint é o URL CNAME para https://mysupport.NetApp.com)
- https://cloudmanager.cloud.NetApp.com/locação
- https://stream.cloudmanager.cloud.NetApp.com
- https://production-artifacts.cloudmanager.cloud.NetApp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  O host pode tentar atualizar os pacotes do sistema operacional durante a instalação. O host pode entrar em Contato com diferentes sites de espelhamento para esses pacotes do sistema operacional.

### Terminais contactados a partir do conetor

O conetor requer acesso de saída à Internet para entrar em Contato com os seguintes endpoints, a fim de gerenciar recursos e processos em seu ambiente de nuvem pública para operações diárias.

Observe que os endpoints listados abaixo são todas as entradas CNAME.

| Endpoints | Finalidade |
|---|---|
| https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects | Para gerenciar recursos no Google Cloud. |
| https://support.NetApp.com https://mysupport.NetApp.com | Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte do NetApp. |

| Endpoints | Finalidade |
| --- | --- |
| https://*.api.BlueXP .NetApp.com<br><br>https://api.BlueXP .NetApp.com<br><br>https://*.cloudmanager.cloud.NetApp.com<br><br>https://cloudmanager.cloud.NetApp.com<br><br>https://NetApp-cloud-account.auth0.com | Para fornecer recursos e serviços SaaS no BlueXP .<br><br>Observe que o conetor está entrando em Contato atualmente com "cloudmanager.cloud.NetApp.com ", mas começará a entrar em Contato com "API.BlueXP .NetApp.com" em uma próxima versão. |
| https://*.blob.core.windows.net<br><br>https://cloudmanagerinfraprod.azurecr.io | Para atualizar o conetor e seus componentes do Docker. |

**Servidor proxy**

Se a sua empresa exigir a implantação de um servidor proxy para todo o tráfego de saída da Internet, obtenha as seguintes informações sobre o proxy HTTP ou HTTPS. Você precisará fornecer essas informações durante a instalação. Observe que o BlueXP  não oferece suporte a servidores proxy transparentes.

- Endereço IP
- Credenciais
- Certificado HTTPS

**Portas**

Não há tráfego de entrada para o conetor, a menos que você o inicie ou se o conetor for usado como um proxy para enviar mensagens AutoSupport do Cloud Volumes ONTAP para o suporte da NetApp.

- HTTP (80) e HTTPS (443) fornecem acesso à IU local, que você usará em circunstâncias raras.
- SSH (22) só é necessário se você precisar se conetar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 são necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída à Internet não está disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída à Internet para enviar mensagens AutoSupport, o BlueXP  configura automaticamente esses sistemas para usar um servidor proxy incluído no conetor. O único requisito é garantir que o grupo de segurança do conetor permita conexões de entrada pela porta 3128. Você precisará abrir essa porta depois de implantar o conetor.

**Ativar NTP**

Se estiver a planear utilizar a classificação BlueXP  para analisar as suas fontes de dados empresariais, deve ativar um serviço de Protocolo de tempo de rede (NTP) no sistema de conetores BlueXP  e no sistema de classificação BlueXP  para que o tempo seja sincronizado entre os sistemas. "Saiba mais sobre a classificação BlueXP"

### Passo 4: Configurar permissões para o conetor

Uma conta de serviço do Google Cloud é necessária para fornecer ao conetor as permissões que o BlueXP precisa para gerenciar recursos no Google Cloud. Ao criar o conetor, você precisará associar essa conta de serviço à VM do conetor.

É sua responsabilidade atualizar a função personalizada à medida que novas permissões são adicionadas em versões subsequentes. Se novas permissões forem necessárias, elas serão listadas nas notas de versão.

**Passos**

1. Crie uma função personalizada no Google Cloud:

   a. Crie um arquivo YAML que inclua o conteúdo do "Permissões de conta de serviço para o conetor".

   b. No Google Cloud, ative o shell da nuvem.

   c. Carregue o arquivo YAML que inclui as permissões necessárias.

   d. Crie uma função personalizada usando o `gcloud iam roles create` comando.

      O exemplo a seguir cria uma função chamada "Connector" no nível do projeto:

      ```
      gcloud iam roles create connector --project=myproject --file=connector.yaml
      ```

   "Google Cloud docs: Criando e gerenciando funções personalizadas"

2. Crie uma conta de serviço no Google Cloud e atribua a função à conta de serviço:

   a. No serviço IAM e Admin, selecione **Contas de serviço > criar conta de serviço**.

   b. Insira os detalhes da conta de serviço e selecione **criar e continuar**.

   c. Selecione a função que você acabou de criar.

   d. Conclua as etapas restantes para criar a função.

      "Google Cloud docs: Criando uma conta de serviço"

3. Se você planeja implantar sistemas Cloud Volumes ONTAP em projetos diferentes do projeto em que o conetor reside, precisará fornecer à conta de serviço do conetor acesso a esses projetos.

   Por exemplo, digamos que o conetor está no projeto 1 e você deseja criar sistemas Cloud Volumes ONTAP no projeto 2. Você precisará conceder acesso à conta de serviço no projeto 2.

   a. No serviço IAM e Admin, selecione o projeto Google Cloud onde você deseja criar sistemas Cloud Volumes ONTAP.

   b. Na página **IAM**, selecione **Grant Access** e forneça os detalhes necessários.

      - Introduza o e-mail da conta de serviço do conetor.
      - Selecione a função personalizada do conetor.
      - Selecione **Guardar**.

   Para obter mais detalhes, consulte "Documentação do Google Cloud"

**Resultado**

A conta de serviço da VM Connector é configurada.

### Etapa 5: Configurar permissões de VPC compartilhadas

Se você estiver usando uma VPC compartilhada para implantar recursos em um projeto de serviço, precisará preparar suas permissões.

Essa tabela é para referência e seu ambiente deve refletir a tabela de permissões quando a configuração do IAM estiver concluída.

**Exibir permissões de VPC compartilhadas**

| Identidade | Criador | Hospedado em | Permissões do projeto de serviço | Permissões do projeto de host | Finalidade |
|---|---|---|---|---|---|
| Conta Google para implantar o conetor | Personalizado | Projeto de Serviço | "Política de implantação do conetor" | compute.networkUser | Implantando o conetor no projeto de serviço |
| Conta de serviço do conetor | Personalizado | Projeto de serviço | "Política de conta de serviço do conetor" | compute.networkUser deploymentmanager.editor | Implantação e manutenção de Cloud Volumes ONTAP e serviços no projeto de serviço |
| Conta de serviço Cloud Volumes ONTAP | Personalizado | Projeto de serviço | Membro Storage.admin: Conta de serviço BlueXP como serviceAccount.user | N/A. | (Opcional) para disposição de dados em categorias e backup e recuperação do BlueXP |
| Agente de serviços de APIs do Google | Google Cloud | Projeto de serviço | (Predefinição) Editor | compute.networkUser | Interage com as APIs do Google Cloud em nome da implantação. Permite que o BlueXP utilize a rede partilhada. |
| Conta de serviço padrão do Google Compute Engine | Google Cloud | Projeto de serviço | (Predefinição) Editor | compute.networkUser | Implanta instâncias do Google Cloud e infraestrutura de computação em nome da implantação. Permite que o BlueXP utilize a rede partilhada. |

Notas:

1. Deploymentmanager.editor só é necessário no projeto host se você não estiver passando regras de firewall para a implantação e estiver escolhendo permitir que o BlueXP as crie para você. O BlueXP criará uma implantação no projeto host que contém a regra de firewall VPC0 se nenhuma regra for especificada.
2. Firewall.create e firewall.delete só são necessários se você não estiver passando regras de firewall para a implantação e estiver escolhendo permitir que o BlueXP as crie para você. Essas permissões residem no arquivo .yaml da conta do BlueXP . Se você estiver implantando um par de HA usando uma VPC compartilhada, essas permissões serão usadas para criar as regras de firewall para VPC1, 2 e 3. Para todas as outras implantações, essas permissões também serão usadas para criar regras para VPC0.
3. Para categorização de dados, a conta de serviço de disposição em categorias precisa ter a função serviceAccount.user na conta de serviço, não apenas no nível do projeto. Atualmente, se você atribuir serviceAccount.user no nível do projeto, as permissões não serão exibidas quando você consultar a conta de serviço com getIAMPolicy.

### Etapa 6: Habilite as APIs do Google Cloud

Várias APIs do Google Cloud devem estar ativadas antes de implantar sistemas Cloud Volumes ONTAP no Google Cloud.

**Passo**

1. Ative as seguintes APIs do Google Cloud em seu projeto:
    - API do Cloud Deployment Manager V2
    - API Cloud Logging
    - API do Cloud Resource Manager
    - API do mecanismo de computação
    - API de gerenciamento de identidade e acesso (IAM)
    - API do Cloud Key Management Service (KMS)

      (Necessário somente se você estiver planejando usar o backup e a recuperação do BlueXP com chaves de criptografia gerenciadas pelo cliente (CMEK))

"Documentação do Google Cloud: Habilitando APIs"

### Passo 7: Instale o conetor

Após a conclusão dos pré-requisitos, você pode instalar manualmente o software em seu próprio host Linux.

**Antes de começar**

Você deve ter o seguinte:

- Root Privileges para instalar o conetor.
- Detalhes sobre um servidor proxy, se for necessário um proxy para acesso à Internet a partir do conetor.

  Você tem a opção de configurar um servidor proxy após a instalação, mas isso requer a reinicialização do conetor.

  Observe que o BlueXP não oferece suporte a servidores proxy transparentes.

- Um certificado assinado pela CA, se o servidor proxy usar HTTPS ou se o proxy for um proxy intercetor.

**Sobre esta tarefa**

O instalador disponível no site de suporte da NetApp pode ser uma versão anterior. Após a instalação, o conetor se atualiza automaticamente se uma nova versão estiver disponível.

**Passos**

1. Se as variáveis de sistema *http_proxy* ou *https_proxy* estiverem definidas no host, remova-as:

   ```
   unset http_proxy
   unset https_proxy
   ```

   Se você não remover essas variáveis do sistema, a instalação falhará.

2. Faça o download do software Connector do "Site de suporte da NetApp"e copie-o para o host Linux.

   Você deve baixar o instalador do conetor "online" destinado a ser usado em sua rede ou na nuvem. Um instalador "offline" separado está disponível para o conetor, mas só é suportado com implantações de modo privado.

3. Atribua permissões para executar o script.

   ```
   chmod +x BlueXP-Connector-Cloud-<version>
   ```

   Onde <version> é a versão do conetor que você baixou.

4. Execute o script de instalação.

   ```
    ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
   --cacert <path and file name of a CA-signed certificate>
   ```

   Os parâmetros --proxy e --cacert são opcionais. Se você tiver um servidor proxy, será necessário inserir os parâmetros como mostrado. O instalador não solicita que você forneça informações sobre um proxy.

   Aqui está um exemplo do comando usando ambos os parâmetros opcionais:

   ```
    ./BlueXP-Connector-Cloud-v3.9.40--proxy
   https://user:password@10.0.0.30:8080/ --cacert
   /tmp/cacert/certificate.cer
   ```

   --proxy configura o conetor para usar um servidor proxy HTTP ou HTTPS usando um dos seguintes formatos:

   - http://address:port
   - http://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port
   - https://user-name:password@address:port
   - https://domain-name%92user-name:password@address:port

     Observe o seguinte:

     - O usuário pode ser um usuário local ou usuário de domínio.
     - Para um usuário de domínio, você deve usar o código ASCII para a como mostrado acima.
     - O BlueXP  não suporta nomes de usuário ou senhas que incluem o caractere A.
     - Se a senha incluir qualquer um dos seguintes carateres especiais, você deve escapar desse caractere especial, prependendo-o com uma barra invertida: & Ou !

       Por exemplo:

http://bxpproxyuser:netapp1\!@address:3128

--cacert especifica um certificado assinado pela CA a ser usado para acesso HTTPS entre o conetor e o servidor proxy. Este parâmetro só é necessário se especificar um servidor proxy HTTPS ou se o proxy for um proxy intercetor.

5. Aguarde até que a instalação seja concluída.

   No final da instalação, o serviço de conetor (occm) será reiniciado duas vezes se você tiver especificado um servidor proxy.

6. Abra um navegador da Web a partir de um host que tenha uma conexão com a máquina virtual do conetor e insira o seguinte URL:

   <a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

7. Depois de iniciar sessão, configure o conetor:
   a. Especifique a organização BlueXP  a associar ao conetor.
   b. Introduza um nome para o sistema.
   c. Em **você está executando em um ambiente seguro?** mantenha o modo restrito desativado.

      Você deve manter o modo restrito desativado porque estas etapas descrevem como usar o BlueXP  no modo padrão. Você deve habilitar o modo restrito somente se tiver um ambiente seguro e quiser desconetar essa conta dos serviços de back-end do BlueXP . Se for esse o caso"Siga os passos para começar a utilizar o BlueXP  no modo restrito", .

   d. Selecione **vamos começar**.

**Resultado**

O conetor está agora instalado e está configurado com a sua organização BlueXP .

Se você tiver buckets do Google Cloud Storage na mesma conta do Google Cloud onde criou o conetor, verá um ambiente de trabalho do Google Cloud Storage aparecer automaticamente na tela do BlueXP . "Saiba como gerenciar o Google Cloud Storage da BlueXP "

### Passo 8: Forneça permissões para o BlueXP

Você precisa fornecer ao BlueXP  as permissões do Google Cloud que você configurou anteriormente. O fornecimento de permissões permite que o BlueXP  gerencie sua infraestrutura de dados e armazenamento no Google Cloud.

**Passos**

1. Vá para o portal do Google Cloud e atribua a conta de serviço à instância da VM Connector.

   "Documentação do Google Cloud: Alterando a conta de serviço e os escopos de acesso para uma instância"

2. Se você quiser gerenciar recursos em outros projetos do Google Cloud, conceda acesso adicionando a conta de serviço com a função BlueXP  a esse projeto. Você precisará repetir esta etapa para cada projeto.

**Resultado**

O BlueXP  agora tem as permissões necessárias para executar ações no Google Cloud em seu nome.

### Instale e configure um conetor no local

Um conetor é o software NetApp executado em sua rede na nuvem ou na rede local que permite usar todos os recursos e serviços do BlueXP . Para executar o conetor no local, você precisa analisar os requisitos de host, configurar sua rede, preparar permissões de nuvem, instalar o conetor, configurar o conetor e, em seguida, fornecer as permissões que você preparou.

#### Antes de começar

- Você deve ter um "Compreensão dos conetores".
- Você deve rever "Limitações do conetor".

#### Etapa 1: Revise os requisitos do host

O software do conetor deve ser executado em um host que atenda a requisitos específicos do sistema operacional, requisitos de RAM, requisitos de porta, etc. Certifique-se de que o seu host atenda a esses requisitos antes de instalar o conetor.

**Host dedicado**

O conetor não é suportado em um host que é compartilhado com outros aplicativos. O host deve ser um host dedicado.

**Hipervisor**

É necessário um hypervisor bare metal ou hospedado certificado para executar um sistema operacional suportado.

**requisitos de sistema operacional e contentor**

O BlueXP  suporta o conetor com os seguintes sistemas operacionais ao usar o BlueXP  no modo padrão ou no modo restrito. Uma ferramenta de orquestração de contêineres é necessária antes de instalar o conetor.

| Sistema operacional | Versões de OS compatíveis | Versões de conetor suportadas | Ferramenta de recipiente necessária | SELinux |
|---|---|---|---|---|
| Red Hat Enterprise Linux | 9,1 a 9,4<br><br>8,6 a 8,10 | 3.9.40 ou posterior com BlueXP  no modo padrão ou modo restrito | Podman versão 4.6.1 ou 4.9.4<br><br>Veja os requisitos de configuração do Podman. | Suporte no modo de execução ou modo permissivo 1 |
| Ubuntu | 24,04 LTS | 3.9.45 ou posterior com BlueXP  no modo padrão ou modo restrito | Docker Engine 26.0.0 | Não suportado |

Notas:

1. O gerenciamento de sistemas Cloud Volumes ONTAP não é suportado por conetores que tenham o SELinux habilitado no sistema operacional.

2. O conetor é suportado em versões em inglês destes sistemas operativos.
3. Para o RHEL, o host deve estar registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar repositórios para atualizar o software necessário de 3rd partes durante a instalação do conetor.

**CPU**

8 núcleos ou 8 vCPUs

**RAM**

32 GB

**Espaço em disco em /opt**

100 GiB de espaço deve estar disponível

O BlueXP usa `/opt` para instalar o `/opt/application/netapp` diretório e seu conteúdo.

**Espaço em disco em /var**

20 GiB de espaço deve estar disponível

O BlueXP requer esse espaço `/var` porque o Docker ou o Podman são arquitetados para criar os contentores dentro desse diretório. Especificamente, eles irão criar contentores no `/var/lib/containers/storage` diretório. Montagens externas ou links simbólicos não funcionam para este espaço.

#### Passo 2: Instale o Podman ou Docker Engine

Dependendo do seu sistema operacional, o Podman ou o Docker Engine são necessários antes de instalar o conetor.

- O Podman é necessário para o Red Hat Enterprise Linux 8 e 9.

  Veja as versões do Podman suportadas pelo BlueXP .

- Docker Engine é necessário para o Ubuntu.

  Veja as versões do Docker Engine que o BlueXP suporta.

**Exemplo 4. Passos**

**Podman**

Siga estas etapas para instalar o Podman e configurá-lo para atender aos seguintes requisitos:

- O serviço podman.socket deve ser ativado e iniciado
- python3 deve ser instalado
- O pacote podman-compose versão 1.0.6 deve ser instalado
- Podman-compose deve ser adicionado à variável de ambiente PATH

**Passos**

1. Remova o pacote podman-docker se ele estiver instalado no host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Instale o Podman.

   O Podman está disponível nos repositórios oficiais do Red Hat Enterprise Linux.

   Para Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

   Onde o <version> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas pelo BlueXP .

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

   Onde o <version> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas pelo BlueXP .

3. Ative e inicie o serviço podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Instale o python3.

```
sudo dnf install python3
```

5. Instale o pacote do repositório EPEL se ainda não estiver disponível no seu sistema.

Esta etapa é necessária porque o podman-compose está disponível no repositório extra Packages for Enterprise Linux (EPEL).

Para Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

Para Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Instale o pacote podman-compose 1,0.6.

```
sudo dnf install podman-compose-1.0.6
```

> Usar o `dnf install` comando atende ao requisito para adicionar podman-compose à variável de ambiente PATH. O comando installation adiciona podman-compose ao /usr/bin, que já está incluído na `secure_path` opção no host.

**Docker Engine**

Siga a documentação do Docker para instalar o Docker Engine.

**Passos**

1. "Veja as instruções de instalação do Docker"

   Certifique-se de seguir as etapas para instalar uma versão específica do Docker Engine. Instalar a versão mais recente irá instalar uma versão do Docker que o BlueXP  não suporta.

2. Verifique se o Docker está ativado e em execução.

```
sudo systemctl enable docker && sudo systemctl start docker
```

#### Passo 3: Configurar a rede

Configure sua rede para que o conetor possa gerenciar recursos e processos em seu ambiente de nuvem híbrida. Por exemplo, você precisa garantir que as conexões estejam disponíveis para redes de destino e que o acesso de saída à Internet esteja disponível.

**Conexões com redes de destino**

Um conetor requer uma conexão de rede com o local onde você está planejando criar e gerenciar ambientes de trabalho. Por exemplo, a rede em que você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de storage em seu ambiente local.

### Acesso de saída à Internet

O local de rede onde você implantar o conetor deve ter uma conexão de saída de Internet para contatar pontos de extremidade específicos.

### Endpoints contatados de computadores ao usar o console baseado na Web do BlueXP

Os computadores que acessam o console BlueXP  a partir de um navegador da Web devem ter a capacidade de entrar em Contato com vários endpoints. Você precisará usar o console BlueXP  para configurar o conetor e para uso diário do BlueXP .

"Prepare a rede para o console BlueXP ".

### Terminais contactados durante a instalação manual

Quando você instala manualmente o conetor em seu próprio host Linux, o instalador do conetor requer acesso aos seguintes URLs durante o processo de instalação:

- https://mysupport.NetApp.com
- https://signin.b2c.NetApp.com (este endpoint é o URL CNAME para https://mysupport.NetApp.com)
- https://cloudmanager.cloud.NetApp.com/locação
- https://stream.cloudmanager.cloud.NetApp.com
- https://production-artifacts.cloudmanager.cloud.NetApp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  O host pode tentar atualizar os pacotes do sistema operacional durante a instalação. O host pode entrar em Contato com diferentes sites de espelhamento para esses pacotes do sistema operacional.

### Terminais contactados a partir do conetor

O conetor requer acesso de saída à Internet para entrar em Contato com os seguintes endpoints, a fim de gerenciar recursos e processos em seu ambiente de nuvem pública para operações diárias.

Observe que os endpoints listados abaixo são todas as entradas CNAME.

| Endpoints | Finalidade |
|---|---|
| Serviços da AWS (amazonaws.com):<br>• CloudFormation<br>• Nuvem de computação elástica (EC2)<br>• Gerenciamento de identidade e acesso (IAM)<br>• Key Management Service (KMS)<br>• Serviço de token de segurança (STS)<br>• Serviço de armazenamento simples (S3) | Para gerenciar recursos na AWS. O endpoint exato depende da região da AWS que você está usando. "Consulte a documentação da AWS para obter detalhes" |
| https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net | Para gerenciar recursos em regiões públicas do Azure. |

| Endpoints | Finalidade |
| --- | --- |
| https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn | Para gerenciar recursos nas regiões do Azure China. |
| https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects | Para gerenciar recursos no Google Cloud. |
| https://support.NetApp.com https://mysupport.NetApp.com | Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte do NetApp. |
| https://*.api.BlueXP .NetApp.com<br><br>https://api.BlueXP .NetApp.com<br><br>https://*.cloudmanager.cloud.NetApp.com<br><br>https://cloudmanager.cloud.NetApp.com<br><br>https://NetApp-cloud-account.auth0.com | Para fornecer recursos e serviços SaaS no BlueXP .<br><br>Observe que o conetor está entrando em Contato atualmente com "cloudmanager.cloud.NetApp.com ", mas começará a entrar em Contato com "API.BlueXP .NetApp.com" em uma próxima versão. |
| https://*.blob.core.windows.net<br><br>https://cloudmanagerinfraprod.azurecr.io | Para atualizar o conetor e seus componentes do Docker. |

**Servidor proxy**

Se a sua empresa exigir a implantação de um servidor proxy para todo o tráfego de saída da Internet, obtenha as seguintes informações sobre o proxy HTTP ou HTTPS. Você precisará fornecer essas informações durante a instalação. Observe que o BlueXP  não oferece suporte a servidores proxy transparentes.

- Endereço IP
- Credenciais
- Certificado HTTPS

**Portas**

Não há tráfego de entrada para o conetor, a menos que você o inicie ou se o conetor for usado como um proxy para enviar mensagens AutoSupport do Cloud Volumes ONTAP para o suporte da NetApp.

- HTTP (80) e HTTPS (443) fornecem acesso à IU local, que você usará em circunstâncias raras.

- SSH (22) só é necessário se você precisar se conetar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 são necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída à Internet não está disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída à Internet para enviar mensagens AutoSupport, o BlueXP configura automaticamente esses sistemas para usar um servidor proxy incluído no conetor. O único requisito é garantir que o grupo de segurança do conetor permita conexões de entrada pela porta 3128. Você precisará abrir essa porta depois de implantar o conetor.

### Ativar NTP

Se estiver a planear utilizar a classificação BlueXP para analisar as suas fontes de dados empresariais, deve ativar um serviço de Protocolo de tempo de rede (NTP) no sistema de conetores BlueXP e no sistema de classificação BlueXP para que o tempo seja sincronizado entre os sistemas. "Saiba mais sobre a classificação BlueXP"

#### Etapa 4: Configurar permissões de nuvem

Se você quiser usar os serviços do BlueXP na AWS ou no Azure com um conetor no local, precisará configurar permissões no seu provedor de nuvem para que você possa adicionar as credenciais ao conetor depois de instalá-lo.

Por que não o Google Cloud? Quando o conetor é instalado em suas instalações, ele não pode gerenciar seus recursos no Google Cloud. O conetor precisa ser instalado no Google Cloud para gerenciar todos os recursos que residem lá.

**AWS**

Quando o conetor é instalado no local, você precisa fornecer permissões da AWS ao BlueXP adicionando chaves de acesso para um usuário do IAM que tenha as permissões necessárias.

Você deve usar esse método de autenticação se o conetor estiver instalado no local. Você não pode usar uma função do IAM.

**Passos**

1. Faça login no console da AWS e navegue até o serviço do IAM.
2. Criar uma política:

    a. Selecione **políticas > criar política**.

    b. Selecione **JSON** e copie e cole o conteúdo do "Política do IAM para o conetor".

    c. Conclua as etapas restantes para criar a política.

    Dependendo dos serviços do BlueXP que você está planejando usar, talvez seja necessário criar uma segunda política.

    Para regiões padrão, as permissões são distribuídas em duas políticas. Duas políticas são necessárias devido a um limite máximo de tamanho de caractere para políticas gerenciadas na AWS. "Saiba mais sobre as políticas do IAM para o conetor".

3. Anexe as políticas a um usuário do IAM.
    - "Documentação da AWS: Criando funções do IAM"
    - "Documentação da AWS: Adicionando e removendo políticas do IAM"
4. Certifique-se de que o utilizador tem uma chave de acesso que pode adicionar ao BlueXP depois de instalar o conetor.

**Resultado**

Agora você deve ter chaves de acesso para um usuário do IAM que tenha as permissões necessárias. Depois de instalar o conetor, você precisará associar essas credenciais ao conetor do BlueXP .

**Azure**

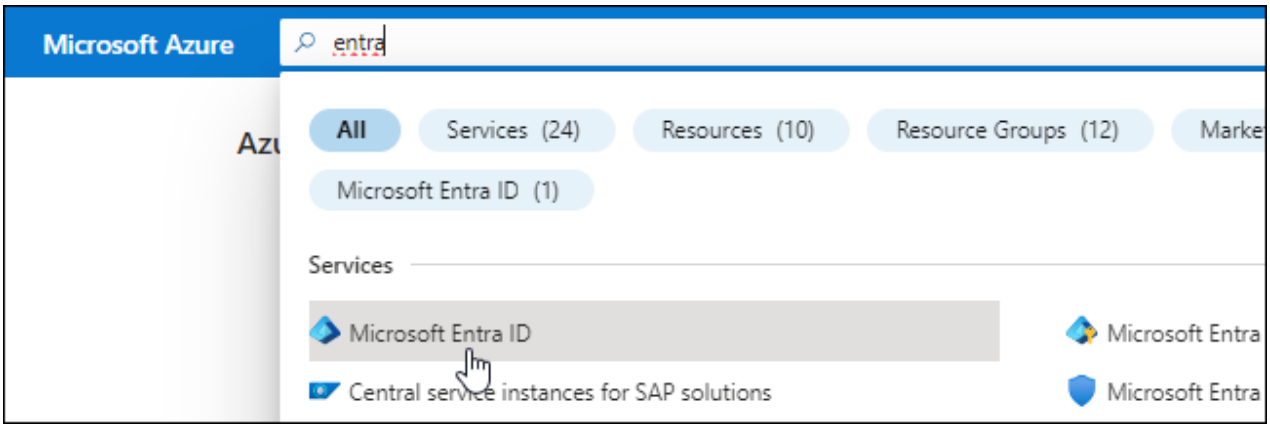
Quando o conetor é instalado no local, você precisa fornecer permissões do Azure ao BlueXP configurando um responsável de serviço no Microsoft Entra ID e obtendo as credenciais do Azure de que o BlueXP precisa.

**Crie um aplicativo Microsoft Entra para controle de acesso baseado em funções**

1. Certifique-se de ter permissões no Azure para criar um aplicativo do ative Directory e atribuir o aplicativo a uma função.

    Para obter mais informações, consulte "Documentação do Microsoft Azure: Permissões necessárias"

2. No portal do Azure, abra o serviço **Microsoft Entra ID**.




3. No menu, selecione **inscrições de aplicativos**.
4. Selecione **novo registo**.
5. Especifique detalhes sobre o aplicativo:
   - **Nome**: Insira um nome para o aplicativo.
   - **Tipo de conta**: Selecione um tipo de conta (qualquer funcionará com o BlueXP ).
   - * URI de redirecionamento*: Você pode deixar este campo em branco.
6. Selecione **Registe-se**.

   Você criou o aplicativo AD e o principal de serviço.

**Atribua a aplicação a uma função**

1. Crie uma função personalizada:

   Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se você preferir usar um método diferente, consulte "Documentação do Azure"

   a. Copie o conteúdo do "Permissões de função personalizadas para o conetor" e salve-o em um arquivo JSON.
   b. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

      Você deve adicionar o ID para cada assinatura do Azure a partir da qual os usuários criarão sistemas Cloud Volumes ONTAP.

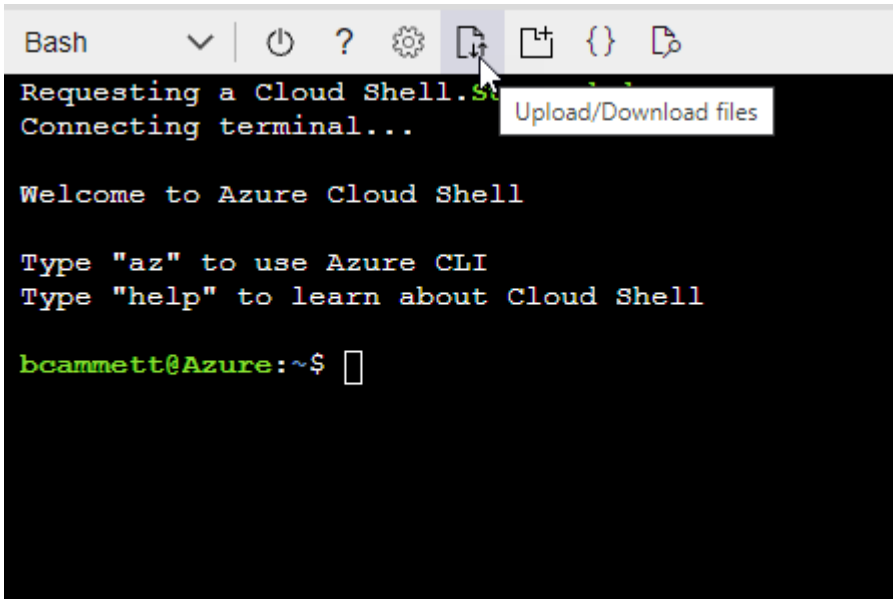
      **Exemplo**

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ```

   c. Use o arquivo JSON para criar uma função personalizada no Azure.

      As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

- Comece "Azure Cloud Shell" e escolha o ambiente Bash.
- Carregue o arquivo JSON.




- Use a CLI do Azure para criar a função personalizada:

```
az role definition create --role-definition
Connector_Policy.json
```

Agora você deve ter uma função personalizada chamada Operador BlueXP  que você pode atribuir à máquina virtual do conetor.

2. Atribua o aplicativo à função:

   a. No portal do Azure, abra o serviço **Subscrições**.

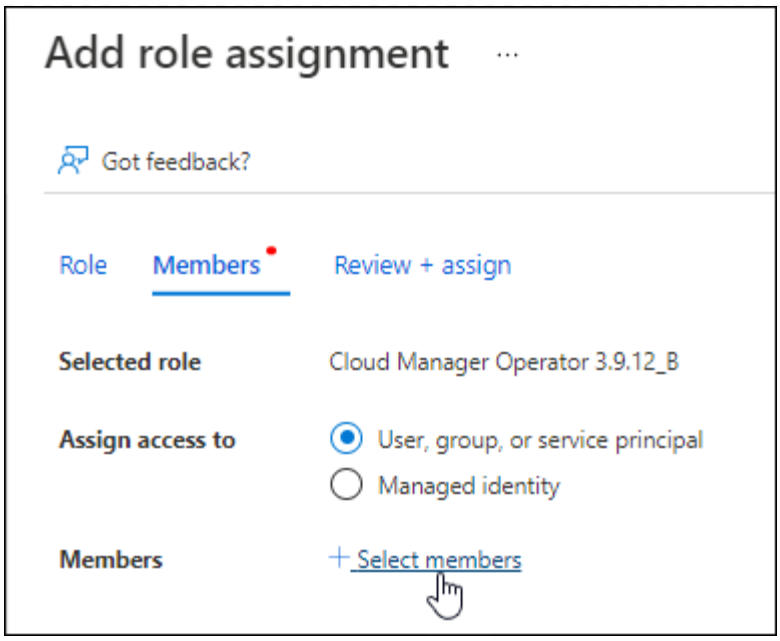
   b. Selecione a subscrição.

   c. Selecione **Access Control (IAM) > Add > Add > Add Role assignment** (Adicionar controlo de acesso).

   d. Na guia **função**, selecione a função **Operador BlueXP**  e selecione **seguinte**.

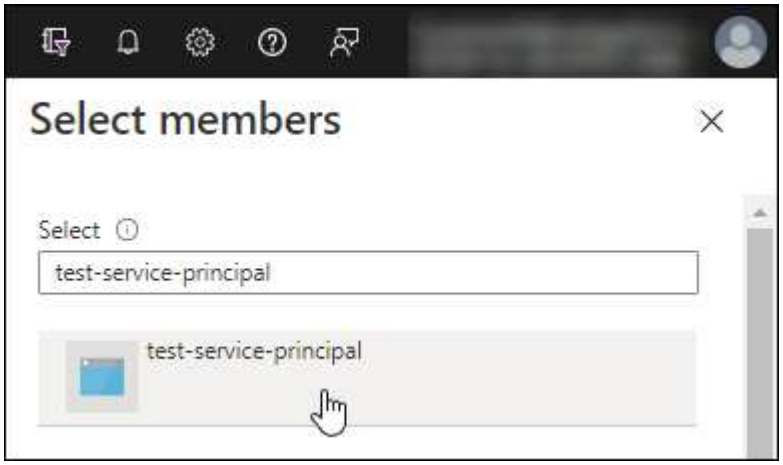
   e. Na guia **Membros**, execute as seguintes etapas:

      - Mantenha **Usuário, grupo ou responsável do serviço** selecionado.
      - Selecione **Selecionar membros**.




- Procure o nome da aplicação.

  Aqui está um exemplo:




- Selecione a aplicação e selecione **Select**.
- Selecione **seguinte**.

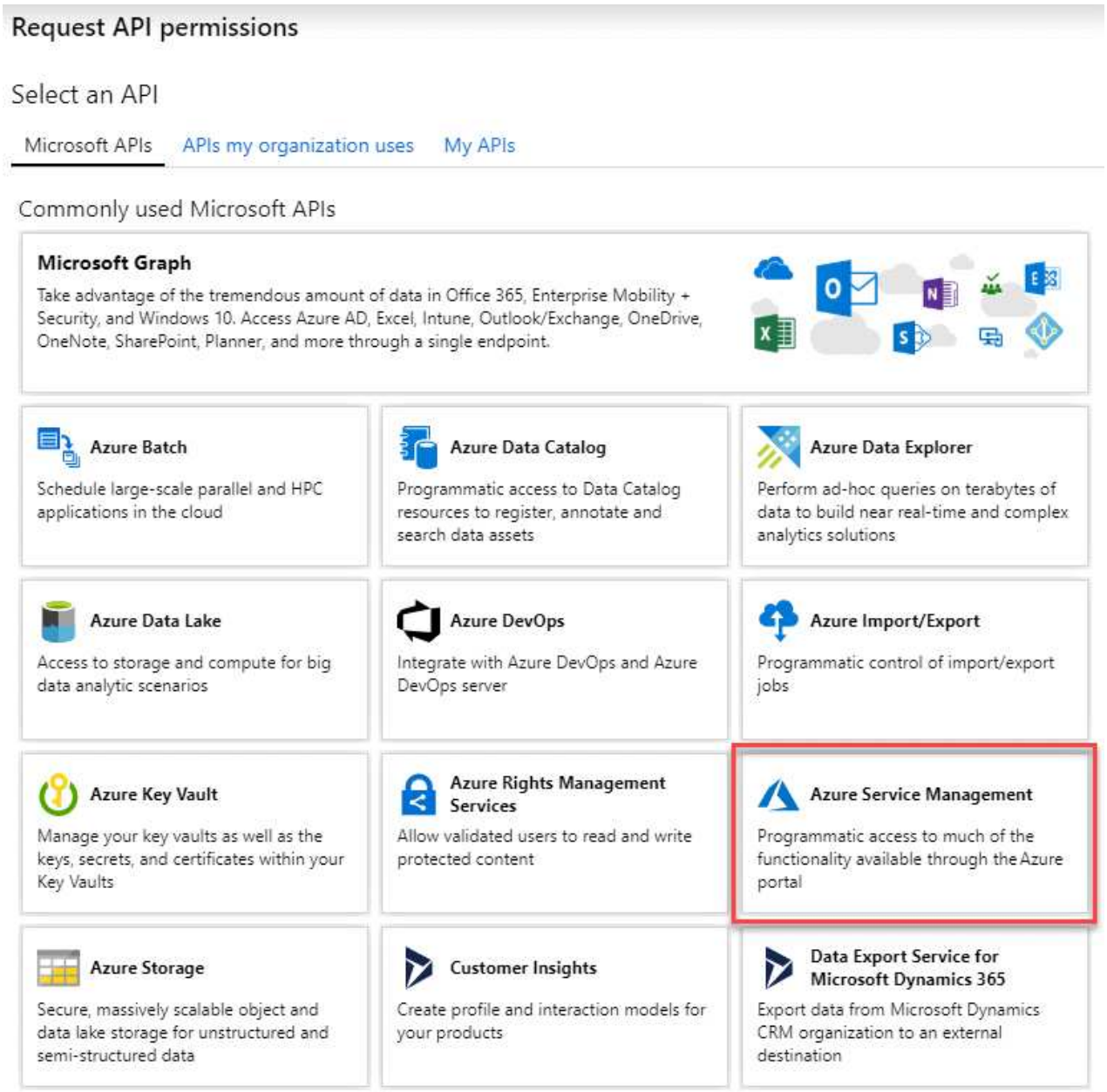
f. Selecione **Rever e atribuir**.

O principal de serviço agora tem as permissões necessárias do Azure para implantar o conetor.

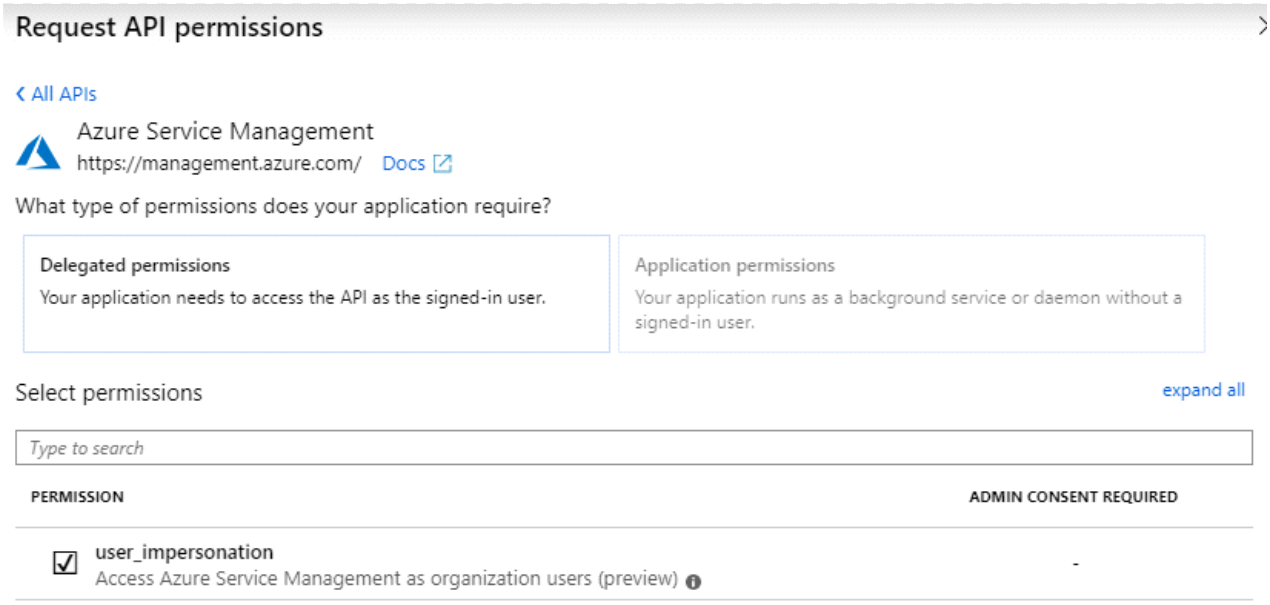
Se você quiser implantar o Cloud Volumes ONTAP a partir de várias assinaturas do Azure, então você deve vincular o principal de serviço a cada uma dessas assinaturas. O BlueXP  permite que você selecione a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

**Adicione permissões da API de Gerenciamento de Serviços do Windows Azure**

1. No serviço **Microsoft Entra ID**, selecione **inscrições de aplicativos** e selecione o aplicativo.
2. Selecione **permissões de API > Adicionar uma permissão**.
3. Em **Microsoft APIs**, selecione **Azure Service Management**.

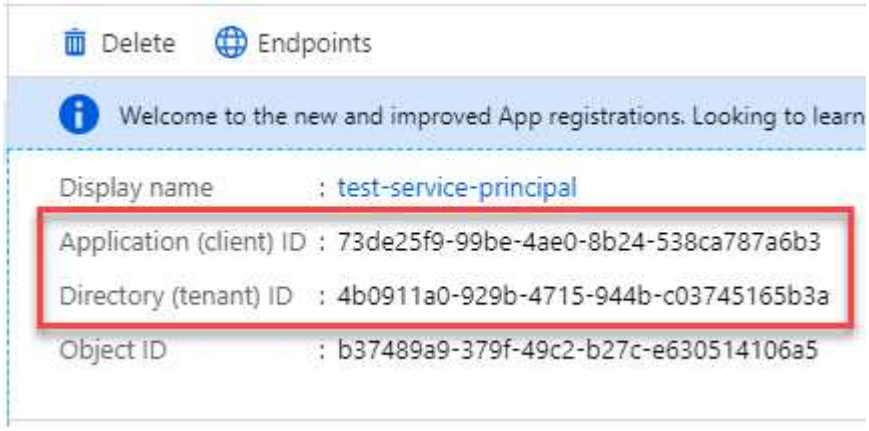



4. Selecione **Acesse o Gerenciamento de Serviços do Azure como usuários da organização** e selecione **Adicionar permissões**.




**Obtenha o ID do aplicativo e o ID do diretório para o aplicativo**

1. No serviço **Microsoft Entra ID**, selecione **inscrições de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.




Quando você adiciona a conta do Azure ao BlueXP , você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O BlueXP  usa os IDs para fazer login programaticamente.

**Crie um segredo de cliente**

1. Abra o serviço **Microsoft Entra ID**.
2. Selecione **inscrições de aplicativos** e selecione sua inscrição.
3. Selecione **certificados e segredos > segredo de novo cliente**.
4. Forneça uma descrição do segredo e uma duração.
5. Selecione **Adicionar**.
6. Copie o valor do segredo do cliente.


Agora você tem um segredo de cliente que o BlueXP pode usá-lo para autenticar com o Microsoft Entra ID.

**Resultado**

Seu responsável de serviço está configurado e você deve ter copiado o ID do aplicativo (cliente), o ID do diretório (locatário) e o valor do segredo do cliente. Depois de instalar o conetor, você precisará associar essas credenciais ao conetor do BlueXP .

#### Passo 5: Instale o conetor

Baixe e instale o software Connector em um host Linux existente no local.

**Antes de começar**

Você deve ter o seguinte:

- Root Privileges para instalar o conetor.
- Detalhes sobre um servidor proxy, se for necessário um proxy para acesso à Internet a partir do conetor.

  Você tem a opção de configurar um servidor proxy após a instalação, mas isso requer a reinicialização do conetor.

  Observe que o BlueXP não oferece suporte a servidores proxy transparentes.

- Um certificado assinado pela CA, se o servidor proxy usar HTTPS ou se o proxy for um proxy intercetor.

**Sobre esta tarefa**

O instalador disponível no site de suporte da NetApp pode ser uma versão anterior. Após a instalação, o conetor se atualiza automaticamente se uma nova versão estiver disponível.

**Passos**

1. Se as variáveis de sistema *http_proxy* ou *https_proxy* estiverem definidas no host, remova-as:

   ```
   unset http_proxy
   unset https_proxy
   ```

   Se você não remover essas variáveis do sistema, a instalação falhará.

2. Faça o download do software Connector do "Site de suporte da NetApp"e copie-o para o host Linux.

   Você deve baixar o instalador do conetor "online" destinado a ser usado em sua rede ou na nuvem. Um instalador "offline" separado está disponível para o conetor, mas só é suportado com implantações de

modo privado.

3. Atribua permissões para executar o script.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

Onde <version> é a versão do conetor que você baixou.

4. Execute o script de instalação.

```
 ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
--cacert <path and file name of a CA-signed certificate>
```

Os parâmetros --proxy e --cacert são opcionais. Se você tiver um servidor proxy, será necessário inserir os parâmetros como mostrado. O instalador não solicita que você forneça informações sobre um proxy.

Aqui está um exemplo do comando usando ambos os parâmetros opcionais:

```
 ./BlueXP-Connector-Cloud-v3.9.40--proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

--proxy configura o conetor para usar um servidor proxy HTTP ou HTTPS usando um dos seguintes formatos:

- http://address:port
- http://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Observe o seguinte:

  - O usuário pode ser um usuário local ou usuário de domínio.
  - Para um usuário de domínio, você deve usar o código ASCII para a como mostrado acima.
  - O BlueXP  não suporta nomes de usuário ou senhas que incluem o caractere A.
  - Se a senha incluir qualquer um dos seguintes carateres especiais, você deve escapar desse caractere especial, prependendo-o com uma barra invertida: & Ou !

    Por exemplo:

  http://bxpproxyuser:netapp1\!@address:3128

--cacert especifica um certificado assinado pela CA a ser usado para acesso HTTPS entre o conetor e o servidor proxy. Este parâmetro só é necessário se especificar um servidor proxy HTTPS ou se o proxy for

um proxy intercetor.

**Resultado**

O conetor está agora instalado. No final da instalação, o serviço de conetor (occm) será reiniciado duas vezes se você tiver especificado um servidor proxy.

#### Passo 6: Configure o conetor

Inscreva-se ou inicie sessão e, em seguida, configure o conetor para trabalhar com a sua organização BlueXP .

**Passos**

1. Abra um navegador da Web e insira o seguinte URL:

   <a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

   *Ipaddress* pode ser localhost, um endereço IP privado ou um endereço IP público, dependendo da configuração do host. Por exemplo, se o conetor estiver na nuvem pública sem um endereço IP público, você deverá inserir um endereço IP privado de um host que tenha uma conexão com o host do conetor.

2. Inscreva-se ou faça login.
3. Depois de iniciar sessão, configure o BlueXP :
   a. Especifique a organização BlueXP  a associar ao conetor.
   b. Introduza um nome para o sistema.
   c. Em **você está executando em um ambiente seguro?** mantenha o modo restrito desativado.

      Você deve manter o modo restrito desativado porque estas etapas descrevem como usar o BlueXP  no modo padrão. (Além disso, o modo restrito não é suportado quando o conetor é instalado no local.)

   d. Selecione **vamos começar**.

**Resultado**

O BlueXP  está agora configurado com o conetor que acabou de instalar.

#### Passo 7: Forneça permissões para o BlueXP

Depois de instalar e configurar o conetor, adicione suas credenciais de nuvem para que o BlueXP  tenha as permissões necessárias para executar ações na AWS ou no Azure.

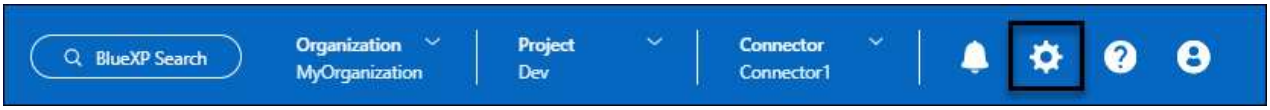
### AWS

#### Antes de começar

Se você acabou de criar essas credenciais na AWS, pode levar alguns minutos até que elas estejam disponíveis para uso. Aguarde alguns minutos antes de adicionar as credenciais ao BlueXP .

#### Passos

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.




2. Selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Localização das credenciais**: Selecione **Amazon Web Services > Connector**.
   b. **Definir credenciais**: Insira uma chave de acesso da AWS e uma chave secreta.
   c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.
   d. **Revisão**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

#### Resultado

O BlueXP  agora tem as permissões necessárias para executar ações na AWS em seu nome.

Agora você pode ir para o "Consola BlueXP" para começar a usar o conetor com BlueXP .

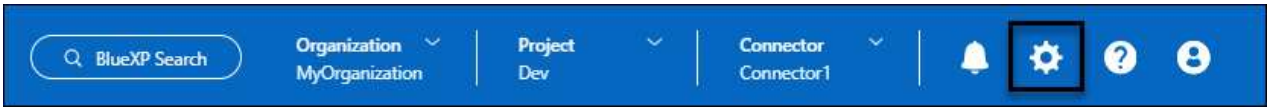
### Azure

#### Antes de começar

Se você acabou de criar essas credenciais no Azure, pode levar alguns minutos até que elas estejam disponíveis para uso. Aguarde alguns minutos antes de adicionar as credenciais ao BlueXP .

#### Passos

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.




2. Selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Credentials Location**: Selecione **Microsoft Azure > Connector**.
   b. **Definir credenciais**: Insira informações sobre o responsável do serviço Microsoft Entra que concede as permissões necessárias:
      - ID da aplicação (cliente)
      - ID do diretório (locatário)
      - Segredo Cliente
   c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.

d. **Revisão**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

**Resultado**

O BlueXP agora tem as permissões necessárias para executar ações no Azure em seu nome. Agora você pode ir para o "Consola BlueXP" para começar a usar o conetor com BlueXP .

## Assinar BlueXP (modo padrão)

Inscreva-se no BlueXP no mercado do seu fornecedor de nuvem para pagar os serviços da BlueXP a uma taxa por hora (PAYGO) ou por meio de um contrato anual. Se você comprou uma licença da NetApp (BYOL), também precisará se inscrever na oferta de mercado. A sua licença é sempre cobrada primeiro, mas você será cobrado à taxa por hora se exceder a sua capacidade licenciada ou se o prazo da licença expirar.

Uma assinatura do mercado permite o carregamento dos seguintes serviços BlueXP :

- Backup e recuperação
- Classificação
- Cloud Volumes ONTAP
- Disposição em camadas

**Antes de começar**

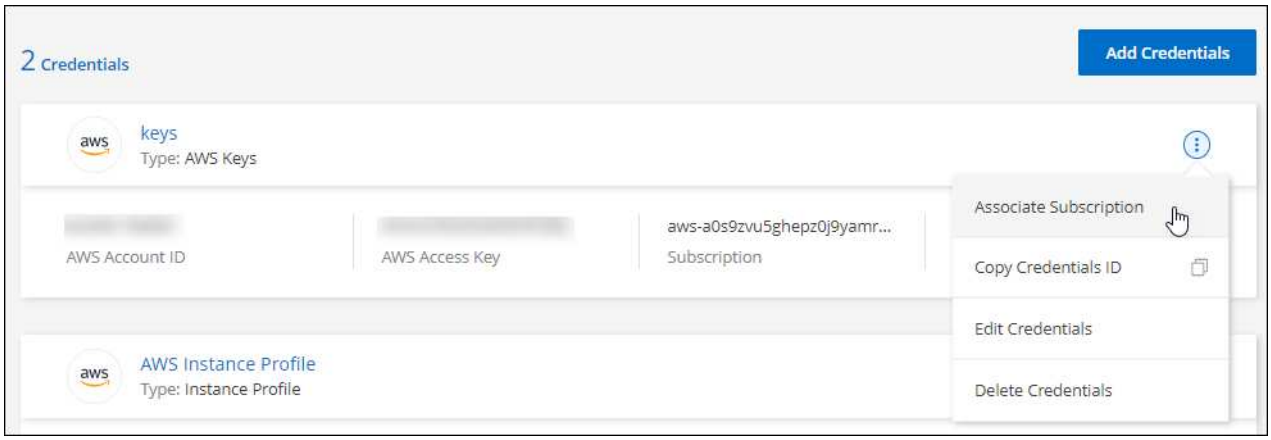
A assinatura do BlueXP envolve a associação de mercado às credenciais de nuvem associadas a um conector. Se você seguiu o fluxo de trabalho "começar com o modo padrão", então você já deve ter um conetor. Para saber mais, consulte o "Início rápido para BlueXP no modo padrão".

**AWS**

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Selecione o menu de ação para um conjunto de credenciais e, em seguida, selecione **assinatura associada**.

   Você deve selecionar credenciais associadas a um conetor. Não é possível associar uma assinatura do marketplace a credenciais associadas ao BlueXP .




3. Para associar as credenciais a uma assinatura existente, selecione a assinatura na lista suspensa e selecione **Associate**.
4. Para associar as credenciais a uma nova assinatura, selecione **Adicionar assinatura > continuar** e siga as etapas no AWS Marketplace:

   a. Selecione **Ver opções de compra**.

   b. Selecione **Subscribe**.

   c. Selecione **Configurar a sua conta**.

      Você será redirecionado para o site da BlueXP .

   d. Na página **atribuição de assinatura**:

      - Selecione as organizações ou contas do BlueXP às quais você deseja associar essa assinatura.
      - No campo **Substituir subscrição existente**, escolha se pretende substituir automaticamente a subscrição existente de uma organização ou conta por esta nova subscrição.

        O BlueXP substitui a assinatura existente para todas as credenciais na organização ou conta por essa nova assinatura. Se um conjunto de credenciais nunca foi associado a uma assinatura, essa nova assinatura não será associada a essas credenciais.

   Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo estas etapas.

      - Selecione **Guardar**.

        O vídeo a seguir mostra as etapas para se inscrever no AWS Marketplace:

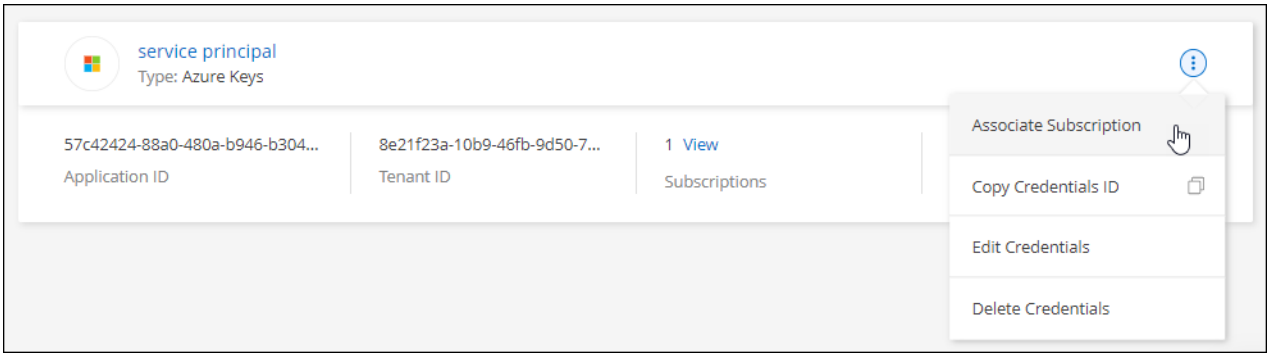
Inscreva-se no BlueXP  no AWS Marketplace

**Azure**

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Selecione o menu de ação para um conjunto de credenciais e, em seguida, selecione **assinatura associada**.

   Você deve selecionar credenciais associadas a um conetor. Não é possível associar uma assinatura do marketplace a credenciais associadas ao BlueXP .




3. Para associar as credenciais a uma assinatura existente, selecione a assinatura na lista suspensa e selecione **Associate**.
4. Para associar as credenciais a uma nova assinatura, selecione **Adicionar assinatura > continuar** e siga as etapas no Azure Marketplace:

   a. Se solicitado, faça login na sua conta do Azure.

   b. Selecione **Subscribe**.

   c. Preencha o formulário e selecione **Subscribe**.

   d. Depois que o processo de assinatura estiver concluído, selecione **Configurar conta agora**.

      Você será redirecionado para o site da BlueXP .

   e. Na página **atribuição de assinatura**:

      - Selecione as organizações ou contas do BlueXP  às quais você deseja associar essa assinatura.
      - No campo **Substituir subscrição existente**, escolha se pretende substituir automaticamente a subscrição existente de uma organização ou conta por esta nova subscrição.

        O BlueXP  substitui a assinatura existente para todas as credenciais na organização ou conta por essa nova assinatura. Se um conjunto de credenciais nunca foi associado a uma assinatura, essa nova assinatura não será associada a essas credenciais.

   Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo estas etapas.

      - Selecione **Guardar**.

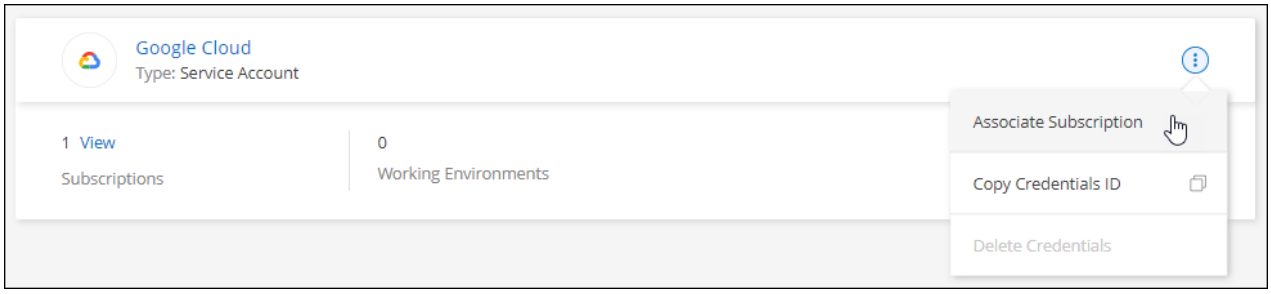
O vídeo a seguir mostra as etapas para se inscrever no Azure Marketplace:

Inscreva-se no BlueXP  a partir do Azure Marketplace

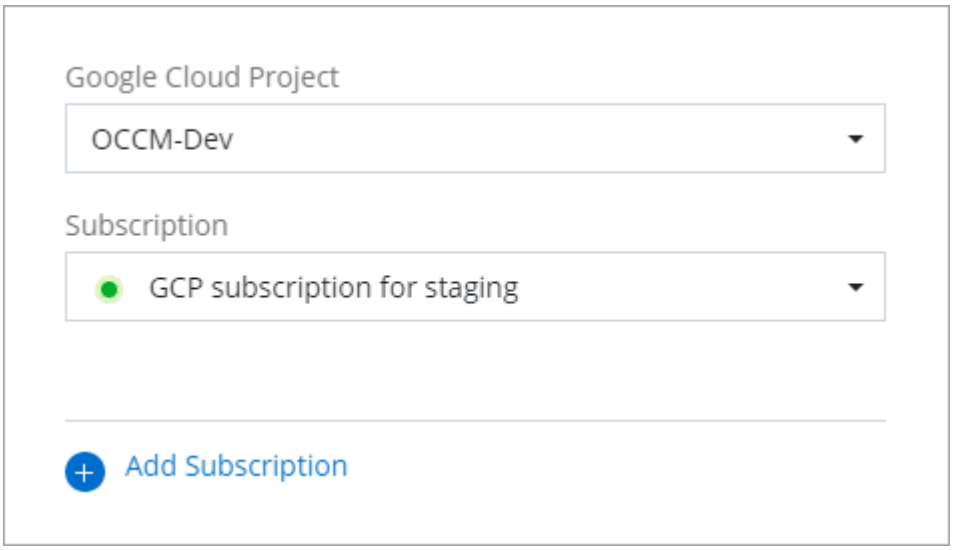
**Google Cloud**

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Selecione o menu de ação para um conjunto de credenciais e, em seguida, selecione **assinatura associada**.



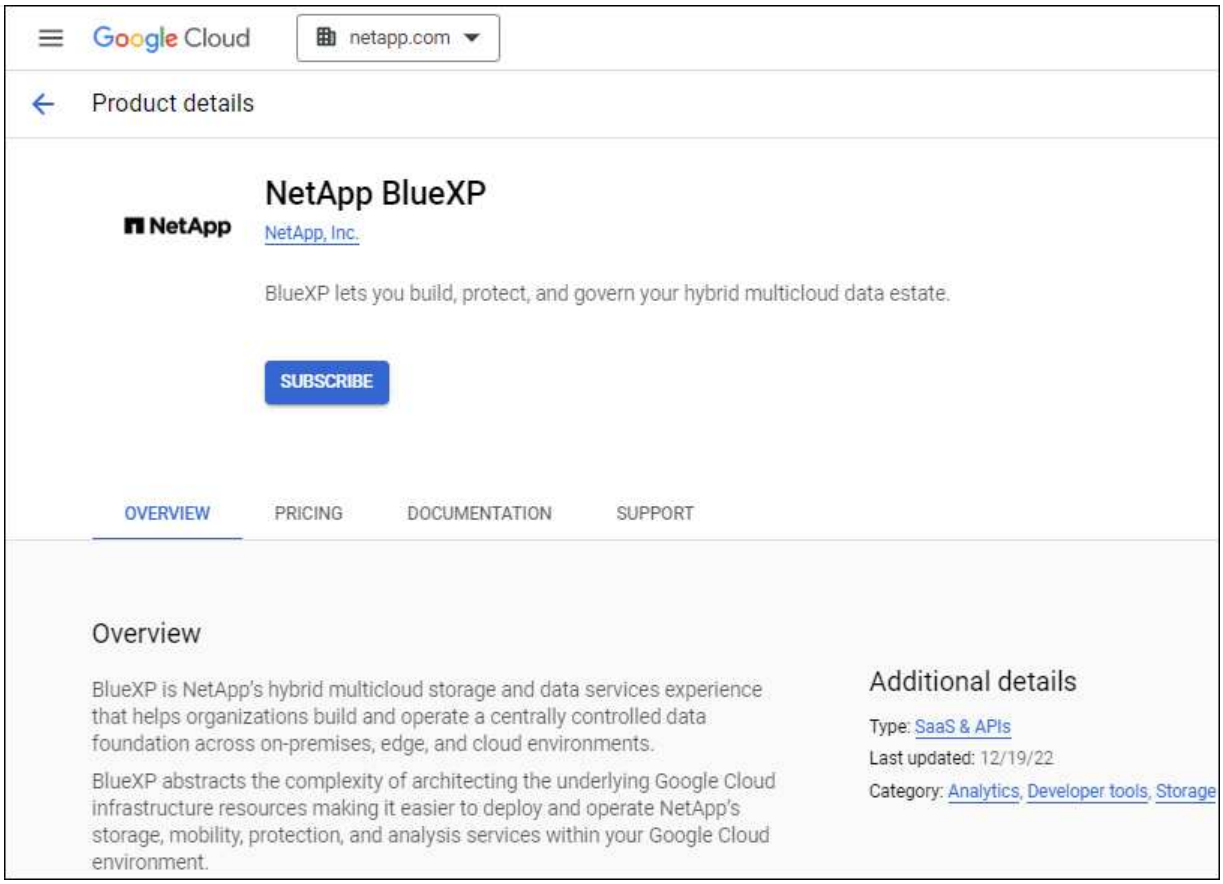

3. Para associar as credenciais a uma assinatura existente, selecione um projeto e assinatura do Google Cloud na lista suspensa e, em seguida, selecione **Associate**.




4. Se você ainda não tiver uma assinatura, selecione **Adicionar assinatura > continuar** e siga as etapas no Google Cloud Marketplace.

Antes de concluir as etapas a seguir, certifique-se de que você tenha o Privileges de Administração de faturamento na sua conta do Google Cloud, bem como um login no BlueXP .

a. Depois de ser redirecionado para o "Página do NetApp BlueXP  no Google Cloud Marketplace", certifique-se de que o projeto correto está selecionado no menu de navegação superior.

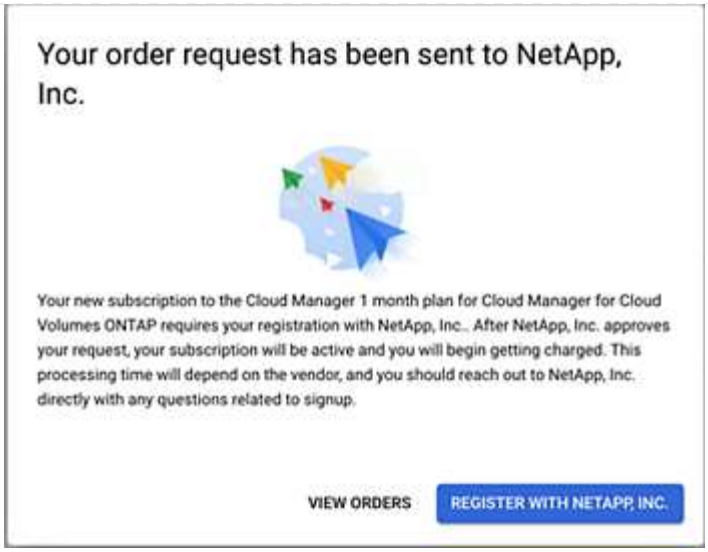



b. Selecione **Subscribe**.
c. Selecione a conta de faturamento apropriada e concorde com os termos e condições.
d. Selecione **Subscribe**.

   Esta etapa envia sua solicitação de transferência para o NetApp.

e. Na caixa de diálogo pop-up, selecione **Register with NetApp, Inc.**

   Essa etapa deve ser concluída para vincular a assinatura do Google Cloud à sua organização ou conta do BlueXP . O processo de vinculação de uma assinatura não está concluído até que você seja redirecionado desta página e, em seguida, entre no BlueXP .




f. Conclua as etapas na página **atribuição de assinatura**:

> Se alguém da sua organização já se inscreveu na assinatura do NetApp BlueXP da sua conta de faturamento, então você será redirecionado para "A página Cloud Volumes ONTAP no site da BlueXP ". Se isso for inesperado, entre em Contato com sua equipe de vendas da NetApp. O Google ativa apenas uma assinatura por conta de faturamento do Google.

- Selecione as organizações ou contas do BlueXP  às quais você deseja associar essa assinatura.
- No campo **Substituir subscrição existente**, escolha se pretende substituir automaticamente a subscrição existente de uma organização ou conta por esta nova subscrição.

  O BlueXP  substitui a assinatura existente para todas as credenciais na organização ou conta por essa nova assinatura. Se um conjunto de credenciais nunca foi associado a uma assinatura, essa nova assinatura não será associada a essas credenciais.

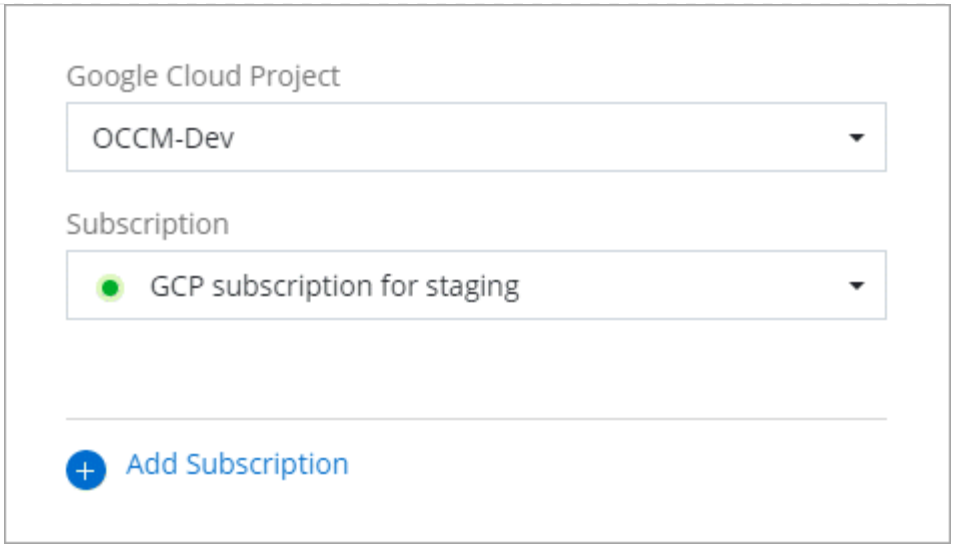
Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo estas etapas.

- Selecione **Guardar**.

  O vídeo a seguir mostra as etapas para se inscrever no Google Cloud Marketplace:

Inscreva-se no BlueXP  no Google Cloud Marketplace

a. Quando esse processo estiver concluído, navegue de volta para a página credenciais no BlueXP e selecione essa nova assinatura.




**Informações relacionadas**

- "Gerenciar licenças baseadas em capacidade BYOL para Cloud Volumes ONTAP"
- "Gerenciar licenças BYOL para serviços de dados BlueXP "
- "Gerenciar credenciais e assinaturas da AWS para o BlueXP "
- "Gerencie credenciais e assinaturas do Azure para o BlueXP "
- "Gerenciar credenciais e assinaturas do Google Cloud para o BlueXP "

### O que você pode fazer a seguir (modo padrão)

Agora que você fez login e configurou o BlueXP  no modo padrão, os usuários podem criar e descobrir ambientes de trabalho e usar os serviços de dados do BlueXP .

Se você instalou um conector na AWS, no Microsoft Azure ou no Google Cloud, o BlueXP detetará automaticamente informações sobre os buckets do Amazon S3, o storage Blob do Azure ou os buckets do Google Cloud Storage no local onde o conector é instalado. Um ambiente de trabalho é adicionado automaticamente à tela BlueXP .

Para obter ajuda, vá para a "Página inicial para a documentação do BlueXP " para visualizar os documentos de todos os serviços do BlueXP .

**Link relacionado**

"Modos de implantação do BlueXP"

# Comece com o modo restrito

### Fluxo de trabalho de introdução (modo restrito)

Comece a usar o BlueXP  no modo restrito, preparando seu ambiente, implantando o conetor e assinando o BlueXP .

O modo restrito geralmente é usado por governos estaduais e locais e empresas regulamentadas, incluindo

implantações nas regiões do governo do AWS GovCloud e do Azure. Antes de começar, você deve ter uma compreensão de "Contas BlueXP ", "Conetores"e "modos de implantação".

### 1 "Prepare-se para a implantação"

1. Prepare um host Linux dedicado que atenda aos requisitos de CPU, RAM, espaço em disco, ferramenta de orquestração de contentores e muito mais.
2. Configure a rede que fornece acesso às redes de destino, acesso à Internet de saída para instalações manuais e Internet de saída para acesso diário.
3. Configure permissões no seu provedor de nuvem para que você possa associar essas permissões à instância do Connector depois de implantá-la.

### 2 "Implante o conetor"

1. Instale o conetor do mercado do seu provedor de nuvem ou instalando manualmente o software em seu próprio host Linux.
2. Configure o BlueXP  abrindo um navegador da Web e inserindo o endereço IP do host Linux.
3. Forneça ao BlueXP  as permissões que você configurou anteriormente.

### 3 "Inscreva-se no BlueXP "

Inscreva-se no BlueXP  no mercado do seu fornecedor de nuvem para pagar os serviços da BlueXP  a uma taxa por hora (PAYGO) ou por meio de um contrato anual.

## Prepare-se para a implantação no modo restrito

Prepare seu ambiente antes de implantar o BlueXP  no modo restrito. Por exemplo, você precisa analisar os requisitos do host, preparar a rede, configurar permissões e muito mais.

#### Passo 1: Entenda como o modo restrito funciona

Antes de começar, você deve ter uma compreensão de como o BlueXP  funciona no modo restrito.

Por exemplo, você deve entender que precisa usar a interface baseada em navegador que está disponível localmente a partir do conetor BlueXP  que você precisa instalar. Não é possível acessar o BlueXP  a partir do console baseado na Web fornecido pela camada SaaS.

Além disso, nem todos os serviços BlueXP  estão disponíveis.

"Saiba como o modo restrito funciona".

#### Passo 2: Reveja as opções de instalação

No modo restrito, você só pode instalar o conetor na nuvem. Estão disponíveis as seguintes opções de instalação:

- No AWS Marketplace
- A partir do Azure Marketplace

- Instalar manualmente o conetor no seu próprio host Linux em execução na AWS, Azure ou Google Cloud

### Etapa 3: Revise os requisitos do host

O software do conetor deve ser executado em um host que atenda a requisitos específicos do sistema operacional, requisitos de RAM, requisitos de porta, etc.

Ao implantar o conetor do AWS ou do Azure Marketplace, a imagem inclui os componentes de software e sistema operacional necessários. Você simplesmente precisa escolher um tipo de instância que atenda aos requisitos de CPU e RAM.

**Host dedicado**

O conetor não é suportado em um host que é compartilhado com outros aplicativos. O host deve ser um host dedicado.

**Hipervisor**

É necessário um hypervisor bare metal ou hospedado certificado para executar um sistema operacional suportado.

**requisitos de sistema operacional e contentor**

O BlueXP  suporta o conetor com os seguintes sistemas operacionais ao usar o BlueXP  no modo padrão ou no modo restrito. Uma ferramenta de orquestração de contêineres é necessária antes de instalar o conetor.

| Sistema operacional | Versões de OS compatíveis | Versões de conetor suportadas | Ferramenta de recipiente necessária | SELinux |
|---|---|---|---|---|
| Red Hat Enterprise Linux | 9,1 a 9,4<br><br>8,6 a 8,10 | 3.9.40 ou posterior com BlueXP  no modo padrão ou modo restrito | Podman versão 4.6.1 ou 4.9.4<br><br>Veja os requisitos de configuração do Podman. | Suporte no modo de execução ou modo permissivo 1 |
| Ubuntu | 24,04 LTS | 3.9.45 ou posterior com BlueXP  no modo padrão ou modo restrito | Docker Engine 26.0.0 | Não suportado |

Notas:

1. O gerenciamento de sistemas Cloud Volumes ONTAP não é suportado por conetores que tenham o SELinux habilitado no sistema operacional.
2. O conetor é suportado em versões em inglês destes sistemas operativos.
3. Para o RHEL, o host deve estar registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar repositórios para atualizar o software necessário de 3rd partes durante a instalação do conetor.

**CPU**

8 núcleos ou 8 vCPUs

**RAM**

32 GB

**Tipo de instância do AWS EC2**

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos t3,2xlarge.

**Tamanho da VM do Azure**

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos Standard_D8s_v3.

**Tipo de máquina Google Cloud**

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos n2-standard-8.

O conetor é compatível com o Google Cloud em uma instância de VM com um sistema operacional compatível "Recursos de VM blindados"

**Espaço em disco em /opt**

100 GiB de espaço deve estar disponível

O BlueXP usa `/opt` para instalar o `/opt/application/netapp` diretório e seu conteúdo.

**Espaço em disco em /var**

20 GiB de espaço deve estar disponível

O BlueXP requer esse espaço `/var` porque o Docker ou o Podman são arquitetados para criar os contentores dentro desse diretório. Especificamente, eles irão criar contentores no `/var/lib/containers/storage` diretório. Montagens externas ou links simbólicos não funcionam para este espaço.

### Passo 4: Instale o Podman ou Docker Engine

Se você está planejando instalar manualmente o software Connector, você precisa preparar o host instalando Podman ou Docker Engine.

Dependendo do seu sistema operacional, o Podman ou o Docker Engine são necessários antes de instalar o conetor.

- O Podman é necessário para o Red Hat Enterprise Linux 8 e 9.

  Veja as versões do Podman suportadas pelo BlueXP .

- Docker Engine é necessário para o Ubuntu.

  Veja as versões do Docker Engine que o BlueXP suporta.

**Exemplo 5. Passos**

**Podman**

Siga estas etapas para instalar o Podman e configurá-lo para atender aos seguintes requisitos:

- O serviço podman.socket deve ser ativado e iniciado
- python3 deve ser instalado
- O pacote podman-compose versão 1.0.6 deve ser instalado
- Podman-compose deve ser adicionado à variável de ambiente PATH

**Passos**

1. Remova o pacote podman-docker se ele estiver instalado no host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Instale o Podman.

   O Podman está disponível nos repositórios oficiais do Red Hat Enterprise Linux.

   Para Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

   Onde o <version> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas pelo BlueXP .

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

   Onde o <version> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas pelo BlueXP .

3. Ative e inicie o serviço podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Instale o python3.

```
sudo dnf install python3
```

5. Instale o pacote do repositório EPEL se ainda não estiver disponível no seu sistema.

Esta etapa é necessária porque o podman-compose está disponível no repositório extra Packages for Enterprise Linux (EPEL).

Para Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

Para Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Instale o pacote podman-compose 1,0.6.

```
sudo dnf install podman-compose-1.0.6
```

Usar o `dnf install` comando atende ao requisito para adicionar podman-compose à variável de ambiente PATH. O comando installation adiciona podman-compose ao /usr/bin, que já está incluído na `secure_path` opção no host.

**Docker Engine**

Siga a documentação do Docker para instalar o Docker Engine.

**Passos**

1. "Veja as instruções de instalação do Docker"

   Certifique-se de seguir as etapas para instalar uma versão específica do Docker Engine. Instalar a versão mais recente irá instalar uma versão do Docker que o BlueXP  não suporta.

2. Verifique se o Docker está ativado e em execução.

```
sudo systemctl enable docker && sudo systemctl start docker
```

### Passo 5: Prepare a rede

Configure sua rede para que o conetor possa gerenciar recursos e processos em seu ambiente de nuvem pública. Além de ter uma rede virtual e uma sub-rede para o conetor, você precisará garantir que os seguintes requisitos sejam atendidos.

**Conexões com redes de destino**

O conetor deve ter uma conexão de rede com o local onde você planeja gerenciar o armazenamento. Por exemplo, a VPC ou o VNet onde você pretende implantar o Cloud Volumes ONTAP ou o data center onde residem seus clusters ONTAP no local.

### Prepare a rede para o acesso do usuário ao console BlueXP

No modo restrito, a interface do utilizador do BlueXP  é acessível a partir do conetor. À medida que você usa a interface de usuário do BlueXP , ele entra em Contato com alguns endpoints para concluir as tarefas de gerenciamento de dados. Esses endpoints são contatados do computador de um usuário ao concluir ações específicas do console BlueXP .

| Endpoints | Finalidade |
|---|---|
| https://api.BlueXP .NetApp.com | O console baseado na Web do BlueXP  entra em Contato com esse endpoint para interagir com a API do BlueXP  para ações relacionadas a autorização, licenciamento, assinaturas, credenciais, notificações e muito mais. |
| https://signin.b2c.NetApp.com | Necessário para atualizar as credenciais do site de suporte da NetApp (NSS) ou para adicionar novas credenciais NSS ao BlueXP . |
| https://NetApp-cloud-account.auth0.com<br>https://cdn.auth0.com<br>https://services.cloud.NetApp.com | Seu navegador da Web se coneta a esses endpoints para autenticação de usuário centralizada por meio do BlueXP . |
| https://widget.intercom.io | Para um bate-papo no produto que permite conversar com especialistas em nuvem da NetApp. |

### Terminais contactados durante a instalação manual

Quando você instala manualmente o conetor em seu próprio host Linux, o instalador do conetor requer acesso aos seguintes URLs durante o processo de instalação:

- https://mysupport.NetApp.com
- https://signin.b2c.NetApp.com (este endpoint é o URL CNAME para https://mysupport.NetApp.com)
- https://cloudmanager.cloud.NetApp.com/locação
- https://stream.cloudmanager.cloud.NetApp.com
- https://production-artifacts.cloudmanager.cloud.NetApp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  Este endpoint não é necessário nas regiões do Azure Government.

- https://occmclientinfragov.azurecr.us

  Esse endpoint só é necessário nas regiões do Azure Government.

O host pode tentar atualizar os pacotes do sistema operacional durante a instalação. O host pode entrar em Contato com diferentes sites de espelhamento para esses pacotes do sistema operacional.

### Acesso de saída à Internet para operações diárias

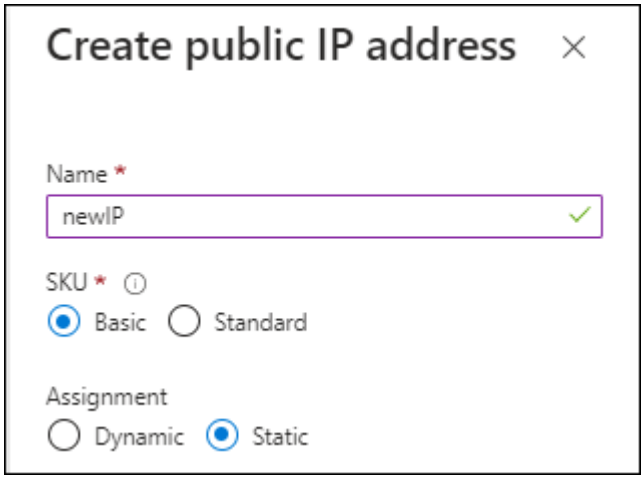
O local de rede onde você implantar o conetor deve ter uma conexão de saída de Internet. O conetor requer acesso de saída à Internet para contactar os seguintes endpoints, a fim de gerir recursos e processos no seu ambiente de nuvem pública.

| Endpoints | Finalidade |
| --- | --- |
| Serviços da AWS (amazonaws.com):<br>• CloudFormation<br>• Nuvem de computação elástica (EC2)<br>• Gerenciamento de identidade e acesso (IAM)<br>• Key Management Service (KMS)<br>• Serviço de token de segurança (STS)<br>• Serviço de armazenamento simples (S3) | Para gerenciar recursos na AWS. O endpoint exato depende da região da AWS que você está usando. "Consulte a documentação da AWS para obter detalhes" |
| https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net | Para gerenciar recursos em regiões públicas do Azure. |
| https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net | Para gerenciar recursos nas regiões do Azure Government. |
| https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn | Para gerenciar recursos nas regiões do Azure China. |
| https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects | Para gerenciar recursos no Google Cloud. |
| https://support.NetApp.com https://mysupport.NetApp.com | Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte do NetApp. |
| https://*.api.BlueXP .NetApp.com<br><br>https://api.BlueXP .NetApp.com<br><br>https://*.cloudmanager.cloud.NetApp.com<br><br>https://cloudmanager.cloud.NetApp.com<br><br>https://NetApp-cloud-account.auth0.com | Para fornecer recursos e serviços SaaS no BlueXP .<br><br>Observe que o conetor está entrando em Contato atualmente com "cloudmanager.cloud.NetApp.com", mas começará a entrar em Contato com "API.BlueXP .NetApp.com" em uma próxima versão. |

| Endpoints | Finalidade |
| --- | --- |
| https://*.blob.core.windows.net<br><br>https://cloudmanagerinfraprod.azurecr.io este endpoint não é necessário nas regiões do Azure Government.<br><br>https://occmclientinfragov.azurecr.us este endpoint só é necessário nas regiões do governo do Azure. | Para atualizar o conetor e seus componentes do Docker. |

**Endereço IP público no Azure**

Se você quiser usar um endereço IP público com a VM do conetor no Azure, o endereço IP deve usar uma SKU básica para garantir que o BlueXP  use esse endereço IP público.




Se você usar um endereço IP SKU padrão, o BlueXP  usará o endereço IP *private* do conetor, em vez do IP público. Se a máquina que você está usando para acessar o Console do BlueXP  não tiver acesso a esse endereço IP privado, as ações do Console do BlueXP  falharão.

"Documentação do Azure: SKU IP público"

**Servidor proxy**

Se a sua empresa exigir a implantação de um servidor proxy para todo o tráfego de saída da Internet, obtenha as seguintes informações sobre o proxy HTTP ou HTTPS. Você precisará fornecer essas informações durante a instalação. Observe que o BlueXP  não oferece suporte a servidores proxy transparentes.

- Endereço IP
- Credenciais
- Certificado HTTPS

**Portas**

Não há tráfego de entrada para o conetor, a menos que você o inicie ou se o conetor for usado como um proxy para enviar mensagens AutoSupport do Cloud Volumes ONTAP para o suporte da NetApp.

- HTTP (80) e HTTPS (443) fornecem acesso à IU local, que você usará em circunstâncias raras.
- SSH (22) só é necessário se você precisar se conetar ao host para solução de problemas.

- Conexões de entrada pela porta 3128 são necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída à Internet não está disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída à Internet para enviar mensagens AutoSupport, o BlueXP  configura automaticamente esses sistemas para usar um servidor proxy incluído no conetor. O único requisito é garantir que o grupo de segurança do conetor permita conexões de entrada pela porta 3128. Você precisará abrir essa porta depois de implantar o conetor.

**Ativar NTP**

Se estiver a planear utilizar a classificação BlueXP  para analisar as suas fontes de dados empresariais, deve ativar um serviço de Protocolo de tempo de rede (NTP) no sistema de conetores BlueXP  e no sistema de classificação BlueXP  para que o tempo seja sincronizado entre os sistemas. "Saiba mais sobre a classificação BlueXP"

Se você está planejando criar o conetor a partir do mercado do seu provedor de nuvem, então você precisará implementar esse requisito de rede depois de criar o conetor.

### Etapa 6: Preparar permissões na nuvem

O BlueXP  requer permissões do seu provedor de nuvem para implantar o Cloud Volumes ONTAP em uma rede virtual e usar os serviços de dados do BlueXP . Você precisa configurar permissões em seu provedor de nuvem e associá-las ao conetor.

Para exibir as etapas necessárias, selecione a opção de autenticação que deseja usar para o provedor de nuvem.

**Função do AWS IAM**

Use uma função do IAM para fornecer permissões ao conetor.

Se você estiver criando o conetor no AWS Marketplace, será solicitado que você selecione essa função do IAM ao iniciar a instância do EC2.

Se você estiver instalando manualmente o conetor em seu próprio host Linux, será necessário anexar a função à instância EC2.

**Passos**

1. Faça login no console da AWS e navegue até o serviço do IAM.
2. Criar uma política:
   a. Selecione **políticas > criar política**.
   b. Selecione **JSON** e copie e cole o conteúdo do "Política do IAM para o conetor".
   c. Conclua as etapas restantes para criar a política.
3. Crie uma função do IAM:
   a. Selecione **funções > criar função**.
   b. Selecione **AWS Service > EC2**.
   c. Adicione permissões anexando a política que você acabou de criar.
   d. Conclua as etapas restantes para criar a função.

**Resultado**

Agora você tem uma função do IAM para a instância do Connector EC2.

**Chave de acesso da AWS**

Configurar permissões e uma chave de acesso para um usuário do IAM. Você precisará fornecer à BlueXP a chave de acesso da AWS depois de instalar o conetor e configurar o BlueXP .

**Passos**

1. Faça login no console da AWS e navegue até o serviço do IAM.
2. Criar uma política:
   a. Selecione **políticas > criar política**.
   b. Selecione **JSON** e copie e cole o conteúdo do "Política do IAM para o conetor".
   c. Conclua as etapas restantes para criar a política.

      Dependendo dos serviços do BlueXP que você está planejando usar, talvez seja necessário criar uma segunda política.

   Para regiões padrão, as permissões são distribuídas em duas políticas. Duas políticas são necessárias devido a um limite máximo de tamanho de caractere para políticas gerenciadas na AWS. "Saiba mais sobre as políticas do IAM para o conetor".
3. Anexe as políticas a um usuário do IAM.
   - "Documentação da AWS: Criando funções do IAM"
   - "Documentação da AWS: Adicionando e removendo políticas do IAM"

4. Certifique-se de que o utilizador tem uma chave de acesso que pode adicionar ao BlueXP  depois de instalar o conetor.

**Resultado**

A conta agora tem as permissões necessárias.

**Função do Azure**

Crie uma função personalizada do Azure com as permissões necessárias. Você atribuirá essa função à VM do conetor.

Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se você preferir usar um método diferente, consulte "Documentação do Azure"

**Passos**

1. Se você estiver planejando instalar manualmente o software em seu próprio host, habilite uma identidade gerenciada atribuída ao sistema na VM para que você possa fornecer as permissões necessárias do Azure por meio de uma função personalizada.

   "Documentação do Microsoft Azure: Configure identidades gerenciadas para recursos do Azure em uma VM usando o portal do Azure"

2. Copie o conteúdo do "Permissões de função personalizadas para o conetor" e salve-o em um arquivo JSON.
3. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

   Você deve adicionar o ID para cada assinatura do Azure que deseja usar com o BlueXP .

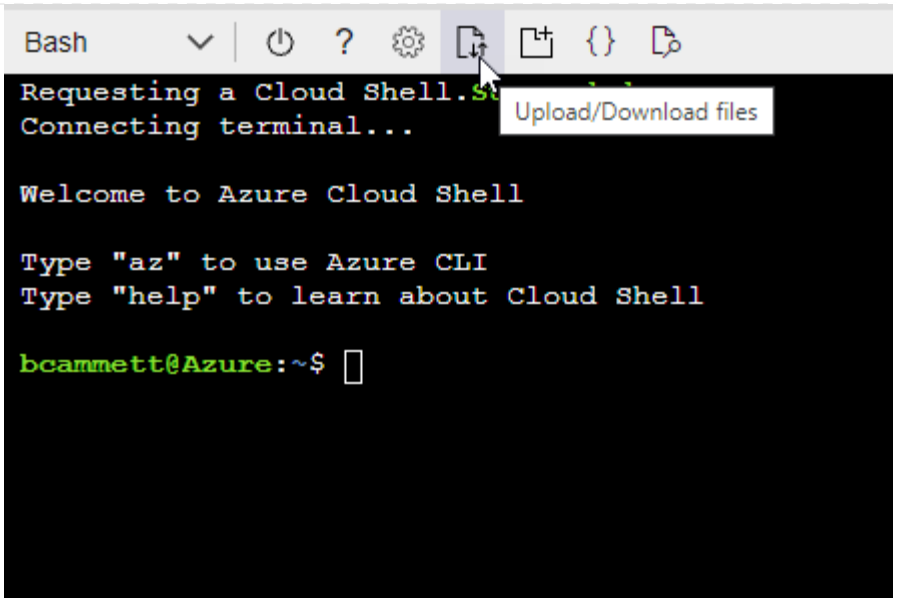
   **Exemplo**

   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

4. Use o arquivo JSON para criar uma função personalizada no Azure.

   As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

   a. Comece "Azure Cloud Shell" e escolha o ambiente Bash.
   b. Carregue o arquivo JSON.




c. Use a CLI do Azure para criar a função personalizada:

```
az role definition create --role-definition Connector_Policy.json
```

**Resultado**

Agora você deve ter uma função personalizada chamada Operador BlueXP  que você pode atribuir à máquina virtual do conetor.

**Diretor de serviço do Azure**

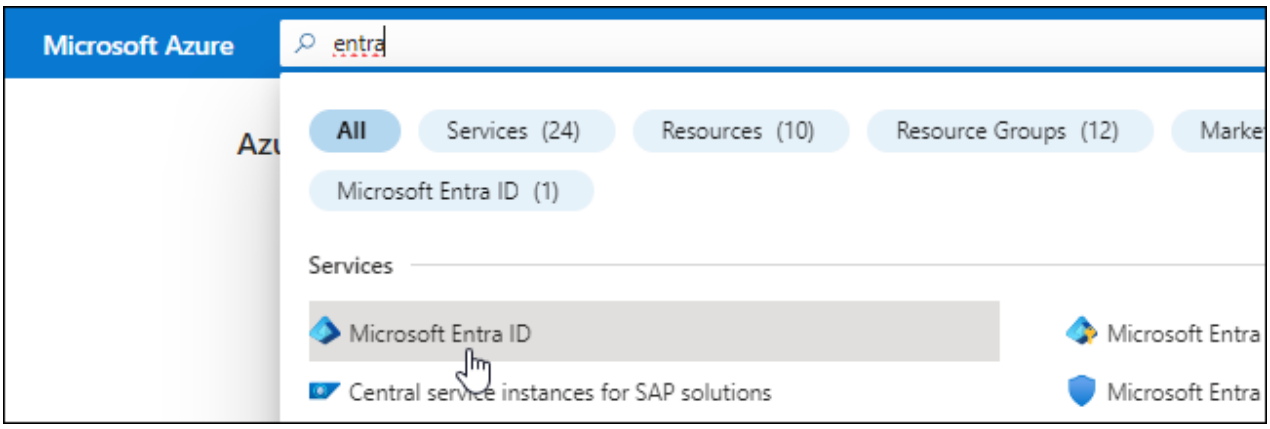
Crie e configure um princípio de serviço no Microsoft Entra ID e obtenha as credenciais do Azure de que o BlueXP  precisa. Você precisará fornecer essas credenciais ao BlueXP  depois de instalar o conetor e configurar o BlueXP .

**Crie um aplicativo Microsoft Entra para controle de acesso baseado em funções**

1. Certifique-se de ter permissões no Azure para criar um aplicativo do ative Directory e atribuir o aplicativo a uma função.

   Para obter mais informações, consulte "Documentação do Microsoft Azure: Permissões necessárias"

2. No portal do Azure, abra o serviço **Microsoft Entra ID**.



3. No menu, selecione **inscrições de aplicativos**.
4. Selecione **novo registo**.
5. Especifique detalhes sobre o aplicativo:
   - **Nome**: Insira um nome para o aplicativo.
   - **Tipo de conta**: Selecione um tipo de conta (qualquer funcionará com o BlueXP ).
   - * URI de redirecionamento*: Você pode deixar este campo em branco.
6. Selecione **Registe-se**.

   Você criou o aplicativo AD e o principal de serviço.

**Atribua a aplicação a uma função**

1. Crie uma função personalizada:

   Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se você preferir usar um método diferente, consulte "Documentação do Azure"

   a. Copie o conteúdo do "Permissões de função personalizadas para o conetor" e salve-o em um arquivo JSON.

   b. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

      Você deve adicionar o ID para cada assinatura do Azure a partir da qual os usuários criarão sistemas Cloud Volumes ONTAP.

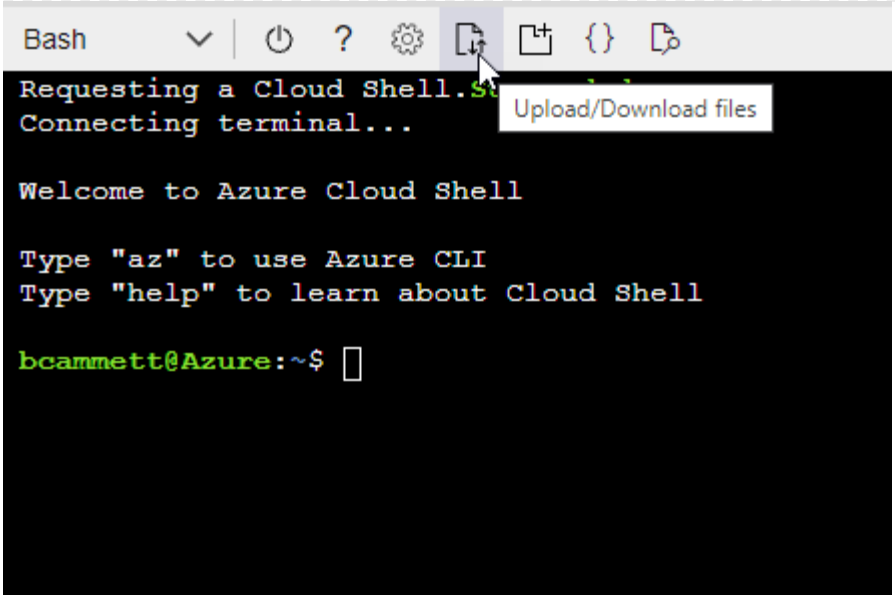
      **Exemplo**

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ```

   c. Use o arquivo JSON para criar uma função personalizada no Azure.

      As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

      - Comece "Azure Cloud Shell" e escolha o ambiente Bash.
      - Carregue o arquivo JSON.




- Use a CLI do Azure para criar a função personalizada:

```
az role definition create --role-definition
Connector_Policy.json
```

Agora você deve ter uma função personalizada chamada Operador BlueXP que você pode atribuir à máquina virtual do conetor.

2. Atribua o aplicativo à função:

   a. No portal do Azure, abra o serviço **Subscrições**.

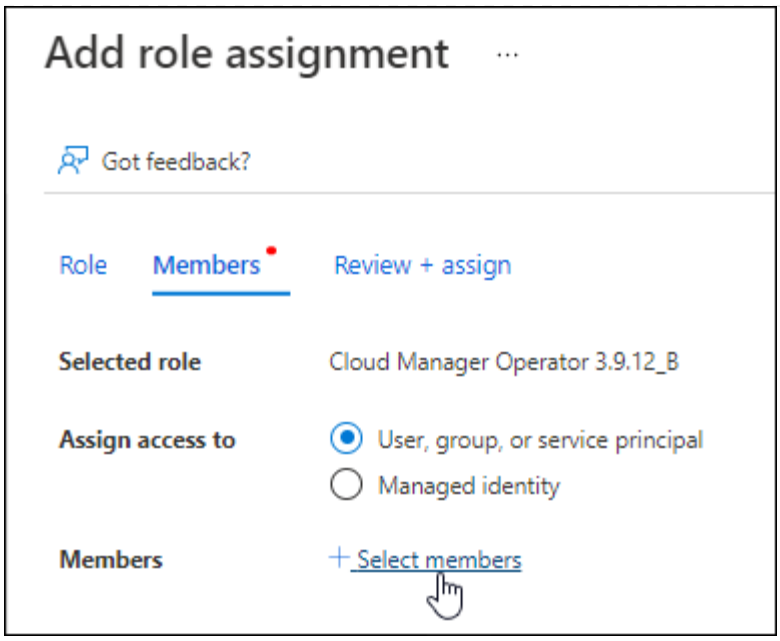
   b. Selecione a subscrição.

   c. Selecione **Access Control (IAM) > Add > Add > Add Role assignment** (Adicionar controlo de acesso).

   d. Na guia **função**, selecione a função **Operador BlueXP** e selecione **seguinte**.

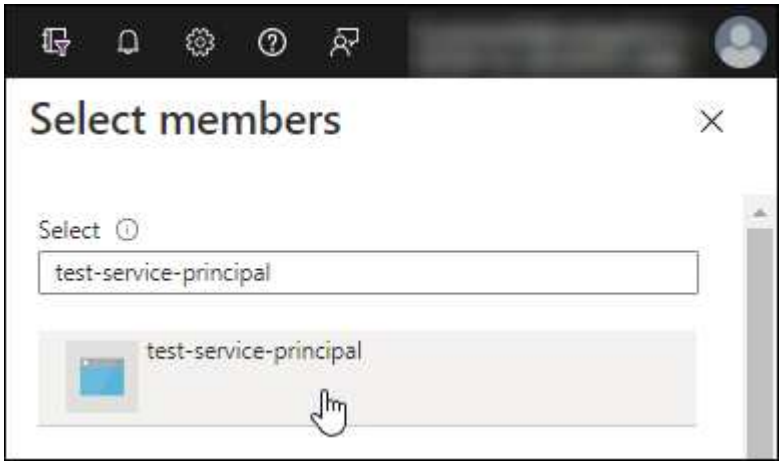
   e. Na guia **Membros**, execute as seguintes etapas:

      - Mantenha **Usuário, grupo ou responsável do serviço** selecionado.
      - Selecione **Selecionar membros**.




- Procure o nome da aplicação.

  Aqui está um exemplo:




- Selecione a aplicação e selecione **Select**.
- Selecione **seguinte**.

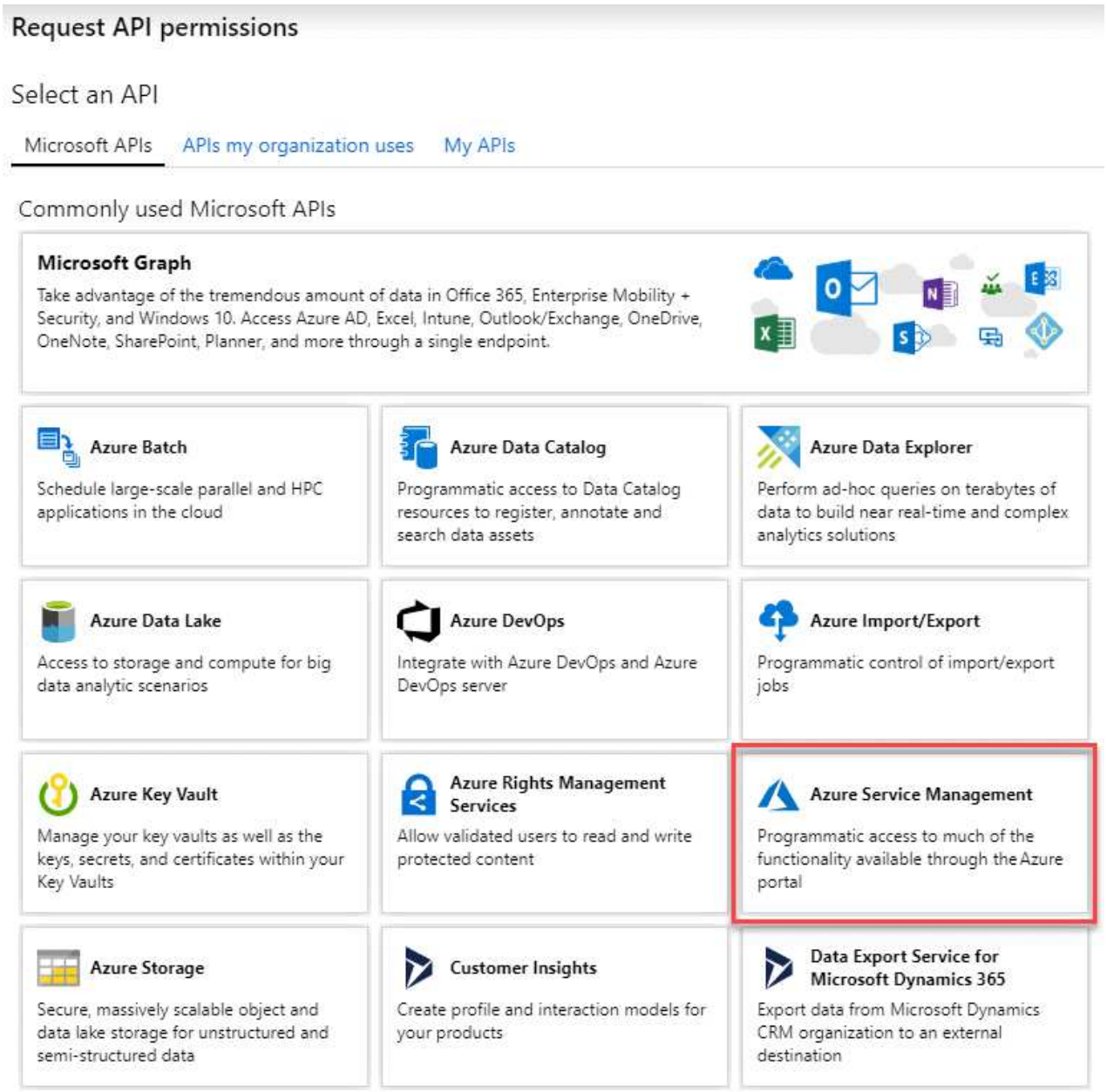
f. Selecione **Rever e atribuir**.

O principal de serviço agora tem as permissões necessárias do Azure para implantar o conetor.

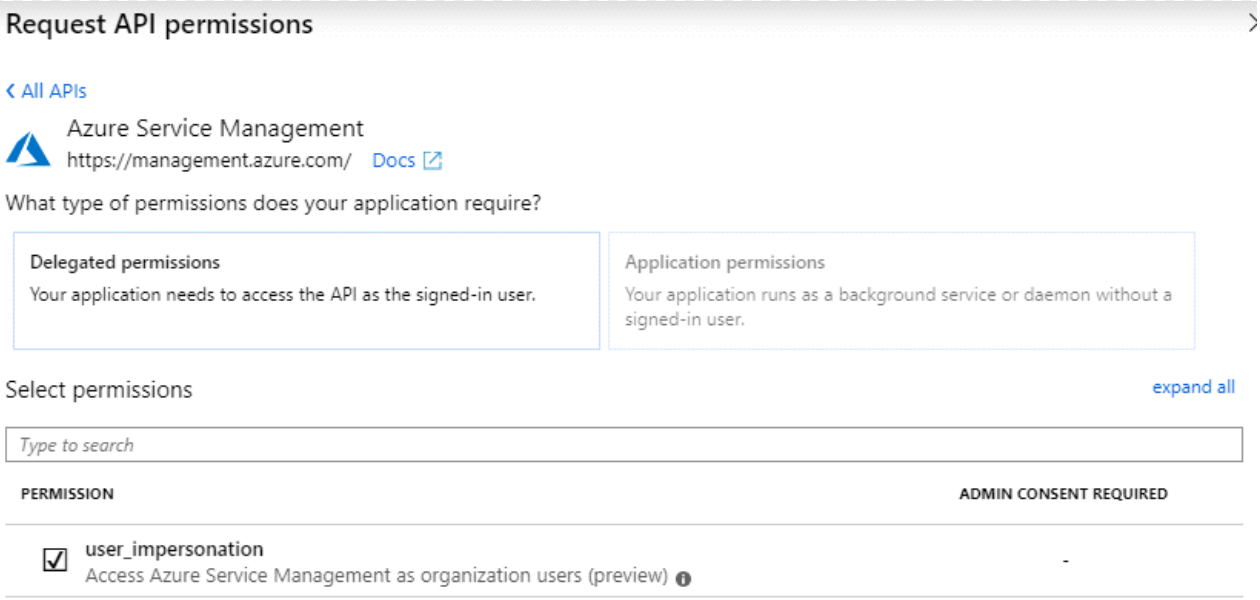
Se você quiser implantar o Cloud Volumes ONTAP a partir de várias assinaturas do Azure, então você deve vincular o principal de serviço a cada uma dessas assinaturas. O BlueXP  permite que você selecione a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

**Adicione permissões da API de Gerenciamento de Serviços do Windows Azure**

1. No serviço **Microsoft Entra ID**, selecione **inscrições de aplicativos** e selecione o aplicativo.
2. Selecione **permissões de API > Adicionar uma permissão**.
3. Em **Microsoft APIs**, selecione **Azure Service Management**.

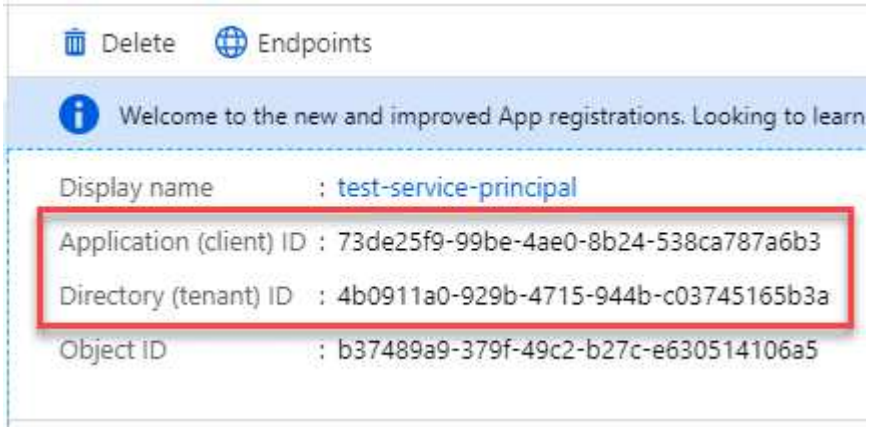



4. Selecione **Acesse o Gerenciamento de Serviços do Azure como usuários da organização** e selecione **Adicionar permissões**.




**Obtenha o ID do aplicativo e o ID do diretório para o aplicativo**

1. No serviço **Microsoft Entra ID**, selecione **inscrições de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.




Quando você adiciona a conta do Azure ao BlueXP , você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O BlueXP  usa os IDs para fazer login programaticamente.

**Crie um segredo de cliente**

1. Abra o serviço **Microsoft Entra ID**.
2. Selecione **inscrições de aplicativos** e selecione sua inscrição.
3. Selecione **certificados e segredos > segredo de novo cliente**.
4. Forneça uma descrição do segredo e uma duração.
5. Selecione **Adicionar**.
6. Copie o valor do segredo do cliente.


Agora você tem um segredo de cliente que o BlueXP pode usá-lo para autenticar com o Microsoft Entra ID.

**Resultado**

Seu responsável de serviço está configurado e você deve ter copiado o ID do aplicativo (cliente), o ID do diretório (locatário) e o valor do segredo do cliente. Você precisa inserir essas informações no BlueXP ao adicionar uma conta do Azure.

**Conta de serviço do Google Cloud**

Crie uma função e aplique-a a uma conta de serviço que você usará para a instância de VM Connector.

**Passos**

1. Crie uma função personalizada no Google Cloud:

   a. Crie um arquivo YAML que inclua as permissões definidas no "Política de conetores para Google Cloud".

   b. No Google Cloud, ative o shell da nuvem.

   c. Carregue o arquivo YAML que inclui as permissões necessárias para o conetor.

   d. Crie uma função personalizada usando o `gcloud iam roles create` comando.

      O exemplo a seguir cria uma função chamada "Connector" no nível do projeto:

```
gcloud iam roles create connector --project=myproject
--file=connector.yaml
```

   +
   "Google Cloud docs: Criando e gerenciando funções personalizadas"

2. Crie uma conta de serviço no Google Cloud:

   a. No serviço IAM e Admin, selecione **Contas de serviço > criar conta de serviço**.

   b. Insira os detalhes da conta de serviço e selecione **criar e continuar**.

   c. Selecione a função que você acabou de criar.

   d. Conclua as etapas restantes para criar a função.

      "Google Cloud docs: Criando uma conta de serviço"

**Resultado**

Agora você tem uma conta de serviço que pode atribuir à instância de VM Connector.

#### Etapa 7: Habilite as APIs do Google Cloud

Várias APIs são necessárias para implantar o Cloud Volumes ONTAP no Google Cloud.

**Passo**

1. "Ative as seguintes APIs do Google Cloud em seu projeto"
    - API do Cloud Deployment Manager V2
    - API Cloud Logging
    - API do Cloud Resource Manager
    - API do mecanismo de computação
    - API de gerenciamento de identidade e acesso (IAM)
    - API do Cloud Key Management Service (KMS)

      (Necessário somente se você estiver planejando usar o backup e a recuperação do BlueXP com chaves de criptografia gerenciadas pelo cliente (CMEK))

## Implante o conetor no modo restrito

Implante o conetor no modo restrito para que você possa usar o BlueXP com conetividade de saída limitada à camada de software como serviço (SaaS) da BlueXP . Para começar, instale o conetor, configure o BlueXP acessando a interface do usuário que está sendo executada no conetor e, em seguida, forneça as permissões de nuvem que você configurou anteriormente.

#### Passo 1: Instale o conetor

Instale o conetor do mercado do seu provedor de nuvem ou instalando manualmente o software em seu próprio host Linux.

**AWS Commercial Marketplace**

**Antes de começar**

Você deve ter o seguinte:

- VPC e sub-rede que atendem aos requisitos de rede.

  "Saiba mais sobre os requisitos de rede"

- Uma função do IAM com uma política anexada que inclui as permissões necessárias para o conetor.

  "Saiba como configurar permissões da AWS"

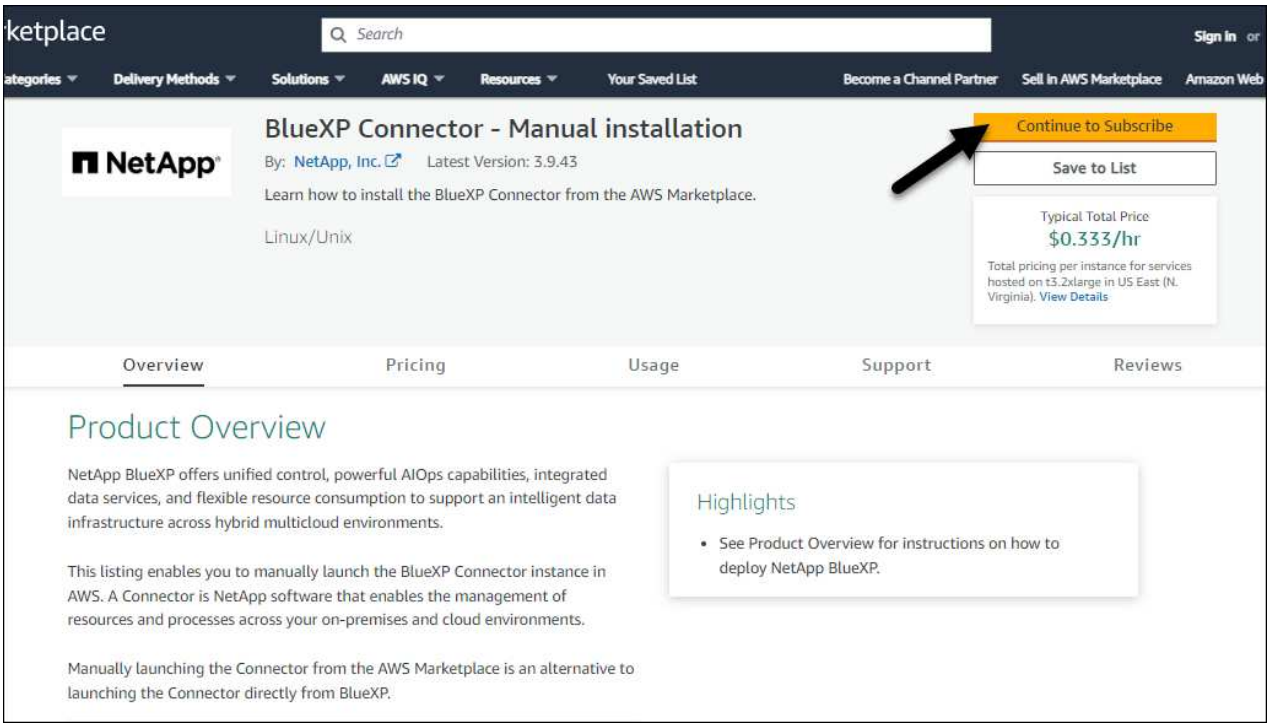
- Permissões para se inscrever e cancelar a assinatura do AWS Marketplace para seu usuário do IAM.
- Uma compreensão dos requisitos de CPU e RAM para a instância.

  "Revise os requisitos de instância".

- Um par de chaves para a instância EC2.

**Passos**

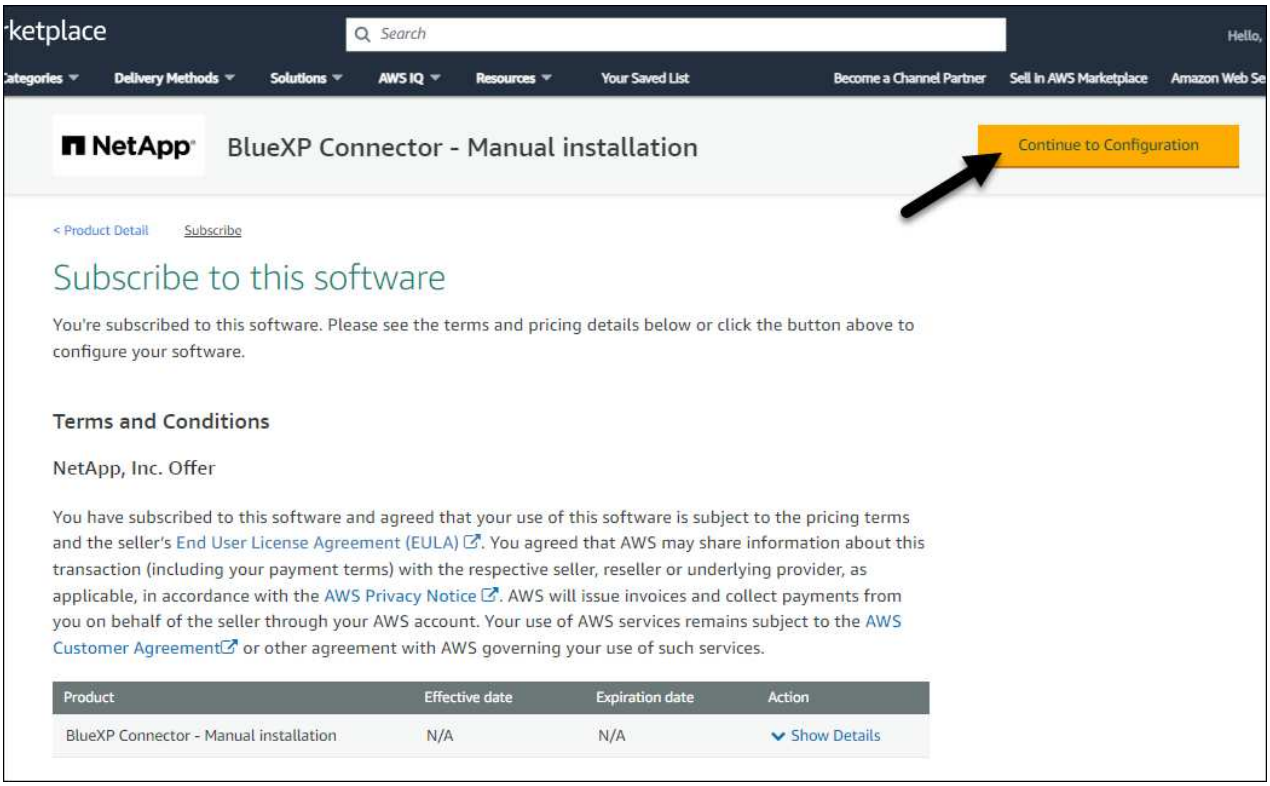
1. Vá para "Listagem do BlueXP  Connector no AWS Marketplace"
2. Na página Marketplace, selecione **Continue to Subscribe**.




3. Para assinar o software, selecione **aceitar termos**.

   O processo de assinatura pode levar alguns minutos.

4. Depois que o processo de assinatura estiver concluído, selecione **Continue to Configuration**.




5. Na página **Configure this software**, certifique-se de que selecionou a região correta e selecione **Continue to Launch**.
6. Na página **Launch this software**, em **Choose Action**, selecione **Launch through EC2** e, em seguida, selecione **Launch**.

   Estas etapas descrevem como iniciar a instância a partir do Console EC2 porque o console permite que você anexe uma função do IAM à instância do conetor. Isso não é possível usando a ação **Launch from Website**.

7. Siga as instruções para configurar e implantar a instância:
   - **Nome e tags**: Insira um nome e tags para a instância.
   - **Imagens de aplicativos e SO**: Pule esta seção. O AMI do conetor já está selecionado.
   - **Tipo de instância**: Dependendo da disponibilidade da região, escolha um tipo de instância que atenda aos requisitos de RAM e CPU (t3,2xlarge é pré-selecionado e recomendado).
   - **Par de chaves (login)**: Selecione o par de chaves que você deseja usar para se conetar com segurança à instância.
   - **Configurações de rede**: Edite as configurações de rede conforme necessário:
     - Escolha a VPC e a sub-rede desejadas.
     - Especifique se a instância deve ter um endereço IP público.
     - Especifique as configurações do grupo de segurança que ativam os métodos de conexão necessários para a instância do conetor: SSH, HTTP e HTTPS.

       "Veja as regras do grupo de segurança da AWS".

   - **Configurar armazenamento**: Mantenha o tamanho padrão e o tipo de disco para o volume raiz.

     Se você quiser ativar a criptografia do Amazon EBS no volume raiz, selecione **Avançado**,

expanda **volume 1**, selecione **criptografado** e escolha uma chave KMS.

- **Detalhes avançados**: Em **Perfil de instância do IAM**, escolha a função do IAM que inclui as permissões necessárias para o conetor.
- **Summary**: Revise o resumo e selecione **Launch instance**.

**Resultado**

A AWS inicia o software com as configurações especificadas. A instância do conetor e o software devem estar sendo executados em aproximadamente cinco minutos.

**O que se segue?**

Configure o BlueXP .

**AWS Gov Marketplace**

**Antes de começar**

Você deve ter o seguinte:

- VPC e sub-rede que atendem aos requisitos de rede.

  "Saiba mais sobre os requisitos de rede"

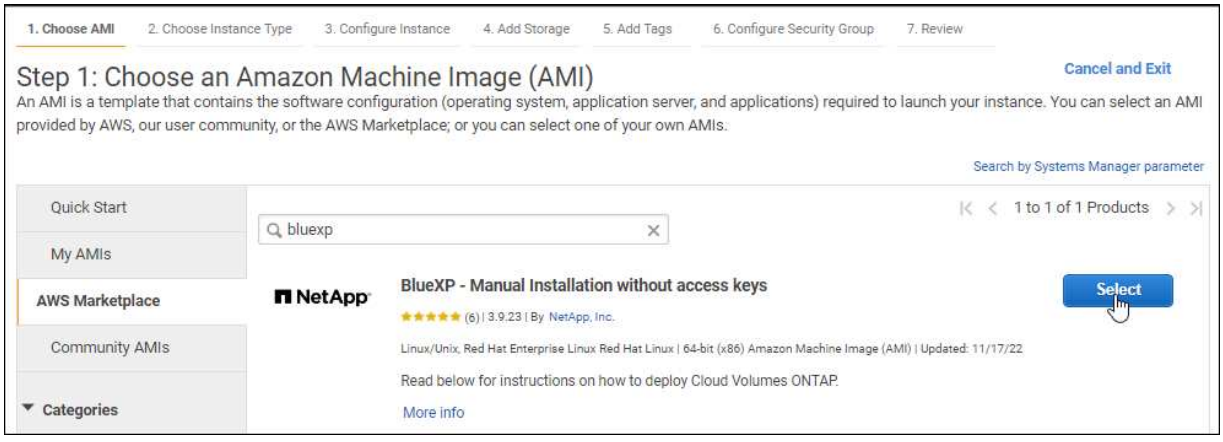
- Uma função do IAM com uma política anexada que inclui as permissões necessárias para o conetor.

  "Saiba como configurar permissões da AWS"

- Permissões para se inscrever e cancelar a assinatura do AWS Marketplace para seu usuário do IAM.
- Um par de chaves para a instância EC2.

**Passos**

1. Vá para a oferta BlueXP  no AWS Marketplace.
   a. Abra o serviço EC2 e selecione **Launch instance**.
   b. Selecione **AWS Marketplace**.
   c. Procure por BlueXP  e selecione a oferta.

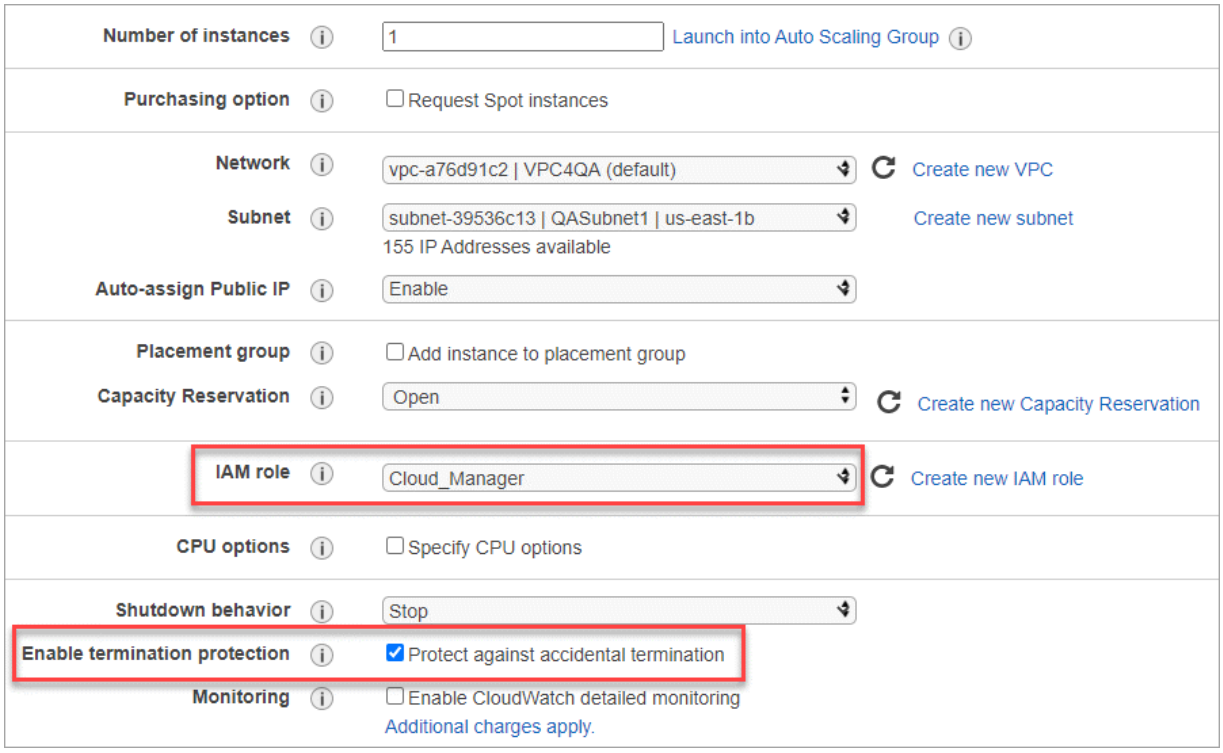



   d. Selecione **continuar**.
2. Siga as instruções para configurar e implantar a instância:
   - **Escolha um tipo de instância**: Dependendo da disponibilidade da região, escolha um dos tipos

de instância compatíveis (t3,2xlarge é recomendado).

"Revise os requisitos da instância".

- **Configurar Detalhes da instância**: Selecione uma VPC e uma sub-rede, escolha a função do IAM que você criou na etapa 1, ative a proteção de terminação (recomendada) e escolha quaisquer outras opções de configuração que atendam aos seus requisitos.




- **Adicionar armazenamento**: Mantenha as opções de armazenamento padrão.
- **Add Tags**: Insira tags para a instância, se desejado.
- **Configurar grupo de segurança**: Especifique os métodos de conexão necessários para a instância do conetor: SSH, HTTP e HTTPS.
- **Revisão**: Revise suas seleções e selecione **Lançamento**.

**Resultado**

A AWS inicia o software com as configurações especificadas. A instância do conetor e o software devem estar sendo executados em aproximadamente cinco minutos.

**O que se segue?**

Configure o BlueXP .

**Azure Marketplace**

**Antes de começar**

Você deve ter o seguinte:

- Uma VNet e uma sub-rede que atenda aos requisitos de rede.

  "Saiba mais sobre os requisitos de rede"

- Uma função personalizada do Azure que inclui as permissões necessárias para o conetor.

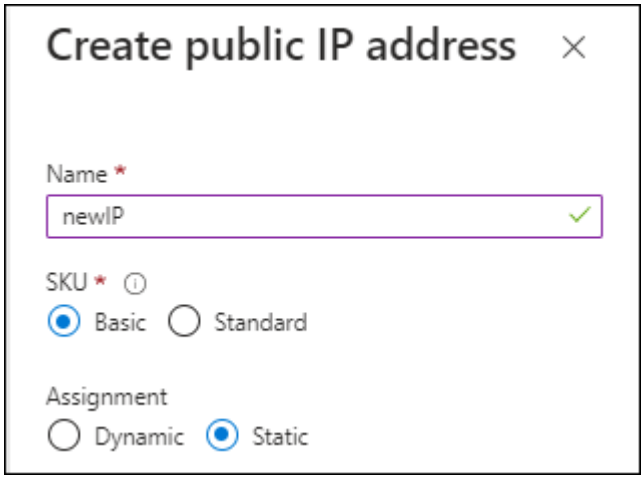
"Saiba como configurar permissões do Azure"

**Passos**

1. Vá para a página VM do NetApp Connector no Azure Marketplace.
   - "Página do Azure Marketplace para regiões comerciais"
   - "Página do Azure Marketplace para regiões do Azure Government"
2. Selecione **Obtenha agora** e, em seguida, selecione **continuar**.
3. No portal do Azure, selecione **criar** e siga as etapas para configurar a máquina virtual.

   Observe o seguinte ao configurar a VM:

   - **Tamanho da VM**: Escolha um tamanho de VM que atenda aos requisitos de CPU e RAM. Recomendamos Standard_D8s_v3.
   - **Disks**: O conetor pode funcionar de forma ideal com discos HDD ou SSD.
   - **IP público**: Se você quiser usar um endereço IP público com a VM do conetor, o endereço IP deve usar um SKU básico para garantir que o BlueXP  use esse endereço IP público.

     Se você usar um endereço IP SKU padrão, o BlueXP  usará o endereço IP *private* do conetor, em vez do IP público. Se a máquina que você está usando para acessar o Console do BlueXP  não tiver acesso a esse endereço IP privado, as ações do Console do BlueXP  falharão.

   "Documentação do Azure: SKU IP público"

   - **Grupo de segurança de rede**: O conetor requer conexões de entrada usando SSH, HTTP e HTTPS.

     "Veja as regras do grupo de segurança para o Azure".

   - **Identidade**: Em **Gerenciamento**, selecione **Ativar identidade gerenciada atribuída ao sistema**.

     Essa configuração é importante porque uma identidade gerenciada permite que a máquina virtual do conetor se identifique com o Microsoft Entra ID sem fornecer credenciais. "Saiba mais sobre identidades gerenciadas para recursos do Azure".

4. Na página **Revisão e criação**, revise suas seleções e selecione **criar** para iniciar a implantação.

**Resultado**

O Azure implanta a máquina virtual com as configurações especificadas. A máquina virtual e o software do conetor devem estar funcionando em aproximadamente cinco minutos.

**O que se segue?**

Configure o BlueXP .

**Instalação manual**

**Antes de começar**

Você deve ter o seguinte:

- Root Privileges para instalar o conetor.
- Detalhes sobre um servidor proxy, se for necessário um proxy para acesso à Internet a partir do conetor.

  Você tem a opção de configurar um servidor proxy após a instalação, mas isso requer a reinicialização do conetor.

  Observe que o BlueXP  não oferece suporte a servidores proxy transparentes.
- Um certificado assinado pela CA, se o servidor proxy usar HTTPS ou se o proxy for um proxy intercetor.
- Dependendo do seu sistema operacional, o Podman ou o Docker Engine são necessários antes de instalar o conetor.

**Sobre esta tarefa**

O instalador disponível no site de suporte da NetApp pode ser uma versão anterior. Após a instalação, o conetor se atualiza automaticamente se uma nova versão estiver disponível.

**Passos**

1. Se as variáveis de sistema *http_proxy* ou *https_proxy* estiverem definidas no host, remova-as:

   ```
   unset http_proxy
   unset https_proxy
   ```

   Se você não remover essas variáveis do sistema, a instalação falhará.

2. Faça o download do software Connector do "Site de suporte da NetApp"e copie-o para o host Linux.

   Você deve baixar o instalador do conetor "online" destinado a ser usado em sua rede ou na nuvem. Um instalador "offline" separado está disponível para o conetor, mas só é suportado com implantações de modo privado.

3. Atribua permissões para executar o script.

   ```
   chmod +x BlueXP-Connector-Cloud-<version>
   ```

   Onde <version> é a versão do conetor que você baixou.

4. Execute o script de instalação.

```
 ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

Os parâmetros --proxy e --cacert são opcionais. Se você tiver um servidor proxy, será necessário inserir os parâmetros como mostrado. O instalador não solicita que você forneça informações sobre um proxy.

Aqui está um exemplo do comando usando ambos os parâmetros opcionais:

```
 ./BlueXP-Connector-Cloud-v3.9.40--proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

--proxy configura o conetor para usar um servidor proxy HTTP ou HTTPS usando um dos seguintes formatos:

- http://address:port
- http://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Observe o seguinte:

  - O usuário pode ser um usuário local ou usuário de domínio.
  - Para um usuário de domínio, você deve usar o código ASCII para a como mostrado acima.
  - O BlueXP  não suporta nomes de usuário ou senhas que incluem o caractere A.
  - Se a senha incluir qualquer um dos seguintes carateres especiais, você deve escapar desse caractere especial, prependendo-o com uma barra invertida: & Ou !

    Por exemplo:

  http://bxpproxyuser:netapp1\!@address:3128

--cacert especifica um certificado assinado pela CA a ser usado para acesso HTTPS entre o conetor e o servidor proxy. Este parâmetro só é necessário se especificar um servidor proxy HTTPS ou se o proxy for um proxy intercetor.

**Resultado**

O conetor está agora instalado. No final da instalação, o serviço de conetor (occm) será reiniciado duas vezes se você tiver especificado um servidor proxy.

**O que se segue?**

Configure o BlueXP .

### Passo 2: Configurar o BlueXP

Ao acessar o console BlueXP  pela primeira vez, você será solicitado a escolher uma conta para associar o conetor e precisará ativar o modo restrito.

#### Antes de começar

A pessoa que configura o BlueXP  Connector deve fazer login no BlueXP  usando um login que não pertence a uma conta ou organização do BlueXP .

Se o seu login do BlueXP  estiver associado a outra conta ou organização, você precisará se inscrever com um novo login do BlueXP . Caso contrário, você não verá a opção de ativar o modo restrito na tela de configuração.

#### Passos

1. Abra um navegador da Web a partir de um host que tenha uma conexão com a instância do conetor e insira o seguinte URL:

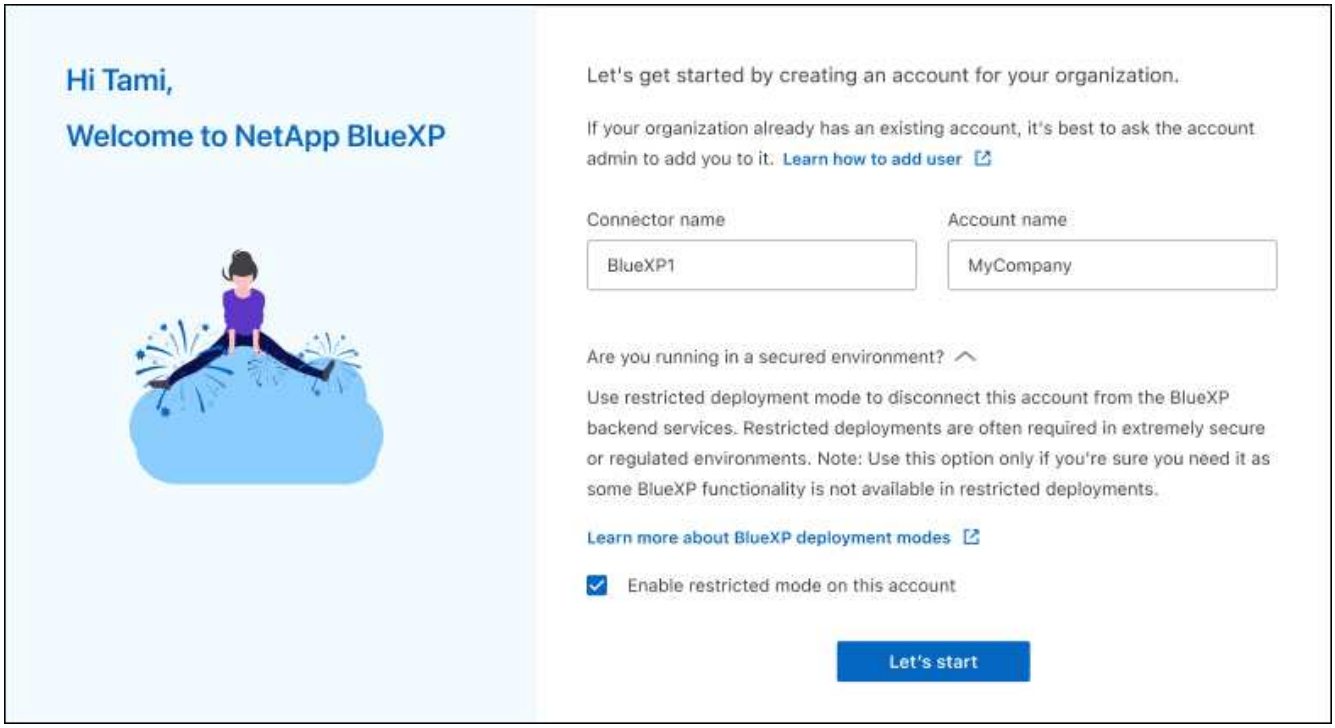
   <a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

2. Inscreva-se ou faça login no BlueXP .
3. Depois de iniciar sessão, configure o BlueXP :

   a. Introduza um nome para o conetor.
   b. Introduza um nome para uma nova conta BlueXP .
   c. Selecione **você está executando em um ambiente seguro?**
   d. Selecione **Ativar modo restrito nesta conta**.

      Observe que você não pode alterar essa configuração depois que o BlueXP  criar a conta. Não é possível ativar o modo restrito mais tarde e não é possível desativá-lo mais tarde.

      Se você implantou o conetor em uma região governamental, a caixa de seleção já está ativada e não pode ser alterada. Isso ocorre porque o modo restrito é o único modo suportado em regiões governamentais.




a. Selecione **vamos começar**.

**Resultado**

O conetor está agora instalado e configurado com a sua conta BlueXP . Todos os usuários precisam acessar o BlueXP  usando o endereço IP da instância do conetor.

**O que se segue?**

Forneça ao BlueXP  as permissões que você configurou anteriormente.

### Passo 3: Forneça permissões para o BlueXP

Se você implantou o conetor do Azure Marketplace ou instalou manualmente o software Connector, precisará fornecer as permissões que você configurou anteriormente para que você possa usar os serviços do BlueXP .

Essas etapas não se aplicam se você implantou o conetor no AWS Marketplace porque escolheu a função IAM necessária durante a implantação.

"Saiba como preparar permissões na nuvem".

**Função do AWS IAM**

Anexe a função do IAM que você criou anteriormente à instância do EC2 onde você instalou o conetor.

Estas etapas se aplicam somente se você instalou manualmente o conetor na AWS. Para implantações do AWS Marketplace, você já associou a instância do Connector a uma função do IAM que inclui as permissões necessárias.

**Passos**

1. Vá para o console do Amazon EC2.
2. Selecione **instâncias**.
3. Selecione a instância do conetor.
4. Selecione **ações > Segurança > Modificar função do IAM**.
5. Selecione a função do IAM e selecione **Atualizar função do IAM**.

**Resultado**

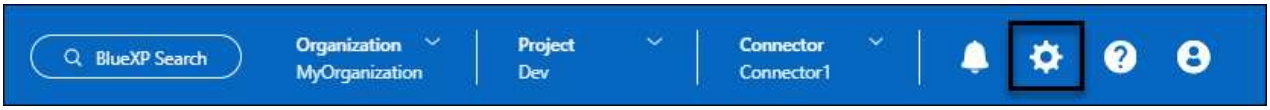
O BlueXP  agora tem as permissões necessárias para executar ações na AWS em seu nome.

**Chave de acesso da AWS**

Forneça ao BlueXP  a chave de acesso da AWS para um usuário do IAM que tenha as permissões necessárias.

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.




2. Selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Localização das credenciais**: Selecione **Amazon Web Services > Connector**.
   b. **Definir credenciais**: Insira uma chave de acesso da AWS e uma chave secreta.
   c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.
   d. **Revisão**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

**Resultado**

O BlueXP  agora tem as permissões necessárias para executar ações na AWS em seu nome.

**Função do Azure**

Vá para o portal do Azure e atribua a função personalizada do Azure à máquina virtual Connector para uma ou mais subscrições.

**Passos**

1. No Portal do Azure, abra o serviço **Subscrições** e selecione a sua subscrição.

   É importante atribuir a função do serviço **Subscrições** porque especifica o escopo da atribuição de função no nível da assinatura. O *scope* define o conjunto de recursos aos quais o acesso se aplica.

Se você especificar um escopo em um nível diferente (por exemplo, no nível da máquina virtual), sua capacidade de concluir ações de dentro do BlueXP  será afetada.

"Documentação do Microsoft Azure: Entenda o escopo do Azure RBAC"

2. Selecione **Access control (IAM)** > **Add** > **Add** > **Add role assignment**.
3. Na guia **função**, selecione a função **Operador BlueXP**  e selecione **seguinte**.

   Operador BlueXP  é o nome padrão fornecido na política BlueXP . Se você escolher um nome diferente para a função, selecione esse nome em vez disso.

4. Na guia **Membros**, execute as seguintes etapas:
   a. Atribua acesso a uma **identidade gerenciada**.
   b. Selecione **Selecionar membros**, selecione a assinatura na qual a máquina virtual do conetor foi criada, em **identidade gerenciada**, escolha **Máquina Virtual** e, em seguida, selecione a máquina virtual do conetor.
   c. Selecione **Selecionar**.
   d. Selecione **seguinte**.
   e. Selecione **Rever e atribuir**.
   f. Se você quiser gerenciar recursos em assinaturas adicionais do Azure, mude para essa assinatura e repita essas etapas.

**Resultado**

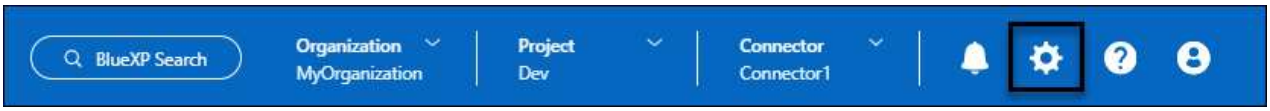
O BlueXP  agora tem as permissões necessárias para executar ações no Azure em seu nome.

**Diretor de serviço do Azure**

Forneça ao BlueXP  as credenciais para o responsável de serviço do Azure que você configurou anteriormente.

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.




2. Selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Credentials Location**: Selecione **Microsoft Azure > Connector**.
   b. **Definir credenciais**: Insira informações sobre o responsável do serviço Microsoft Entra que concede as permissões necessárias:
      - ID da aplicação (cliente)
      - ID do diretório (locatário)
      - Segredo Cliente
   c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.
   d. **Revisão**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

**Resultado**

O BlueXP  agora tem as permissões necessárias para executar ações no Azure em seu nome.

**Conta de serviço do Google Cloud**

Associe a conta de serviço à VM do conetor.

**Passos**

1. Vá para o portal do Google Cloud e atribua a conta de serviço à instância da VM Connector.

   "Documentação do Google Cloud: Alterando a conta de serviço e os escopos de acesso para uma instância"

2. Se você quiser gerenciar recursos em outros projetos, conceda acesso adicionando a conta de serviço com a função BlueXP  a esse projeto. Você precisará repetir esta etapa para cada projeto.

**Resultado**

O BlueXP  agora tem as permissões necessárias para executar ações no Google Cloud em seu nome.

## Assinar BlueXP  (modo restrito)

Inscreva-se no BlueXP  no mercado do seu fornecedor de nuvem para pagar os serviços da BlueXP  a uma taxa por hora (PAYGO) ou por meio de um contrato anual. Se você comprou uma licença da NetApp (BYOL), também precisará se inscrever na oferta de mercado. A sua licença é sempre cobrada primeiro, mas você será cobrado à taxa por hora se exceder a sua capacidade licenciada ou se o prazo da licença expirar.

Uma assinatura de mercado permite o carregamento dos seguintes serviços BlueXP  com modo restrito:

- Backup e recuperação
- Classificação
- Cloud Volumes ONTAP

**Antes de começar**

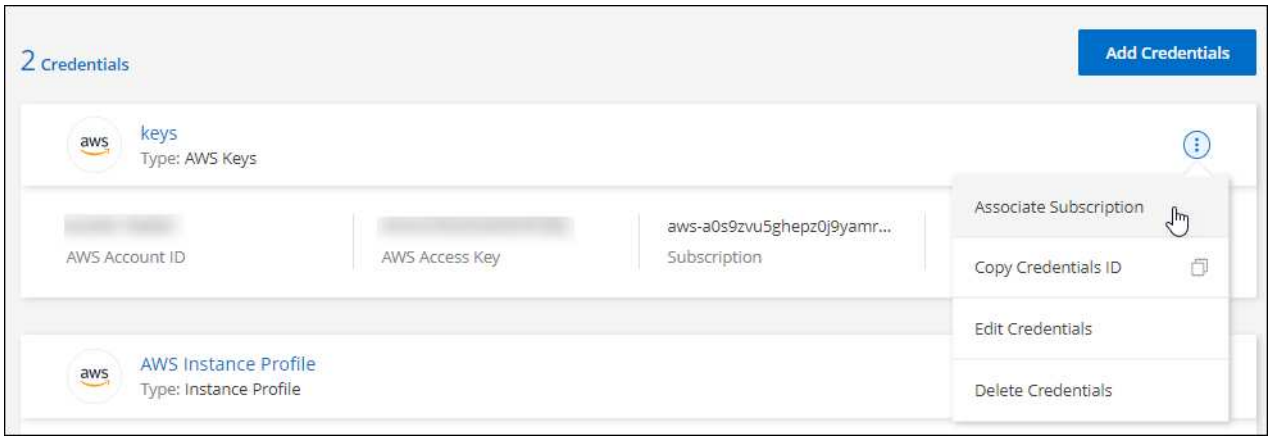
A assinatura do BlueXP  envolve a associação de mercado às credenciais de nuvem associadas a um conector. Se você seguiu o fluxo de trabalho "começar com modo restrito", então você já deve ter um conetor. Para saber mais, consulte o "Início rápido para BlueXP  no modo restrito".

**AWS**

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Selecione o menu de ação para um conjunto de credenciais e, em seguida, selecione **assinatura associada**.

   Você deve selecionar credenciais associadas a um conetor. Não é possível associar uma assinatura do marketplace a credenciais associadas ao BlueXP .




3. Para associar as credenciais a uma assinatura existente, selecione a assinatura na lista suspensa e selecione **Associate**.
4. Para associar as credenciais a uma nova assinatura, selecione **Adicionar assinatura > continuar** e siga as etapas no AWS Marketplace:

   a. Selecione **Ver opções de compra**.

   b. Selecione **Subscribe**.

   c. Selecione **Configurar a sua conta**.

      Você será redirecionado para o site da BlueXP .

   d. Na página **atribuição de assinatura**:

      - Selecione as organizações ou contas do BlueXP às quais você deseja associar essa assinatura.
      - No campo **Substituir subscrição existente**, escolha se pretende substituir automaticamente a subscrição existente de uma organização ou conta por esta nova subscrição.

        O BlueXP substitui a assinatura existente para todas as credenciais na organização ou conta por essa nova assinatura. Se um conjunto de credenciais nunca foi associado a uma assinatura, essa nova assinatura não será associada a essas credenciais.

   Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo estas etapas.

      - Selecione **Guardar**.

        O vídeo a seguir mostra as etapas para se inscrever no AWS Marketplace:

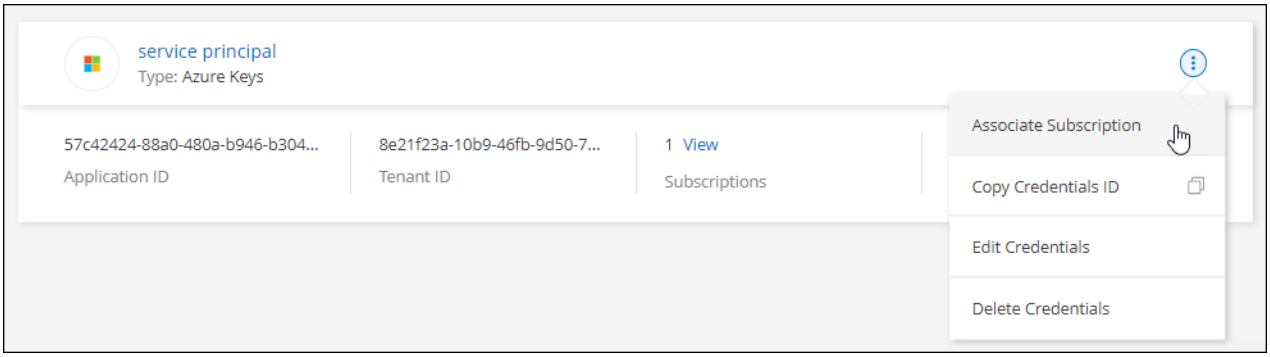
Inscreva-se no BlueXP  no AWS Marketplace

**Azure**

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Selecione o menu de ação para um conjunto de credenciais e, em seguida, selecione **assinatura associada**.

   Você deve selecionar credenciais associadas a um conetor. Não é possível associar uma assinatura do marketplace a credenciais associadas ao BlueXP .




3. Para associar as credenciais a uma assinatura existente, selecione a assinatura na lista suspensa e selecione **Associate**.
4. Para associar as credenciais a uma nova assinatura, selecione **Adicionar assinatura > continuar** e siga as etapas no Azure Marketplace:

   a. Se solicitado, faça login na sua conta do Azure.

   b. Selecione **Subscribe**.

   c. Preencha o formulário e selecione **Subscribe**.

   d. Depois que o processo de assinatura estiver concluído, selecione **Configurar conta agora**.

      Você será redirecionado para o site da BlueXP .

   e. Na página **atribuição de assinatura**:

      - Selecione as organizações ou contas do BlueXP  às quais você deseja associar essa assinatura.
      - No campo **Substituir subscrição existente**, escolha se pretende substituir automaticamente a subscrição existente de uma organização ou conta por esta nova subscrição.

        O BlueXP  substitui a assinatura existente para todas as credenciais na organização ou conta por essa nova assinatura. Se um conjunto de credenciais nunca foi associado a uma assinatura, essa nova assinatura não será associada a essas credenciais.

   Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo estas etapas.

      - Selecione **Guardar**.

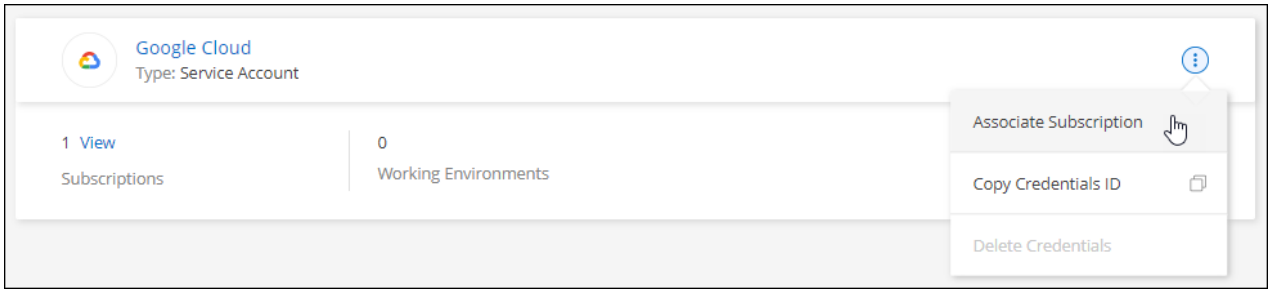
O vídeo a seguir mostra as etapas para se inscrever no Azure Marketplace:

Inscreva-se no BlueXP  a partir do Azure Marketplace

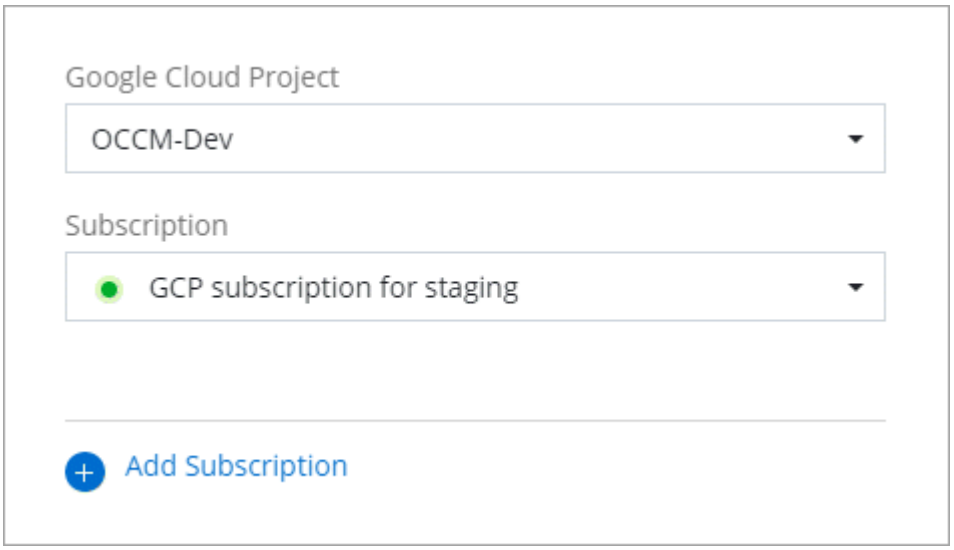
**Google Cloud**

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Selecione o menu de ação para um conjunto de credenciais e, em seguida, selecione **assinatura associada**.



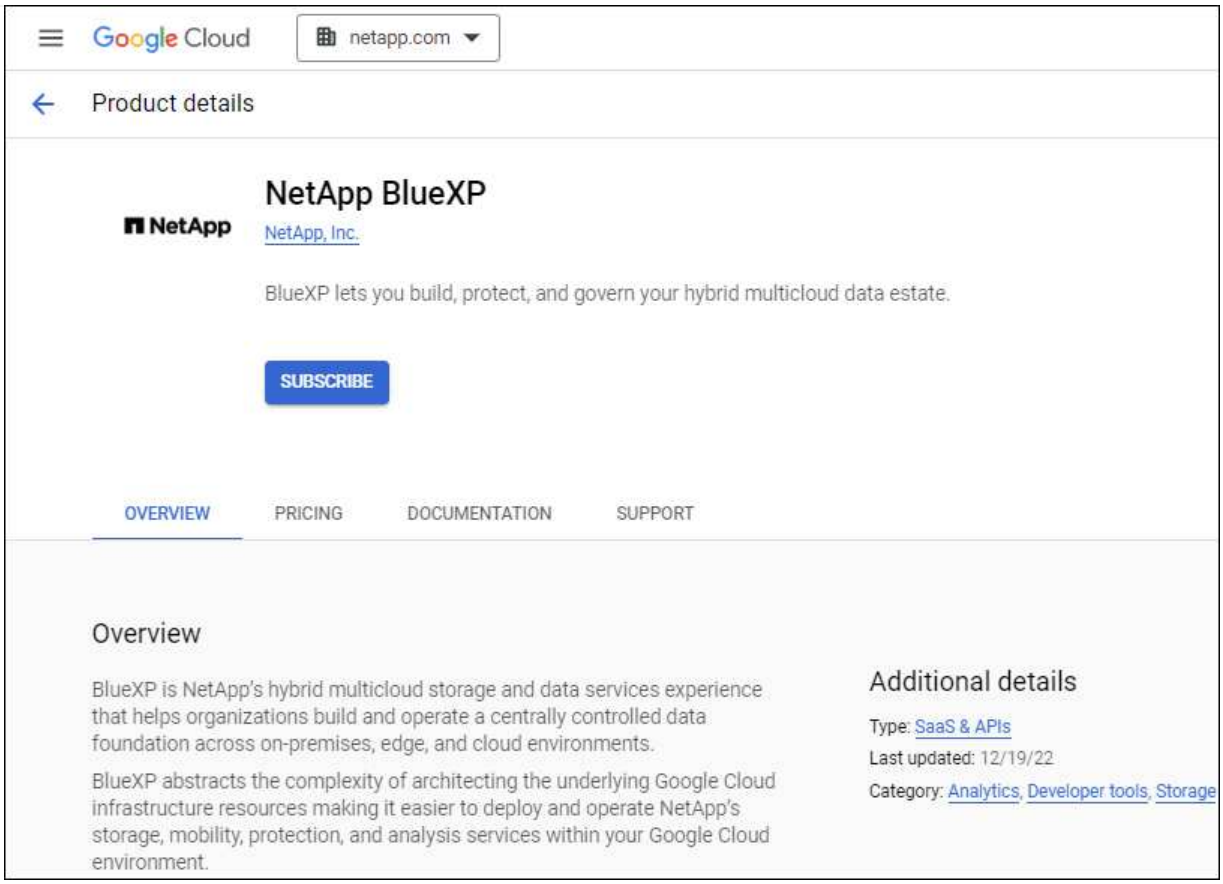

3. Para associar as credenciais a uma assinatura existente, selecione um projeto e assinatura do Google Cloud na lista suspensa e, em seguida, selecione **Associate**.




4. Se você ainda não tiver uma assinatura, selecione **Adicionar assinatura > continuar** e siga as etapas no Google Cloud Marketplace.

Antes de concluir as etapas a seguir, certifique-se de que você tenha o Privileges de Administração de faturamento na sua conta do Google Cloud, bem como um login no BlueXP .

a. Depois de ser redirecionado para o "Página do NetApp BlueXP  no Google Cloud Marketplace", certifique-se de que o projeto correto está selecionado no menu de navegação superior.

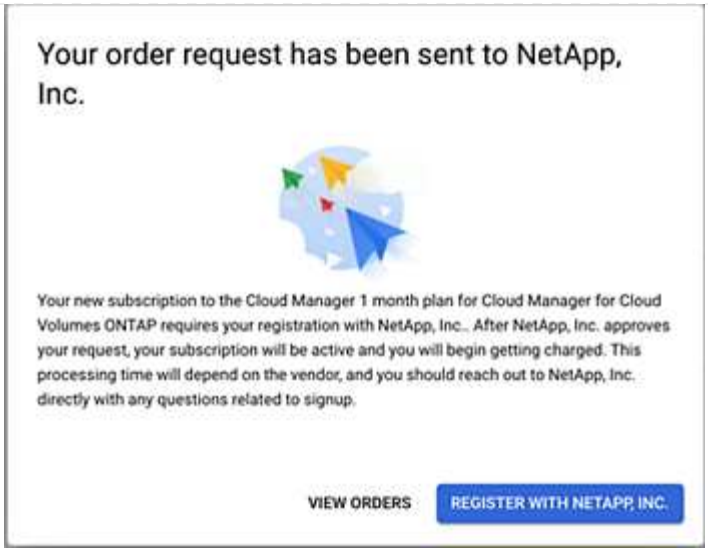



b. Selecione **Subscribe**.
c. Selecione a conta de faturamento apropriada e concorde com os termos e condições.
d. Selecione **Subscribe**.

   Esta etapa envia sua solicitação de transferência para o NetApp.

e. Na caixa de diálogo pop-up, selecione **Register with NetApp, Inc.**

   Essa etapa deve ser concluída para vincular a assinatura do Google Cloud à sua organização ou conta do BlueXP . O processo de vinculação de uma assinatura não está concluído até que você seja redirecionado desta página e, em seguida, entre no BlueXP .




f. Conclua as etapas na página **atribuição de assinatura**:

> Se alguém da sua organização já se inscreveu na assinatura do NetApp BlueXP da sua conta de faturamento, então você será redirecionado para "A página Cloud Volumes ONTAP no site da BlueXP ". Se isso for inesperado, entre em Contato com sua equipe de vendas da NetApp. O Google ativa apenas uma assinatura por conta de faturamento do Google.

- Selecione as organizações ou contas do BlueXP  às quais você deseja associar essa assinatura.
- No campo **Substituir subscrição existente**, escolha se pretende substituir automaticamente a subscrição existente de uma organização ou conta por esta nova subscrição.

  O BlueXP  substitui a assinatura existente para todas as credenciais na organização ou conta por essa nova assinatura. Se um conjunto de credenciais nunca foi associado a uma assinatura, essa nova assinatura não será associada a essas credenciais.

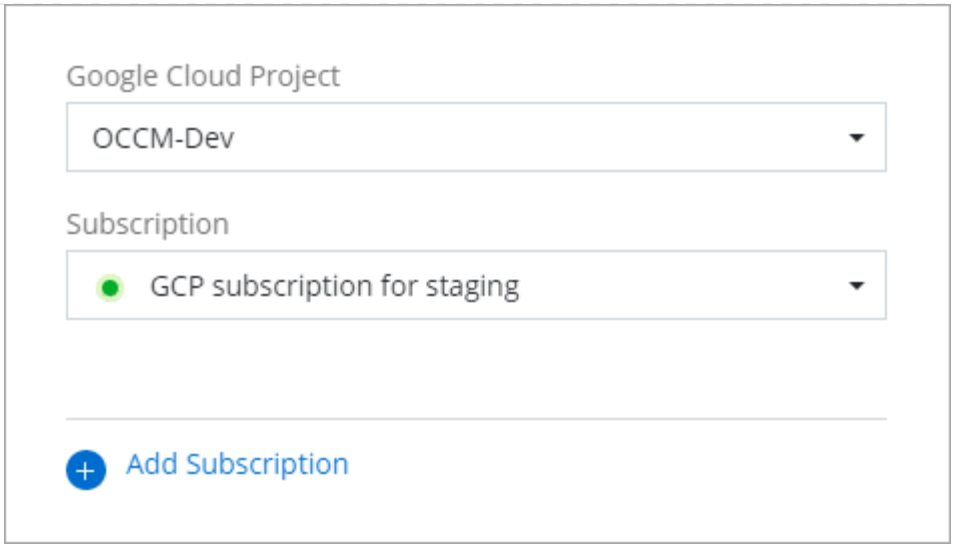
Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo estas etapas.

- Selecione **Guardar**.

  O vídeo a seguir mostra as etapas para se inscrever no Google Cloud Marketplace:

Inscreva-se no BlueXP  no Google Cloud Marketplace

a. Quando esse processo estiver concluído, navegue de volta para a página credenciais no BlueXP e selecione essa nova assinatura.




**Informações relacionadas**

- "Gerenciar licenças baseadas em capacidade BYOL para Cloud Volumes ONTAP"
- "Gerenciar licenças BYOL para serviços de dados BlueXP "
- "Gerenciar credenciais e assinaturas da AWS para o BlueXP "
- "Gerencie credenciais e assinaturas do Azure para o BlueXP "
- "Gerenciar credenciais e assinaturas do Google Cloud para o BlueXP "

### O que você pode fazer a seguir (modo restrito)

Depois de começar a usar o BlueXP  no modo restrito, você pode começar a usar os serviços BlueXP  compatíveis com o modo restrito.

Para obter ajuda, consulte a documentação para estes serviços:

- "Azure NetApp Files docs"
- "Documentos de backup e recuperação"
- "Documentos de classificação"
- "Cloud Volumes ONTAP docs"
- "Carteira digital docs"
- "Documentos de cluster do ONTAP no local"
- "Documentos de replicação"

**Link relacionado**

"Modos de implantação do BlueXP"

# Comece com o modo privado

## Fluxo de trabalho de introdução (modo privado)

Comece a usar o BlueXP  no modo privado, preparando seu ambiente e implantando o conetor.

O modo privado é normalmente utilizado com ambientes locais que não têm ligação à Internet e com regiões de nuvem seguras, que incluem "Nuvem secreta da AWS", "Nuvem secreta principal da AWS" e. "Azure IL6"

Antes de começar, você deve ter uma compreensão de "Contas BlueXP ", "Conetores"e "modos de implantação".

### 1 "Prepare-se para a implantação"

1. Prepare um host Linux dedicado que atenda aos requisitos de CPU, RAM, espaço em disco, ferramenta de orquestração de contentores e muito mais.
2. Configure a rede que forneça acesso às redes de destino.
3. Para implantações de nuvem, configure permissões no seu provedor de nuvem para que você possa associar essas permissões ao conetor depois de instalar o software.

### 2 "Implante o conetor"

1. Instale o software Connector em seu próprio host Linux.
2. Configure o BlueXP  abrindo um navegador da Web e inserindo o endereço IP do host Linux.
3. Para implantações de nuvem, forneça ao BlueXP  as permissões que você configurou anteriormente.

## Prepare-se para a implantação no modo privado

Prepare seu ambiente antes de implantar o BlueXP  no modo privado. Por exemplo, você precisa analisar os requisitos do host, preparar a rede, configurar permissões e muito mais.

Se quiser usar o BlueXP  no "Nuvem secreta da AWS" ou no "Nuvem secreta principal da AWS", siga instruções separadas para começar nesses ambientes. "Saiba como começar a usar o Cloud Volumes ONTAP na nuvem secreta da AWS ou na nuvem secreta principal"

#### Passo 1: Entenda como o modo privado funciona

Antes de começar, você deve ter uma compreensão de como o BlueXP  funciona no modo privado.

Por exemplo, você deve entender que precisa usar a interface baseada em navegador que está disponível localmente a partir do conetor BlueXP  que você precisa instalar. Não é possível acessar o BlueXP  a partir do console baseado na Web fornecido pela camada SaaS.

Além disso, nem todos os serviços BlueXP  estão disponíveis.

"Saiba como o modo privado funciona".

### Passo 2: Reveja as opções de instalação

No modo privado, você pode instalar o conetor no local ou na nuvem instalando manualmente o conetor em seu próprio host Linux.

Quando você instala o conetor determina quais serviços e recursos do BlueXP  estão disponíveis ao usar o modo privado. Por exemplo, o conetor deve ser instalado na nuvem se você quiser implantar e gerenciar o Cloud Volumes ONTAP. "Saiba mais sobre o modo privado".

### Etapa 3: Revise os requisitos do host

O software do conetor deve ser executado em um host que atenda a requisitos específicos do sistema operacional, requisitos de RAM, requisitos de porta, etc.

#### Host dedicado

O conetor não é suportado em um host que é compartilhado com outros aplicativos. O host deve ser um host dedicado.

#### requisitos de sistema operacional e contentor

O BlueXP  suporta o conetor com os seguintes sistemas operacionais ao usar o BlueXP  no modo privado. Uma ferramenta de orquestração de contêineres é necessária antes de instalar o conetor.

| Sistema operacional | Versões de OS compatíveis | Versões de conetor suportadas | Ferramenta de recipiente necessária | SELinux |
|---|---|---|---|---|
| Red Hat Enterprise Linux | 9,1 a 9,4<br><br>8,6 a 8,10 | 3.9.42 ou posterior com BlueXP  em modo privado | Podman versão 4.6.1 ou 4.9.4<br><br>Veja os requisitos de configuração do Podman. | Suporte no modo de execução ou modo permissivo 1 |
| Ubuntu | 22,04 LTS | 3.9.29 ou posterior | Docker Engine 23.0.6 a 26.0.0<br><br>26.0.0 é suportado com *new* Connector 3.9.44 ou instalações posteriores | Não suportado |

Notas:

1. O gerenciamento de sistemas Cloud Volumes ONTAP não é suportado por conetores que tenham o SELinux habilitado no sistema operacional.
2. O conetor é suportado em versões em inglês destes sistemas operativos.
3. Para o RHEL, o host deve estar registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar repositórios para atualizar o software necessário de 3rd partes durante a instalação do conetor.

**Hipervisor**

É necessário um hypervisor bare metal ou hospedado certificado para executar um sistema operacional suportado.

**CPU**

8 núcleos ou 8 vCPUs

**RAM**

32 GB

**Tipo de instância do AWS EC2**

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos t3,2xlarge.

**Tamanho da VM do Azure**

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos Standard_D8s_v3.

**Tipo de máquina Google Cloud**

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos n2-standard-8.

O conetor é compatível com o Google Cloud em uma instância de VM com um sistema operacional compatível "Recursos de VM blindados"

**Espaço em disco em /opt**

100 GiB de espaço deve estar disponível

O BlueXP usa `/opt` para instalar o `/opt/application/netapp` diretório e seu conteúdo.

**Espaço em disco em /var**

20 GiB de espaço deve estar disponível

O BlueXP requer esse espaço `/var` porque o Docker ou o Podman são arquitetados para criar os contentores dentro desse diretório. Especificamente, eles irão criar contentores no `/var/lib/containers/storage` diretório. Montagens externas ou links simbólicos não funcionam para este espaço.

### Passo 4: Instale o Podman ou Docker Engine

Você precisa preparar o host para o conetor instalando Podman ou Docker Engine.

Dependendo do seu sistema operacional, o Podman ou o Docker Engine são necessários antes de instalar o conetor.

- O Podman é necessário para o Red Hat Enterprise Linux 8 e 9.

  Veja as versões do Podman suportadas pelo BlueXP .

- Docker Engine é necessário para o Ubuntu.

  Veja as versões do Docker Engine que o BlueXP suporta.

**Exemplo 6. Passos**

**Podman**

Siga estas etapas para instalar o Podman e configurá-lo para atender aos seguintes requisitos:

- O serviço podman.socket deve ser ativado e iniciado
- python3 deve ser instalado
- O pacote podman-compose versão 1.0.6 deve ser instalado
- Podman-compose deve ser adicionado à variável de ambiente PATH

**Passos**

1. Remova o pacote podman-docker se ele estiver instalado no host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Instale o Podman.

   O Podman está disponível nos repositórios oficiais do Red Hat Enterprise Linux.

   Para Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

   Onde o <version> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas pelo BlueXP .

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

   Onde o <version> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas pelo BlueXP .

3. Ative e inicie o serviço podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Instale o python3.

```
sudo dnf install python3
```

5. Instale o pacote do repositório EPEL se ainda não estiver disponível no seu sistema.

Esta etapa é necessária porque o podman-compose está disponível no repositório extra Packages for Enterprise Linux (EPEL).

Para Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

Para Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Instale o pacote podman-compose 1,0.6.

```
sudo dnf install podman-compose-1.0.6
```

Usar o `dnf install` comando atende ao requisito para adicionar podman-compose à variável de ambiente PATH. O comando installation adiciona podman-compose ao /usr/bin, que já está incluído na `secure_path` opção no host.

**Docker Engine**

Siga a documentação do Docker para instalar o Docker Engine.

**Passos**

1. "Veja as instruções de instalação do Docker"

   Certifique-se de seguir as etapas para instalar uma versão específica do Docker Engine. Instalar a versão mais recente irá instalar uma versão do Docker que o BlueXP  não suporta.

2. Verifique se o Docker está ativado e em execução.

```
sudo systemctl enable docker && sudo systemctl start docker
```

### Passo 5: Prepare a rede

Configure sua rede para que o conetor possa gerenciar recursos e processos em seu ambiente de nuvem pública. Além de ter uma rede virtual e uma sub-rede para o conetor, você precisará garantir que os seguintes requisitos sejam atendidos.

**Conexões com redes de destino**

O conetor deve ter uma conexão de rede com o local onde você planeja gerenciar o armazenamento. Por exemplo, a VPC ou o VNet onde você pretende implantar o Cloud Volumes ONTAP ou o data center onde residem seus clusters ONTAP no local.

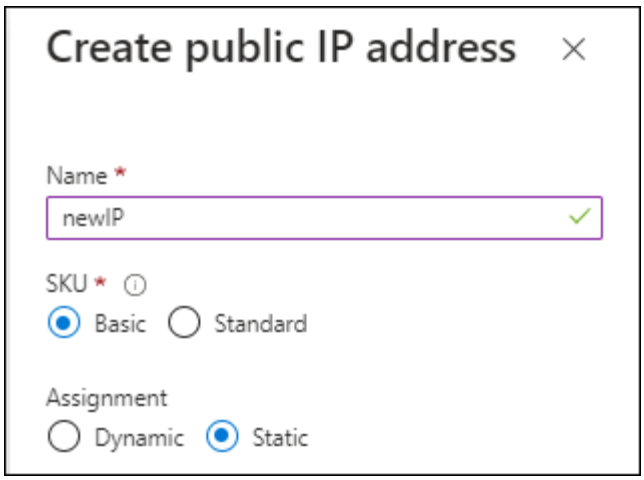
### Endpoints para operações diárias

Se você está planejando criar sistemas Cloud Volumes ONTAP, o conetor precisa de conetividade para endpoints nos recursos disponíveis publicamente do seu provedor de nuvem.

| Endpoints | Finalidade |
|---|---|
| Serviços da AWS (amazonaws.com):<br>• CloudFormation<br>• Nuvem de computação elástica (EC2)<br>• Gerenciamento de identidade e acesso (IAM)<br>• Key Management Service (KMS)<br>• Serviço de token de segurança (STS)<br>• Serviço de armazenamento simples (S3) | Para gerenciar recursos na AWS. O endpoint exato depende da região da AWS que você está usando. "Consulte a documentação da AWS para obter detalhes" |
| https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net | Para gerenciar recursos em regiões públicas do Azure. |
| https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud | Para gerenciar recursos na região do Azure IL6. |
| https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn | Para gerenciar recursos nas regiões do Azure China. |
| https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects | Para gerenciar recursos no Google Cloud. |

### Endereço IP público no Azure

Se você quiser usar um endereço IP público com a VM do conetor no Azure, o endereço IP deve usar uma SKU básica para garantir que o BlueXP  use esse endereço IP público.




Se você usar um endereço IP SKU padrão, o BlueXP usará o endereço IP *private* do conetor, em vez do IP público. Se a máquina que você está usando para acessar o Console do BlueXP não tiver acesso a esse endereço IP privado, as ações do Console do BlueXP falharão.

"Documentação do Azure: SKU IP público"

**Servidor proxy**

Se a sua empresa exigir a implantação de um servidor proxy para todo o tráfego de saída da Internet, obtenha as seguintes informações sobre o proxy HTTP ou HTTPS. Você precisará fornecer essas informações durante a instalação. Observe que o BlueXP não oferece suporte a servidores proxy transparentes.

- Endereço IP
- Credenciais
- Certificado HTTPS

  Com o modo privado, a única vez que o BlueXP envia tráfego de saída é para o seu provedor de nuvem para criar um sistema Cloud Volumes ONTAP.

**Portas**

Não há tráfego de entrada para o conetor, a menos que você o inicie.

HTTP (80) e HTTPS (443) fornecem acesso ao console BlueXP . SSH (22) só é necessário se você precisar se conetar ao host para solução de problemas.

**Ativar NTP**

Se estiver a planear utilizar a classificação BlueXP para analisar as suas fontes de dados empresariais, deve ativar um serviço de Protocolo de tempo de rede (NTP) no sistema de conetores BlueXP e no sistema de classificação BlueXP para que o tempo seja sincronizado entre os sistemas. "Saiba mais sobre a classificação BlueXP"

**Etapa 6: Preparar permissões na nuvem**

Se o conetor estiver instalado na nuvem e você estiver planejando criar sistemas Cloud Volumes ONTAP, o BlueXP precisará de permissões do seu provedor de nuvem. Você precisa configurar permissões no seu provedor de nuvem e associá-las à instância do Connector depois de instalá-la.

Para exibir as etapas necessárias, selecione a opção de autenticação que deseja usar para o provedor de

nuvem.

**Função do AWS IAM**

Use uma função do IAM para fornecer permissões ao conetor. Você precisará anexar manualmente a função à instância EC2 para o conetor.

**Passos**

1. Faça login no console da AWS e navegue até o serviço do IAM.
2. Criar uma política:
   a. Selecione **políticas > criar política**.
   b. Selecione **JSON** e copie e cole o conteúdo do "Política do IAM para o conetor".
   c. Conclua as etapas restantes para criar a política.
3. Crie uma função do IAM:
   a. Selecione **funções > criar função**.
   b. Selecione **AWS Service > EC2**.
   c. Adicione permissões anexando a política que você acabou de criar.
   d. Conclua as etapas restantes para criar a função.

**Resultado**

Agora você tem uma função do IAM para a instância do Connector EC2.

**Chave de acesso da AWS**

Configurar permissões e uma chave de acesso para um usuário do IAM. Você precisará fornecer à BlueXP a chave de acesso da AWS depois de instalar o conetor e configurar o BlueXP .

**Passos**

1. Faça login no console da AWS e navegue até o serviço do IAM.
2. Criar uma política:
   a. Selecione **políticas > criar política**.
   b. Selecione **JSON** e copie e cole o conteúdo do "Política do IAM para o conetor".
   c. Conclua as etapas restantes para criar a política.

      Dependendo dos serviços do BlueXP que você está planejando usar, talvez seja necessário criar uma segunda política.

   Para regiões padrão, as permissões são distribuídas em duas políticas. Duas políticas são necessárias devido a um limite máximo de tamanho de caractere para políticas gerenciadas na AWS. "Saiba mais sobre as políticas do IAM para o conetor".
3. Anexe as políticas a um usuário do IAM.
   - "Documentação da AWS: Criando funções do IAM"
   - "Documentação da AWS: Adicionando e removendo políticas do IAM"
4. Certifique-se de que o utilizador tem uma chave de acesso que pode adicionar ao BlueXP depois de instalar o conetor.

**Resultado**

A conta agora tem as permissões necessárias.

**Função do Azure**

Crie uma função personalizada do Azure com as permissões necessárias. Você atribuirá essa função à VM do conetor.

Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se você preferir usar um método diferente, consulte "Documentação do Azure"

**Passos**

1. Ative uma identidade gerenciada atribuída ao sistema na VM onde você planeja instalar o conetor para que você possa fornecer as permissões necessárias do Azure por meio de uma função personalizada.

   "Documentação do Microsoft Azure: Configure identidades gerenciadas para recursos do Azure em uma VM usando o portal do Azure"

2. Copie o conteúdo do "Permissões de função personalizadas para o conetor" e salve-o em um arquivo JSON.
3. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

   Você deve adicionar o ID para cada assinatura do Azure que deseja usar com o BlueXP .

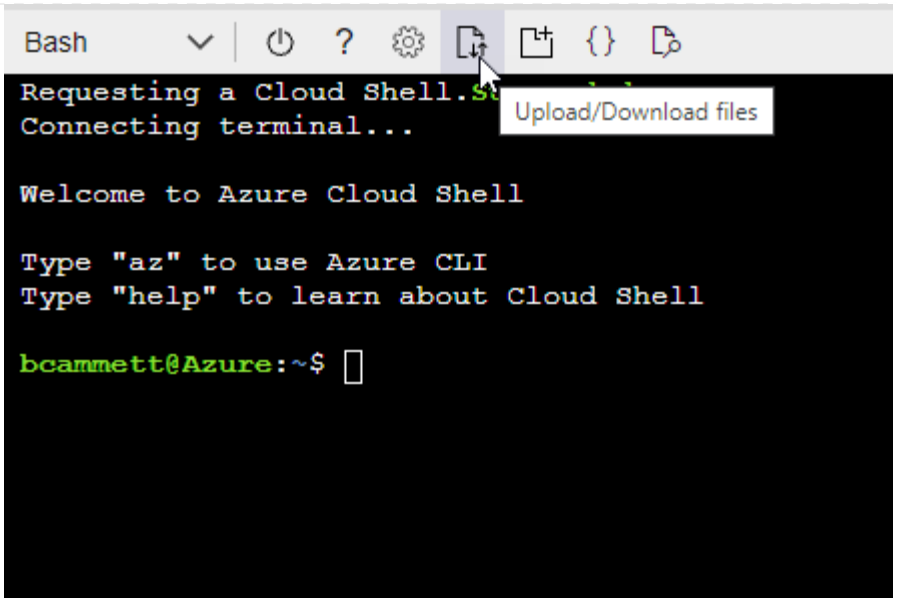
   **Exemplo**

   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

4. Use o arquivo JSON para criar uma função personalizada no Azure.

   As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

   a. Comece "Azure Cloud Shell" e escolha o ambiente Bash.
   b. Carregue o arquivo JSON.




c. Use a CLI do Azure para criar a função personalizada:

```
az role definition create --role-definition Connector_Policy.json
```

**Resultado**

Agora você deve ter uma função personalizada chamada Operador BlueXP  que você pode atribuir à máquina virtual do conetor.

**Diretor de serviço do Azure**

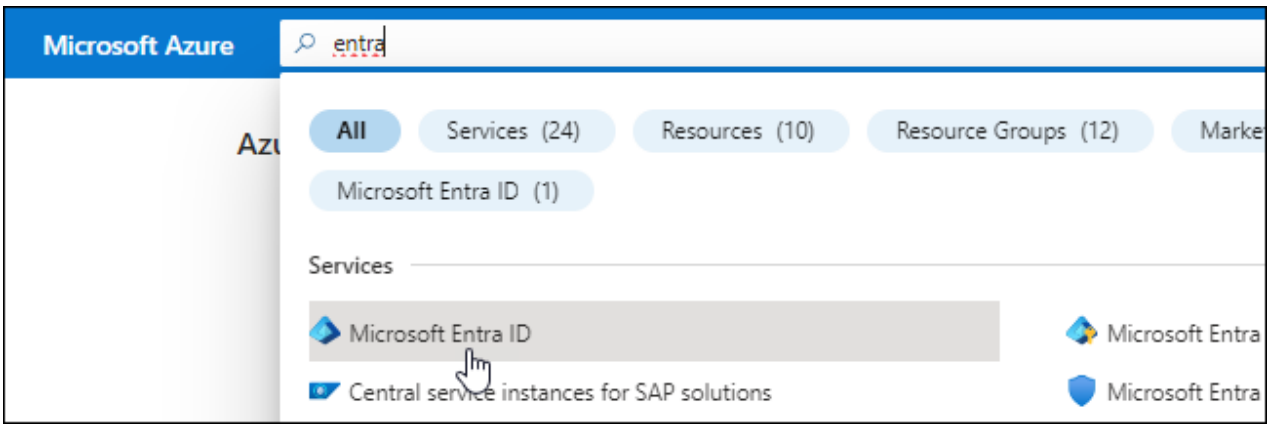
Crie e configure um princípio de serviço no Microsoft Entra ID e obtenha as credenciais do Azure de que o BlueXP  precisa. Você precisará fornecer essas credenciais ao BlueXP  depois de instalar o conetor e configurar o BlueXP .

**Crie um aplicativo Microsoft Entra para controle de acesso baseado em funções**

1. Certifique-se de ter permissões no Azure para criar um aplicativo do ative Directory e atribuir o aplicativo a uma função.

   Para obter mais informações, consulte "Documentação do Microsoft Azure: Permissões necessárias"

2. No portal do Azure, abra o serviço **Microsoft Entra ID**.



3. No menu, selecione **inscrições de aplicativos**.
4. Selecione **novo registo**.
5. Especifique detalhes sobre o aplicativo:
   - **Nome**: Insira um nome para o aplicativo.
   - **Tipo de conta**: Selecione um tipo de conta (qualquer funcionará com o BlueXP ).
   - * URI de redirecionamento*: Você pode deixar este campo em branco.
6. Selecione **Registe-se**.

   Você criou o aplicativo AD e o principal de serviço.

**Atribua a aplicação a uma função**

1. Crie uma função personalizada:

   Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se você preferir usar um método diferente, consulte "Documentação do Azure"

   a. Copie o conteúdo do "Permissões de função personalizadas para o conetor" e salve-o em um arquivo JSON.

   b. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

      Você deve adicionar o ID para cada assinatura do Azure a partir da qual os usuários criarão sistemas Cloud Volumes ONTAP.

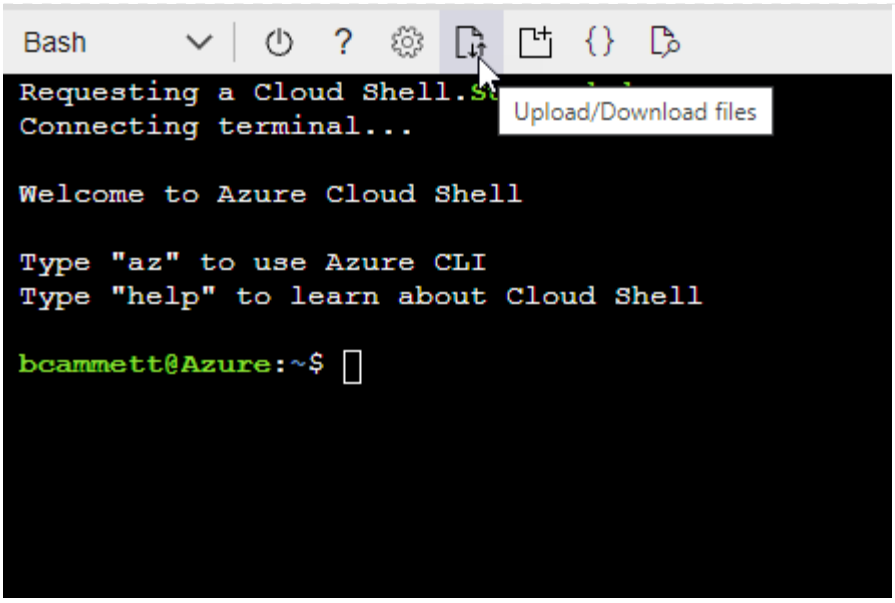
      **Exemplo**

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ```

   c. Use o arquivo JSON para criar uma função personalizada no Azure.

      As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

      - Comece "Azure Cloud Shell" e escolha o ambiente Bash.
      - Carregue o arquivo JSON.




- Use a CLI do Azure para criar a função personalizada:

```
az role definition create --role-definition
Connector_Policy.json
```

Agora você deve ter uma função personalizada chamada Operador BlueXP  que você pode atribuir à máquina virtual do conetor.

2. Atribua o aplicativo à função:

   a. No portal do Azure, abra o serviço **Subscrições**.

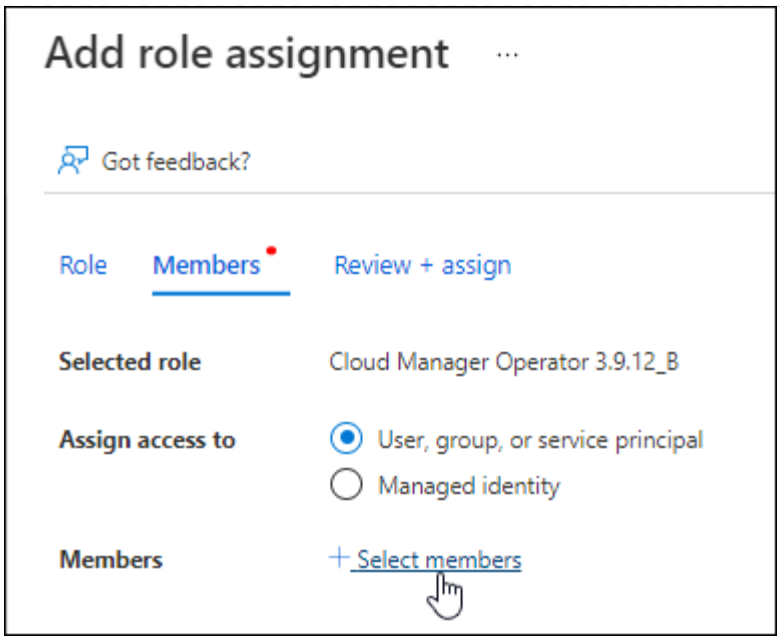
   b. Selecione a subscrição.

   c. Selecione **Access Control (IAM) > Add > Add > Add Role assignment** (Adicionar controlo de acesso).

   d. Na guia **função**, selecione a função **Operador BlueXP**  e selecione **seguinte**.

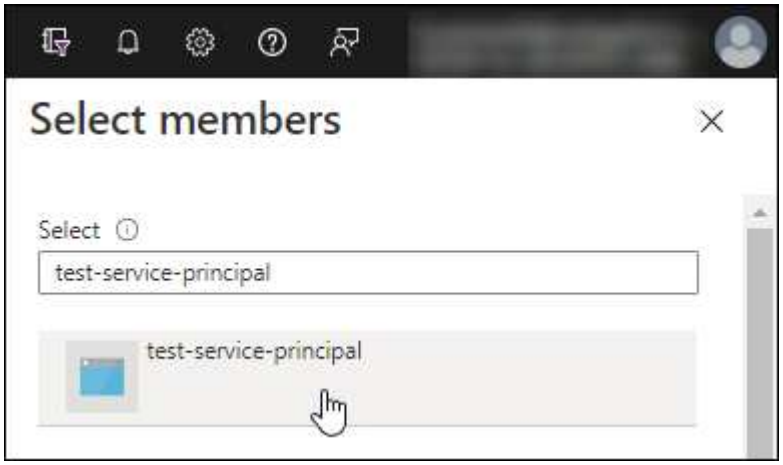
   e. Na guia **Membros**, execute as seguintes etapas:

      - Mantenha **Usuário, grupo ou responsável do serviço** selecionado.
      - Selecione **Selecionar membros**.




- Procure o nome da aplicação.

  Aqui está um exemplo:




- Selecione a aplicação e selecione **Select**.
- Selecione **seguinte**.

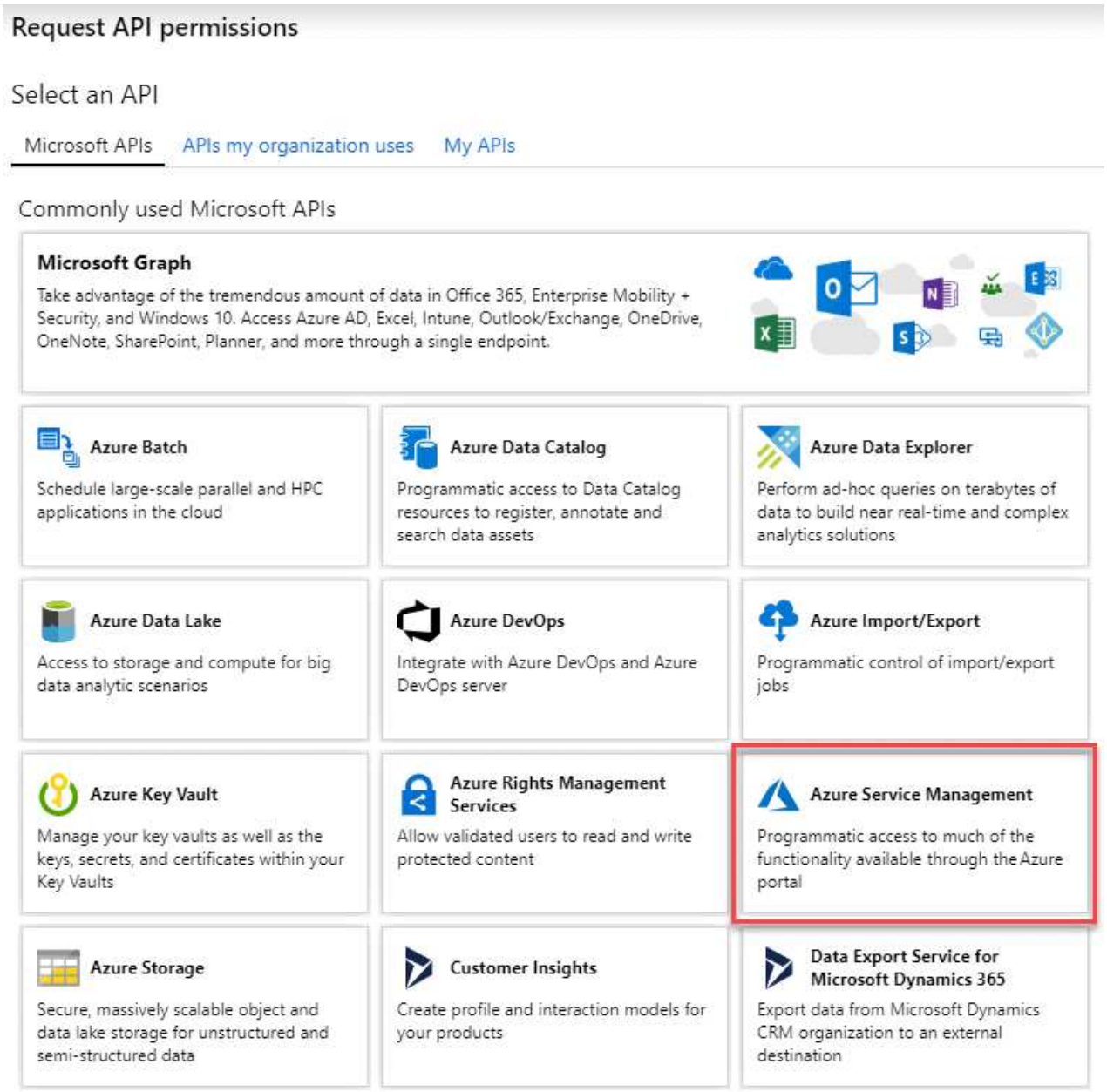
f. Selecione **Rever e atribuir**.

O principal de serviço agora tem as permissões necessárias do Azure para implantar o conetor.

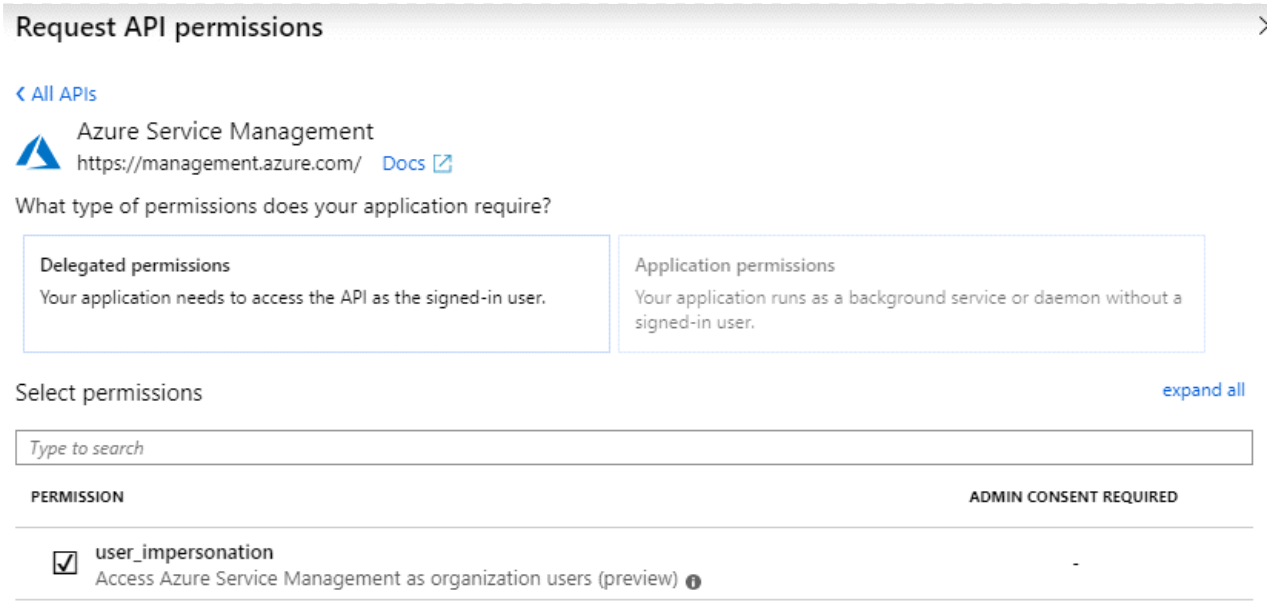
Se você quiser implantar o Cloud Volumes ONTAP a partir de várias assinaturas do Azure, então você deve vincular o principal de serviço a cada uma dessas assinaturas. O BlueXP  permite que você selecione a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

**Adicione permissões da API de Gerenciamento de Serviços do Windows Azure**

1. No serviço **Microsoft Entra ID**, selecione **inscrições de aplicativos** e selecione o aplicativo.
2. Selecione **permissões de API > Adicionar uma permissão**.
3. Em **Microsoft APIs**, selecione **Azure Service Management**.

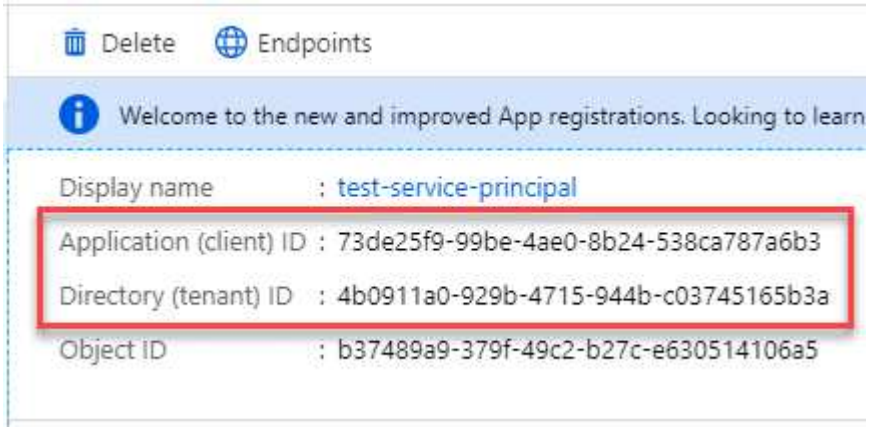



4. Selecione **Acesse o Gerenciamento de Serviços do Azure como usuários da organização** e selecione **Adicionar permissões**.




**Obtenha o ID do aplicativo e o ID do diretório para o aplicativo**

1. No serviço **Microsoft Entra ID**, selecione **inscrições de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.




Quando você adiciona a conta do Azure ao BlueXP , você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O BlueXP  usa os IDs para fazer login programaticamente.

**Crie um segredo de cliente**

1. Abra o serviço **Microsoft Entra ID**.
2. Selecione **inscrições de aplicativos** e selecione sua inscrição.
3. Selecione **certificados e segredos > segredo de novo cliente**.
4. Forneça uma descrição do segredo e uma duração.
5. Selecione **Adicionar**.
6. Copie o valor do segredo do cliente.


Agora você tem um segredo de cliente que o BlueXP pode usá-lo para autenticar com o Microsoft Entra ID.

**Resultado**

Seu responsável de serviço está configurado e você deve ter copiado o ID do aplicativo (cliente), o ID do diretório (locatário) e o valor do segredo do cliente. Você precisa inserir essas informações no BlueXP ao adicionar uma conta do Azure.

**Conta de serviço do Google Cloud**

Crie uma função e aplique-a a uma conta de serviço que você usará para a instância de VM Connector.

**Passos**

1. Crie uma função personalizada no Google Cloud:

   a. Crie um arquivo YAML que inclua as permissões definidas no "Política de conetores para Google Cloud".

   b. No Google Cloud, ative o shell da nuvem.

   c. Carregue o arquivo YAML que inclui as permissões necessárias para o conetor.

   d. Crie uma função personalizada usando o `gcloud iam roles create` comando.

      O exemplo a seguir cria uma função chamada "Connector" no nível do projeto:

```
gcloud iam roles create connector --project=myproject
--file=connector.yaml
```

   +
   "Google Cloud docs: Criando e gerenciando funções personalizadas"

2. Crie uma conta de serviço no Google Cloud:

   a. No serviço IAM e Admin, selecione **Contas de serviço > criar conta de serviço**.

   b. Insira os detalhes da conta de serviço e selecione **criar e continuar**.

   c. Selecione a função que você acabou de criar.

   d. Conclua as etapas restantes para criar a função.

      "Google Cloud docs: Criando uma conta de serviço"

**Resultado**

Agora você tem uma conta de serviço que pode atribuir à instância de VM Connector.

#### Etapa 7: Habilite as APIs do Google Cloud

Várias APIs são necessárias para implantar o Cloud Volumes ONTAP no Google Cloud.

**Passo**

1. "Ative as seguintes APIs do Google Cloud em seu projeto"
    - API do Cloud Deployment Manager V2
    - API Cloud Logging
    - API do Cloud Resource Manager
    - API do mecanismo de computação
    - API de gerenciamento de identidade e acesso (IAM)
    - API do Cloud Key Management Service (KMS)

      (Necessário somente se você estiver planejando usar o backup e a recuperação do BlueXP com chaves de criptografia gerenciadas pelo cliente (CMEK))

## Implante o conetor no modo privado

Implante o conetor no modo privado para que você possa usar o BlueXP sem conetividade de saída à camada de software como serviço (SaaS) da BlueXP . Para começar, instale o conetor, configure o BlueXP acessando a interface do usuário que está sendo executada no conetor e, em seguida, forneça as permissões de nuvem que você configurou anteriormente.

#### Passo 1: Instale o conetor

Baixe o instalador do produto no site de suporte da NetApp e instale manualmente o conetor em seu próprio host Linux.

Se quiser usar o BlueXP no "Nuvem secreta da AWS" ou no "Nuvem secreta principal da AWS", siga instruções separadas para começar nesses ambientes. "Saiba como começar a usar o Cloud Volumes ONTAP na nuvem secreta da AWS ou na nuvem secreta principal"

**Antes de começar**

- Os Privileges raiz são necessários para instalar o conetor.
- Dependendo do seu sistema operacional, o Podman ou o Docker Engine são necessários antes de instalar o conetor.

**Passos**

1. Transfira o software do conetor a partir do "Site de suporte da NetApp"

   Certifique-se de baixar o instalador offline para redes privadas sem acesso à Internet.

2. Copie o instalador para o host Linux.
3. Atribua permissões para executar o script.

```
chmod +x /path/BlueXP-Connector-offline-<version>
```

Onde <version> é a versão do conetor que você baixou.

4. Execute o script de instalação:

```
sudo /path/BlueXP-Connector-offline-<version>
```

Onde <version> é a versão do conetor que você baixou.

**Resultado**

O software do conetor está instalado. Agora você pode configurar o BlueXP .

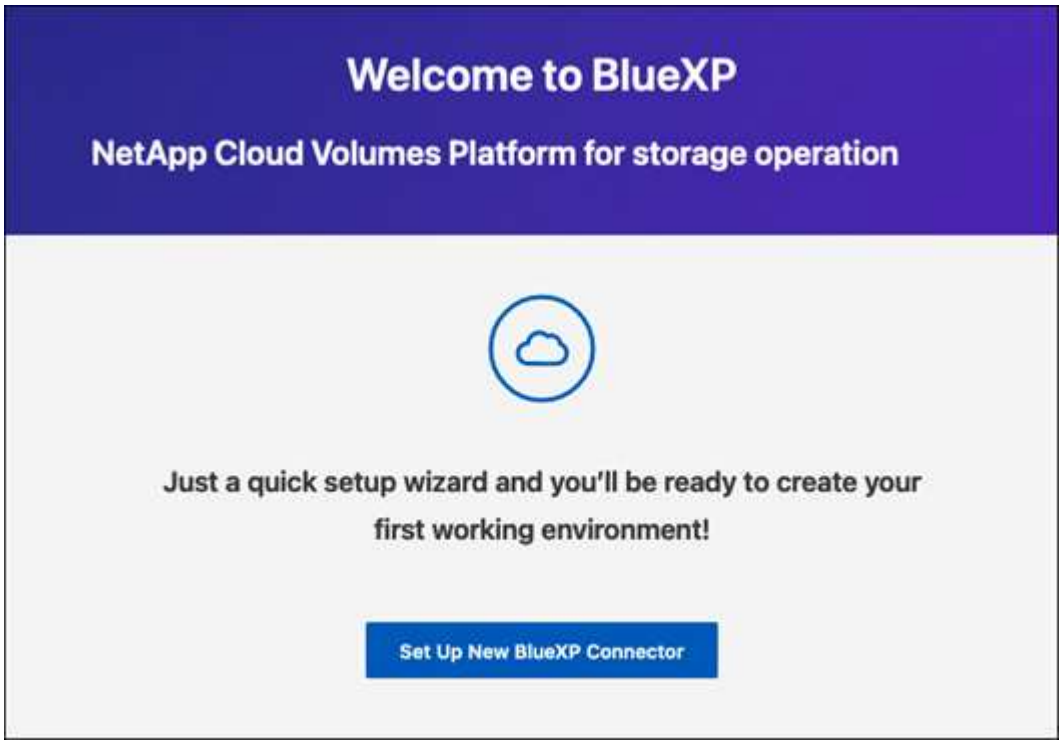
### Passo 2: Configurar o BlueXP

Ao acessar o console BlueXP  pela primeira vez, você será solicitado a configurar o BlueXP .

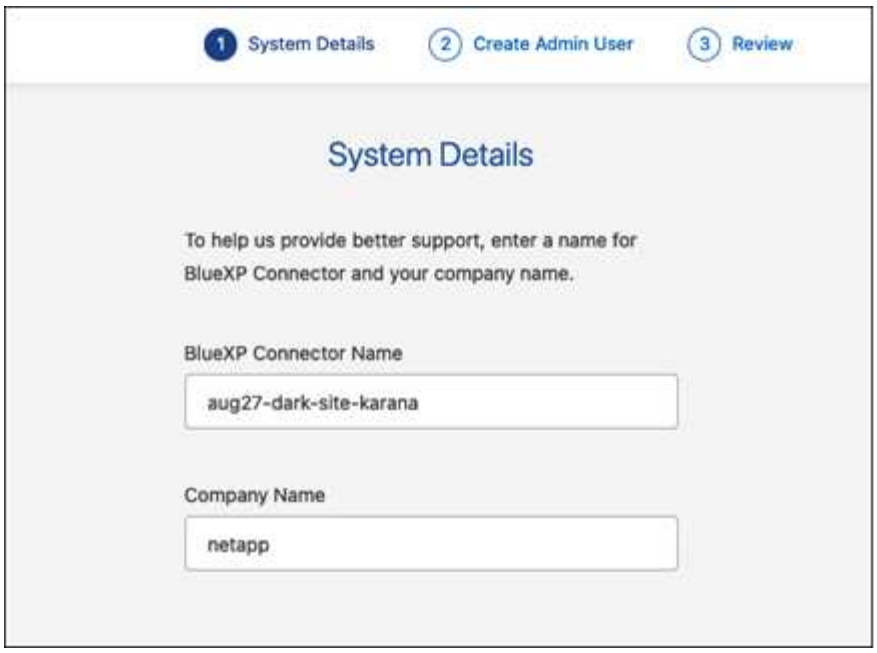
**Passos**

1. Abra um navegador da Web e digite <a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a> onde <em>ipaddress</em> é o endereço IP do host Linux onde você instalou o conetor.

   Você deve ver a seguinte tela.




2. Selecione **Configurar novo conetor BlueXP**  e siga as instruções para configurar o sistema.
   - **Detalhes do sistema**: Insira um nome para o conetor e o nome da sua empresa.




- **Criar um usuário Admin**: Crie o usuário admin para o sistema.

  Esta conta de utilizador é executada localmente no sistema. Não há conexão com o serviço auth0 disponível através do BlueXP .

- **Revisão**: Revise os detalhes, aceite o contrato de licença e selecione **Configurar**.

3. Faça login no BlueXP  usando o usuário admin que você acabou de criar.

**Resultado**

O conetor está agora instalado e configurado.

Quando novas versões do software Connector estiverem disponíveis, elas serão postadas no site de suporte da NetApp. "Saiba como atualizar o conetor".

**O que se segue?**

Forneça ao BlueXP  as permissões que você configurou anteriormente.

### Passo 3: Forneça permissões para o BlueXP

Se você quiser criar ambientes de trabalho do Cloud Volumes ONTAP, precisará fornecer ao BlueXP  as permissões de nuvem que você configurou anteriormente.

"Saiba como preparar permissões na nuvem".

**Função do AWS IAM**

Anexe a função do IAM que você criou anteriormente à instância do Connector EC2.

**Passos**

1. Vá para o console do Amazon EC2.
2. Selecione **instâncias**.
3. Selecione a instância do conetor.
4. Selecione **ações > Segurança > Modificar função do IAM**.
5. Selecione a função do IAM e selecione **Atualizar função do IAM**.

**Resultado**

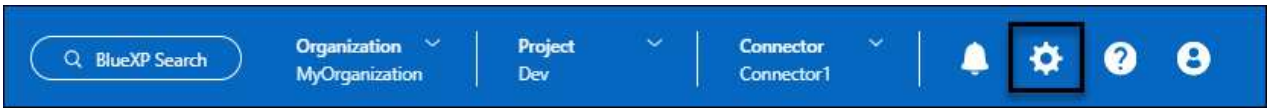
O BlueXP  agora tem as permissões necessárias para executar ações na AWS em seu nome.

**Chave de acesso da AWS**

Forneça ao BlueXP  a chave de acesso da AWS para um usuário do IAM que tenha as permissões necessárias.

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.




2. Selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Localização das credenciais**: Selecione **Amazon Web Services > Connector**.
   b. **Definir credenciais**: Insira uma chave de acesso da AWS e uma chave secreta.
   c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.
   d. **Revisão**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

**Resultado**

O BlueXP  agora tem as permissões necessárias para executar ações na AWS em seu nome.

**Função do Azure**

Vá para o portal do Azure e atribua a função personalizada do Azure à máquina virtual Connector para uma ou mais subscrições.

**Passos**

1. No Portal do Azure, abra o serviço **Subscrições** e selecione a sua subscrição.

   É importante atribuir a função do serviço **Subscrições** porque especifica o escopo da atribuição de função no nível da assinatura. O *scope* define o conjunto de recursos aos quais o acesso se aplica. Se você especificar um escopo em um nível diferente (por exemplo, no nível da máquina virtual), sua capacidade de concluir ações de dentro do BlueXP  será afetada.

   "Documentação do Microsoft Azure: Entenda o escopo do Azure RBAC"

2. Selecione **Access control (IAM)** > **Add** > **Add** > **Add role assignment**.
3. Na guia **função**, selecione a função **Operador BlueXP** e selecione **seguinte**.

   Operador BlueXP é o nome padrão fornecido na política BlueXP . Se você escolher um nome diferente para a função, selecione esse nome em vez disso.

4. Na guia **Membros**, execute as seguintes etapas:
   a. Atribua acesso a uma **identidade gerenciada**.
   b. Selecione **Selecionar membros**, selecione a assinatura na qual a máquina virtual do conetor foi criada, em **identidade gerenciada**, escolha **Máquina Virtual** e, em seguida, selecione a máquina virtual do conetor.
   c. Selecione **Selecionar**.
   d. Selecione **seguinte**.
   e. Selecione **Rever e atribuir**.
   f. Se você quiser gerenciar recursos em assinaturas adicionais do Azure, mude para essa assinatura e repita essas etapas.

**Resultado**

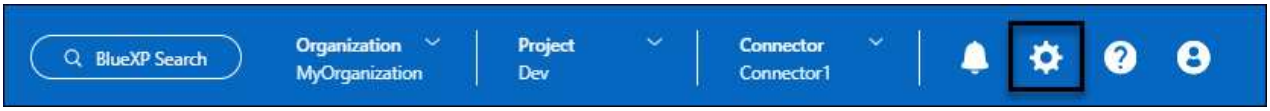
O BlueXP agora tem as permissões necessárias para executar ações no Azure em seu nome.

**Diretor de serviço do Azure**

Forneça ao BlueXP as credenciais para o responsável de serviço do Azure que você configurou anteriormente.

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.




2. Selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Credentials Location**: Selecione **Microsoft Azure > Connector**.
   b. **Definir credenciais**: Insira informações sobre o responsável do serviço Microsoft Entra que concede as permissões necessárias:
      - ID da aplicação (cliente)
      - ID do diretório (locatário)
      - Segredo Cliente
   c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.
   d. **Revisão**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

**Resultado**

O BlueXP agora tem as permissões necessárias para executar ações no Azure em seu nome.

**Conta de serviço do Google Cloud**

Associe a conta de serviço à VM do conetor.

**Passos**

1. Vá para o portal do Google Cloud e atribua a conta de serviço à instância da VM Connector.

   "Documentação do Google Cloud: Alterando a conta de serviço e os escopos de acesso para uma instância"

2. Se você quiser gerenciar recursos em outros projetos, conceda acesso adicionando a conta de serviço com a função BlueXP  a esse projeto. Você precisará repetir esta etapa para cada projeto.

**Resultado**

O BlueXP  agora tem as permissões necessárias para executar ações no Google Cloud em seu nome.

### O que você pode fazer a seguir (modo privado)

Depois de iniciar e executar com o BlueXP  no modo privado, você pode começar a usar os serviços do BlueXP  que são compatíveis com o modo privado.

Para obter ajuda, consulte a seguinte documentação:

- "Criar sistemas Cloud Volumes ONTAP"
- "Descubra clusters ONTAP no local"
- "Replique dados"
- "Analise dados de volume ONTAP on-premise usando a classificação BlueXP "
- "Fazer backup de dados de volume do ONTAP no local para o StorageGRID usando o backup e a recuperação do BlueXP "

**Link relacionado**

"Modos de implantação do BlueXP"

# Inicie sessão no BlueXP

A forma como inicia sessão no BlueXP  depende do modo de implementação do BlueXP que está a utilizar para a sua conta.

O conetor inclui uma IU local, acessível a partir do host do conetor. Esta interface de usuário é fornecida para clientes que estão usando o BlueXP  no modo restrito ou no modo privado. Quando utilizar o BlueXP  no modo padrão, deve aceder à interface do utilizador a partir do "Console BlueXP  SaaS"

"Saiba mais sobre os modos de implantação do BlueXP".

**Modo padrão**

Depois de se inscrever no BlueXP , você poderá fazer login no console baseado na Web para começar a gerenciar sua infraestrutura de dados e armazenamento.

**Sobre esta tarefa**

Você pode fazer login no console baseado na Web do BlueXP  usando uma das seguintes opções:

- Suas credenciais existentes do site de suporte da NetApp (NSS)
- Um login na nuvem do NetApp usando seu endereço de e-mail e uma senha
- Uma conexão federada

  Você pode usar o logon único para fazer login usando credenciais de seu diretório corporativo (identidade federada). "Saiba como usar a federação de identidade com o BlueXP ".

**Passos**

1. Abra um navegador da Web e aceda ao "Consola BlueXP"
2. Na página **Log in**, insira o endereço de e-mail associado ao seu login.
3. Dependendo do método de autenticação associado ao seu login, você será solicitado a inserir suas credenciais:
   - Credenciais de nuvem do NetApp: Insira sua senha
   - Usuário federado: Insira suas credenciais de identidade federada
   - Conta do site de suporte da NetApp: Insira suas credenciais do site de suporte da NetApp

**Resultado**

Agora você está logado e pode começar a usar o BlueXP  para gerenciar sua infraestrutura multicloud híbrida.

**Modo restrito**

Quando você usa o BlueXP  no modo restrito, você precisa fazer login no console do BlueXP  a partir da interface do usuário que é executada localmente no conetor.

**Sobre esta tarefa**

O BlueXP  oferece suporte ao login com uma das seguintes opções quando sua conta está configurada no modo restrito:

- Um login na nuvem do NetApp usando seu endereço de e-mail e uma senha
- Uma conexão federada

  Você pode usar o logon único para fazer login usando credenciais de seu diretório corporativo (identidade federada). "Saiba como usar a federação de identidade com o BlueXP ".

**Passos**

1. Abra um navegador da Web e insira o seguinte URL:

   <a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

   *Ipaddress* pode ser localhost, um endereço IP privado ou um endereço IP público, dependendo da configuração do host onde você instalou o conetor. Por exemplo, talvez seja necessário inserir um

endereço IP privado de um host que tenha uma conexão com o host do conetor.

2. Introduza o seu nome de utilizador e palavra-passe para iniciar sessão.

**Resultado**

Agora você está logado e pode começar a usar o BlueXP  para gerenciar sua infraestrutura multicloud híbrida.

**Modo privado**

Quando você usa o BlueXP  no modo privado, você precisa fazer login no console do BlueXP  a partir da interface do usuário que é executada localmente no conetor.

**Sobre esta tarefa**

O modo privado suporta a gestão e o acesso de utilizadores locais. A autenticação não é fornecida através do serviço de nuvem da BlueXP .

**Passos**

1. Abra um navegador da Web e insira o seguinte URL:

   <a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

   *Ipaddress* pode ser localhost, um endereço IP privado ou um endereço IP público, dependendo da configuração do host onde você instalou o conetor. Por exemplo, talvez seja necessário inserir um endereço IP privado de um host que tenha uma conexão com o host do conetor.

2. Introduza o seu nome de utilizador e palavra-passe para iniciar sessão.

**Resultado**

Agora você está logado e pode começar a usar o BlueXP  para gerenciar sua infraestrutura multicloud híbrida.

# Administrar o BlueXP

## Gerenciamento de identidade e acesso

### Saiba mais sobre o gerenciamento de identidades e acesso do BlueXP

O BlueXP  Identity and Access Management (IAM) permite organizar e controlar o acesso aos seus recursos do NetApp. Você pode organizar seus recursos de acordo com a hierarquia da sua organização. Por exemplo, você pode organizar recursos por localização geográfica, local ou unidade de negócios. Em seguida, você pode atribuir permissões a membros em partes específicas da hierarquia, o que impede o acesso a recursos em outras partes da hierarquia.

O BlueXP  IAM substitui e aprimora a funcionalidade anterior fornecida pelas contas do BlueXP . "Saiba mais sobre a introdução do BlueXP  IAM".

O BlueXP  IAM é suportado ao usar o BlueXP  no modo padrão. Se você estiver usando o BlueXP  no modo restrito ou privado, use uma conta *BlueXP*  para gerenciar usuários e recursos.

- "Saiba mais sobre as contas do BlueXP "
- "Saiba mais sobre os modos de implantação do BlueXP"

#### Como o BlueXP  IAM funciona

O BlueXP  IAM permite que você conceda acesso aos recursos da sua organização, definindo quais membros têm permissões para partes específicas da hierarquia da organização. Por exemplo, um membro pode ter permissões de administrador de projeto para um projeto que tenha cinco recursos associados.

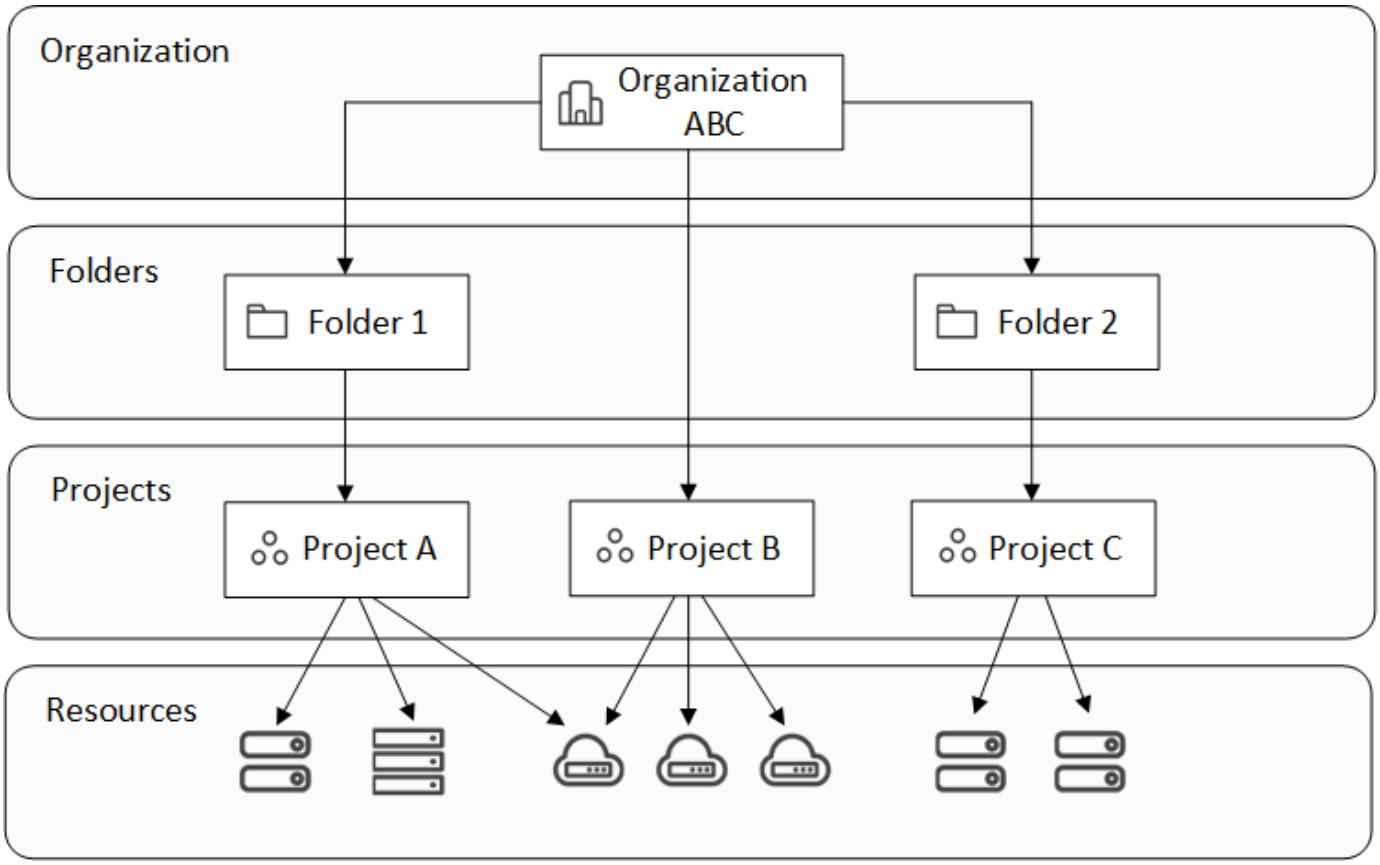
Ao usar o BlueXP  IAM, você gerenciará os seguintes componentes:

- A organização
- Pastas
- Projetos
- Recursos
- Membros
- Funções e permissões
- Conetores

Os recursos do BlueXP  são organizados hierarquicamente:

- A organização é o topo da hierarquia.
- Pastas são filhos da organização ou de outra pasta.
- Os projetos são filhos da organização ou de uma pasta.
- Os recursos estão associados a uma ou mais pastas ou projetos.

A imagem a seguir ilustra essa hierarquia em um nível básico.




**Organização**

Uma *organização* é o nível superior do sistema IAM da BlueXP  e normalmente representa a sua empresa. Sua organização consiste em pastas, projetos, membros, funções e recursos. Os conetores estão associados a projetos específicos na organização.

Ao se inscrever no BlueXP , você será solicitado a criar uma nova organização.

**Pastas**

Uma *folder* permite agrupar projetos relacionados e separá-los de outros projetos em sua organização. Por exemplo, uma pasta pode representar uma localização geográfica (UE ou Leste dos EUA), um site (Londres ou Toronto) ou uma unidade de negócios (engenharia ou marketing).

As pastas podem conter projetos, outras pastas ou uma combinação de ambos.

Você não precisa criar pastas. Eles são opcionais.

**Projetos**

Um *project* representa um espaço de trabalho no BlueXP  que os membros da organização acessam a partir da tela BlueXP  para gerenciar recursos. Por exemplo, um projeto pode incluir um sistema Cloud Volumes ONTAP, um cluster ONTAP no local ou um sistema de arquivos FSX for ONTAP.

Uma organização pode ter um ou muitos projetos. Um projeto pode residir diretamente abaixo da organização ou dentro de uma pasta.

#### Recursos

Um *resource* é um ambiente de trabalho que você criou ou descobriu no BlueXP .

Quando você cria ou descobre um recurso, o recurso é associado ao projeto selecionado atualmente. Esse pode ser o único projeto com o qual você deseja associar esse recurso. Mas você pode optar por associar o recurso a projetos adicionais em sua organização.

Por exemplo, você pode associar um sistema Cloud Volumes ONTAP a um projeto adicional ou a todos os projetos em sua organização. A forma como você associa um recurso depende das necessidades da sua organização.

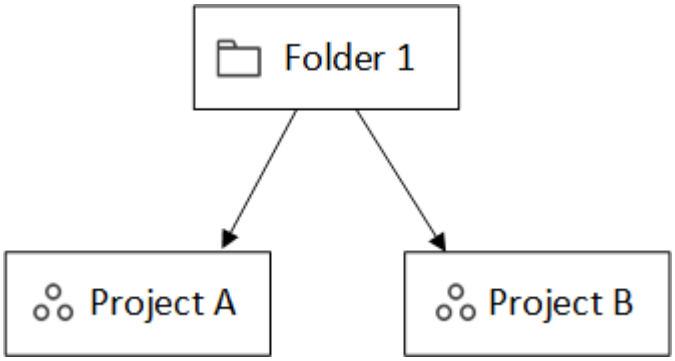
Você também pode associar um conetor a outra pasta ou projeto em sua organização. Saiba mais sobre como usar conetores com o BlueXP  IAM.

#### Quando associar um recurso a uma pasta

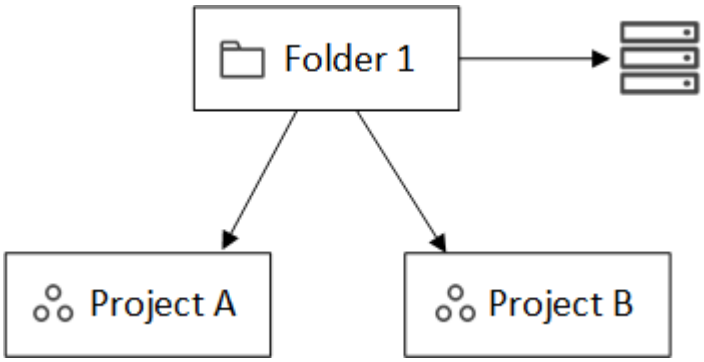
Você também tem a opção de associar um recurso a uma pasta, mas isso é opcional e atende às necessidades de um caso de uso específico.

Um *administrador da organização* pode associar um recurso a uma pasta para que um *Folder ou administrador de projeto* possa associar esse recurso aos projetos apropriados que residem na pasta.

Por exemplo, digamos que você tem uma pasta que contém dois projetos:

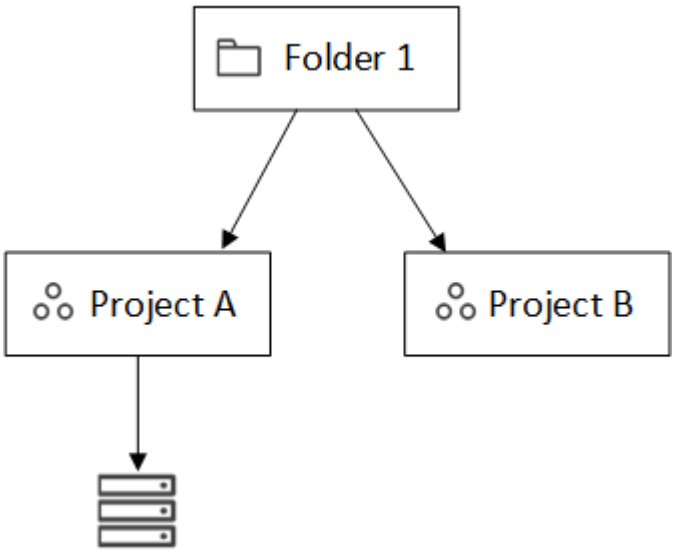



O *Organization admin* pode associar um recurso à pasta:




Associar o recurso à pasta não torna esse recurso automaticamente acessível a partir de todos os projetos na pasta. Mas a *pasta ou o administrador do projeto* pode então decidir para quais projetos esse recurso deve ser disponibilizado. Depois de tomar essa decisão, o administrador pode então associar o recurso aos projetos certos.

Neste exemplo, o administrador associa o recurso ao Projeto A:




Os membros que têm permissões para o projeto A agora podem acessar o recurso.

#### Membros

Os membros da sua organização são contas de utilizador ou contas de serviço. Uma conta de serviço é normalmente usada por um aplicativo para concluir tarefas especificadas sem intervenção humana.

Uma organização tem pelo menos um usuário com a função *Organization admin* (o usuário que cria a organização recebe essa função automaticamente). Você pode adicionar outros membros à organização e atribuir permissões diferentes em diferentes níveis da hierarquia de recursos.

#### Funções e permissões

No BlueXP  IAM, você não concede permissões diretamente aos membros da organização. Em vez disso, você concede a cada membro uma função. Uma função contém um conjunto de permissões que permite que um membro execute ações específicas em um nível específico da hierarquia de recursos.

Ao fornecer permissões em uma parte específica da hierarquia de recursos, você pode restringir os direitos de acesso apenas aos recursos que um membro precisa para concluir suas tarefas.

### Onde você pode atribuir funções na hierarquia

Quando você associa um membro a uma função, você precisa selecionar toda a organização, uma pasta específica ou um projeto específico. A função selecionada dá a um membro permissões para os recursos na parte selecionada da hierarquia.

### Herança de função

Quando você atribui uma função, a função é herdada pela hierarquia da organização:

**Organização**
: As funções que você concede no nível da organização são herdadas por todas as pastas, projetos e recursos da organização. Isso significa que o membro tem permissões para tudo na organização.

**Pastas**

As funções que você concede no nível da pasta são herdadas por todas as pastas, projetos e recursos na pasta.

Por exemplo, se você atribuir uma função no nível da pasta e essa pasta tiver três projetos, o membro terá permissões para esses três projetos e quaisquer recursos associados.

**Projetos**

As funções que você concede no nível do projeto são herdadas por todos os recursos associados a esse projeto.

### Várias funções

Você pode atribuir a cada membro da organização uma função em diferentes níveis da hierarquia da organização. Pode ser o mesmo papel ou um papel diferente. Por exemplo, você pode atribuir uma função de membro A para o projeto 1 e o projeto 2. Ou você pode atribuir uma função de membro A para o projeto 1 e a função B para o projeto 2.

### Funções predefinidas

O BlueXP  suporta várias funções predefinidas que podem ser atribuídas aos membros da sua organização.

"Saiba mais sobre as funções predefinidas do IAM".

#### Conetores

Quando um *administrador da organização* cria um conetor, o BlueXP  associa automaticamente esse conetor à organização e ao projeto atualmente selecionado. O *Organization admin* tem acesso automaticamente a esse conetor de qualquer lugar da organização. Mas se você tiver outros membros em sua organização com funções diferentes, esses membros só poderão acessar esse conetor do projeto em que ele foi criado, a menos que você associe esse conetor a outros projetos.

Você pode querer disponibilizar um conetor para uso com outro projeto nos seguintes casos:

- Você deseja permitir que os membros da sua organização usem um conetor existente para criar ou descobrir ambientes de trabalho adicionais em outro projeto
- Você associou um recurso existente a outro projeto e esse recurso é gerenciado por um conetor

  Se um recurso associado a um projeto adicional for descoberto usando um conetor BlueXP , você também precisará associar o conetor ao projeto ao qual o recurso está agora associado. Caso contrário, o conetor e seu recurso associado não são acessíveis a partir da tela do BlueXP  por membros que não têm a função *administrador da organização*.

Você pode criar uma associação a partir da página **Connectors** no BlueXP  IAM:

- Associar um conetor a um projeto

  Quando você associa um conetor a um projeto, esse conetor é acessível a partir da tela BlueXP  ao visualizar o projeto.

- Associar um conetor a uma pasta

  Associar um conetor a uma pasta não torna esse conetor acessível automaticamente a partir de todos os projetos na pasta. Os membros da organização não podem acessar um conetor de um projeto até que

você associe o conetor a esse projeto específico.

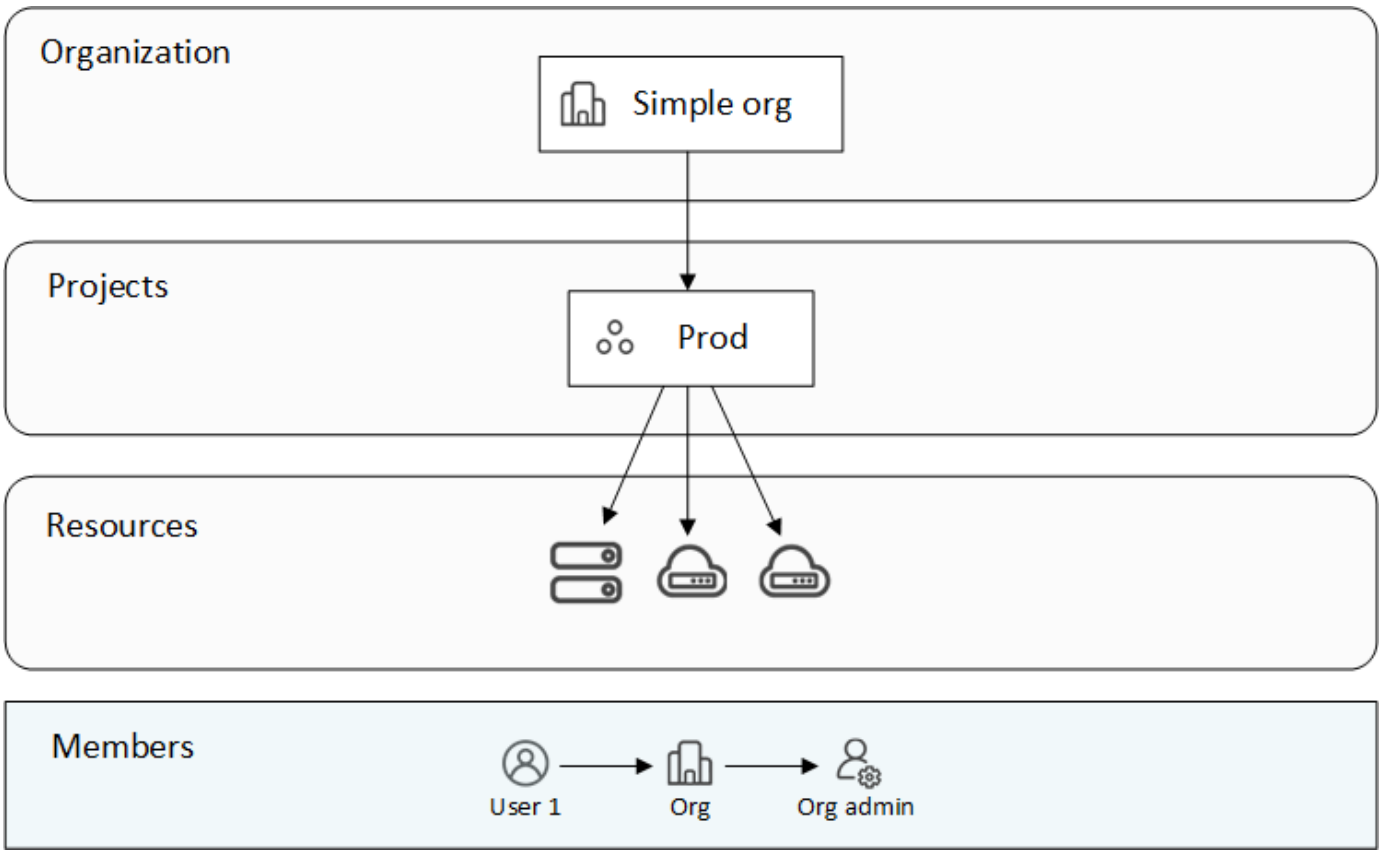
Um *administrador da organização* pode associar um conetor a uma pasta para que o *Folder ou o administrador do projeto* possa tomar a decisão de associar esse conetor aos projetos apropriados que residem na pasta.

## Exemplos do IAM

Os exemplos a seguir mostram como você pode configurar sua organização.

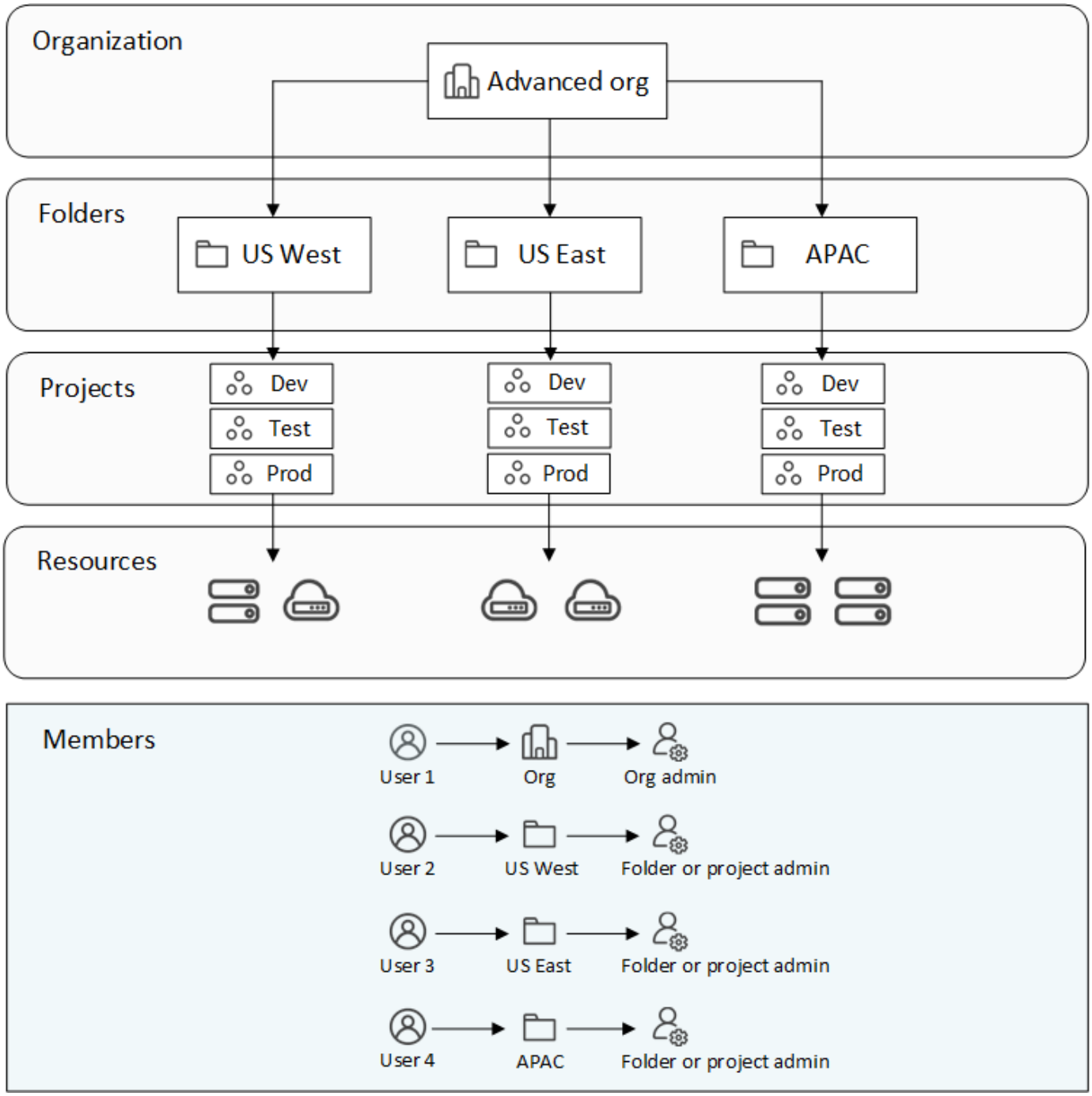
#### Organização simples

O diagrama a seguir mostra um exemplo simples de uma organização que usa o projeto padrão e nenhuma pasta. Um único membro gerencia toda a organização.




#### Organização avançada

O diagrama a seguir mostra uma organização que usa pastas para organizar os projetos para cada localização geográfica na empresa. Cada projeto tem seu próprio conjunto de recursos associados. Os membros incluem um administrador da organização e um administrador para cada pasta na organização.




**O que você pode fazer com o BlueXP  IAM**

Os exemplos a seguir descrevem como você pode usar o IAM para gerenciar sua organização do BlueXP :

- Conceda funções específicas a membros específicos para que eles possam apenas concluir as tarefas necessárias.
- Modifique as permissões dos membros porque mudaram de departamentos ou porque têm responsabilidades adicionais.
- Remova um usuário que deixou a empresa.
- Adicione pastas ou projetos à sua hierarquia porque uma nova unidade de negócios adicionou armazenamento NetApp.

- Associar um recurso a outro projeto porque esse recurso tem capacidade que outra equipe pode utilizar.
- Veja os recursos que um membro pode acessar.
- Veja os membros e recursos associados a um projeto específico.

**Onde ir a seguir**

- "Comece a usar o BlueXP  IAM"
- "Organize seus recursos no BlueXP  com pastas e projetos"
- "Gerenciar membros do BlueXP  e suas permissões"
- "Gerencie a hierarquia de recursos em sua organização do BlueXP "
- "Associar conetores a pastas e projetos"
- "Alterne entre projetos e organizações da BlueXP "
- "Renomeie sua organização do BlueXP "
- "Monitorar ou auditar a atividade do IAM"
- "Funções do IAM predefinidas do BlueXP "
- "Saiba mais sobre a API para BlueXP  IAM"

## Comece a usar o gerenciamento de identidade e acesso do BlueXP

Ao se inscrever no BlueXP , você será solicitado a criar uma nova organização. A organização inclui um membro (um administrador da organização) e um projeto padrão. Para configurar o gerenciamento de identidade e acesso do BlueXP  (IAM) para atender às necessidades da sua empresa, você precisará personalizar a hierarquia da sua organização, adicionar membros adicionais, adicionar ou descobrir recursos e associar esses recursos em toda a sua hierarquia.

Você deve ter permissões **administrador da organização** para administrar toda a organização a partir do BlueXP  IAM. Se você tiver permissões **Folder ou Project admin**, você só poderá administrar as pastas e projetos para os quais você tem permissões.

Siga estas etapas para configurar uma nova organização do BlueXP . A ordem em que você conclui essas etapas pode ser diferente, dependendo das necessidades da sua organização.

### 1 Edite o projeto padrão ou adicione à hierarquia da organização

Você pode simplesmente usar o projeto padrão ou criar projetos e pastas adicionais que correspondam à hierarquia de sua empresa.

"Saiba como organizar seus recursos com pastas e projetos".

### 2 Associe membros à sua organização

Se várias pessoas da sua empresa precisarem acessar e gerenciar recursos do BlueXP , você precisará associar suas contas de usuário à sua organização e fornecer as permissões apropriadas em toda a hierarquia de recursos. Você também tem a opção de adicionar contas de serviço à sua organização.

"Saiba como gerenciar membros e suas permissões".

**3** **Adicione ou descubra recursos**

Adicione ou descubra recursos no BlueXP como *ambientes de trabalho*. Um ambiente de trabalho representa um sistema de storage que os membros da organização gerenciam dentro de um projeto. Por exemplo, um sistema Cloud Volumes ONTAP ou um cluster ONTAP no local.

Saiba como criar ou descobrir recursos a partir da tela BlueXP :

- "Amazon FSX para NetApp ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "Sistemas e-Series"
- "Clusters ONTAP on-premises"
- "StorageGRID"

**4** **Associar recursos a projetos adicionais**

Quando você cria ou descobre um recurso no BlueXP , esse recurso é automaticamente associado ao projeto selecionado quando você criou ou descobriu o ambiente de trabalho. Se você quiser disponibilizar esse recurso para outro projeto em sua organização, precisará criar uma associação entre eles. Se o recurso for gerenciado por um conetor, você também precisará criar uma associação entre o projeto e o conetor associado.

- "Saiba como gerenciar a hierarquia de recursos da sua organização".
- "Saiba como associar um conetor a uma pasta ou projeto".

**Informações relacionadas**

- "Saiba mais sobre o gerenciamento de identidades e acesso do BlueXP "
- "Saiba mais sobre a API para BlueXP IAM"

## Organize seus recursos no BlueXP IAM com pastas e projetos

O BlueXP Identity and Access Management (IAM) permite que você organize seus recursos do NetApp usando projetos e pastas. Um *project* representa um workspace no BlueXP que os membros da organização acessam para gerenciar *resources* (por exemplo, um sistema Cloud Volumes ONTAP). Uma *folder* agrupa os projetos relacionados. Depois de organizar seus recursos em pastas e projetos, você pode conceder acesso granular a recursos fornecendo aos membros da organização permissões para pastas e projetos específicos.

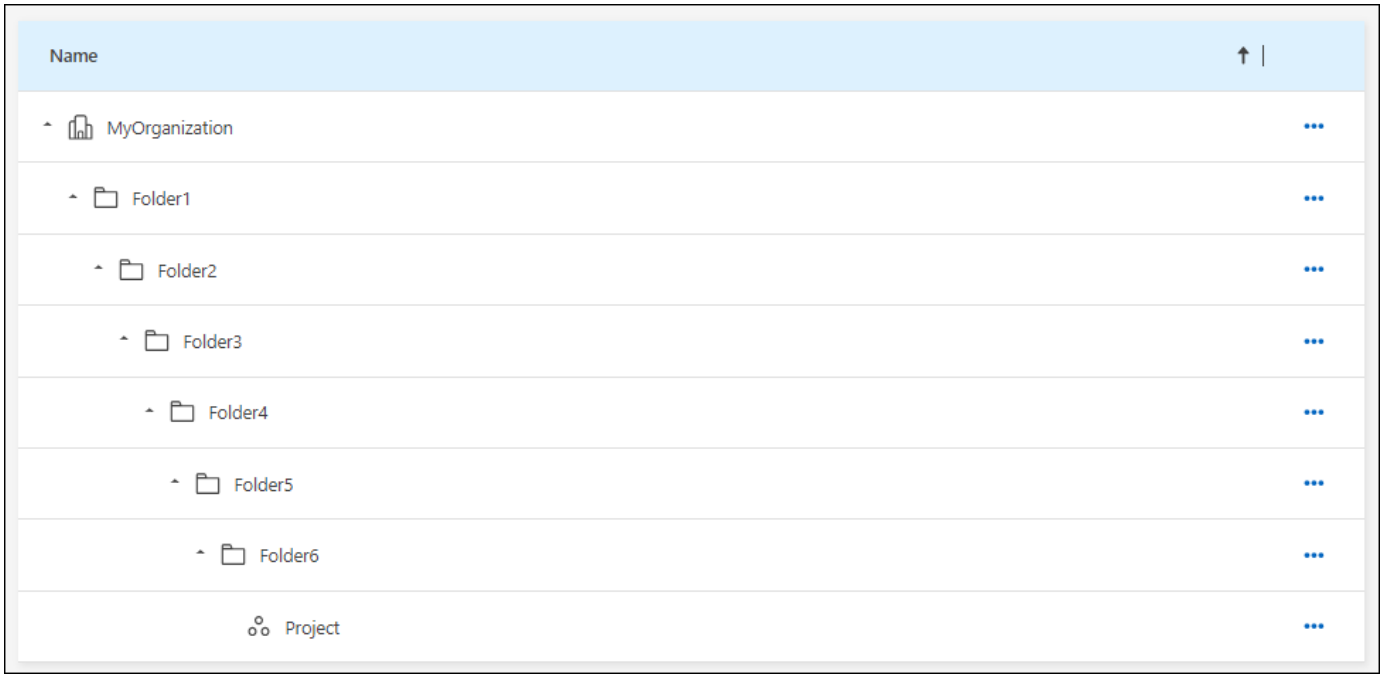
### Adicione uma pasta ou projeto

Quando você cria sua organização do BlueXP , ele inclui um único projeto. Você pode criar projetos adicionais para gerenciar os recursos da sua organização. Opcionalmente, você pode criar pastas para agrupar projetos relacionados.

**Sobre esta tarefa**

A profundidade da hierarquia da sua organização pode descer para 7 níveis. Como resultado, você pode criar pastas aninhadas até 6 níveis. A última pasta aninhada pode então incluir projetos no sétimo nível da hierarquia.

A imagem a seguir ilustra a profundidade máxima da hierarquia da sua organização:




**Passos**

1. No canto superior direito do console BlueXP , selecione > **Gerenciamento de identidade e acesso**.
2. Na página **Organização**, selecione **Adicionar pasta ou projeto**.
3. Selecione **pasta** ou **Projeto**.
4. Forneça detalhes sobre a pasta ou projeto:

    - **Nome e localização**: Insira um nome e escolha um local na hierarquia para a pasta ou projeto. Uma pasta ou projeto pode residir diretamente abaixo da organização ou dentro de uma pasta.
    - **Recursos**: Selecione os recursos que você deseja associar a essa pasta ou projeto.

      Você só pode selecionar a partir dos recursos que estão associados ao pai da pasta ou projeto. Se o pai for a organização, você poderá escolher entre qualquer recurso na organização. Se o pai for uma pasta, você só poderá selecionar os recursos associados à pasta.

      "Saiba quando você pode associar um recurso a uma pasta".

    - **Access**: Visualize os membros que terão acesso à pasta ou projeto com base nas permissões existentes já definidas na hierarquia de recursos.

      Se necessário, selecione **Adicionar um membro** para especificar membros adicionais da organização que devem ter acesso à pasta ou projeto e, em seguida, selecione uma função. Uma função define as permissões que os membros têm para a pasta ou projeto.

"Saiba mais sobre as funções predefinidas do IAM".

5. Selecione **Adicionar**.

**Resultado**

O BlueXP  cria a pasta ou projeto e associa os recursos e membros especificados.

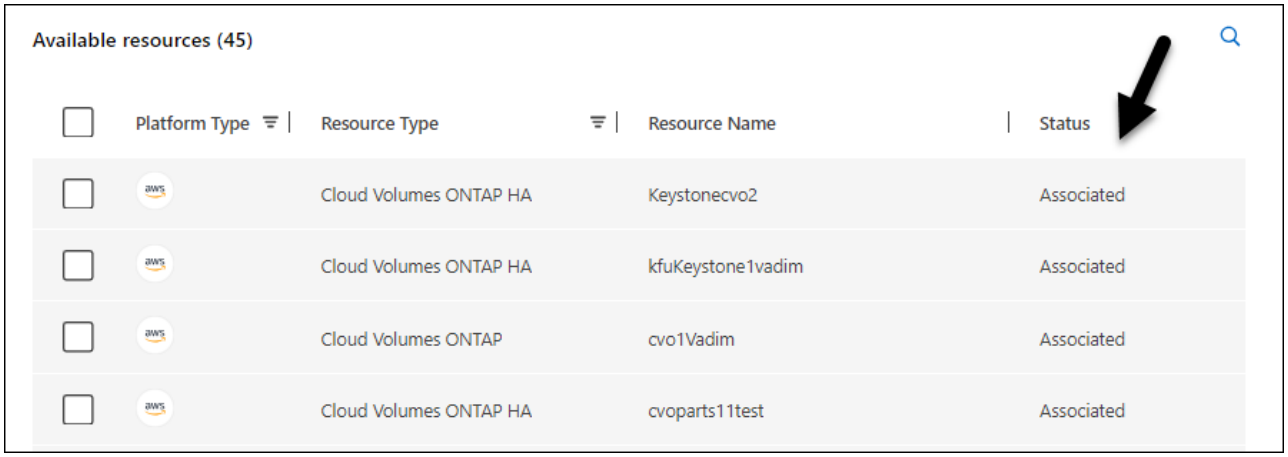
### Exibir os recursos e membros associados a uma pasta ou projeto

Para verificar se seus recursos estão organizados de forma adequada e acessíveis aos membros certos na sua organização, você pode ver quais recursos e membros estão associados a uma pasta ou projeto.

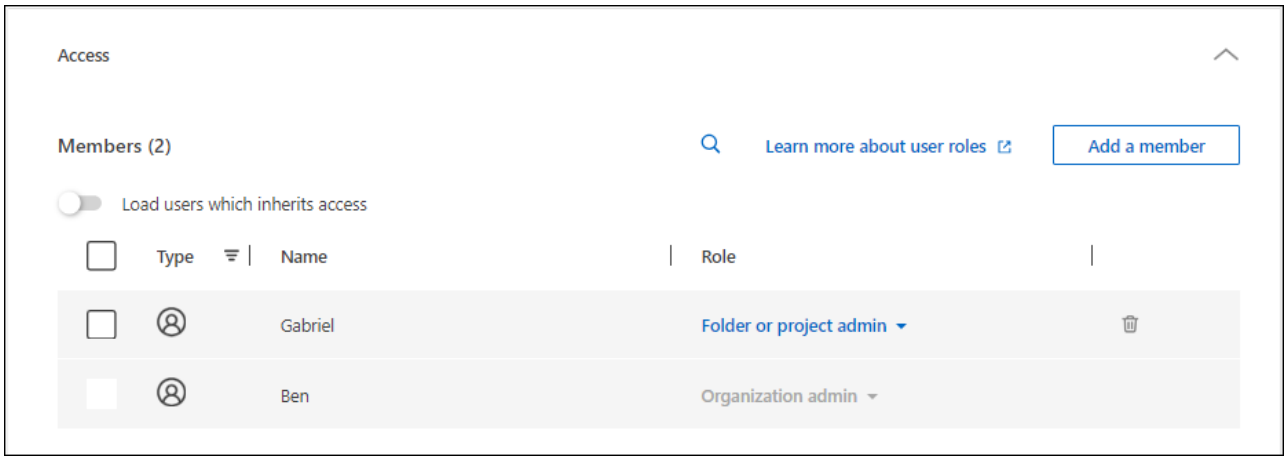
**Passos**

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, ••• selecione e selecione **Editar pasta** ou **Editar projeto**.


2. Na página **Editar**, veja detalhes sobre os recursos associados e o acesso aos membros:
   - Selecione **Resources** para exibir os recursos associados. Na tabela, a coluna **Status** identifica os recursos associados à pasta ou projeto.




   - Selecione **Access** para ver os membros que têm acesso à pasta ou projeto.




**O que se segue?**

Se necessário, você pode modifique os recursos associados ou modifique o acesso de membro.

## Modifique os recursos associados a uma pasta ou projeto

Você pode modificar os recursos associados a uma pasta ou projeto associando ou desassociando um recurso. Por exemplo, você pode querer associar um recurso a outro projeto porque esse recurso tem capacidade que outra equipe pode utilizar.

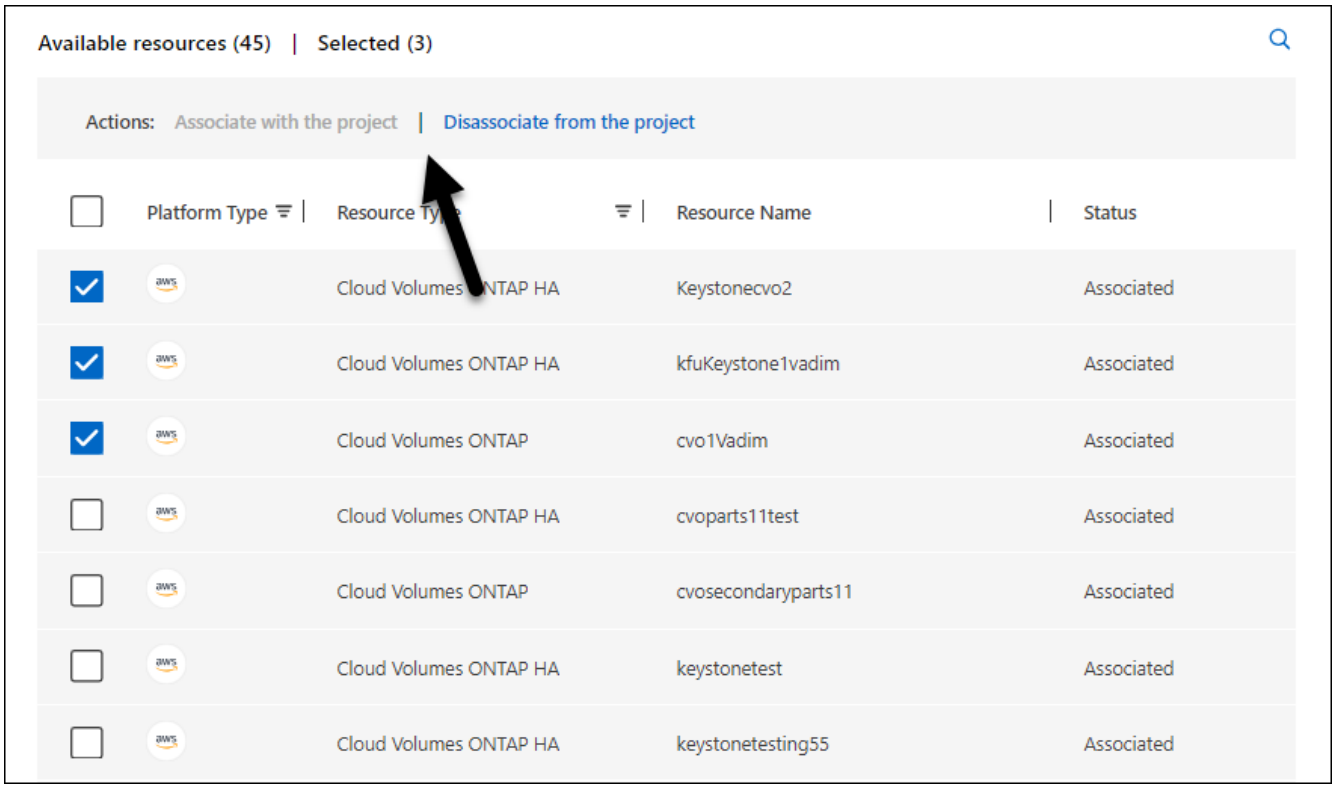
**Antes de começar**

"Saiba quando você pode associar um recurso a uma pasta".

**Passos**

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, ••• selecione e selecione **Editar pasta** ou **Editar projeto**.
2. Na página **Editar**, selecione **recursos**.

   Na tabela, a coluna **Status** identifica os recursos associados à pasta ou projeto.
3. Selecione os recursos que você deseja associar ou desassociar.
4. Dependendo dos recursos selecionados, selecione **associar ao projeto** ou **desassociar do projeto**.




5. Selecione **aplicar**

**Resultado**

O BlueXP associa os recursos à pasta ou ao projeto. Os membros da organização que têm permissões para essa pasta ou projeto agora podem acessar os recursos associados.

### Modifique o acesso de membro a uma pasta ou projeto

Modifique o acesso de membro a uma pasta ou projeto para garantir que os membros direitos tenham acesso aos recursos associados à pasta ou projeto.

**Passos**

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, ••• selecione e selecione **Editar pasta** ou **Editar projeto**.
2. Na página **Editar**, selecione **Acesso**.

   O BlueXP exibe a lista de membros que têm acesso à pasta ou projeto.

3. Modificar acesso de membro:

   - **Adicionar um membro**: Selecione o membro que você deseja adicionar à pasta ou projeto e atribua a ele uma função.
   - **Alterar a função de um membro**: Para quaisquer membros com uma função diferente de Administrador da Organização, selecione sua função existente e, em seguida, escolha uma nova função.

     Se uma função foi fornecida em um nível mais alto da hierarquia (no nível de pasta ou organização), então você deve considerar se deve alterar a função no nível mais baixo ou superior. Por exemplo, se você atribuiu a função *pasta ou admin* do projeto no nível da pasta, alterar a função no nível do projeto para permissões de nível inferior não alterará as permissões para o membro. Como as funções são

herdadas na hierarquia da organização, o membro ainda teria permissões de administrador no nível do projeto.

"Saiba mais sobre a herança de funções".

- **Remover acesso de membro**: Para membros que têm uma função definida na pasta ou projeto para o qual você está visualizando, você pode remover seu acesso.

  Se o acesso de membro foi fornecido em um nível mais alto da hierarquia (no nível da pasta ou da organização), então você não pode remover o acesso de membro ao visualizar essa pasta ou projeto. Você precisa mudar para essa parte da hierarquia. Alternativamente, você pode "Gerenciar permissões a partir da página Membros".

4. Selecione **aplicar**.

**Resultado**

O BlueXP  atualiza os membros que têm acesso à pasta ou projeto.

### Obtenha o ID de um projeto

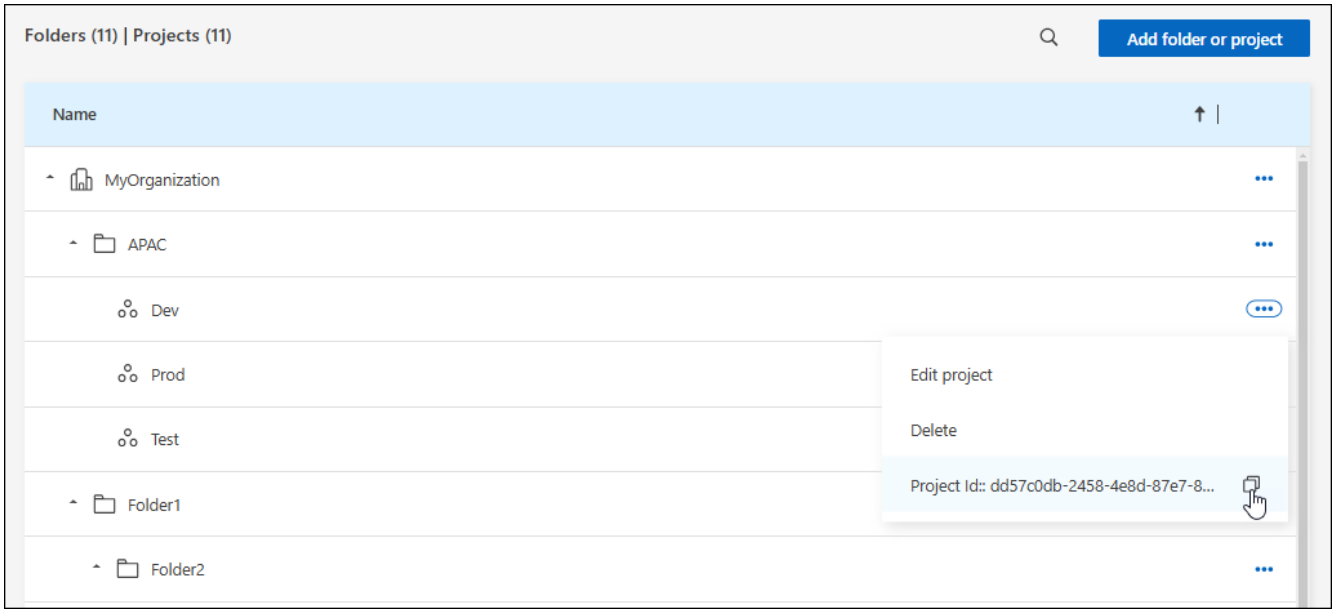
Se você estiver usando a API do BlueXP , talvez seja necessário obter o ID de um projeto. Por exemplo, ao criar um ambiente de trabalho Cloud Volumes ONTAP.

**Passos**

1. Na página **Organização**, navegue até um projeto na tabela e selecione •••

   O ID do projeto é exibido.

2. Para copiar a ID, selecione o botão Copy (cópia).




### Renomeie uma pasta ou projeto

Se necessário, você pode alterar o nome de suas pastas e projetos.

**Passos**

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, ••• selecione e selecione **Editar pasta** ou **Editar projeto**.
2. Na página **Editar**, insira um novo nome e selecione **aplicar**.

**Resultado**

O BlueXP  atualiza o nome da pasta ou projeto.

### Excluir uma pasta ou projeto

Você pode excluir as pastas e projetos que você não precisa mais.

**Antes de começar**

- A pasta ou projeto não deve ter recursos associados. Saiba como desassociar recursos.
- Uma pasta não deve conter subpastas ou projetos. Você precisa excluir essas pastas e projetos primeiro.

**Passos**

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, ••• selecione e selecione **Excluir**.
2. Confirme se deseja excluir a pasta ou o projeto.

**Resultado**

O BlueXP  exclui a pasta ou o projeto. Essa pasta ou projeto não está mais disponível para os membros da organização.

### Informações relacionadas

- "Saiba mais sobre o gerenciamento de identidades e acesso do BlueXP "
- "Comece a usar o BlueXP  IAM"
- "Saiba mais sobre a API para BlueXP  IAM"

## Adicione membros do BlueXP  IAM e gerencie suas permissões

O BlueXP  Identity and Access Management (IAM) permite adicionar membros à sua organização e atribuir-lhes uma ou mais funções na hierarquia de recursos. Um *role* contém um conjunto de permissões que permite que um membro execute ações específicas em um nível específico da hierarquia de recursos. Você pode associar novas contas de usuário e contas de serviço, gerenciar funções de membro e muito mais.

Para garantir que você não perca o acesso à sua organização do BlueXP , é uma prática recomendada ter dois membros com a função de administrador da organização.

**Sobre esta tarefa**

Quando um *Folder ou administrador de projeto* exibe a página **Membros**, a página exibe todos os membros da organização. No entanto, um membro com essa função só pode exibir e gerenciar permissões de membro para as pastas e projetos para os quais eles têm permissões. "Saiba mais sobre as ações que um *Folder ou administrador de projeto* pode concluir".

### Adicione membros à sua organização

Você pode adicionar dois tipos de membros à sua organização: Uma conta de usuário e uma conta de serviço.

Uma conta de serviço é normalmente usada por um aplicativo para concluir tarefas especificadas sem intervenção humana.

**Conta de utilizador**

**Passos**

1. Se o utilizador ainda não o tiver feito, peça-lhe para ir ao "Site da NetApp BlueXP" e se inscrever.

   Quando o usuário se inscrever, ele deve preencher a página **Inscrever-se**, verificar seu endereço de e-mail e, em seguida, fazer login. Quando solicitado a criar uma organização, o usuário deve fechar o BlueXP  e informar que criou sua conta de usuário. Em seguida, você pode adicionar o usuário à sua organização BlueXP  existente.

   "Saiba como se inscrever no BlueXP ".

2. No canto superior direito do console BlueXP ,  selecione > **Gerenciamento de identidade e acesso**.
3. Selecione **Membros**.
4. Selecione **Adicionar um membro**.
5. Para adicionar o membro, execute as etapas na caixa de diálogo:
   - **Tipo de entidade**: Mantenha **Usuário** selecionado.
   - **E-mail do usuário**: Insira o endereço de e-mail do usuário associado ao login do BlueXP  que ele criou.
   - **Selecione uma organização, pasta ou projeto**: Escolha o nível da hierarquia de recursos para o qual o membro deve ter permissões.

     Observe o seguinte:

     - Você só pode selecionar a partir das pastas e projetos para os quais você tem permissões de administrador.
     - Se você selecionar a organização ou uma pasta, o membro terá permissões para tudo o que reside dentro da organização ou pasta.
   - **Selecione uma função**: Escolha uma função que forneça ao membro permissões para os recursos associados à organização, pasta ou projeto selecionado.
     - Se você selecionou a organização, você pode escolher entre qualquer função que não seja **Folder ou Project admin**.
     - Se você selecionou uma pasta ou projeto, você pode escolher entre qualquer função que não seja **Organization admin**.

       "Saiba mais sobre as funções predefinidas do IAM".
   - **Adicionar função**: Se você quiser fornecer acesso a pastas ou projetos adicionais dentro de sua organização, selecione **Adicionar função**, especifique outra pasta ou projeto e escolha uma função.
6. Selecione **Adicionar**.

**Resultado**

O BlueXP  adiciona o usuário à organização.

**O que se segue?**

O usuário deve receber um e-mail do NetApp BlueXP . O e-mail inclui informações que o membro pode

usar para acessar o BlueXP .

**Conta de serviço**

**Passos**

1. No canto superior direito do console BlueXP ,  selecione > **Gerenciamento de identidade e acesso**.
2. Selecione **Membros**.
3. Selecione **Adicionar um membro**.
4. Para adicionar o membro, execute as etapas na caixa de diálogo:
   - **Tipo de entidade**: Selecione **conta de serviço**.
   - **Nome da conta de serviço**: Insira um nome para a conta de serviço.
   - **Selecione uma organização, pasta ou projeto**: Escolha o nível da hierarquia de recursos para o qual o membro deve ter permissões.

     Observe o seguinte:

     - Você só pode selecionar a partir das pastas e projetos para os quais você tem permissões de administrador.
     - Se você selecionar a organização ou uma pasta, o membro terá permissões para tudo o que reside dentro da organização ou pasta.
   - **Selecione uma função**: Escolha uma função que forneça ao membro permissões para os recursos associados à organização, pasta ou projeto selecionado.
     - Se você selecionou a organização, você pode escolher entre qualquer função que não seja **Folder ou Project admin**.
     - Se você selecionou uma pasta ou projeto, você pode escolher entre qualquer função que não seja **Organization admin**.

       "Saiba mais sobre as funções predefinidas do IAM".
   - **Adicionar função**: Se você quiser fornecer acesso a pastas ou projetos adicionais dentro de sua organização, selecione **Adicionar função**, especifique outra pasta ou projeto e escolha uma função.
5. Selecione **Adicionar**.
6. Baixe ou copie o ID do cliente e o segredo do cliente.

   O segredo do cliente é visível apenas uma vez e não é armazenado em nenhum lugar pelo BlueXP . Copie ou baixe o segredo e guarde-o em segurança. Observe que você pode recriar o ID do cliente e o segredo do cliente mais tarde, conforme necessário.
7. Selecione **Fechar**.

**Resultado**

O BlueXP  adiciona a conta de serviço à sua organização.

### Veja os membros da organização

Você pode exibir uma lista de todos os membros da sua organização do BlueXP . Para entender quais

recursos e permissões estão disponíveis para um membro, você pode exibir as funções atribuídas ao membro em diferentes níveis da hierarquia de recursos da sua organização.

**Sobre esta tarefa**

A página **Membros** mostra detalhes sobre dois tipos de membros: Contas de usuário e contas de serviço.

**Passos**

1. No canto superior direito do console BlueXP , selecione > **Gerenciamento de identidade e acesso**.
2. Selecione **Membros**.

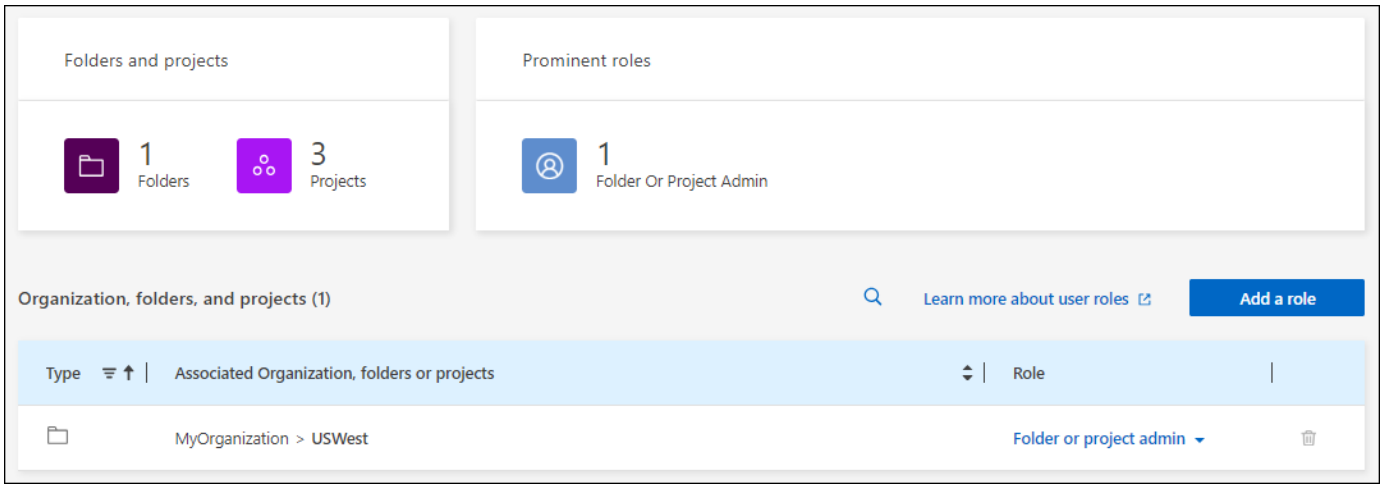
   Os membros da sua organização aparecem na tabela **Membros**.

3. Na página **Membros**, navegue até um membro na tabela, selecione e selecione **Exibir detalhes**.

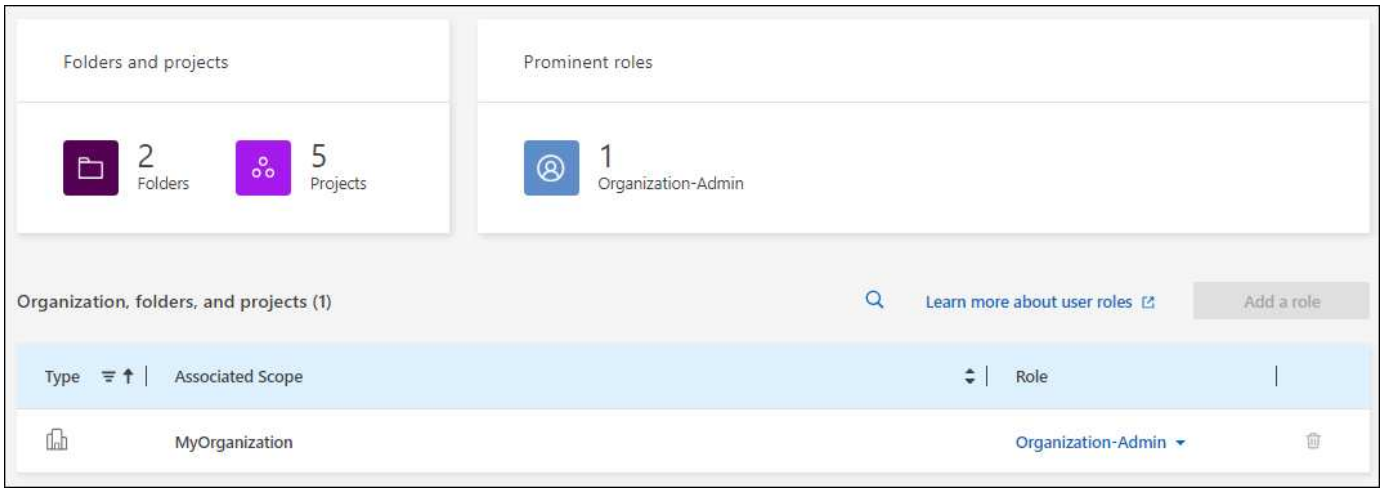
**Resultado**

O BlueXP  exibe detalhes sobre o membro, que inclui as pastas e projetos para os quais o membro tem permissões na hierarquia de recursos da sua organização.

Aqui está um exemplo de um membro que é atribuído a função *pasta ou administrador do projeto* para uma pasta, que fornece permissões para os três projetos na pasta.




Aqui está outro exemplo que mostra um membro que tem a função de administrador da organização, que dá ao usuário acesso a todos os recursos da organização.



### Informações relacionadas

"Veja todos os membros associados a uma pasta ou projeto específico".

## Gerencie as permissões de um membro

Uma função define as permissões atribuídas a um membro no nível da organização, pasta ou projeto. Cada membro da organização pode ter uma função atribuída em diferentes níveis da hierarquia da organização. Pode ser o mesmo papel ou um papel diferente. Por exemplo, você pode atribuir uma função de membro A para o projeto 1 e a função B para o projeto 2.

Um membro que tenha a função de administrador da organização não pode ser atribuído a nenhuma função adicional. Eles já têm permissões em toda a organização.

#### Adicione uma função a um membro

Forneça permissões adicionais a um membro em sua organização adicionando funções que se aplicam ao nível da organização, pasta ou projeto.

### Passos

1. Na página **Membros**, navegue até um membro na tabela, selecione e selecione **Adicionar uma função**.
2. Para adicionar uma função, execute as etapas na caixa de diálogo:
   - **Selecione uma organização, pasta ou projeto**: Escolha o nível da hierarquia de recursos para o qual o membro deve ter permissões.

     Se você selecionar a organização ou uma pasta, o membro terá permissões para tudo o que reside dentro da organização ou pasta.

   - **Selecione uma função**: Escolha uma função que forneça ao membro permissões para os recursos associados à organização, pasta ou projeto selecionado.
     - Se você selecionou a organização, você pode escolher entre qualquer função que não seja **Folder ou Project admin**.
     - Se você selecionou uma pasta ou projeto, você pode escolher entre qualquer função que não seja **Organization admin**.

     "Saiba mais sobre as funções predefinidas do IAM".

   - **Adicionar função**: Se você quiser fornecer acesso a pastas ou projetos adicionais dentro de sua organização, selecione **Adicionar função**, especifique outra pasta ou projeto e escolha uma função.
3. Selecione **Adicionar novas funções**.

### Resultado

BlueXP  adiciona as funções. O membro agora tem permissões para os recursos na organização, pasta ou projeto selecionado.

#### Mude de uma função para outra

Se você precisar modificar as permissões de um membro, poderá alterar a função associada a esse membro no nível da organização, pasta ou projeto.

Se você precisar alterar as funções de vários membros em sua organização, use uma ação em massa para

concluir as alterações de uma só vez.

**Um membro**

**Passos**

1. Na página **Membros**, navegue até um membro na tabela, •••selecione e selecione **Exibir detalhes**.
2. Na tabela, navegue até a organização, pasta ou projeto e selecione uma nova função.

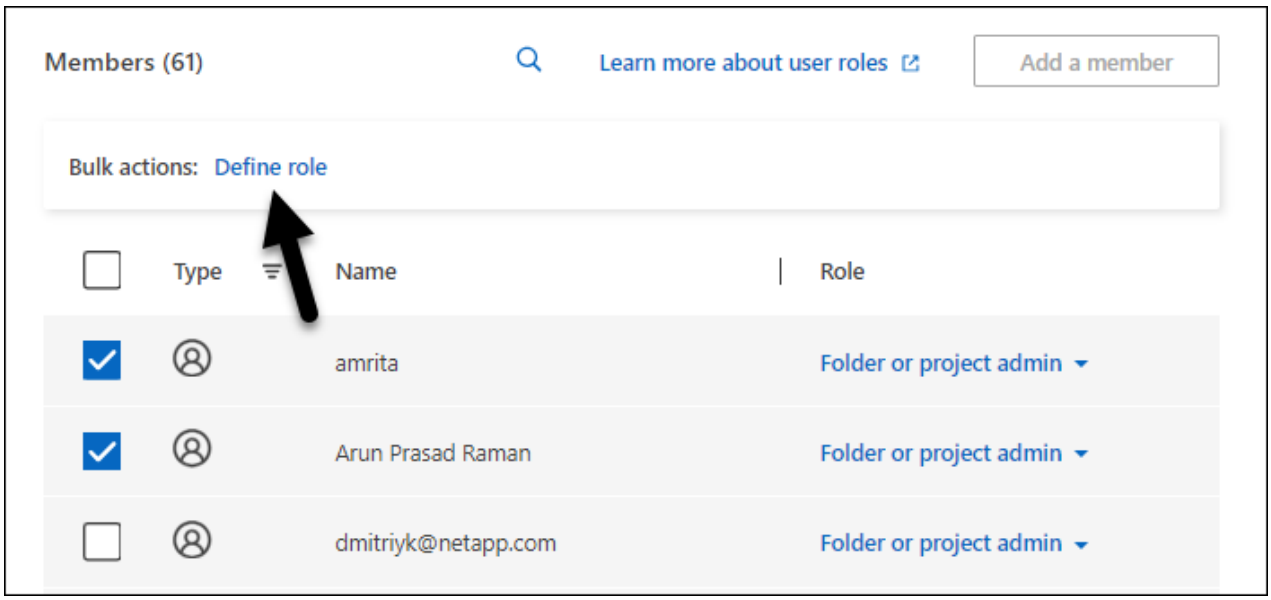
**Resultado**

O BlueXP  atualiza as funções associadas a esse membro no nível da organização, pasta e projeto.

**Vários membros**

**Passos**

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, •••selecione e selecione **Editar organização**, **Editar pasta** ou **Editar projeto**.
2. Na página **Editar**, selecione **Acesso**.
3. Selecione todos os membros ou selecione individualmente dois ou mais membros.
4. Selecione **Definir função**.




5. Selecione a função que deseja atribuir aos membros e selecione **Definir**.

**Resultado**

O BlueXP  atualiza as funções de todos os membros selecionados.

#### Remover permissões para uma pasta ou projeto

Você pode remover as permissões de um membro para uma pasta ou projeto específico removendo sua função.

**Sobre esta tarefa**

Se um membro tiver permissões em sua organização para *somente* uma pasta ou projeto, você não poderá remover essa função. Você tem duas opções:

- Se você quiser que o membro tenha permissões para outra parte da hierarquia de recursos, você precisa adicionar essa função primeiro e excluir a função existente.
- Se você não quiser que o membro tenha permissões para nada, então você pode simplesmente remover o membro da sua organização.

**Passos**

1. Na página **Membros**, navegue até um membro na tabela, selecione e selecione **Exibir detalhes**.
2. Na tabela, navegue até a pasta ou o nível do projeto e selecione

**Resultado**

O BlueXP  remove permissões para esse membro no nível de pasta ou projeto.

### Recrie as credenciais de uma conta de serviço

Você pode recriar as credenciais (ID do cliente e segredo do cliente) para uma conta de serviço a qualquer momento. Você pode recriar as credenciais se as perder ou se a sua empresa exigir que você gire as credenciais de segurança após um período de tempo.

**Sobre esta tarefa**

Recriar as credenciais exclui as credenciais existentes para a conta de serviço e cria novas credenciais. Você não poderá usar as credenciais anteriores.

**Passos**

1. No canto superior direito do console BlueXP , selecione > **Gerenciamento de identidade e acesso**.
2. Selecione **Membros**.
3. Na tabela **Membros**, navegue até uma conta de serviço, selecione e selecione **recriar segredos**.
4. Selecione **recrie**.
5. Baixe ou copie o ID do cliente e o segredo do cliente.

   O segredo do cliente é visível apenas uma vez e não é armazenado em nenhum lugar pelo BlueXP . Copie ou baixe o segredo e guarde-o em segurança.

6. Selecione **Fechar**.

**Resultado**

Um novo ID de cliente e segredo de cliente estão agora associados à conta de serviço.

### Remova um membro da sua organização

Talvez seja necessário remover um membro da sua organização, por exemplo, se ele deixou a sua empresa.

**Sobre esta tarefa**

Esta tarefa não exclui a conta do BlueXP  do membro ou a conta do site de suporte da NetApp. Ele simplesmente remove o membro e suas permissões associadas de sua organização.

**Passos**

1. Na página **Membros**, navegue até um membro na tabela, selecione e selecione **Excluir usuário**.
2. Confirme se deseja remover o membro da sua organização.

### Resultado

BlueXP  remove o membro. Se esse membro fizer login no BlueXP  novamente, ele não terá mais acesso à sua organização do BlueXP .

### Informações relacionadas

- "Saiba mais sobre o gerenciamento de identidades e acesso do BlueXP "
- "Comece a usar o BlueXP  IAM"
- "Funções do IAM predefinidas do BlueXP "
- "Saiba mais sobre a API para BlueXP  IAM"

## Gerencie a hierarquia de recursos em sua organização do BlueXP

Quando você usa o gerenciamento de identidade e acesso do BlueXP  (IAM) para associar um membro à sua organização, você fornece permissões no nível da organização, pasta ou projeto. Para garantir que esses membros tenham permissões para acessar os recursos certos, você precisará gerenciar a hierarquia de recursos de sua organização associando recursos a projetos e pastas específicos. Um *resource* é um ambiente de trabalho que o BlueXP  já gerencia.

### Veja os recursos na sua organização

Para começar a gerenciar sua hierarquia de recursos, você deve estar ciente dos recursos associados à sua organização.

### Passos

1. No canto superior direito do console BlueXP , selecione > **Gerenciamento de identidade e acesso**.
2. Selecione **recursos**.

### Resultado

Os recursos associados à sua organização são exibidos na tabela **recursos**.

### O que se segue?

Para encontrar um recurso específico, você pode pesquise e filtre o conteúdo da tabela.

Depois de encontrar o recurso que você está procurando, você pode concluir qualquer uma das seguintes ações:

- Exiba as pastas e projetos associados ao recurso
- Associe o recurso a pastas e projetos adicionais
- Remova o recurso de uma pasta ou projeto

### Encontre recursos específicos em sua organização

Se você tiver um grande número de recursos em sua organização, poderá usar as opções de pesquisa e filtro para encontrar um recurso específico.

### Passos

1. Na página **recursos**, selecione **Pesquisa avançada & filtragem**.
2. Use qualquer uma das opções disponíveis para encontrar o recurso que você está procurando:
   - **Pesquisar por nome do recurso**: Insira uma cadeia de texto e selecione **Adicionar**.
   - **Plataforma**: Selecione uma ou mais plataformas, como Amazon Web Services.
   - **Recursos**: Selecione um ou mais recursos, como o Cloud Volumes ONTAP.
   - **Organização, pasta ou projeto**: Selecione toda a organização, uma pasta específica ou um projeto específico.
3. Selecione **pesquisar**.

**Resultado**

O conteúdo da tabela recursos é atualizado para mostrar os recursos que correspondem às seleções de pesquisa e filtro.

### Associar um recurso a pastas e projetos

Se você quiser disponibilizar um recurso para outra pasta ou projeto em sua organização, precisará criar uma associação entre a pasta ou projeto e o recurso.

**Antes de começar**

Você deve entender como a associação de recursos funciona. "Saiba mais sobre recursos, incluindo quando associar um recurso a uma pasta".

**Passos**

1. Na página **recursos**, navegue até um recurso na tabela, selecione e selecione **associar a pastas ou projetos**.
2. Selecione uma pasta ou projeto e, em seguida, selecione **Accept**.
3. Para associar uma pasta ou projeto adicional, selecione **Adicionar pasta ou projeto** e, em seguida, selecione a pasta ou projeto.

   Observe que você só pode selecionar a partir das pastas e projetos para os quais você tem permissões de administrador.

4. Selecione **recursos associados**.

**Resultado**

O BlueXP  associa o recurso às pastas e projetos selecionados.

- Se você associou o recurso a projetos, os membros que têm permissões para esses projetos agora terão a capacidade de acessar o recurso no BlueXP .
- Se você associou o recurso a uma pasta, um *pasta ou administrador de projeto* agora pode acessar o recurso a partir do BlueXP  IAM. "Saiba mais sobre como associar um recurso a uma pasta".

**Depois de terminar**

Se o recurso associado for descoberto usando um BlueXP  Connector e tiver outros membros em sua organização, você também precisará associar o conetor ao projeto ao qual o recurso está agora associado. Caso contrário, o conetor e seu recurso associado não são acessíveis a partir da tela do BlueXP  por membros que não têm a função *administrador da organização*.

"Saiba como associar um conetor a uma pasta ou projeto".

### Exibir as pastas e projetos associados a um recurso

Para identificar onde um recurso está disponível na hierarquia da sua organização, você pode exibir as pastas e projetos associados a esse recurso.

#### Passos

1. Na página **recursos**, navegue até um recurso na tabela, ••• selecione e selecione **Exibir detalhes**.

#### Resultado

O BlueXP  exibe as pastas e projetos associados ao recurso.

O exemplo a seguir mostra um recurso que está associado a um projeto.


#### O que se segue?

- Você pode associe o recurso a um projeto ou pasta adicional.
- Você pode remova o recurso de uma pasta ou projeto específico.
- Se precisar determinar quais membros da organização têm acesso ao recurso, você pode "visualize os membros que têm acesso às pastas e projetos associados ao recurso".

### Remover um recurso de uma pasta ou projeto

Para remover um recurso de uma pasta ou projeto, você precisa remover a associação entre a pasta ou projeto e o recurso. Depois de remover a associação, os membros da organização não podem mais gerenciar o recurso da pasta ou do projeto.

#### Sobre esta tarefa

Se você quiser remover um recurso descoberto de toda a organização, será necessário remover o ambiente de trabalho da tela BlueXP .

#### Passos

1. Na página **recursos**, navegue até um recurso na tabela, ••• selecione e selecione **Exibir detalhes**.
2. Para a pasta ou projeto para o qual você deseja remover o recurso, selecione 🗑
3. Confirme que deseja remover a associação selecionando **Delete**.

#### Resultado

O BlueXP  remove a associação. Os membros não podem mais acessar o recurso a partir dessa pasta ou projeto.

### Informações relacionadas

- "Saiba mais sobre o gerenciamento de identidades e acesso do BlueXP "

- "Comece a usar o BlueXP  IAM"
- "Saiba mais sobre a API para BlueXP  IAM"

## Associe um conetor BlueXP  a outras pastas e projetos

Um conetor é necessário para gerenciar vários tipos de ambientes de trabalho da BlueXP . Quando um *administrador da organização* cria um conetor, o BlueXP  associa automaticamente esse conetor à organização e ao projeto atualmente selecionado. O *Organization admin* tem acesso automaticamente a esse conetor de qualquer lugar da organização. Outros membros da sua organização só podem acessar esse conetor do projeto no qual ele foi criado, a menos que você associe esse conetor a outros projetos do gerenciamento de identidade e acesso (IAM) do BlueXP .

### Antes de começar

Você deve entender como a associação de conetores funciona. "Saiba mais sobre como usar conetores com o BlueXP  IAM".

### Sobre esta tarefa

- Quando um *Folder ou administrador de projeto* exibe a página **Connectors**, a página exibe todos os conetores na organização. No entanto, um membro com essa função só pode exibir e associar conetores com as pastas e projetos para os quais eles têm permissões. "Saiba mais sobre as ações que um *Folder ou administrador de projeto* pode concluir".

### Passos

1. No canto superior direito do console BlueXP , selecione > **Gerenciamento de identidade e acesso**.
2. Selecione **conetores**.
3. Na tabela, localize o conetor que você deseja associar.

   Para encontrar um conetor específico, você pode usar a pesquisa acima da tabela e filtrar o conteúdo da tabela selecionando uma parte específica da hierarquia de recursos.

4. Para exibir primeiro as pastas e projetos aos quais o conetor está associado, selecione e selecione **Exibir detalhes**.

   O BlueXP  exibe detalhes sobre as pastas e projetos aos quais o conetor está associado.

5. Selecione **associar à pasta ou projeto**.
6. Selecione uma pasta ou projeto e, em seguida, selecione **Accept**.
7. Para associar o conetor a uma pasta ou projeto adicional, selecione **Adicionar uma pasta ou projeto** e, em seguida, selecione a pasta ou projeto.
8. Selecione **conetor associado**.

### Resultado

O BlueXP  associa o conetor às pastas e projetos selecionados. Os membros que têm permissões para essas pastas e projetos agora têm a capacidade de selecionar esse conetor.

### Depois de terminar

Se você quiser associar os recursos que o conetor gerencia com as mesmas pastas e projetos, você pode

fazê-lo na página recursos.

"Saiba como associar um recurso a pastas e projetos".

**Informações relacionadas**

- "Saiba mais sobre conetores BlueXP "
- "Saiba mais sobre o gerenciamento de identidades e acesso do BlueXP "
- "Comece a usar o BlueXP  IAM"
- "Saiba mais sobre a API para BlueXP  IAM"

## Alterne entre organizações, projetos e conetores da BlueXP

Você pode pertencer a várias organizações do BlueXP  ou ter permissões para acessar vários projetos ou conetores em uma organização do BlueXP . Quando necessário, você pode alternar facilmente entre organizações, projetos e conetores para acessar os recursos associados a essa organização, projeto ou conetor.

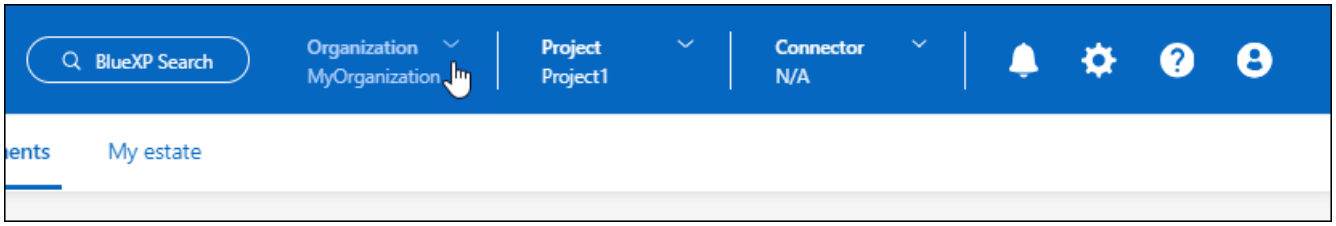
Você pode pertencer a várias organizações se você foi convidado a participar de outra organização ou se você mesmo criou uma organização adicional. Você pode criar uma organização adicional usando a API. "Saiba como criar uma nova organização"

### Alternar entre organizações

Se você é um membro de várias organizações, você pode alternar entre elas a qualquer momento.

**Passos**

1. Na parte superior do BlueXP , selecione **Organização**.




2. Selecione outra organização e, em seguida, selecione **Switch**.

**Resultado**

O BlueXP  muda para a organização selecionada e exibe os recursos associados a essa organização.

### Alternar entre projetos

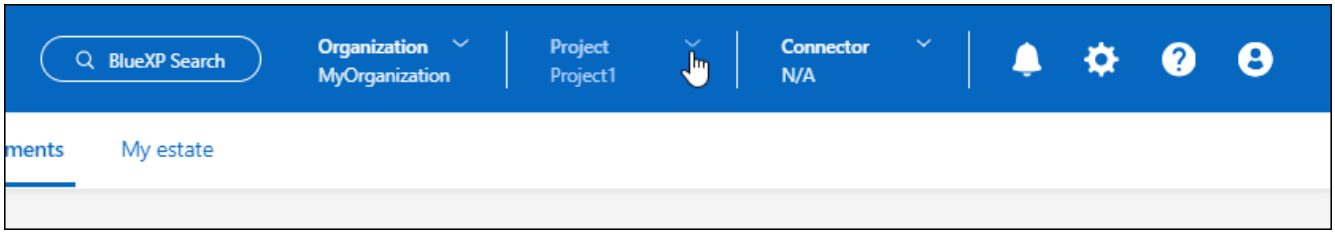
Se sua organização incluir vários projetos e você tiver acesso a esses projetos, poderá alternar entre eles a qualquer momento.

**Antes de começar**

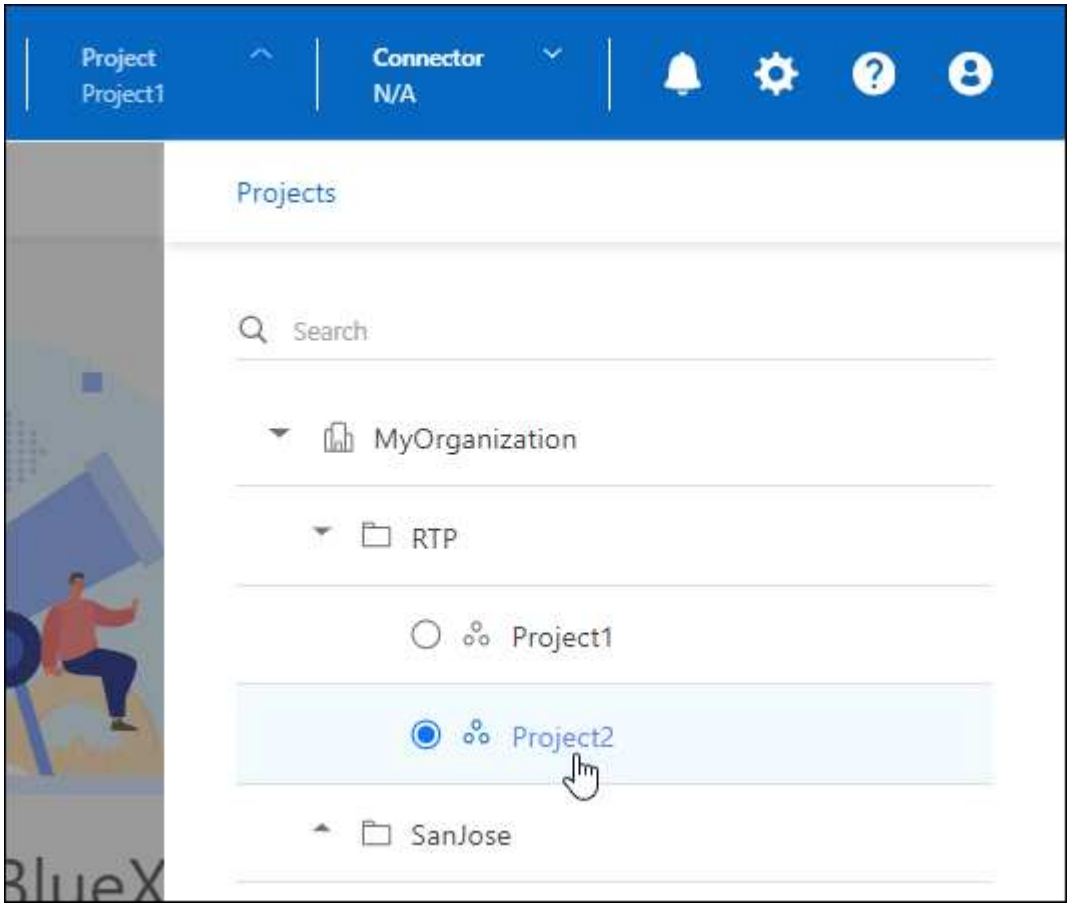
Você deve estar em qualquer página no console do BlueXP  que não seja as páginas de gerenciamento de identidade e acesso (IAM) do BlueXP . Não é possível mudar para outro projeto ao visualizar nenhuma das páginas do IAM.

**Passos**

1. No topo do BlueXP , selecione **Projeto**.




2. Navegue pelas pastas e projetos em sua organização, selecione o projeto desejado e selecione **alternar**.




**Resultado**

O BlueXP  muda para o projeto selecionado e exibe os recursos associados a esse projeto.

### Alternar entre os conetores

Se você tiver vários conetores, pode alternar entre eles para ver os ambientes de trabalho associados a um conetor específico.

**Passos**

1. Na parte superior do BlueXP , selecione **Connector**.
2. Selecione outro conetor e, em seguida, selecione **Switch**.

**Resultado**

O BlueXP  atualiza e mostra os ambientes de trabalho associados ao conetor selecionado.

**Link relacionado**

"Associar conetores a pastas e projetos".

**Informações relacionadas**

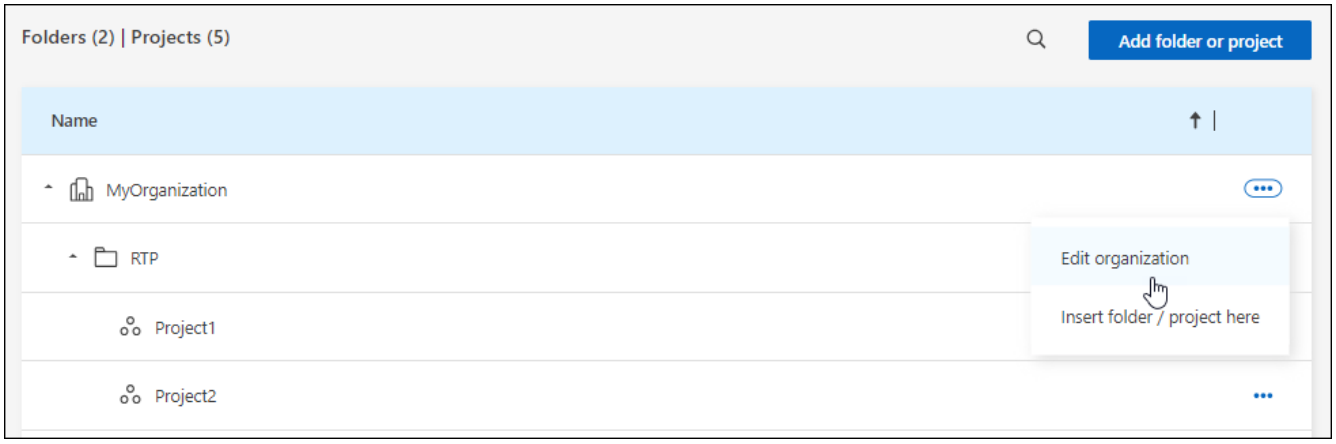
- "Saiba mais sobre o gerenciamento de identidades e acesso do BlueXP "
- "Comece a usar o BlueXP  IAM"
- "Saiba mais sobre a API para BlueXP  IAM"

## Renomeie sua organização do BlueXP

Se necessário, você pode alterar o nome da sua organização do BlueXP  a partir do gerenciamento de identidade e acesso (IAM) do BlueXP . O nome da organização aparece na parte superior do console baseado na Web do BlueXP  e nas páginas do IAM.

**Passos**

1. No canto superior direito do console BlueXP , selecione > **Gerenciamento de identidade e acesso**.
2. Na página **Organização**, navegue até a primeira linha da tabela, selecione e selecione **Editar organização**.




3. Introduza um novo nome de organização e selecione **Apply** (aplicar).

**Resultado**

O BlueXP  atualiza o nome da sua organização. Você deve ver imediatamente o nome atualizado na parte superior do console BlueXP .

**Informações relacionadas**

- "Saiba mais sobre o gerenciamento de identidades e acesso do BlueXP "
- "Comece a usar o BlueXP  IAM"
- "Saiba mais sobre a API para BlueXP  IAM"

## Monitorar ou auditar a atividade do IAM a partir da linha do tempo do BlueXP

Se você precisar monitorar ou auditar uma ação que foi concluída a partir do gerenciamento de identidade e acesso (IAM) do BlueXP , poderá exibir detalhes da linha do tempo do BlueXP . Por exemplo, você pode querer verificar quem adicionou um membro a uma organização ou se um projeto foi excluído com sucesso.

### Passos

1. No canto superior direito do console BlueXP , selecione  > **linha do tempo**.
2. Nos filtros, selecione **Serviço** e, em seguida, selecione **Tenancy**.
3. Use qualquer um dos outros filtros para alterar as ações exibidas na tabela.

   Por exemplo, você pode usar o filtro **User** para mostrar ações relacionadas a uma conta de usuário específica.

### Resultado

A linha do tempo é atualizada para mostrar as ações de gerenciamento concluídas relacionadas ao IAM do BlueXP .

## Funções e permissões do IAM predefinidas do BlueXP

O BlueXP  Identity and Access Management (IAM) inclui várias funções predefinidas que podem ser atribuídas aos membros da sua organização em diferentes níveis da hierarquia de recursos. Antes de atribuir essas funções, você deve entender as permissões que cada função inclui.

### Funções da plataforma

O BlueXP  IAM inclui duas funções de plataforma: Administrador da organização e administrador de pasta ou projeto. A principal diferença entre as duas funções da plataforma IAM do BlueXP  é o escopo. A função de administrador da organização tem permissões em todas as pastas e projetos; enquanto o administrador da pasta ou do projeto só tem permissões na pasta ou projeto ao qual foram atribuídos.

A função de administrador de pasta ou projeto não pode criar conetores.

### Permissões

| Tarefa | Administrador da organização | Administrador de pasta ou Projeto |
|---|---|---|
| Crie conetores | Sim | Não |
| Criar, modificar ou excluir ambientes de trabalho (adicionar ou descobrir novos recursos usando a tela BlueXP ) | Sim | Sim |
| Crie projetos/pastas, incluindo renomeação, exclusão e edição | Sim | Sim |
| Atribua funções e adicione usuários | Sim | Sim |

| Tarefa | Administrador da organização | Administrador de pasta ou Projeto |
|---|---|---|
| Associar recursos e conetores a pastas e projetos | Sim | Sim |
| Gerir credenciais a partir de Definições > credenciais | Sim | Sim |
| Veja a linha do tempo do BlueXP | Sim | Sim |
| Use os serviços do BlueXP | Sim | Sim |
| Registre o BlueXP para obter suporte e enviar casos | Sim | Sim |

**Exemplo para funções de organização em BlueXP para uma grande organização multinacional**

A XYZ Corporation, uma empresa multinacional, tem como objetivo separar o acesso a recursos de storage de dados com base em regiões geográficas: América do Norte, Europa e Ásia-Pacífico. Eles querem que cada região tenha controle exclusivo sobre seus recursos, mantendo a supervisão centralizada.

Para conseguir isso, uma pessoa atribuída à função de administrador da organização no BlueXP da XYZ Corporation cria um ambiente de trabalho inicial e, em seguida, cria pastas separadas no BlueXP para cada região. A pasta de cada região contém projetos (com recursos associados) relacionados a essa região. O administrador da organização atribui a um usuário BlueXP em cada região respetiva a função de administrador de pasta/projeto.

Quando a configuração inicial estiver concluída, os administradores regionais com a função de administrador pasta ou Projeto podem criar novos ambientes de trabalho e adicionar usuários em suas regiões. Esses administradores regionais também podem adicionar/remover/renomear pastas e projetos aos quais são atribuídos. O administrador da organização herda permissões para quaisquer novos ambientes ou recursos de trabalho, mantendo a visibilidade do uso do storage em toda a organização.

### Funções de serviços de dados

As funções de serviços de dados podem concluir suas tarefas em qualquer projeto ou pasta.

#### Administrador do SnapCenter

**Descrição**

Permite fazer backup de snapshots de clusters ONTAP on-premises usando o backup e a recuperação do BlueXP para aplicações.

**Permissões**

Um membro que tenha essa função pode concluir as seguintes ações no BlueXP :

- Conclua qualquer ação a partir de cópia de Segurança e recuperação > aplicações
- Gerencie todos os ambientes de trabalho nos projetos e pastas para os quais eles têm permissões
- Use todos os serviços do BlueXP

#### Visualizador de classificação

**Descrição**

Fornece os resultados do exame de classificação BlueXP  da vista de capacidade.

**Permissões**

Visualize as informações de conformidade e gere relatórios para recursos que eles têm permissão para acessar. Esses usuários não podem ativar ou desativar a digitalização de volumes, buckets ou esquemas de banco de dados.

Nenhuma outra ação está disponível para um membro que tenha essa função.

**Links relacionados**

- "Saiba mais sobre o gerenciamento de identidades e acesso do BlueXP "
- "Comece a usar o BlueXP  IAM"
- "Gerenciar membros do BlueXP  e suas permissões"
- "Saiba mais sobre a API para BlueXP  IAM"

# Contas BlueXP

## Saiba mais sobre as contas do BlueXP

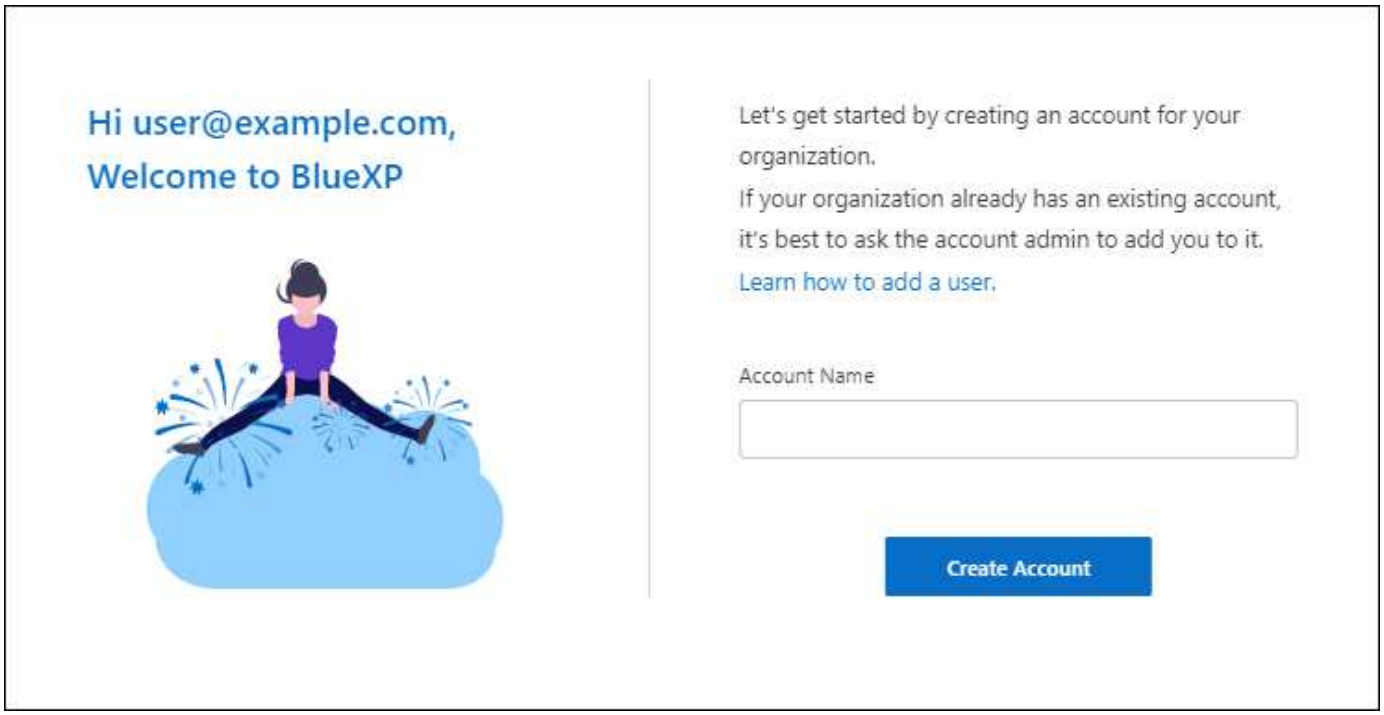
Quando você usa o BlueXP  no modo restrito ou privado, você usará uma conta *BlueXP* para gerenciar usuários e organizar recursos em *workspaces* isolados. Por exemplo, um grupo de usuários pode implantar e gerenciar ambientes de trabalho do Cloud Volumes ONTAP em um workspace que não seja visível para usuários que gerenciam ambientes de trabalho em um workspace diferente.

Se você estiver usando o BlueXP  no modo padrão, você não terá uma conta do BlueXP . Em vez disso, você terá uma organização *BlueXP*  que você gerencia usando o gerenciamento de identidade e acesso do BlueXP (IAM).

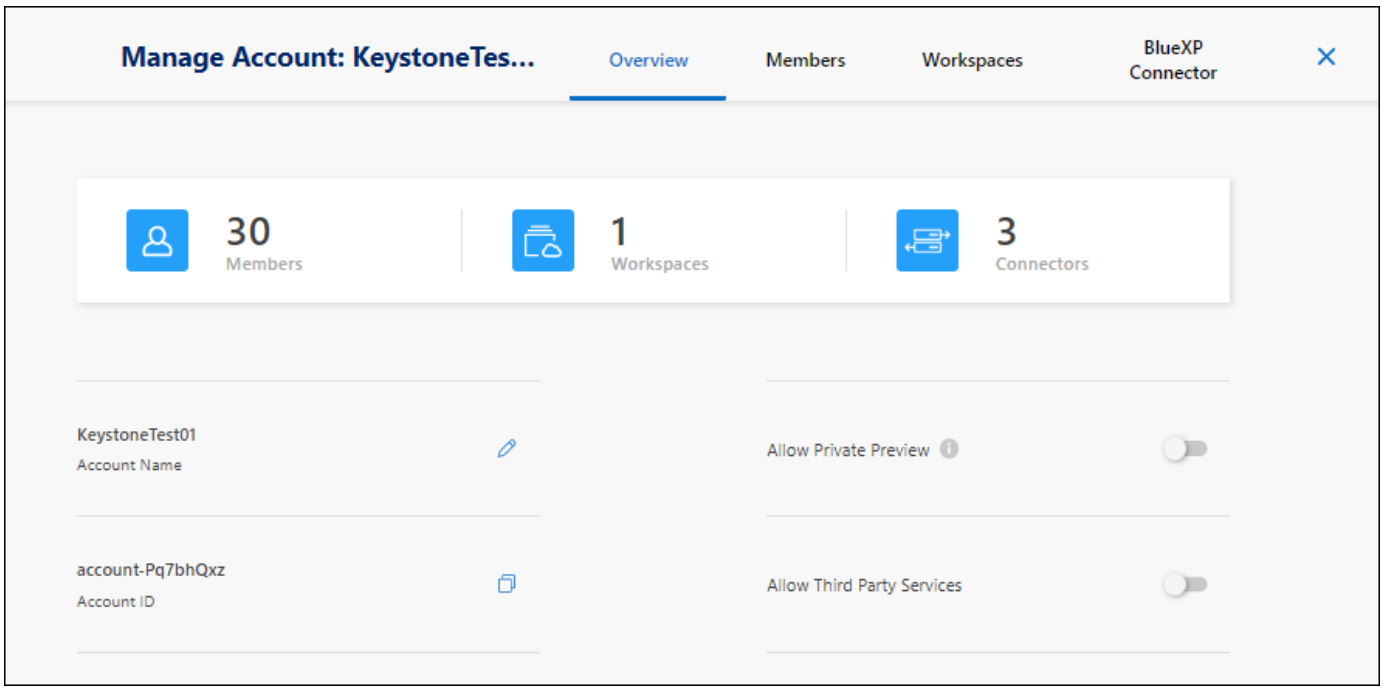
- "Saiba mais sobre o BlueXP  IAM"
- "Saiba mais sobre os modos de implantação do BlueXP"

**Visão geral**

Ao acessar o BlueXP  pela primeira vez, você será solicitado a selecionar ou criar uma conta. Por exemplo, você verá a seguinte tela se ainda não tiver uma conta:




Os administradores de conta do BlueXP  podem modificar as configurações dessa conta gerenciando usuários (membros), espaços de trabalho e conetores:




"Saiba como gerenciar sua conta do BlueXP ".

### Membros

Os membros são usuários do BlueXP  que você associa à sua conta do BlueXP . Associar um usuário a uma conta e um ou mais espaços de trabalho nessa conta permite que esses usuários criem e gerenciem ambientes de trabalho no BlueXP .

Quando você associa um usuário, você atribui a ele uma função:

- *Admin da conta*: Pode executar qualquer ação no BlueXP .
- *Workspace Admin*: Pode criar e gerenciar recursos na área de trabalho atribuída.
- *Visualizador de conformidade*: Só pode exibir informações de conformidade para classificação BlueXP  e gerar relatórios para workspaces que eles têm permissão para acessar.

"Saiba mais sobre essas funções".

### Espaços de trabalho

No BlueXP , uma área de trabalho isola qualquer número de *ambientes de trabalho* de outros usuários na conta. Os administradores do workspace não podem acessar os ambientes de trabalho em um workspace, a menos que o administrador da conta associe o administrador a esse workspace.

Um ambiente de trabalho representa um sistema de storage. Por exemplo:

- Um sistema Cloud Volumes ONTAP
- Um cluster ONTAP no local
- Um sistema StorageGRID

"Saiba como adicionar um espaço de trabalho".

### Conetores

Um conetor executa as ações que o BlueXP  precisa executar para gerenciar sua infraestrutura de dados. O conetor é executado em uma instância de máquina virtual que você implanta em seu provedor de nuvem ou em um host local que você configurou.

Você pode usar um conetor com mais de um serviço BlueXP . Por exemplo, se você estiver usando um conetor para gerenciar o Cloud Volumes ONTAP, poderá usar esse mesmo conetor com outro serviço, como a disposição em camadas do BlueXP .

"Saiba mais sobre conetores".

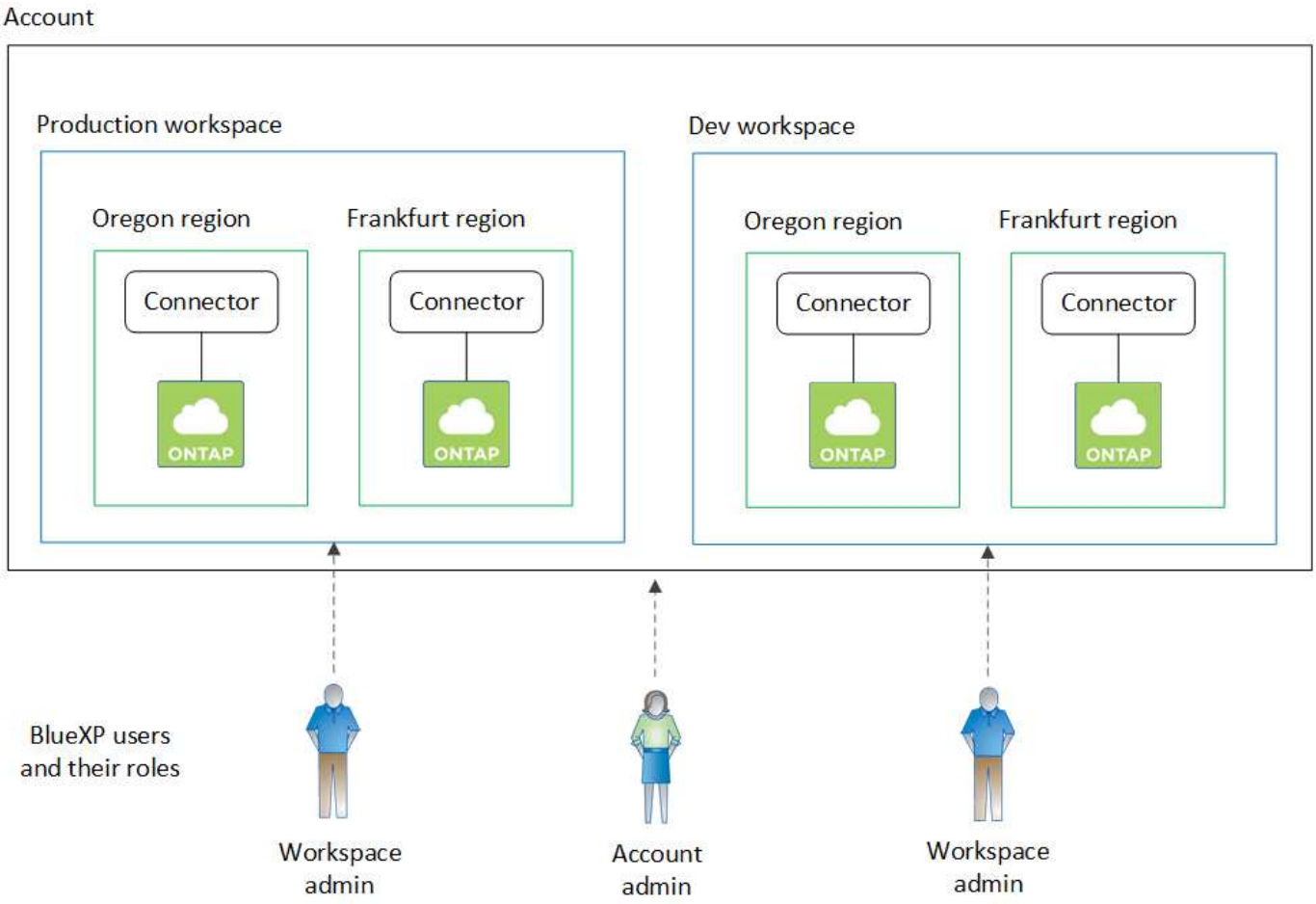
### Exemplos

Os exemplos a seguir descrevem como você pode configurar suas contas.

> Em ambos os exemplos de imagens que se seguem, o conetor e os sistemas Cloud Volumes ONTAP não residem *in* a conta BlueXP  - eles estão sendo executados em um provedor de nuvem. Esta é uma representação conceitual da relação entre cada componente.

#### Vários espaços de trabalho

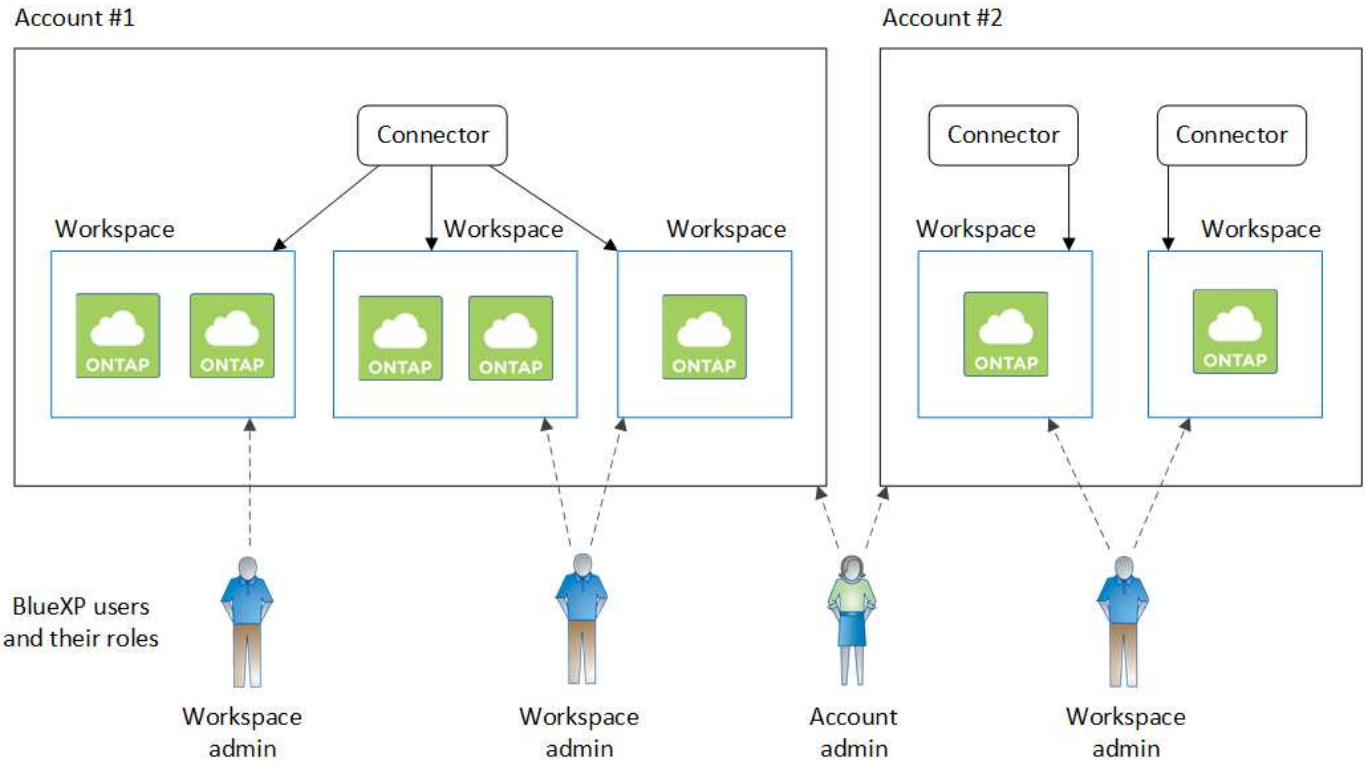
O exemplo a seguir mostra uma conta que usa dois espaços de trabalho para criar ambientes isolados. O primeiro espaço de trabalho é para um ambiente de produção e o segundo é para um ambiente de desenvolvimento.




**Várias contas**

Aqui está outro exemplo que mostra o mais alto nível de alocação a vários clientes usando duas contas BlueXP  separadas. Por exemplo, um provedor de serviços pode usar o BlueXP  em uma conta para fornecer serviços para seus clientes, enquanto usa outra conta para fornecer recuperação de desastres para uma de suas unidades de negócios.

Observe que a conta 2 inclui dois conetores separados. Isso pode acontecer se você tiver sistemas em regiões separadas ou em provedores de nuvem separados.




## Gerencie sua conta do BlueXP

Quando você usa o BlueXP  no modo restrito ou privado, você usará uma conta *BlueXP* para gerenciar usuários e organizar recursos. Quando você cria sua conta, ela inclui apenas um único usuário administrativo e um workspace. Você pode gerenciar a conta de acordo com suas necessidades adicionando usuários, criando contas de serviço para fins de automação, adicionando espaços de trabalho e muito mais.

Se você estiver usando o BlueXP  no modo padrão, você não terá uma conta do BlueXP . Em vez disso, você terá uma organização *BlueXP*  que você gerencia usando o gerenciamento de identidade e acesso do BlueXP (IAM).

- "Saiba mais sobre o BlueXP  IAM"
- "Saiba mais sobre os modos de implantação do BlueXP"

### Gerencie sua conta com a API do Tenancy

Se você quiser gerenciar suas configurações de conta enviando solicitações de API, precisará usar a API *Tenancy*. Essa API é diferente da API do BlueXP , que você usa para criar e gerenciar ambientes de trabalho do Cloud Volumes ONTAP.

"Exibir endpoints para a API do Tenancy"

### Crie e gerencie usuários

Os usuários da sua conta podem acessar e gerenciar os recursos em áreas de trabalho específicas.

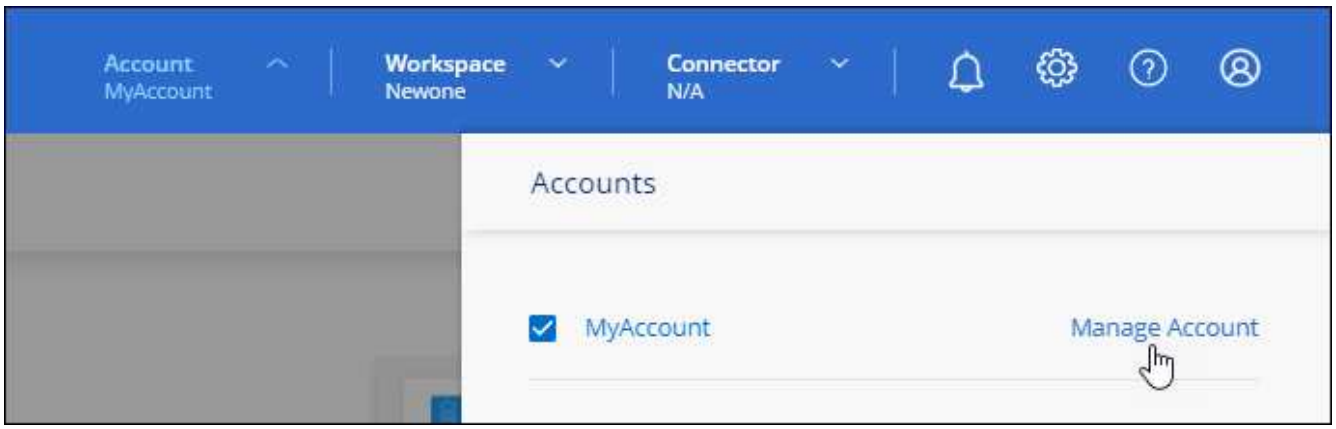
#### Adicionar utilizadores

Associe usuários à sua conta do BlueXP  para que esses usuários possam criar e gerenciar ambientes de trabalho no BlueXP .

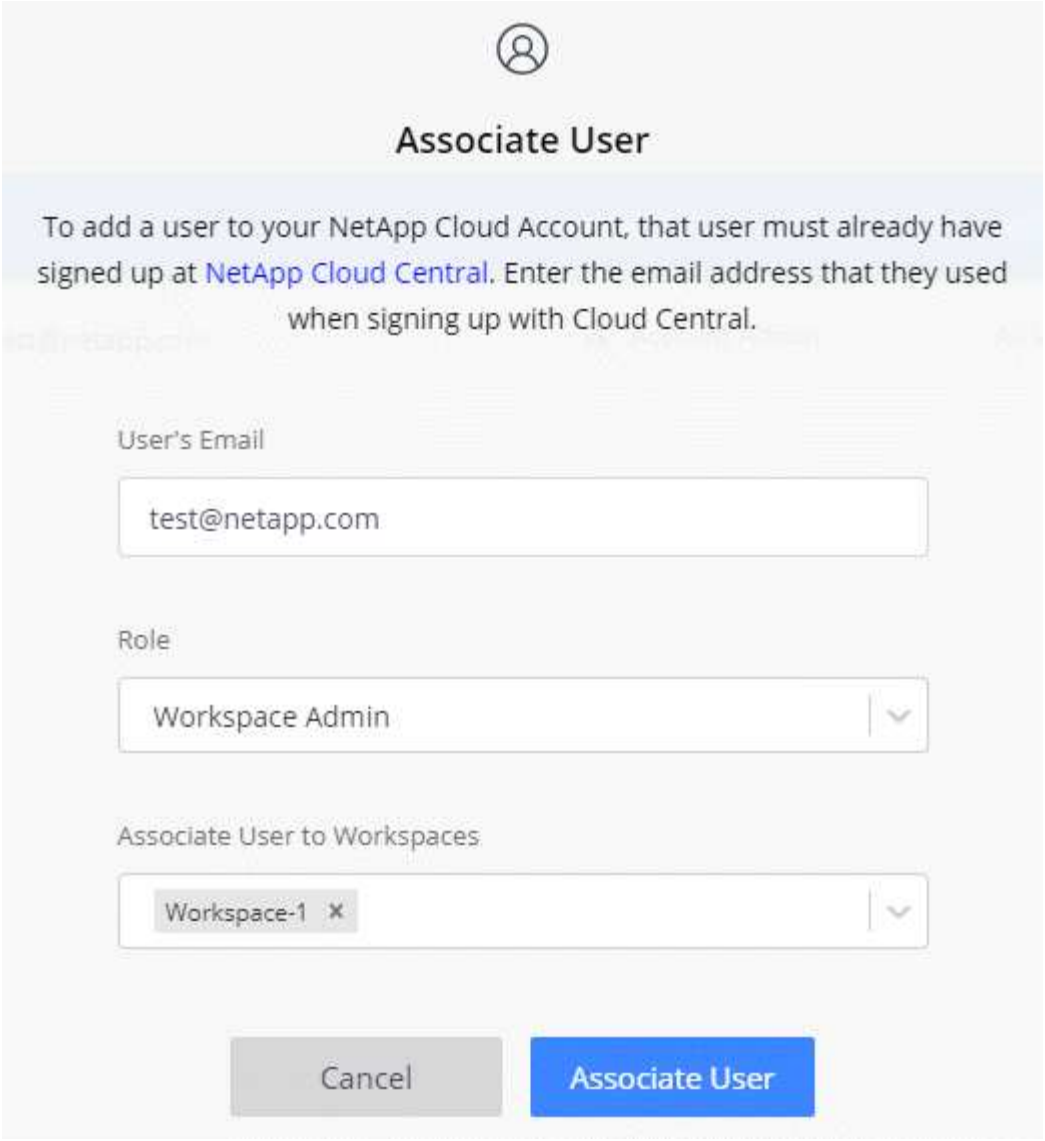
**Passos**

1. Se o usuário ainda não tiver feito isso, peça ao usuário para ir "Site da NetApp BlueXP" e se inscrever.
2. Na parte superior do BlueXP , selecione a lista suspensa **Account**.


3. Selecione **Gerenciar conta** ao lado da conta selecionada no momento.




4. Na guia Membros, selecione **Usuário associado**.
5. Insira o endereço de e-mail do usuário e selecione uma função para o usuário:
   - **Admin da conta**: Pode executar qualquer ação no BlueXP .
   - **Workspace Admin**: Pode criar e gerenciar recursos em workspaces atribuídos.
   - **Visualizador de conformidade**: Só pode visualizar informações de conformidade para classificação BlueXP  e gerar relatórios para espaços de trabalho que eles têm permissão para acessar.
6. Se você selecionou Workspace Admin ou Compliance Viewer, selecione um ou mais workspaces para associar a esse usuário.




7. Selecione **Associate**.

**Resultado**

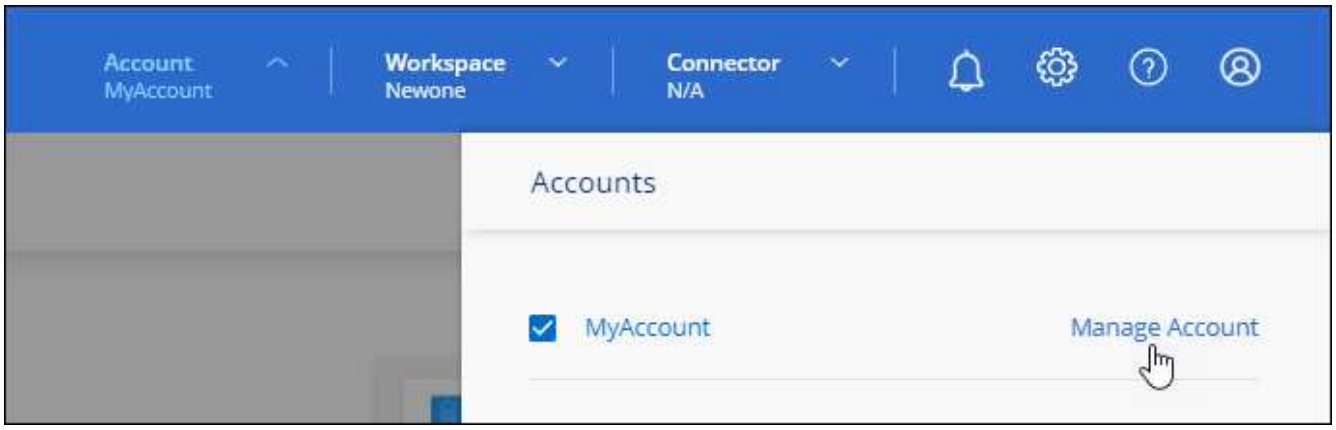
O usuário deve receber um e-mail do NetApp BlueXP  intitulado "Associação de Contas". O e-mail inclui as informações necessárias para acessar o BlueXP .

#### Remover usuários

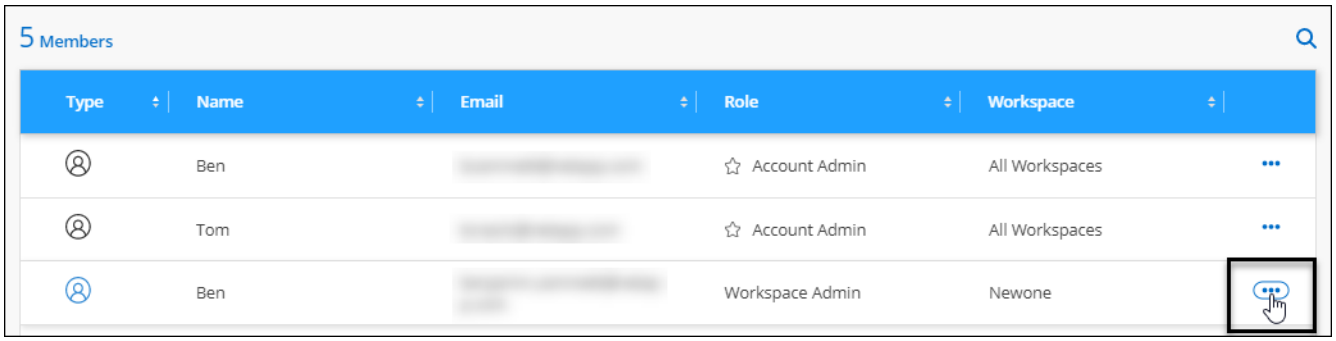
A desassociação de um usuário faz com que ele não possa mais acessar os recursos em uma conta do BlueXP .

**Passos**

1. Na parte superior do BlueXP , selecione a lista suspensa **conta** e selecione **Gerenciar conta**.




2. Na guia Membros, selecione o menu de ação na linha que corresponde ao usuário.




3. Selecione **Disassocie User** e selecione **Disassocie** para confirmar.

**Resultado**

O usuário não pode mais acessar os recursos nesta conta do BlueXP .

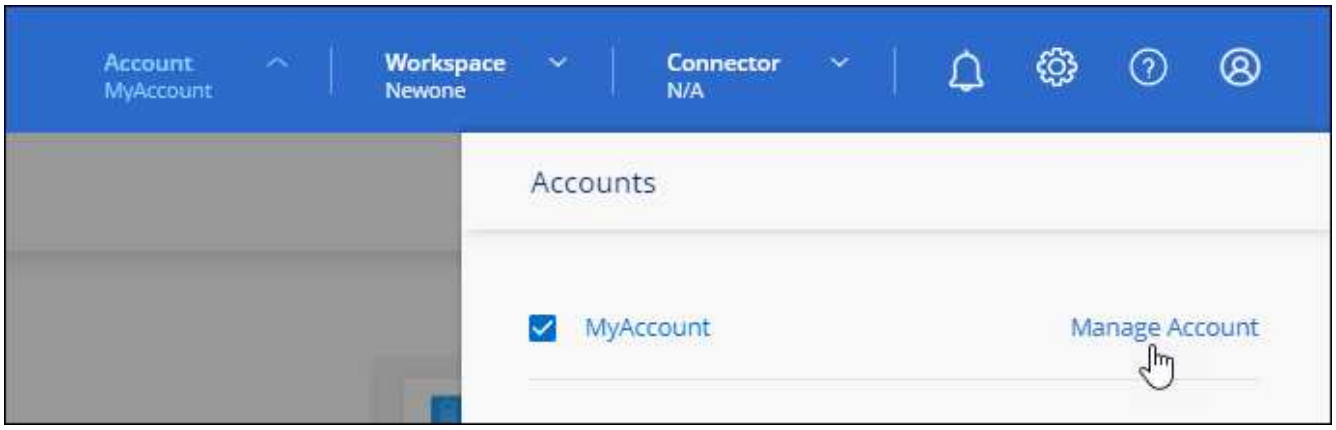
#### Gerenciar os workspaces de um administrador do Workspace

Você pode associar e desassociar administradores do Workspace a workspaces a qualquer momento. Associar o usuário permite que ele crie e visualize os ambientes de trabalho nesse espaço de trabalho.

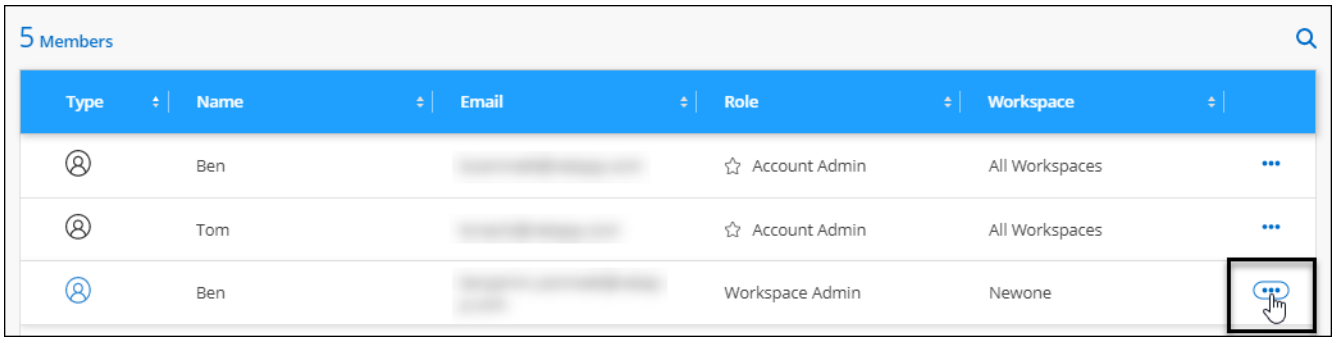
Você também precisa associar o conetor aos workspaces para que os administradores do workspace possam acessar esses workspaces a partir do BlueXP . "Saiba como gerenciar os espaços de trabalho de um conetor".

**Passos**

1. Na parte superior do BlueXP , selecione a lista suspensa **conta** e selecione **Gerenciar conta**.




2. Na guia Membros, selecione o menu de ação na linha que corresponde ao usuário.




3. Selecione **Gerenciar espaços de trabalho**.
4. Selecione os espaços de trabalho a serem associados ao usuário e selecione **Apply**.

**Resultado**

O usuário agora pode acessar esses workspaces a partir do BlueXP , desde que o conetor também esteja associado aos workspaces.

## Criar e gerenciar contas de serviço

Uma conta de serviço atua como um "usuário" que pode fazer chamadas de API autorizadas para o BlueXP para fins de automação. Isso torna mais fácil gerenciar a automação porque você não precisa criar scripts de automação com base na conta de usuário de uma pessoa real que pode sair da empresa a qualquer momento.

Você concede permissões a uma conta de serviço atribuindo-lhe uma função, assim como qualquer outro usuário do BlueXP . Você também pode associar a conta de serviço a espaços de trabalho específicos para controlar os ambientes de trabalho (recursos) que o serviço pode acessar.

Quando você cria a conta de serviço, o BlueXP  permite copiar ou baixar uma ID de cliente e segredo de cliente para a conta de serviço. Este par de chaves é usado para autenticação com o BlueXP .

Observe que um token de atualização não é necessário para operações de API ao usar uma conta de serviço. "Saiba mais sobre os tokens de atualização"

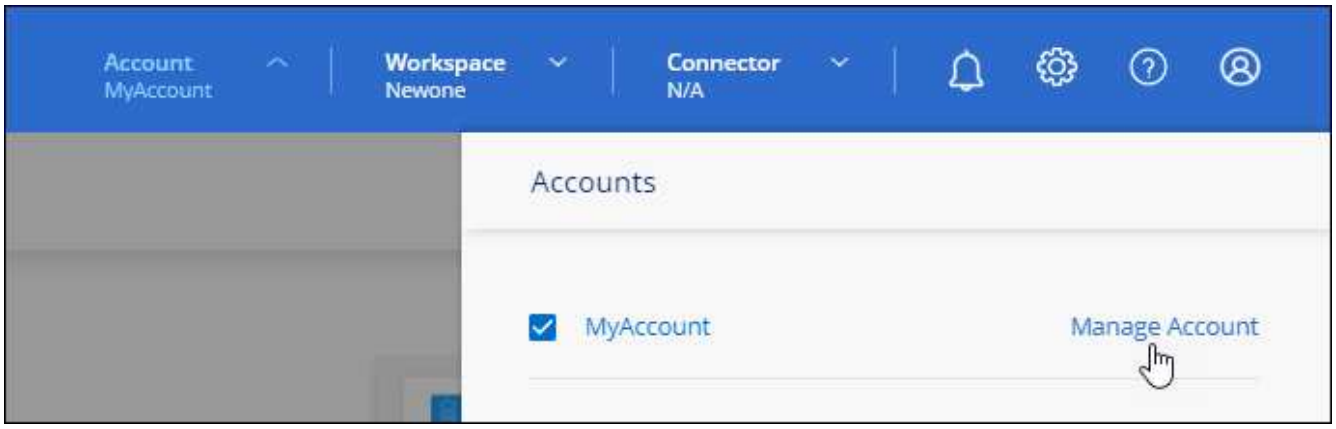
### Crie uma conta de serviço

Crie quantas contas de serviço forem necessárias para gerenciar os recursos em seus ambientes de trabalho.

**Passos**

1. Na parte superior do BlueXP , selecione a lista suspensa **Account**.


2. Selecione **Gerenciar conta** ao lado da conta selecionada no momento.




3. Na guia Membros, selecione **criar conta de serviço**.
4. Introduza um nome e selecione uma função. Se você escolheu uma função diferente de Admin de conta, escolha a área de trabalho a ser associada a essa conta de serviço.
5. Selecione **criar**.
6. Copie ou baixe o ID do cliente e o segredo do cliente.

   O segredo do cliente é visível apenas uma vez e não é armazenado em nenhum lugar pelo BlueXP . Copie ou baixe o segredo e guarde-o em segurança.

7. Selecione **Fechar**.

#### Obter um token de portador para uma conta de serviço

Para fazer chamadas de API para o "API de alocação", você precisará obter um token de portador para uma conta de serviço.

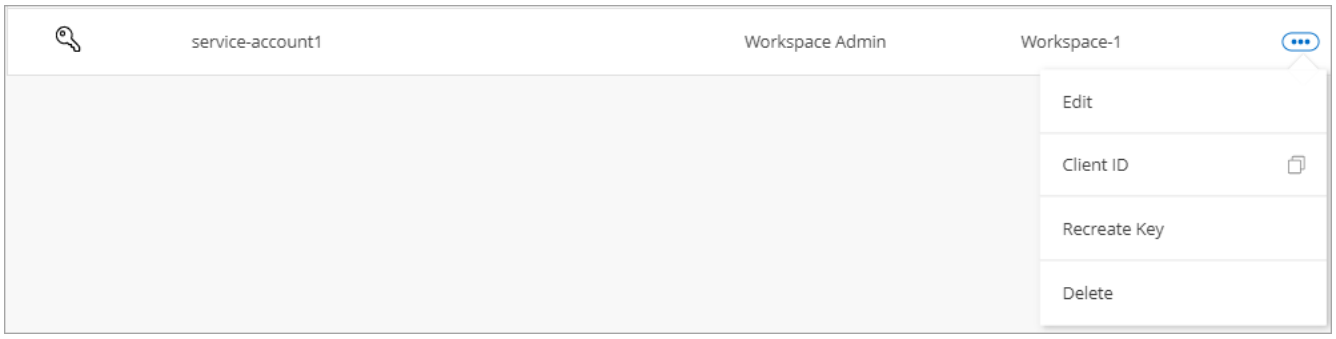
"Saiba como criar um token de conta de serviço"

#### Copie a ID do cliente

Você pode copiar o ID de cliente de uma conta de serviço a qualquer momento.

**Passos**

1. Na guia Membros, selecione o menu de ação na linha que corresponde à conta de serviço.



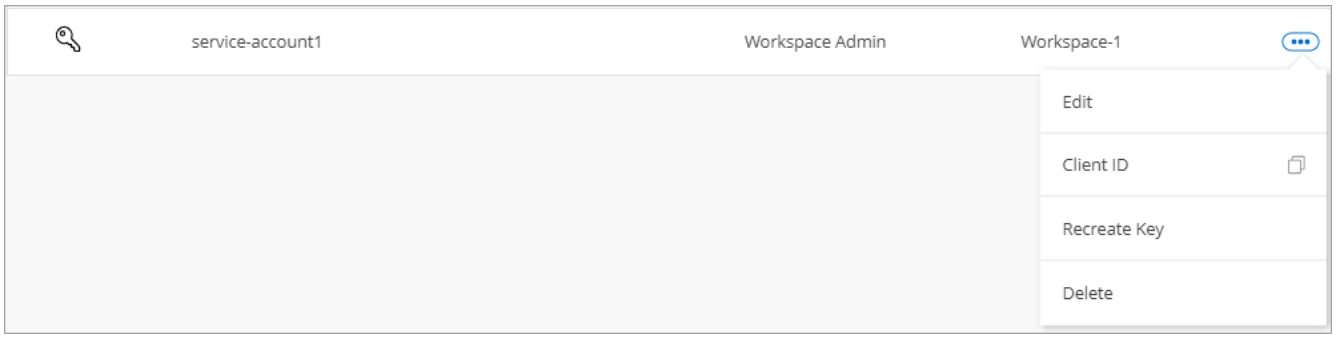

2. Selecione **ID do cliente**.
3. A ID é copiada para a área de transferência.

#### Recrie as teclas

Recriar a chave irá eliminar a chave existente para esta conta de serviço e, em seguida, criar uma nova chave. Você não poderá usar a chave anterior.

**Passos**

1. Na guia Membros, selecione o menu de ação na linha que corresponde à conta de serviço.




2. Selecione **Recrie Key**.
3. Selecione **recrie** para confirmar.
4. Copie ou baixe o ID do cliente e o segredo do cliente.

   O segredo do cliente é visível apenas uma vez e não é armazenado em nenhum lugar pelo BlueXP . Copie ou baixe o segredo e guarde-o em segurança.

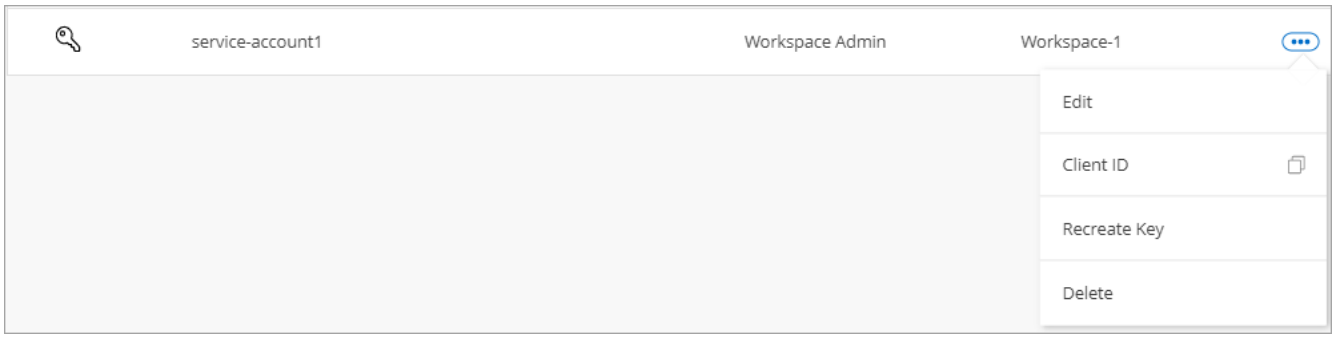
5. Selecione **Fechar**.

#### Eliminar uma conta de serviço

Exclua uma conta de serviço se você não precisar mais usá-la.

**Passos**

1. Na guia Membros, selecione o menu de ação na linha que corresponde à conta de serviço.




2. Selecione **Eliminar**.
3. Selecione **Delete** novamente para confirmar.

### Gerenciar espaços de trabalho

Gerencie seus workspaces criando, renomeando e excluindo-os. Observe que não é possível excluir um workspace se ele contiver recursos. Deve estar vazio.

**Passos**

1. Na parte superior do BlueXP , selecione a lista suspensa **conta** e selecione **Gerenciar conta**.
2. Selecione **Workspaces**.
3. Escolha uma das seguintes opções:
   - Selecione **Adicionar novo espaço de trabalho** para criar um novo espaço de trabalho.
   - Selecione **Renomear** para renomear a área de trabalho.
   - Selecione **Excluir** para excluir a área de trabalho.

   Se você criou uma nova área de trabalho, também deverá adicionar o conetor a essa área de trabalho. Se você não adicionar o conetor, os administradores do Workspace não poderão acessar nenhum dos recursos no workspace. Consulte a seção a seguir para obter mais detalhes.

### Gerenciar espaços de trabalho de um conetor

Você precisa associar o conetor aos workspaces para que os administradores do workspace possam acessar esses workspaces a partir do BlueXP .

Se você tiver apenas administradores de conta, associar o conetor com workspaces não será necessário. Administradores de conta têm a capacidade de acessar todos os espaços de trabalho no BlueXP  por padrão.

"Saiba mais sobre usuários, workspaces e conetores".

**Passos**

1. Na parte superior do BlueXP , selecione a lista suspensa **conta** e selecione **Gerenciar conta**.
2. Selecione **Connector**.
3. Selecione **Manage Workspaces** (gerir espaços de trabalho) para o conetor que pretende associar.
4. Selecione os espaços de trabalho a associar ao conetor e selecione **Apply**.

### Altere o nome da sua conta

Altere o nome da sua conta a qualquer momento para alterá-lo para algo significativo para você.

**Passos**

1. Na parte superior do BlueXP , selecione a lista suspensa **conta** e selecione **Gerenciar conta**.
2. Na guia **Visão geral**, selecione o ícone de edição ao lado do nome da conta.
3. Digite um novo nome de conta e selecione **Salvar**.

#### Permitir pré-visualizações privadas

Permita que visualizações privadas na sua conta tenham acesso a novos serviços disponibilizados como pré-visualização no BlueXP .

Os serviços em pré-visualização privada não são garantidos para se comportarem como esperado e podem sustentar interrupções e estar faltando funcionalidade.

**Passos**

1. Na parte superior do BlueXP , selecione a lista suspensa **conta** e selecione **Gerenciar conta**.
2. Na guia **Visão geral**, ative a configuração **permitir visualização privada**.

#### Permitir serviços de terceiros

Permita que serviços de terceiros na sua conta tenham acesso a serviços de terceiros disponíveis no BlueXP . Os serviços de terceiros são serviços em nuvem semelhantes aos serviços oferecidos pela NetApp, mas são gerenciados e suportados por empresas de terceiros.

**Passos**

1. Na parte superior do BlueXP , selecione a lista suspensa **conta** e selecione **Gerenciar conta**.
2. Na guia **Visão geral**, ative a configuração **permitir serviços de terceiros**.

## Crie outra conta do BlueXP

Ao configurar o BlueXP  no modo restrito ou privado, você será solicitado a criar uma conta *BlueXP* , que permite gerenciar usuários e organizar recursos. Essa conta pode ser tudo o que você precisa, mas se sua empresa precisar de várias contas, você precisará criar contas adicionais usando a API do Tenancy.

Se você estiver usando o BlueXP  no modo padrão, você não terá uma conta do BlueXP . Em vez disso, você terá uma organização que você gerencia usando o gerenciamento de identidade e acesso do BlueXP  (IAM). "Saiba mais sobre o BlueXP  IAM".

**Passos**

1. Use a seguinte chamada de API para criar uma conta BlueXP  adicional:

   POST `/tenancy/account/{accountName}`

   Se você quiser ativar o modo restrito, você precisa incluir o seguinte no corpo da solicitação:

```
{
  "isSaasDisabled": true
}
```

Você não pode alterar a configuração do modo restrito depois que o BlueXP  criar a conta. Não é possível ativar o modo restrito mais tarde e não é possível desativá-lo mais tarde. Ele deve ser definido no momento da criação da conta.

"Saiba como usar essa chamada de API"

**Informações relacionadas**

- "Saiba mais sobre as contas do BlueXP "
- "Saiba mais sobre os modos de implantação do BlueXP"

## Funções de utilizador

Quando você usa o BlueXP  no modo restrito ou privado, você usará uma conta *BlueXP* para gerenciar usuários. Você pode fornecer permissões específicas para usuários em sua conta selecionando uma das seguintes funções: Administrador de conta, Administrador do espaço de trabalho, Visualizador de conformidade e Administrador do SnapCenter

Se você estiver usando o BlueXP  no modo padrão, você não terá uma conta do BlueXP . Em vez disso, você terá uma organização *BlueXP*  que você gerencia usando o gerenciamento de identidade e acesso do BlueXP (IAM).

- "Saiba mais sobre o BlueXP  IAM"
- "Saiba mais sobre os modos de implantação do BlueXP"

| Tarefa | Administrador da conta | Admin da área de trabalho | Visualizador de conformidade | Administrador do SnapCenter |
|---|---|---|---|---|
| Crie conetores | Sim | Não | Não | Não |
| Gerenciar ambientes de trabalho | Sim | Sim | Não | Sim |
| Ativar serviços em ambientes de trabalho | Sim | Sim | Não | Sim |
| Use os serviços do BlueXP | Sim | Sim | Não | Sim |
| Remover ambientes de trabalho de uma área de trabalho | Sim | Sim | Não | Não |
| Eliminar ambientes de trabalho | Sim | Sim | Não | Não |
| Exibir status de replicação de dados | Sim | Sim | Não | Não |
| Veja a linha do tempo | Sim | Sim | Não | Não |
| Alterne entre espaços de trabalho | Sim | Sim | Sim | Sim |

| Tarefa | Administrador da conta | Admin da área de trabalho | Visualizador de conformidade | Administrador do SnapCenter |
|---|---|---|---|---|
| Ver os resultados da análise de classificação BlueXP | Sim | Sim | Sim | Não |
| Receba o relatório Cloud Volumes ONTAP | Sim | Não | Não | Não |
| Gerenciar contas do BlueXP | Sim | Não | Não | Não |
| Gerenciar credenciais | Sim | Sim | Não | Não |
| Modificar as definições do BlueXP | Sim | Sim | Não | Não |
| Visualize e gerencie o Painel de suporte | Sim | Sim | Não | Não |

**Link relacionado**

"Gerencie sua conta do BlueXP "

# Ative o logon único usando a federação de identidade com o BlueXP

*Federação de identidade* ativa o logon único com o BlueXP para que os usuários possam fazer login usando credenciais de sua identidade corporativa. Para começar, saiba como a federação de identidades funciona com o BlueXP e, em seguida, revise uma visão geral do processo de configuração.

## Federação de identidade com credenciais NSS

Se você usar suas credenciais do site de suporte da NetApp (NSS) para fazer login no BlueXP , não deverá seguir as instruções nesta página para configurar a federação de identidade. Em vez disso, você deve fazer o seguinte:

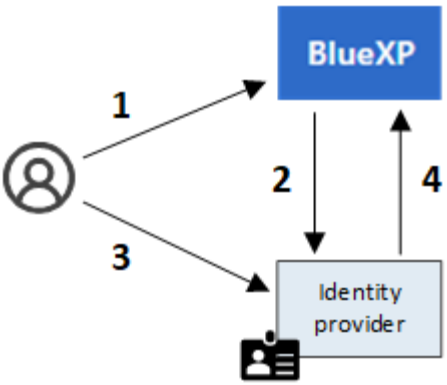
- Baixe e complete o. "Formulário de solicitação de Federação NetApp"
- Envie o formulário para o endereço de e-mail especificado no formulário

A equipe de Gerenciamento de identidade e Acesso do NetApp revisará sua solicitação.

## Como funciona a federação de identidade

A configuração da federação de identidade cria uma conexão confiável entre o provedor de serviços de autenticação (auth0) da BlueXP e seu próprio provedor de gerenciamento de identidade.

A imagem a seguir mostra como a federação de identidade funciona com o BlueXP :




1. Um usuário insere seu endereço de e-mail na página de login do BlueXP .
2. O BlueXP  identifica que o domínio de e-mail faz parte de uma conexão federada e envia a solicitação de autenticação para o provedor de identidade usando a conexão confiável.

   Quando você configura uma conexão federada, o BlueXP  sempre usa essa conexão federada para autenticação.

3. O usuário autentica usando credenciais do diretório corporativo.
4. Seu provedor de identidade autentica a identidade do usuário e o usuário está conetado ao BlueXP .

A federação de identidades usa padrões abertos, como a Security Assertion Markup Language 2,0 (SAML) e o OpenID Connect (OIDC).

## Provedores de identidade suportados

O BlueXP  oferece suporte aos seguintes provedores de identidade:

- Provedores de identidade SAML (Security Assertion Markup Language)
- ID do Microsoft Entra
- Serviços de Federação do ative Directory (ADFS)
- PingFederate

O BlueXP  oferece suporte apenas a SSO iniciado por provedor de serviços (iniciado por SP). SSO iniciado pelo provedor de identidade (iniciado por IDP) não é suportado.

## Visão geral do processo de configuração

Antes de configurar uma conexão entre o BlueXP  e seu provedor de gerenciamento de identidade, você deve entender as etapas que precisará tomar para que você possa se preparar adequadamente.

Essas etapas são específicas para usuários que fazem login no BlueXP  usando um login na nuvem do NetApp. Se você usar suas credenciais NSS para fazer login no BlueXP , Saiba como configurar a federação de identidade com credenciais NSS.

#### Provedor de identidade SAML

Em um alto nível, a configuração de uma conexão federada entre o BlueXP  e um provedor de identidade SAML inclui as seguintes etapas:

| Passo | Concluído por | Descrição |
| --- | --- | --- |
| 1 | Administrador do ative Directory (AD) | Configure seu provedor de identidade SAML para habilitar a federação de identidade com o BlueXP .<br><br>Veja as instruções para o seu provedor de identidade SAML:<br><br>• "ADFS"<br>• "Okta"<br>• "OneLogin"<br>• "PingFederate"<br>• "Salesforce"<br>• "SiteMinder"<br>• "SSOCircle"<br><br>Se o seu provedor de identidade não aparecer na lista acima, "siga estas instruções genéricas"<br><br>Execute *não* as etapas que descrevem como criar uma conexão no auth0. Você criará essa conexão na próxima etapa. |
| 2 | Administrador do BlueXP | Aceda ao "Página Configuração da Federação NetApp" e crie a ligação com o BlueXP .<br><br>Para concluir esta etapa, você precisa obter o seguinte do administrador do AD sobre o provedor de identidade:<br><br>• URL de início de sessão<br>• Um certificado de assinatura X509 (formato PEM ou CER)<br>• URL de saída (opcional)<br><br>Depois de criar a conexão usando essas informações, a página Configuração de Federação lista os parâmetros que você pode enviar para o administrador do AD para concluir a configuração na próxima etapa.<br><br>Anote a data de validade do certificado. Você precisa retornar à página Configuração da Federação e atualizar o certificado *before* que expira. Esta é a sua responsabilidade. O BlueXP  não rastreia a data de expiração. É melhor trabalhar com sua equipe do AD para receber alertas a tempo. |
| 3 | AD admin | Conclua a configuração no provedor de identidade usando os parâmetros mostrados na página Configuração da Federação após concluir a etapa 2. |
| 4 | Administrador do BlueXP | Teste e ative a conexão a partir da "Página Configuração da Federação NetApp" Nota que a página é atualizada entre testar a conexão e ativar a conexão. |

### ID do Microsoft Entra

Em um alto nível, a configuração de uma conexão federada entre o BlueXP  e o Microsoft Entra ID inclui as seguintes etapas:

| Passo | Concluído por | Descrição |
|---|---|---|
| 1 | AD admin | Configure o ID do Microsoft Entra para ativar a federação de identidades com o BlueXP .<br><br>"Veja as instruções para registar a aplicação com o Microsoft Entra ID"<br><br>Execute *não* as etapas que descrevem como criar uma conexão no auth0. Você criará essa conexão na próxima etapa. |
| 2 | Administrador do BlueXP | Aceda ao "Página Configuração da Federação NetApp" e crie a ligação com o BlueXP .<br><br>Para concluir esta etapa, você precisa obter o seguinte de seu administrador do AD:<br><br>• ID do cliente<br>• Valor secreto do cliente<br>• Domínio Microsoft Entra ID<br><br>Depois de criar a conexão usando essas informações, a página Configuração de Federação lista os parâmetros que você pode enviar para o administrador do AD para concluir a configuração na próxima etapa.<br><br>Anote a data de expiração da chave secreta. Você precisa retornar à página Configuração da Federação e atualizar o certificado *before* que expira. Esta é a sua responsabilidade. O BlueXP  não rastreia a data de expiração. É melhor trabalhar com sua equipe do AD para receber alertas a tempo. |
| 3 | AD admin | Conclua a configuração no Microsoft Entra ID usando os parâmetros mostrados na página Configuração da Federação depois de concluir a etapa 2. |
| 4 | Administrador do BlueXP | Teste e ative a conexão a partir da "Página Configuração da Federação NetApp" Nota que a página é atualizada entre testar a conexão e ativar a conexão. |

### ADFS

Em um alto nível, a configuração de uma conexão federada entre o BlueXP  e o ADFS inclui as seguintes etapas:

| Passo | Concluído por | Descrição |
|---|---|---|
| 1 | AD admin | Configure o servidor ADFS para habilitar a federação de identidade com o BlueXP .<br><br>"Veja as instruções para configurar o servidor ADFS com auth0" |

| Passo | Concluído por | Descrição |
| --- | --- | --- |
| 2 | Administrador do BlueXP | Aceda ao "Página Configuração da Federação NetApp" e crie a ligação com o BlueXP .<br><br>Para concluir esta etapa, você precisa obter o seguinte do administrador do AD: O URL do servidor ADFS ou o arquivo de metadados de federação.<br><br>Depois de criar a conexão usando essas informações, a página Configuração de Federação lista os parâmetros que você pode enviar para o administrador do AD para concluir a configuração na próxima etapa.<br><br>Anote a data de validade do certificado. Você precisa retornar à página Configuração da Federação e atualizar o certificado *before* que expira. Esta é a sua responsabilidade. O BlueXP  não rastreia a data de expiração. É melhor trabalhar com sua equipe do AD para receber alertas a tempo. |
| 3 | AD admin | Conclua a configuração no servidor ADFS usando os parâmetros mostrados na página Configuração da Federação depois de concluir a etapa 2. |
| 4 | Administrador do BlueXP | Teste e ative a conexão a partir da "Página Configuração da Federação NetApp" Nota que a página é atualizada entre testar a conexão e ativar a conexão. |

**PingFederate**

Em um alto nível, a configuração de uma conexão federada entre o BlueXP  e um servidor PingFederate inclui as seguintes etapas:

| Passo | Concluído por | Descrição |
| --- | --- | --- |
| 1 | AD admin | Configure seu servidor PingFederate para habilitar a federação de identidade com o BlueXP .<br><br>"Veja as instruções para criar uma conexão"<br><br>Execute *não* as etapas que descrevem como criar uma conexão no auth0. Você criará essa conexão na próxima etapa. |

| Passo | Concluído por | Descrição |
|---|---|---|
| 2 | Administrador do BlueXP | Aceda ao "Página Configuração da Federação NetApp" e crie a ligação com o BlueXP .<br><br>Para concluir esta etapa, você precisa obter o seguinte de seu administrador do AD:<br><br>• O URL para o servidor PingFederate<br>• Um certificado de assinatura X509 (formato PEM ou CER)<br><br>Depois de criar a conexão usando essas informações, a página Configuração de Federação lista os parâmetros que você pode enviar para o administrador do AD para concluir a configuração na próxima etapa.<br><br>Anote a data de validade do certificado. Você precisa retornar à página Configuração da Federação e atualizar o certificado *before* que expira. Esta é a sua responsabilidade. O BlueXP não rastreia a data de expiração. É melhor trabalhar com sua equipe do AD para receber alertas a tempo. |
| 3 | AD admin | Conclua a configuração no servidor PingFederate usando os parâmetros mostrados na página Configuração da Federação depois de concluir a etapa 2. |
| 4 | Administrador do BlueXP | Teste e ative a conexão a partir da "Página Configuração da Federação NetApp" Nota que a página é atualizada entre testar a conexão e ativar a conexão. |

### Atualizando uma conexão federada

Depois que o administrador do BlueXP ativar uma conexão, o administrador pode atualizar a conexão a qualquer momento a partir do "Página Configuração da Federação NetApp"

Por exemplo, talvez seja necessário atualizar a conexão carregando um novo certificado.

O administrador do BlueXP que criou a conexão é o único usuário autorizado que pode atualizar a conexão. Se você quiser adicionar administradores adicionais, entre em Contato com o suporte da NetApp.

# Conetores

### Mantenha o conetor VM e o sistema operacional

Manter o sistema operacional no host do conetor é sua responsabilidade. Por exemplo, você deve aplicar atualizações de segurança ao sistema operacional no host do conetor seguindo os procedimentos padrão da sua empresa para distribuição do sistema operacional.

Se você tiver um conetor existente, você deve estar ciente "Alterações nos sistemas operacionais Linux suportados"do .

### Patches do sistema operacional e o conetor

Você não precisa parar nenhum serviço no host do conetor ao aplicar patches de segurança do sistema operacional.

### Tipo de VM ou instância

Se você criou um conetor diretamente do BlueXP , o BlueXP  implantou uma instância de máquina virtual em seu provedor de nuvem usando uma configuração padrão. Depois de criar o conetor, você não deve mudar para uma instância de VM menor que tenha menos CPU ou RAM.

Os requisitos de CPU e RAM são os seguintes:

**CPU**

8 núcleos ou 8 vCPUs

**RAM**

32 GB

"Saiba mais sobre a configuração padrão do conetor".

### Parar o arranque do conetor VM

Se você precisar parar e, em seguida, iniciar a VM Connector, você deve fazê-lo a partir do console do seu provedor de nuvem ou usando os procedimentos padrão para gerenciamento no local.

"Tenha em atenção que o conetor deve estar sempre operacional".

### Conete-se à VM Linux

Se você precisar se conetar à VM Linux em que o conetor é executado, você pode fazer isso usando as opções de conetividade disponíveis no seu provedor de nuvem.

**AWS**

Quando você criou a instância do Connector na AWS, forneceu uma chave de acesso e uma chave secreta da AWS. Você pode usar esse par de chaves para SSH para a instância. O nome de usuário para a instância do EC2 Linux é ubuntu (para conetores criados antes de maio de 2023, o nome de usuário era EC2-user).

"AWS Docs: Conete-se à sua instância do Linux"

**Azure**

Quando você criou a VM Connector no Azure, você especificou um nome de usuário e escolheu autenticar com uma senha ou chave pública SSH. Use o método de autenticação que você escolheu para se conetar à VM.

"Documentos do Azure: SSH na sua VM"

**Google Cloud**

Não é possível especificar um método de autenticação ao criar um conetor no Google Cloud. No entanto, você pode se conectar à instância de VM do Linux usando o Google Cloud Console ou o Google Cloud CLI (gcloud).

"Google Cloud Docs: Conete-se a VMs Linux"

### Altere o endereço IP de um conetor

Se for necessário para a sua empresa, você pode alterar o endereço IP interno e o endereço IP público da instância do conetor que é atribuído automaticamente pelo seu provedor de nuvem.

**Passos**

1. Siga as instruções do seu provedor de nuvem para alterar o endereço IP local ou o endereço IP público (ou ambos) da instância do conetor.
2. Se você alterou o endereço IP público e precisar se conetar à interface de usuário local em execução no conetor, reinicie a instância do conetor para Registrar o novo endereço IP no BlueXP .
3. Se você alterou o endereço IP privado, atualize o local de backup para os arquivos de configuração do Cloud Volumes ONTAP para que os backups estejam sendo enviados para o novo endereço IP privado no conetor.

   Você precisará atualizar o local de backup para cada sistema Cloud Volumes ONTAP.

   a. Na CLI do Cloud Volumes ONTAP, defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

   b. Execute o seguinte comando para exibir o destino de backup atual:

   ```
   system configuration backup settings show
   ```

   c. Execute o seguinte comando para atualizar o endereço IP para o destino de backup:

   ```
   system configuration backup settings modify -destination <target-
   location>
   ```

### Edite as URIs de um conetor

Adicione e remova o URI (Uniform Resource Identifier) para um conetor.

**Passos**

1. Selecione a lista suspensa **Connector** no cabeçalho BlueXP .
2. Selecione **Gerenciar conetores**.
3. Selecione o menu de ação para um conetor e selecione **Edit URIs**.
4. Adicione e remova URIs e selecione **Apply**.

## Instale um certificado assinado pela CA para acesso ao console baseado na Web

Quando você usa o BlueXP  no modo restrito ou no modo privado, a interface do usuário é acessível a partir da máquina virtual do conetor que é implantada na sua região de nuvem ou no local. Por padrão, o BlueXP  usa um certificado SSL autoassinado para fornecer acesso HTTPS seguro ao console baseado na Web em execução no conetor.

Se exigido pela sua empresa, você pode instalar um certificado assinado por uma autoridade de certificação (CA), que oferece melhor proteção de segurança do que um certificado autoassinado. Depois de instalar o certificado, o BlueXP  usa o certificado assinado pela CA quando os usuários acessam o console baseado na Web.

### Antes de começar

Você precisa criar um conetor antes de poder alterar as configurações do BlueXP . "Saiba como criar um conetor".

### Instale um certificado HTTPS

Instale um certificado assinado por uma CA para acesso seguro ao console baseado na Web executado no conetor.

#### Sobre esta tarefa

Você pode instalar o certificado usando uma das seguintes opções:

- Gere uma solicitação de assinatura de certificado (CSR) do BlueXP , envie a solicitação de certificado para uma CA e instale o certificado assinado pela CA no conetor.

  O par de chaves que o BlueXP  usa para gerar o CSR é armazenado internamente no conetor. O BlueXP recupera automaticamente o mesmo par de chaves (chave privada) quando você instala o certificado no conetor.

- Instale um certificado assinado pela CA que você já possui.

  Com esta opção, o CSR não é gerado através do BlueXP . Você gera a CSR separadamente e armazena a chave privada externamente. Ao instalar o certificado, você fornece a chave privada ao BlueXP .

#### Passos

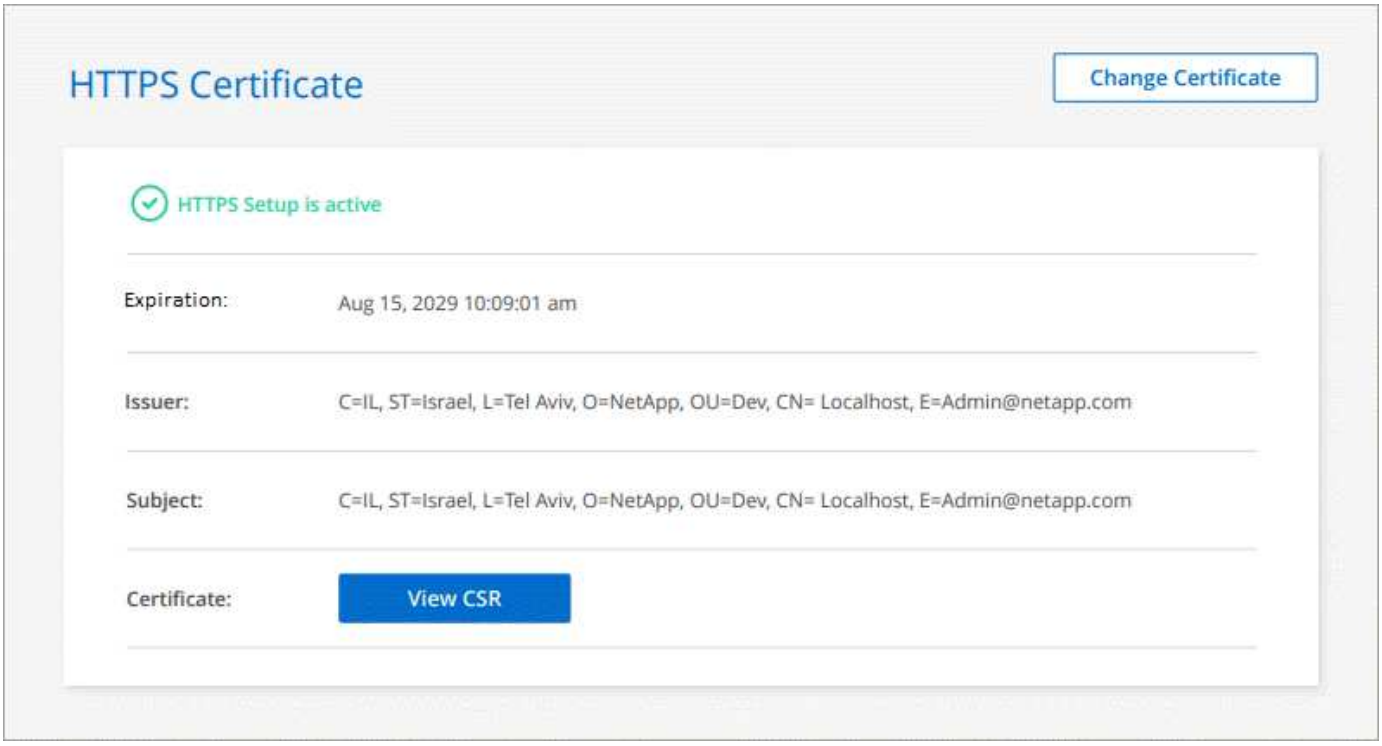
1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **Configuração HTTPS**.


2. Na página Configuração HTTPS, instale um certificado gerando uma solicitação de assinatura de certificado (CSR) ou instalando seu próprio certificado assinado pela CA:

| Opção | Descrição |
| --- | --- |
| Gerar um CSR | a. Insira o nome do host ou DNS do host do conetor (seu Nome Comum) e selecione **Generate CSR**.<br><br>O BlueXP  exibe uma solicitação de assinatura de certificado.<br><br>b. Use o CSR para enviar uma solicitação de certificado SSL a uma CA.<br><br>O certificado deve usar o formato X,509 codificado base-64 de Email Avançado de Privacidade (PEM).<br><br>c. Carregue o arquivo de certificado e selecione **Instalar**. |
| Instale o seu próprio certificado assinado pela CA | a. Selecione **Instalar certificado assinado pela CA**.<br>b. Carregue o arquivo de certificado e a chave privada e selecione **Install**.<br><br>O certificado deve usar o formato X,509 codificado base-64 de Email Avançado de Privacidade (PEM). |

**Resultado**

O BlueXP  agora usa o certificado assinado pela CA para fornecer acesso HTTPS seguro. A imagem a seguir mostra um conetor configurado para acesso seguro:




**Renove o certificado HTTPS BlueXP**

Você deve renovar o certificado HTTPS BlueXP  antes que ele expire para garantir o acesso seguro ao console BlueXP . Se você não renovar o certificado antes que ele expire, um aviso será exibido quando os usuários acessarem o console da Web usando HTTPS.

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **Configuração HTTPS**.

   Detalhes sobre o certificado BlueXP  são exibidos, incluindo a data de expiração.

2. Selecione **alterar certificado** e siga as etapas para gerar um CSR ou instalar seu próprio certificado assinado pela CA.

**Resultado**

O BlueXP  usa o novo certificado assinado pela CA para fornecer acesso HTTPS seguro.

## Configure um conetor para usar um servidor proxy

Se suas políticas corporativas exigirem que você use um servidor proxy para toda a comunicação com a Internet, você precisará configurar seus conetores para usar esse servidor proxy. Se você não configurou um conetor para usar um servidor proxy durante a instalação, então você pode configurar o conetor para usar esse servidor proxy a qualquer momento.

Configurar o conetor para usar um servidor proxy fornece acesso de saída à Internet se um endereço IP público ou um gateway NAT não estiver disponível. Este servidor proxy fornece apenas o conetor com uma conexão de saída. Ele não fornece nenhuma conetividade para sistemas Cloud Volumes ONTAP.

Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída à Internet para enviar mensagens AutoSupport, o BlueXP  configurará automaticamente esses sistemas Cloud Volumes ONTAP para usar um servidor proxy incluído no conetor. O único requisito é garantir que o grupo de segurança do conetor permita conexões de entrada pela porta 3128. Você precisará abrir essa porta depois de implantar o conetor.

### Configurações compatíveis

- O BlueXP  suporta HTTP e HTTPS.
- O servidor proxy pode estar na nuvem ou na rede.
- O BlueXP  não suporta servidores proxy transparentes.

### Ative um proxy em um conetor

Quando você configura um conetor para usar um servidor proxy, esse conetor e os sistemas Cloud Volumes ONTAP que ele gerencia (incluindo quaisquer mediadores de HA), todos usam o servidor proxy.

Tenha em atenção que esta operação reinicia o conetor. Certifique-se de que o conetor não está a efetuar quaisquer operações antes de prosseguir.

**Passos**

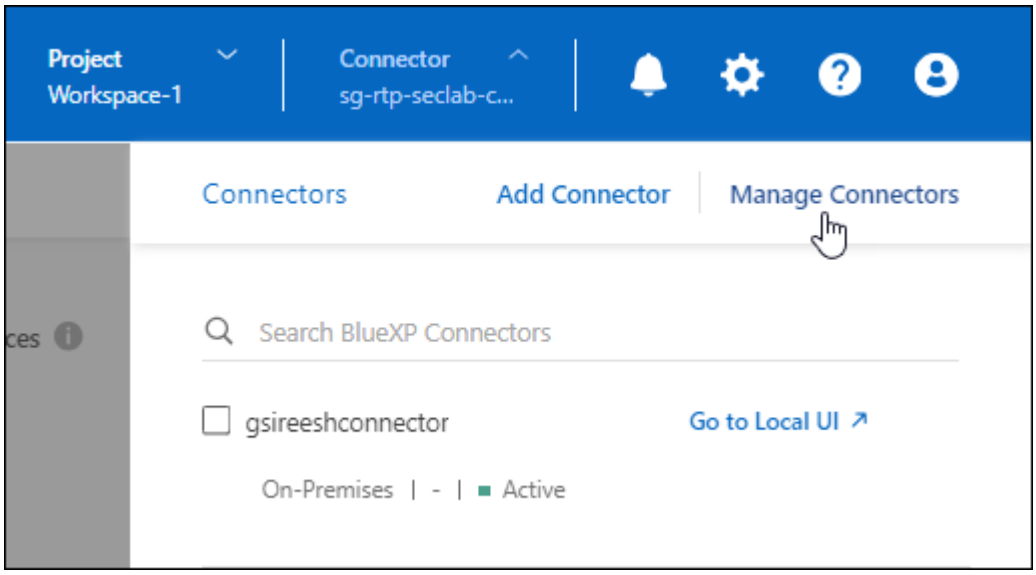
1. Navegue até a página **Edit BlueXP  Connector**.

   A forma como você navega depende se você está usando o BlueXP  no modo padrão (acessando a interface do BlueXP  a partir do site SaaS) ou usando o BlueXP  no modo restrito ou no modo privado (acessando a interface do BlueXP  localmente a partir do host do conetor).

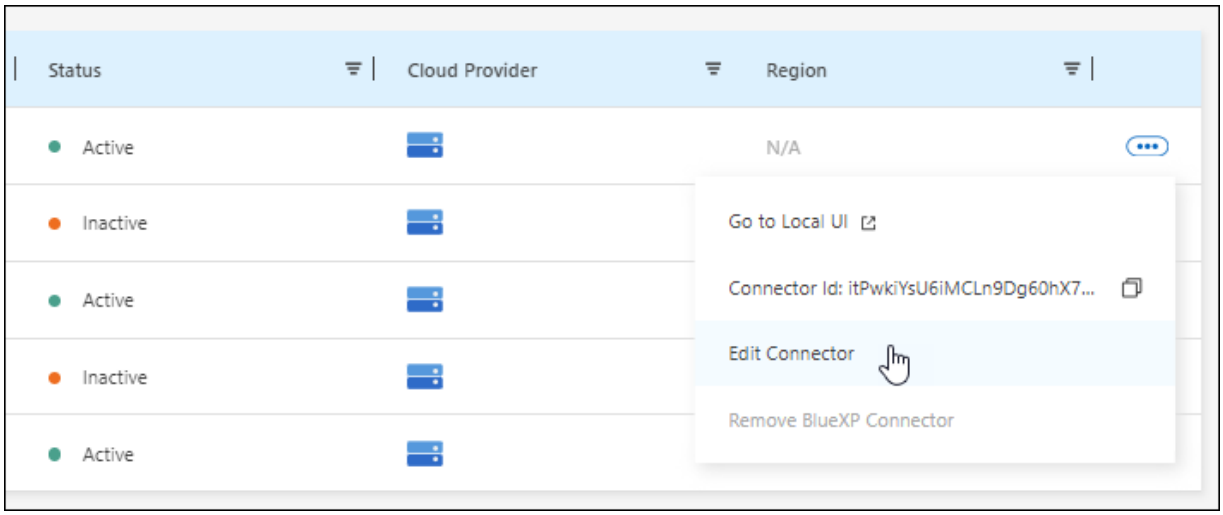
**Modo padrão**

a. Selecione a lista suspensa **Connector** no cabeçalho BlueXP .

b. Selecione **Gerenciar conetores**.



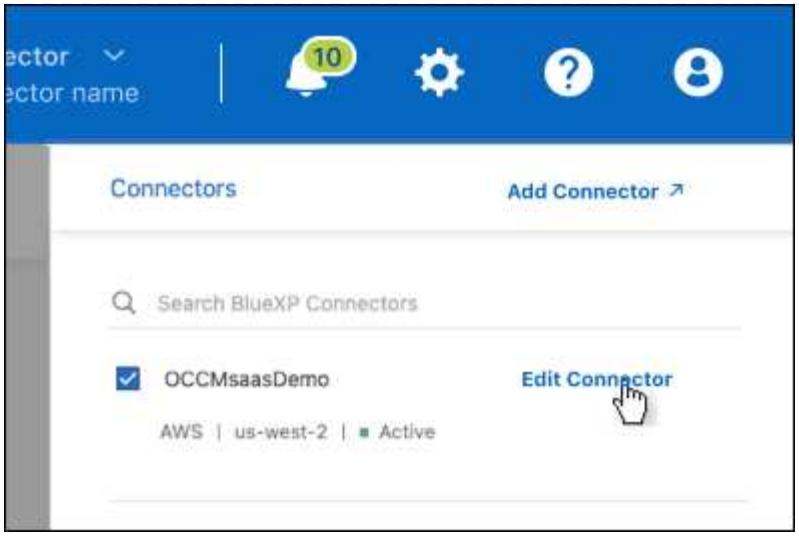

c. Selecione o menu de ação de um conetor e selecione **Editar conetor**.




**Modo restrito ou privado**

a. Selecione a lista suspensa **Connector** no cabeçalho BlueXP .

b. Selecione **Editar conetor**.




2. Selecione **Configuração de proxy HTTP**.
3. Configure o proxy:
   a. Selecione **Ativar proxy**.
   b. Especifique o servidor usando a <a href="http://<em>address:port</em>" class="bare">http://<em>address:port</em></a> sintaxe ou <a href="https://<em>address:port</em>" class="bare">https://<em>address:port</em></a>
   c. Especifique um nome de usuário e uma senha se a autenticação básica for necessária para o servidor.

      Observe o seguinte:

      - O usuário pode ser um usuário local ou usuário de domínio.
      - Para um usuário de domínio, você deve digitar o código ASCII para o nome de domínio%92user-name

        Por exemplo: NetApp%92proxy

      - O BlueXP  não suporta senhas que incluem o caractere A.
   d. Selecione **Guardar**.

### Ative o tráfego direto da API

Se você configurou um conetor para usar um servidor proxy, você pode habilitar o tráfego direto da API no conetor para enviar chamadas de API diretamente para os serviços do provedor de nuvem sem passar pelo proxy. Essa opção é compatível com conetores executados na AWS, no Azure ou no Google Cloud.

Se você desativou o uso de links privados do Azure com o Cloud Volumes ONTAP e estiver usando endpoints de serviço, então você deverá habilitar o tráfego direto da API. Caso contrário, o tráfego não será encaminhado corretamente.

"Saiba mais sobre como usar um link privado do Azure ou endpoints de serviço com o Cloud Volumes ONTAP"

### Passos

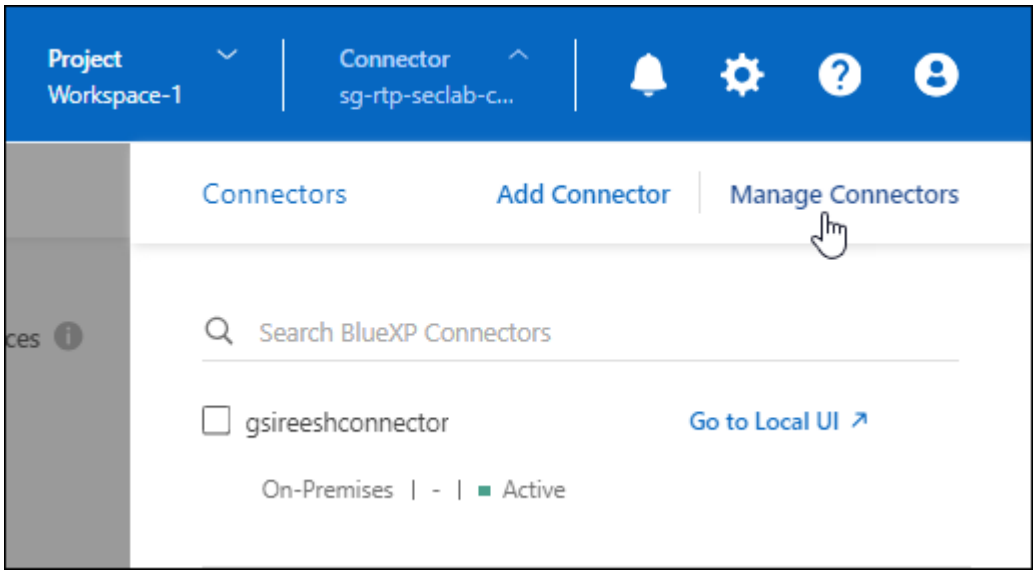
1. Navegue até a página **Edit BlueXP  Connector**:

A forma como você navega depende se você está usando o BlueXP  no modo padrão (acessando a interface do BlueXP  a partir do site SaaS) ou usando o BlueXP  no modo restrito ou no modo privado (acessando a interface do BlueXP  localmente a partir do host do conetor).

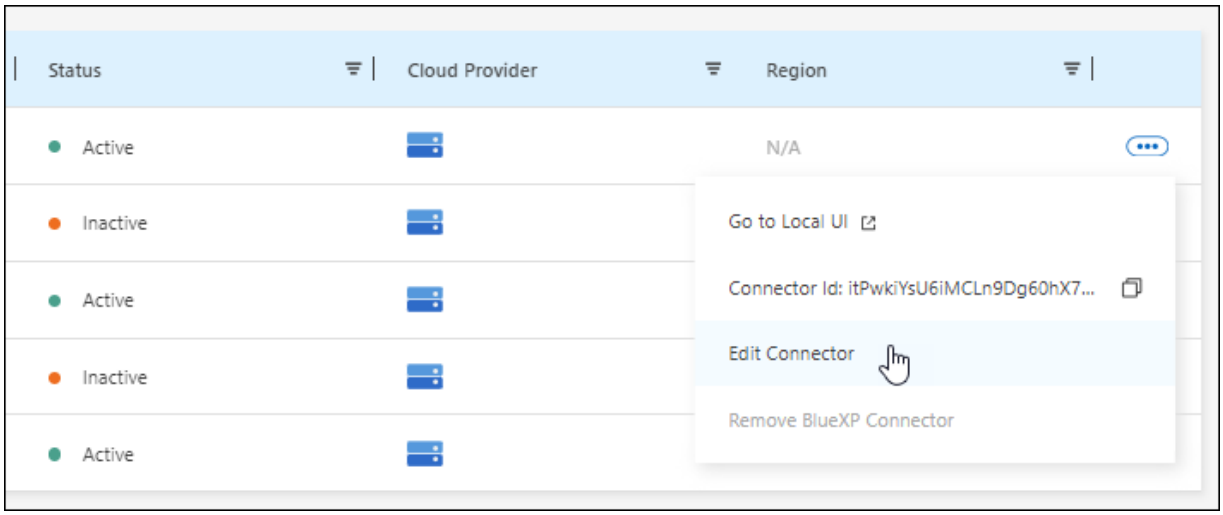
**Modo padrão**

a. Selecione a lista suspensa **Connector** no cabeçalho BlueXP .

b. Selecione **Gerenciar conetores**.



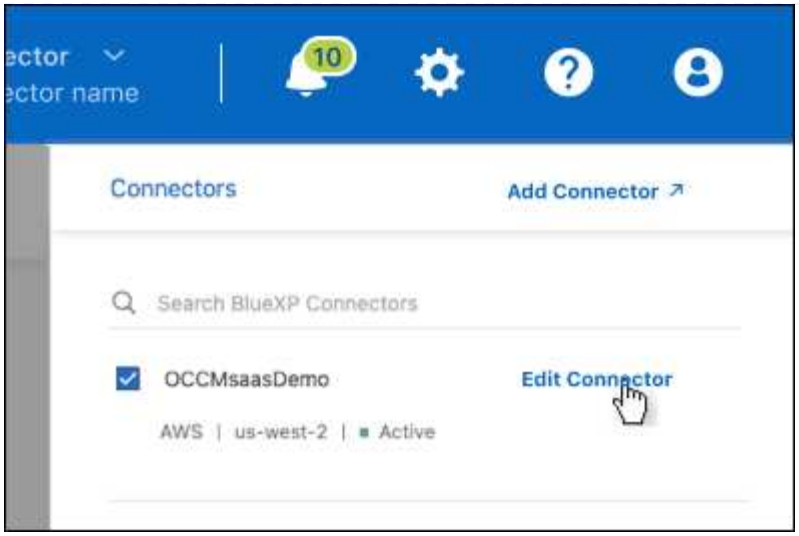

c. Selecione o menu de ação de um conetor e selecione **Editar conetor**.




**Modo restrito ou privado**

a. Selecione a lista suspensa **Connector** no cabeçalho BlueXP .

b. Selecione **Editar conetor**.




2. Selecione **Support Direct API Traffic**.
3. Selecione a caixa de verificação para ativar a opção e, em seguida, selecione **Guardar**.

## Exigir o uso do IMDSv2 em instâncias do Amazon EC2

O BlueXP  oferece suporte ao serviço de metadados de instância do Amazon EC2 versão 2 (IMDSv2) com o conetor 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 ativado 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 conetor 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 após esta versão
- Essa alteração requer 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 fornece proteção aprimorada contra vulnerabilidades. "Saiba mais sobre o IMDSv2 no Blog de Segurança da AWS"

O Serviço de metadados de instância (IMDS) está habilitado da seguinte forma em instâncias EC2:

- Para novas implantações de conetores do BlueXP  ou usando "Scripts do Terraform"o , o IMDSv2 é habilitado por padrão na instância do EC2.
- Se você iniciar uma nova instância do EC2 na AWS e instalar manualmente o software Connector, o IMDSv2 também será habilitado por padrão.

- Se você iniciar o conetor no AWS Marketplace, o IMDSv1 será habilitado por padrão. Você pode configurar manualmente o IMDSv2 na instância do EC2.
- Para os conetores existentes, IMDSv1 ainda é suportado, mas você pode configurar manualmente IMDSv2 na instância 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 de IMDSv2 na instância do conetor:

   a. Conete-se à VM Linux para o conetor.

      Quando você criou a instância do Connector na AWS, forneceu uma chave de acesso e uma chave secreta da AWS. Você pode usar esse par de chaves para SSH para a instância. O nome de usuário para a instância do EC2 Linux é ubuntu (para conetores criados antes de maio de 2023, o nome de usuário era EC2-user).

      "AWS Docs: Conete-se à sua instância do Linux"

   b. Instale a AWS CLI.

      "AWS Docs: Instale ou atualize para a versão mais recente da AWS CLI"

   c. Use o `aws ec2 modify-instance-metadata-options` comando para exigir o uso de IMDSv2 e para 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` parâmetro define IMDSv2 como obrigatório. Quando `http-tokens` for necessário, também tem de definir `http-endpoint` como ativado.

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

   a. Vá para "Console do Amazon EC2"

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

   c. Selecione uma instância do Cloud Volumes ONTAP.

   d. Selecione **ações > Configurações de instância > Modificar opções de metadados de instância**.

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

      - Para **Serviço de metadados de instância**, selecione **Ativar**.
      - Para **IMDSv2**, selecione **obrigatório**.
      - Selecione **Guardar**.

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

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

**Resultado**

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

## Atualize um conetor ao usar o modo privado

Se você estiver usando o BlueXP no modo privado, poderá atualizar o conetor quando uma versão mais recente estiver disponível no site de suporte da NetApp.

Quando você usa o BlueXP no modo padrão ou no modo restrito, você não precisa atualizar manualmente o conetor. O BlueXP atualiza automaticamente um conetor para a versão mais recente, desde que o conetor tenha acesso de saída à Internet para obter a atualização de software.

**Sobre esta tarefa**

O conetor precisa reiniciar durante o processo de atualização para que o console baseado na Web fique indisponível durante a atualização.

**Passos**

1. Transfira o software do conetor a partir do "Site de suporte da NetApp".

   Certifique-se de baixar o instalador offline para redes privadas sem acesso à Internet.

2. Copie o instalador para o host Linux.
3. Atribua permissões para executar o script.

   ```
   chmod +x /path/BlueXP-Connector-offline-<version>
   ```

   Onde <version> é a versão do conetor que você baixou.

4. Execute o script de instalação:

   ```
   sudo /path/BlueXP-Connector-offline-<version>
   ```

   Onde <version> é a versão do conetor que você baixou.

5. Após a conclusão da atualização, você pode verificar a versão do conetor acessando **Ajuda > suporte > conetor**.

## Trabalhe com vários conetores

Se você usar vários conetores, o BlueXP permite alternar entre esses conetores diretamente do console. Você também pode gerenciar um único ambiente de trabalho com vários conetores.

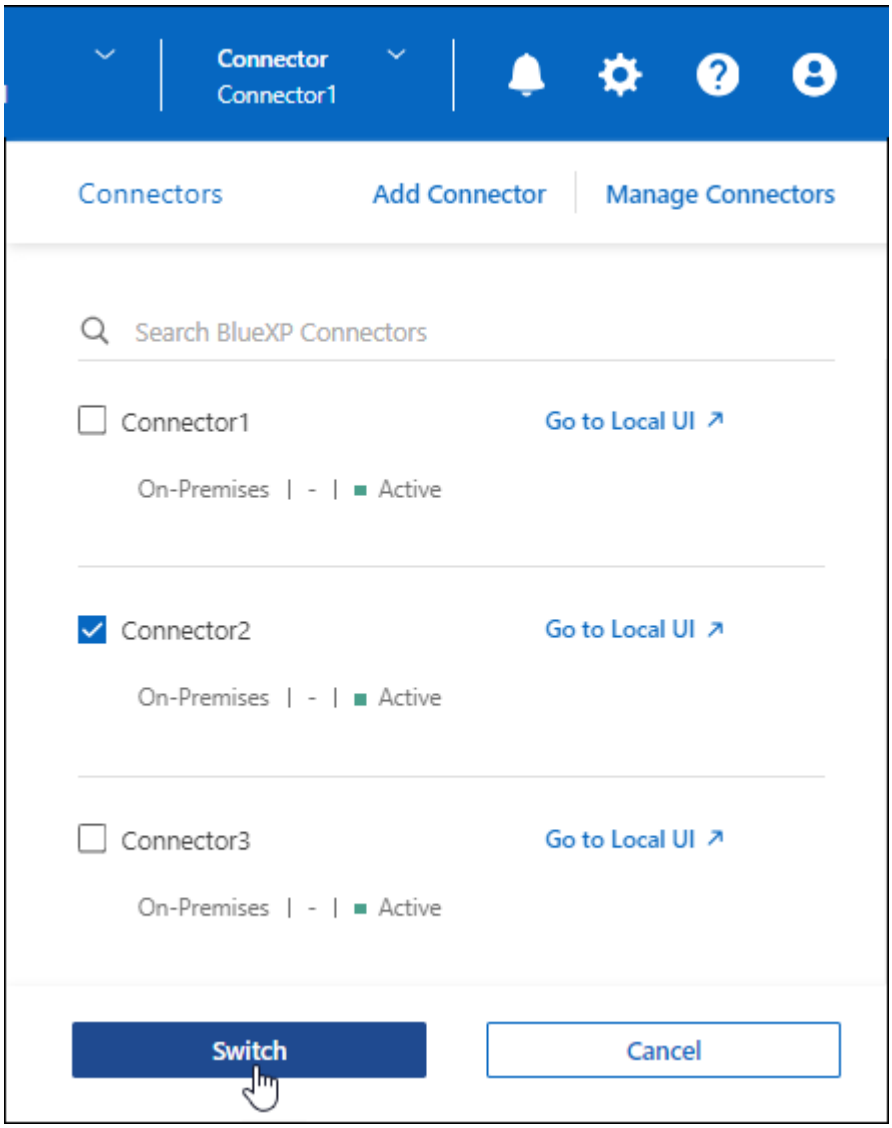
### Alternar entre os conetores

Se você tiver vários conetores, pode alternar entre eles para ver os ambientes de trabalho associados a um conetor específico.

Por exemplo, digamos que você está trabalhando em um ambiente multicloud. Você pode ter um conetor na AWS e outro no Google Cloud. Você precisa alternar entre esses conetores para gerenciar os sistemas Cloud Volumes ONTAP executados nessas nuvens.

**Passo**

1. Selecione a lista suspensa **Connector**, selecione outro conetor e, em seguida, selecione **Switch**.




**Resultado**

O BlueXP  atualiza e mostra os ambientes de trabalho associados ao conetor selecionado.

### Configure uma configuração de recuperação de desastres

Você pode gerenciar um ambiente de trabalho com vários conetores ao mesmo tempo para fins de recuperação de desastres. Se um conetor descer, você pode alternar para o outro conetor para gerenciar imediatamente o ambiente de trabalho.

**Passos**

1. Mude para o outro conetor que você deseja gerenciar com o ambiente de trabalho.
2. Descubra o ambiente de trabalho existente.
   - "Adicione sistemas Cloud Volumes ONTAP existentes ao BlueXP "
   - "Descubra os clusters do ONTAP"
3. Se estiver a gerir um ambiente de trabalho Cloud Volumes ONTAP, selecione **Definições > Definições do conetor** e defina o modo de gestão de capacidade para **modo manual**.

   Para evitar problemas de contenção, apenas o conetor principal deve ser definido como **modo Automático**.

   "Saiba mais sobre o modo de gerenciamento de capacidade"

## Solucione o problema do conetor

Para solucionar problemas com o conetor, você pode trabalhar com o suporte da NetApp, que pode solicitar a ID do sistema, a versão do conetor ou as mensagens mais recentes do AutoSupport. Você também pode visualizar a base de dados de Conhecimento da NetApp para solucionar problemas sozinho.

**Link relacionado**

"Obtenha ajuda do suporte da NetApp".

### Localize a ID do sistema para um conetor

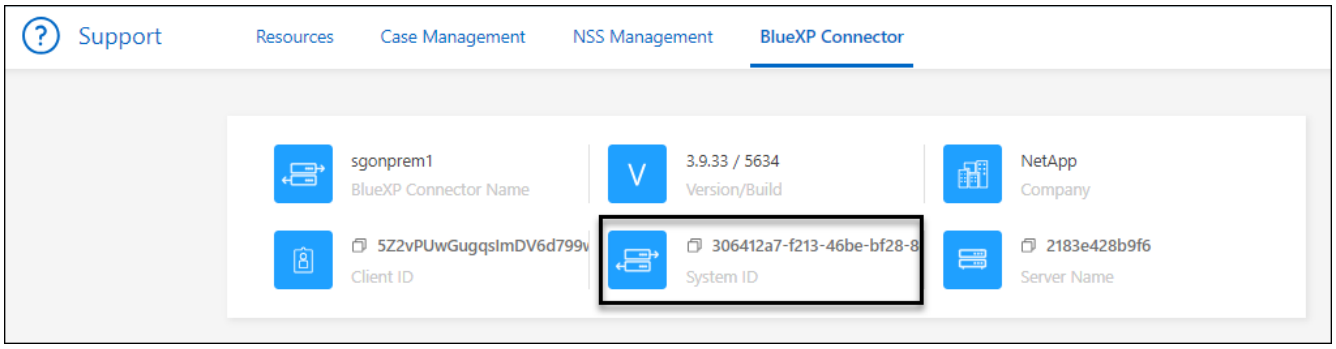
Para ajudá-lo a começar, o representante da NetApp poderá pedir-lhe a ID do sistema do seu conetor. O ID é normalmente utilizado para fins de licenciamento e resolução de problemas.

**Passos**

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda.
2. Selecione **suporte > conetor BlueXP** .

   A ID do sistema aparece na parte superior da página.

   **Exemplo**



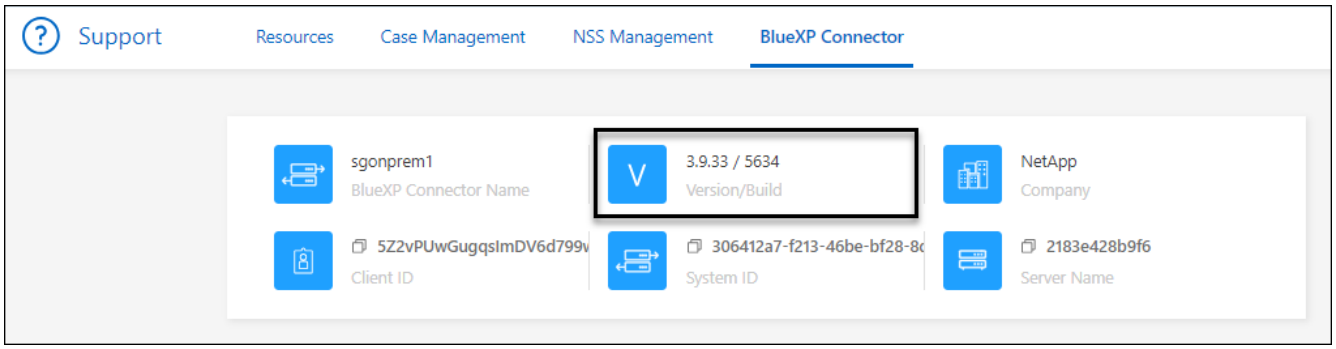
### Ver a versão de um conetor

Você pode visualizar a versão do conetor para verificar se o conetor foi atualizado automaticamente para a versão mais recente ou porque você precisa compartilhá-lo com seu representante da NetApp.

**Passos**

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda.
2. Selecione **suporte > conetor BlueXP** .

   A versão é exibida na parte superior da página.

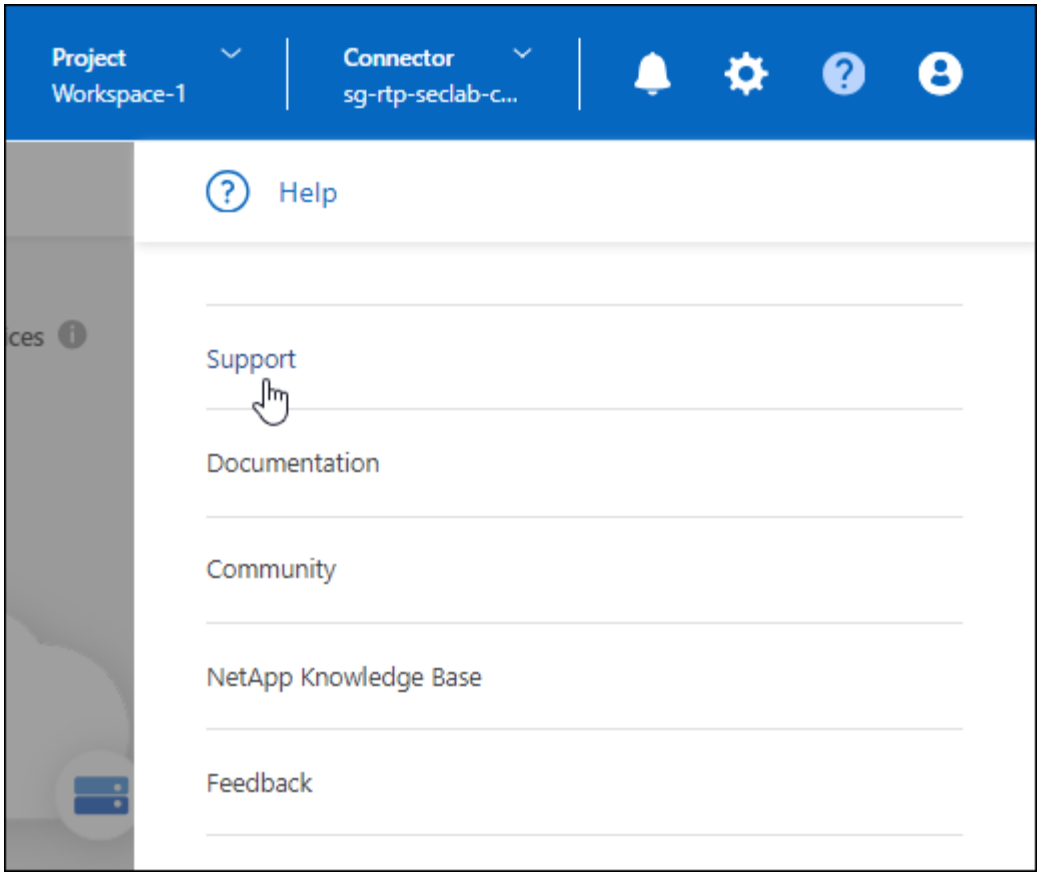



### Transfira ou envie uma mensagem AutoSupport

Se você estiver tendo problemas, a equipe do NetApp pode pedir que você envie uma mensagem do AutoSupport para o suporte do NetApp para fins de solução de problemas.

**Passos**

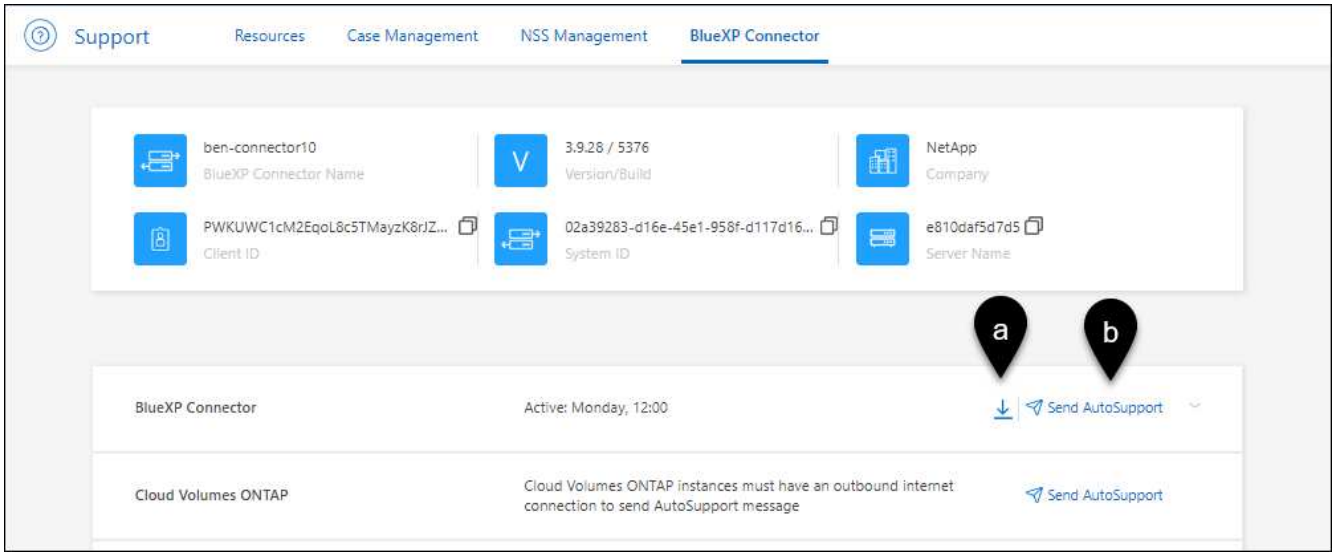
1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda e selecione **suporte**.




2. Selecione **BlueXP  Connector**.
3. Dependendo de como você precisa enviar as informações para o suporte do NetApp, escolha uma das seguintes opções:

   a. Selecione a opção para transferir a mensagem AutoSupport para a sua máquina local. Em seguida, você pode enviá-lo para o suporte da NetApp usando um método preferido.

   b. Selecione **Enviar AutoSupport** para enviar diretamente a mensagem para o suporte da NetApp.



### Corrigir falhas de download ao usar um gateway NAT do Google Cloud

O conetor transfere automaticamente atualizações de software para o Cloud Volumes ONTAP. O download pode falhar se a configuração usar um gateway NAT do Google Cloud. Você pode corrigir esse problema limitando o número de partes nas quais a imagem do software está dividida. Esta etapa deve ser concluída usando a API do BlueXP .

**Passo**

1. Envie uma SOLICITAÇÃO PUT para /occm/config com o seguinte JSON como corpo:

```
{
  "maxDownloadSessions": 32
}
```

   O valor para *maxDownloadSessions* pode ser 1 ou qualquer número inteiro maior que 1. Se o valor for 1, a imagem transferida não será dividida.

   Note que 32 é um valor de exemplo. O valor que você deve usar depende da configuração NAT e do número de sessões que você pode ter simultaneamente.

"Saiba mais sobre a chamada API /occm/config"

### Obtenha ajuda da base de dados de Conhecimento da NetApp

"Veja as informações de solução de problemas criadas pela equipe de suporte da NetApp".

## Desinstale e remova o conetor

Desinstale o software do conetor para solucionar problemas ou remover permanentemente o software do host. As etapas que você precisa usar dependem do modo de implantação que você está usando. Depois de remover um conetor do seu ambiente, você pode removê-lo do BlueXP .

"Saiba mais sobre os modos de implantação do BlueXP".

### Desinstale o conetor ao utilizar o modo padrão ou restrito

Se você estiver usando o BlueXP  no modo padrão ou no modo restrito (em outras palavras, o host do conetor tem conetividade de saída), siga as etapas abaixo para desinstalar o software do conetor.

**Passos**

1. Conete-se à VM Linux para o conetor.
2. A partir do host Linux, execute o script de desinstalação:

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

   *silent* executa o script sem solicitar confirmação.

**Resultado**

O software Connector agora é desinstalado do host Linux.

### Desinstale o conetor ao utilizar o modo privado

Se você estiver usando o BlueXP  no modo privado (em outras palavras, o host do conetor tem conetividade *no* de saída), siga as etapas abaixo para desinstalar o software do conetor.

**Passo**

1. Conete-se à VM Linux para o conetor.
2. A partir do host Linux, execute os seguintes comandos:

```
/opt/application/netapp/ds/cleanup.sh
rm -rf /opt/application/netapp/ds
```

**Resultado**

O software Connector agora é desinstalado do host Linux.

### Remova os conetores do BlueXP

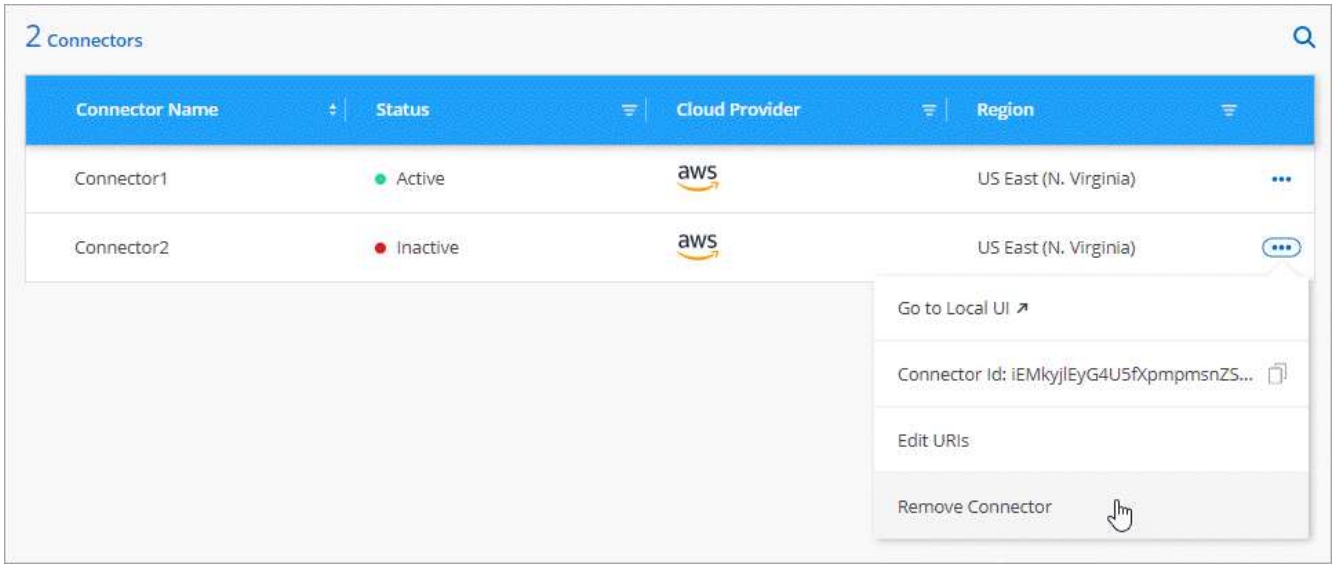
Se um conetor estiver inativo, você pode removê-lo da lista de conetores no BlueXP . Pode fazê-lo se tiver eliminado a máquina virtual do conetor ou se tiver desinstalado o software do conetor.

Observe o seguinte sobre como remover um conetor:

- Esta ação não exclui a máquina virtual.
- Esta ação não pode ser revertida - uma vez que você remover um conetor do BlueXP , você não pode adicioná-lo de volta.

**Passos**

1. Selecione a lista suspensa **Connector** no cabeçalho BlueXP .
2. Selecione **Gerenciar conetores**.
3. Selecione o menu de ação para um conetor inativo e selecione **Remover conetor**.




4. Introduza o nome do conetor para confirmar e, em seguida, selecione **Remover**.

**Resultado**

O BlueXP  remove o conetor dos seus registos.

## Configuração padrão para o conetor

Talvez você queira saber mais sobre a configuração do conetor antes de implantá-lo ou se precisar solucionar problemas.

### Configuração padrão com acesso à Internet

Os detalhes de configuração a seguir se aplicam se você implantou o conetor do BlueXP , a partir do mercado do seu provedor de nuvem, ou se você instalou manualmente o conetor em um host Linux local que tem acesso à Internet.

#### Detalhes AWS

Se você implantou o conetor da BlueXP  ou do mercado do provedor de nuvem, observe o seguinte:

- O tipo de instância EC2 é t3,2xlarge.
- O sistema operacional para a imagem é Ubuntu 22,04 LTS.

  O sistema operacional não inclui uma GUI. Tem de utilizar um terminal para aceder ao sistema.

- A instalação inclui o Docker Engine, que é a ferramenta de orquestração de contentores necessária.
- O nome de usuário para a instância do EC2 Linux é ubuntu (para conetores criados antes de maio de 2023, o nome de usuário era EC2-user).
- O disco padrão do sistema é um disco GP2 de 100 gib.

#### Detalhes do Azure

Se você implantou o conetor da BlueXP  ou do mercado do provedor de nuvem, observe o seguinte:

- O tipo de VM é Standard_D8s_v3.
- O sistema operacional para a imagem é Ubuntu 22,04 LTS.

  O sistema operacional não inclui uma GUI. Tem de utilizar um terminal para aceder ao sistema.

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

#### Detalhes do Google Cloud

Se você implantou o conetor do BlueXP , observe o seguinte:

- A instância da VM é n2-standard-8.
- O sistema operacional para a imagem é Ubuntu 22,04 LTS.

  O sistema operacional não inclui uma GUI. Tem de utilizar um terminal para aceder ao sistema.

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

#### Pasta de instalação

A pasta de instalação do conetor reside no seguinte local:

/opt/application/NetApp/cloudmanager

#### Ficheiros de registo

Os arquivos de log estão contidos nas seguintes pastas:

- /opt/application/NetApp/cloudmanager/log or
- /opt/application/NetApp/service-manager-2/logs (começando com novas instalações 3.9.23)

  Os registos nestas pastas fornecem detalhes sobre o conetor.

- /opt/application/NetApp/cloudmanager/docker_occm/data/log

  Os logs nesta pasta fornecem detalhes sobre os serviços de nuvem e o serviço BlueXP  que é executado no conetor.

#### Serviço do conetor

- O serviço BlueXP  é chamado occm.
- O serviço occm depende do serviço MySQL.

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

#### Portas

O conetor 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 conetor em um host Linux local que não tem acesso à Internet. "Saiba mais sobre esta opção de instalação".

- A pasta de instalação do conetor reside 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 as imagens do conetor e do docker.

- Todos os serviços são executados dentro de contentores docker

  Os serviços dependem do serviço runtime do docker em execução

- O conetor usa as seguintes portas no host Linux:

- 80 para acesso HTTP
- 443 para acesso HTTPS

# Credenciais e assinaturas

## AWS

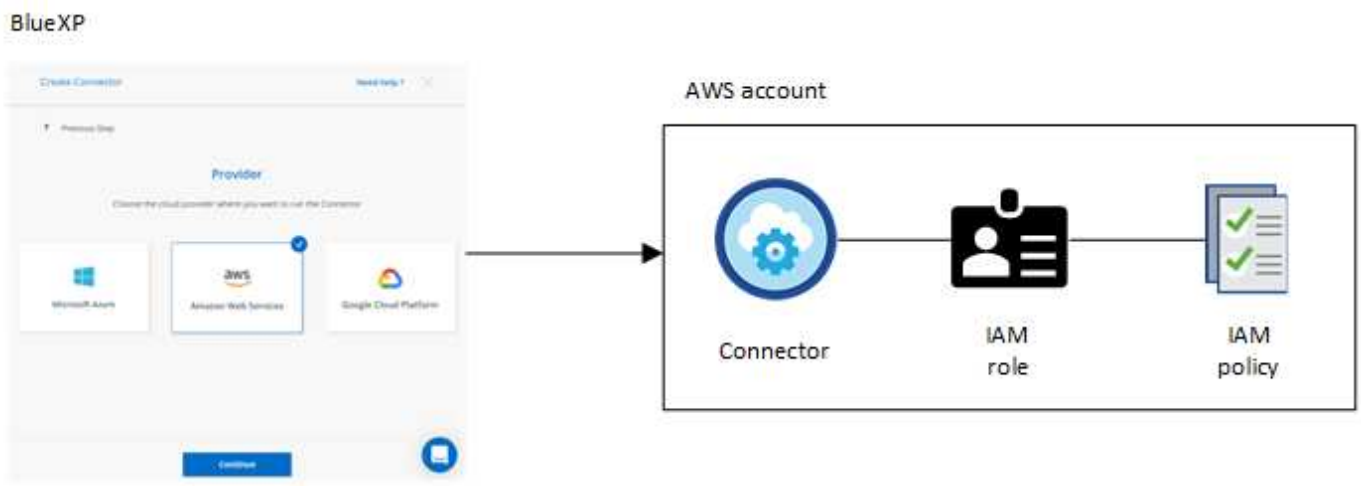
### Saiba mais sobre as credenciais e permissões da AWS

Saiba como o BlueXP  usa credenciais da AWS para executar ações em seu nome e como essas credenciais estão associadas às assinaturas do marketplace. Entender esses detalhes pode ser útil ao gerenciar as credenciais de uma ou mais contas da AWS no BlueXP . Por exemplo, você pode querer saber quando adicionar credenciais adicionais da AWS ao BlueXP .

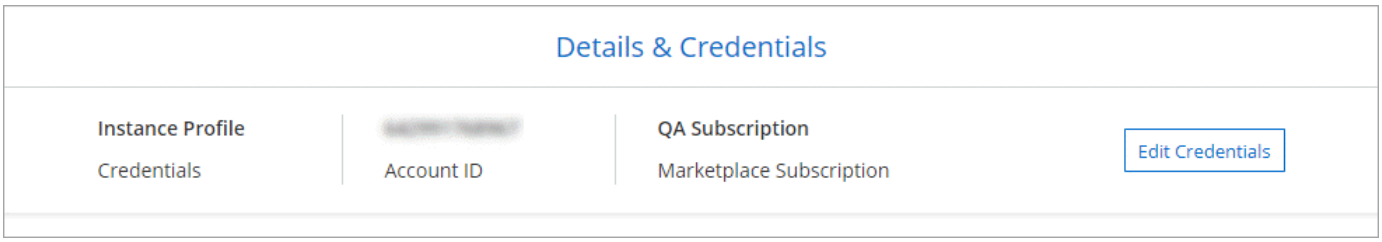
#### Credenciais iniciais da AWS

Ao implantar um conetor do BlueXP , você precisa fornecer o ARN de uma função do IAM ou chaves de acesso para um usuário do IAM. O método de autenticação usado deve ter as permissões necessárias para implantar a instância do conetor na AWS. As permissões necessárias estão listadas no "Política de implantação do Connector para AWS".

Quando o BlueXP  inicia a instância do Connector na AWS, ele cria uma função do IAM e um perfil de instância para a instância. Ele também anexa uma política que fornece ao conetor permissões para gerenciar recursos e processos dentro dessa conta da AWS. "Veja como o BlueXP  usa as permissões".




Se você criar um novo ambiente de trabalho para o Cloud Volumes ONTAP, o BlueXP  selecionará essas credenciais da AWS por padrão:



Você pode implantar todos os seus sistemas Cloud Volumes ONTAP usando as credenciais iniciais da AWS ou adicionar credenciais adicionais.

#### Credenciais adicionais da AWS

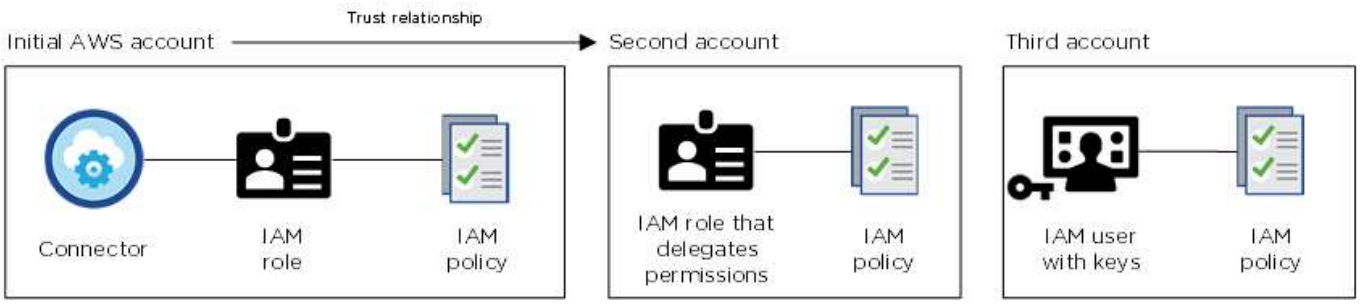
Você pode adicionar credenciais adicionais da AWS ao BlueXP  nos seguintes casos:

- Para usar seu BlueXP  Connector existente com uma conta AWS adicional
- Para criar um novo conetor em uma conta específica da AWS
- Para criar e gerenciar o FSX para sistemas de arquivos ONTAP

Consulte as seções abaixo para obter mais detalhes.

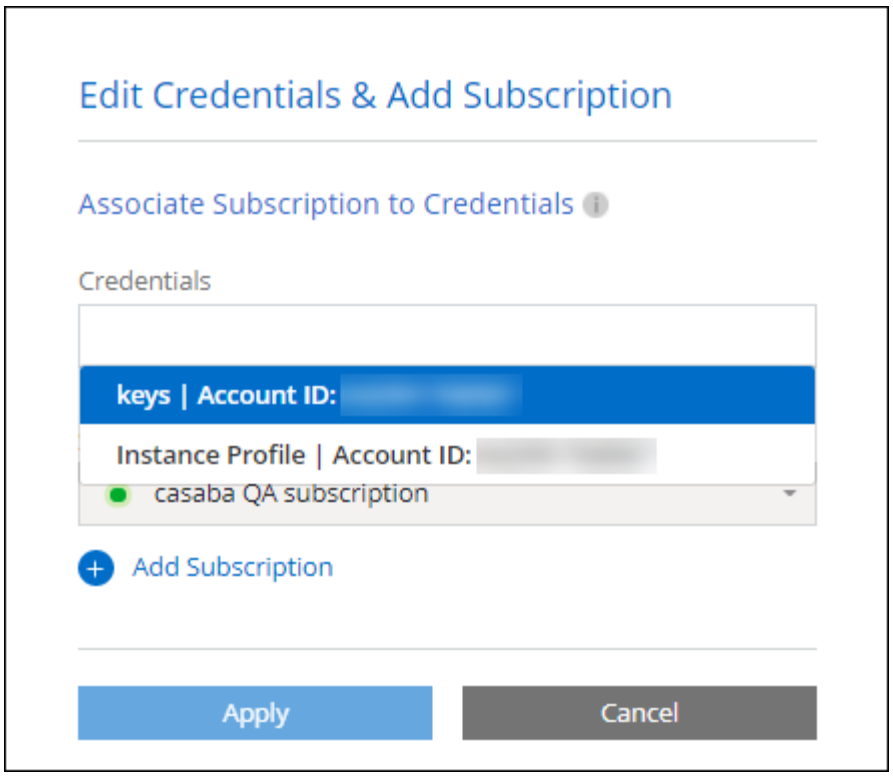
### Adicione credenciais da AWS para usar um conetor com outra conta da AWS

Se você quiser usar o BlueXP  com contas adicionais da AWS, poderá fornecer chaves da AWS para um usuário do IAM ou o ARN de uma função em uma conta confiável. A imagem a seguir mostra duas contas adicionais, uma fornecendo permissões por meio de uma função do IAM em uma conta confiável e outra por meio das chaves da AWS de um usuário do IAM:




Em seguida, você adicionaria as credenciais da conta ao BlueXP  especificando o Nome de recurso do Amazon (ARN) da função do IAM ou as chaves da AWS para o usuário do IAM.

Por exemplo, você pode alternar entre credenciais ao criar um novo ambiente de trabalho do Cloud Volumes ONTAP:




"Saiba como adicionar credenciais da AWS a um conetor existente."

**Adicione credenciais da AWS para criar um conetor**

A adição de novas credenciais da AWS ao BlueXP  fornece as permissões necessárias para criar um conetor.

"Saiba como adicionar credenciais da AWS ao BlueXP  para criar um conetor"

**Adicione credenciais da AWS para o FSX for ONTAP**

Adicionar novas credenciais da AWS ao BlueXP  fornece as permissões necessárias para criar e gerenciar um ambiente de trabalho do FSX for ONTAP.

"Saiba como adicionar credenciais da AWS ao BlueXP  para o Amazon FSX for ONTAP"

**Credenciais e assinaturas de mercado**

As credenciais que você adicionar a um conetor devem estar associadas a uma assinatura do AWS Marketplace para que você possa pagar pelo Cloud Volumes ONTAP a uma taxa por hora (PAYGO) ou por meio de um contrato anual e usar outros serviços da BlueXP .

"Saiba como associar uma assinatura da AWS".

Observe o seguinte sobre as credenciais da AWS e as assinaturas do marketplace:

- Você pode associar apenas uma assinatura do AWS Marketplace a um conjunto de credenciais da AWS
- Você pode substituir uma assinatura existente do mercado por uma nova

**FAQ**

As perguntas a seguir estão relacionadas a credenciais e assinaturas.

### Como posso girar com segurança minhas credenciais da AWS?

Como descrito nas seções acima, o BlueXP  permite que você forneça credenciais da AWS de algumas maneiras: Uma função do IAM associada à instância do Connector, assumindo uma função do IAM em uma conta confiável ou fornecendo chaves de acesso da AWS.

Com as duas primeiras opções, o BlueXP  usa o Serviço de token de segurança da AWS para obter credenciais temporárias que rodam constantemente. Este processo é a melhor prática - é automático e seguro.

Se você fornecer ao BlueXP  as chaves de acesso da AWS, você deve girar as chaves atualizando-as no BlueXP  em um intervalo regular. Este é um processo completamente manual.

### Posso alterar a assinatura do AWS Marketplace para ambientes de trabalho do Cloud Volumes ONTAP?

Sim, você pode. Quando você altera a assinatura do AWS Marketplace associada a um conjunto de credenciais, todos os ambientes de trabalho existentes e novos do Cloud Volumes ONTAP serão cobrados com base na nova assinatura.

"Saiba como associar uma assinatura da AWS".

### Posso adicionar várias credenciais da AWS, cada uma com diferentes assinaturas do marketplace?

Todas as credenciais da AWS que pertencem à mesma conta da AWS serão associadas à mesma assinatura do AWS Marketplace.

Se você tiver várias credenciais da AWS que pertencem a diferentes contas da AWS, essas credenciais poderão ser associadas à mesma assinatura do AWS Marketplace ou a assinaturas diferentes.

### Posso mover os ambientes de trabalho existentes do Cloud Volumes ONTAP para uma conta diferente da AWS?

Não, não é possível mover os recursos da AWS associados ao ambiente de trabalho do Cloud Volumes ONTAP para uma conta diferente da AWS.

### Como as credenciais funcionam para implantações no mercado e implantações locais?

As seções acima descrevem o método de implantação recomendado para o conetor, que é da BlueXP . Você também pode implantar um conetor na AWS a partir do AWS Marketplace e instalar manualmente o software Connector em seu próprio host Linux.

Se você usar o Marketplace, as permissões serão fornecidas da mesma maneira. Você só precisa criar e configurar manualmente a função do IAM e, em seguida, fornecer permissões para quaisquer contas adicionais.

Para implantações locais, você não pode configurar uma função do IAM para o sistema BlueXP , mas pode fornecer permissões usando chaves de acesso da AWS.

Para saber como configurar permissões, consulte as seguintes páginas:

- Modo padrão
  - "Configurar permissões para uma implantação do AWS Marketplace"
  - "Configurar permissões para implantações locais"
- "Configurar permissões para o modo restrito"

- "Configurar permissões para o modo privado"

### Gerencie credenciais da AWS e assinaturas de marketplace para o BlueXP

Adicione e gerencie credenciais da AWS para que o BlueXP  tenha as permissões necessárias para implantar e gerenciar recursos de nuvem em suas contas da AWS. Se você gerenciar várias assinaturas do AWS Marketplace, poderá atribuir cada uma delas a diferentes credenciais da AWS na página credenciais.

#### Visão geral

Você pode adicionar credenciais da AWS a um conetor existente ou diretamente ao BlueXP :

- Adicione credenciais adicionais da AWS a um conetor existente

  A adição de credenciais da AWS a um conetor existente fornece as permissões necessárias para gerenciar recursos e processos em seu ambiente de nuvem pública. Saiba como adicionar credenciais da AWS a um conetor.

- Adicione credenciais da AWS ao BlueXP  para criar um conetor

  A adição de novas credenciais da AWS ao BlueXP  dá ao BlueXP  as permissões necessárias para criar um conetor. Saiba como adicionar credenciais da AWS ao BlueXP .

- Adicione credenciais da AWS ao BlueXP  para o FSX for ONTAP

  Adicionar novas credenciais da AWS ao BlueXP  dá ao BlueXP  as permissões necessárias para criar e gerenciar o FSX for ONTAP. "Saiba como configurar permissões para o FSX for ONTAP"

#### Como girar credenciais

O BlueXP  permite que você forneça credenciais da AWS de algumas maneiras: Uma função do IAM associada à instância do Connector, assumindo uma função do IAM em uma conta confiável ou fornecendo chaves de acesso da AWS. "Saiba mais sobre as credenciais e permissões da AWS".

Com as duas primeiras opções, o BlueXP  usa o Serviço de token de segurança da AWS para obter credenciais temporárias que rodam constantemente. Este processo é a melhor prática porque é automático e seguro.

Se você fornecer ao BlueXP  as chaves de acesso da AWS, você deve girar as chaves atualizando-as no BlueXP  em um intervalo regular. Este é um processo completamente manual.

#### Adicione credenciais adicionais a um conetor

Adicione credenciais adicionais da AWS a um conetor para que ele tenha as permissões necessárias para gerenciar recursos e processos em seu ambiente de nuvem pública. Você pode fornecer o ARN de uma função do IAM em outra conta ou fornecer chaves de acesso da AWS.

Se você está apenas começando com BlueXP "Saiba como o BlueXP  usa credenciais e permissões da AWS", .

### Conceder permissões

Antes de adicionar credenciais da AWS a um conetor, você precisa fornecer as permissões necessárias. As permissões permitem que o BlueXP  gerencie recursos e processos dentro dessa conta da AWS. A forma como você fornece as permissões depende se deseja fornecer ao BlueXP  o ARN de uma função em uma conta confiável ou chaves da AWS.

Se você implantou um conetor do BlueXP , o BlueXP  adicionou automaticamente credenciais da AWS para a conta na qual implantou o conetor. Essa conta inicial não será adicionada se você implantou o conetor do AWS Marketplace ou se instalou manualmente o software Connector em um sistema existente. "Saiba mais sobre as credenciais e permissões da AWS".

### Escolhas

- Conceda permissões assumindo uma função do IAM em outra conta
- Conceda permissões fornecendo chaves da AWS

### Conceda permissões assumindo uma função do IAM em outra conta

Você pode configurar uma relação de confiança entre a conta da AWS de origem na qual implantou a instância do Connector e outras contas da AWS usando funções do IAM. Em seguida, você forneceria ao BlueXP  o ARN das funções do IAM das contas confiáveis.

Se o conetor estiver instalado no local, não poderá utilizar este método de autenticação. Você deve usar as chaves da AWS.

#### Passos

1. Vá para o console do IAM na conta de destino na qual você deseja fornecer permissões ao conetor.
2. Em Gerenciamento de Acesso, selecione **funções > criar função** e siga as etapas para criar a função.

   Certifique-se de fazer o seguinte:

   - Em **tipo de entidade confiável**, selecione **conta AWS**.
   - Selecione **outra conta da AWS** e insira o ID da conta onde reside a instância do conetor.
   - Crie as políticas necessárias copiando e colando o conteúdo "As políticas do IAM para o conetor"do .
3. Copie a função ARN da função IAM para que você possa colá-la no BlueXP  mais tarde.

#### Resultado

A conta agora tem as permissões necessárias. Agora você pode adicionar as credenciais a um conetor.

### Conceda permissões fornecendo chaves da AWS

Se você quiser fornecer ao BlueXP  chaves da AWS para um usuário do IAM, você precisará conceder as permissões necessárias a esse usuário. A política do BlueXP  IAM define as ações e recursos da AWS que o BlueXP  tem permissão para usar.

Você deve usar esse método de autenticação se o conetor estiver instalado no local. Você não pode usar uma função do IAM.

#### Passos

1. No console do IAM, crie políticas copiando e colando o conteúdo "As políticas do IAM para o conetor"do .

"Documentação da AWS: Criando políticas do IAM"

2. Anexe as políticas a uma função do IAM ou a um usuário do IAM.
   - "Documentação da AWS: Criando funções do IAM"
   - "Documentação da AWS: Adicionando e removendo políticas do IAM"

**Resultado**

A conta agora tem as permissões necessárias. Agora você pode adicionar as credenciais a um conetor.

### Adicione as credenciais

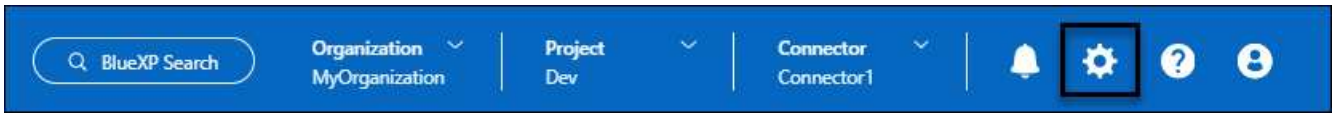
Depois de fornecer uma conta da AWS com as permissões necessárias, você pode adicionar as credenciais dessa conta a um conetor existente. Isso permite que você inicie sistemas Cloud Volumes ONTAP nessa conta usando o mesmo conetor.

**Antes de começar**

Se você acabou de criar essas credenciais no seu provedor de nuvem, talvez demore alguns minutos até que elas estejam disponíveis para uso. Aguarde alguns minutos antes de adicionar as credenciais ao BlueXP .

**Passos**

1. Certifique-se de que o conetor correto está atualmente selecionado no BlueXP .
2. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.



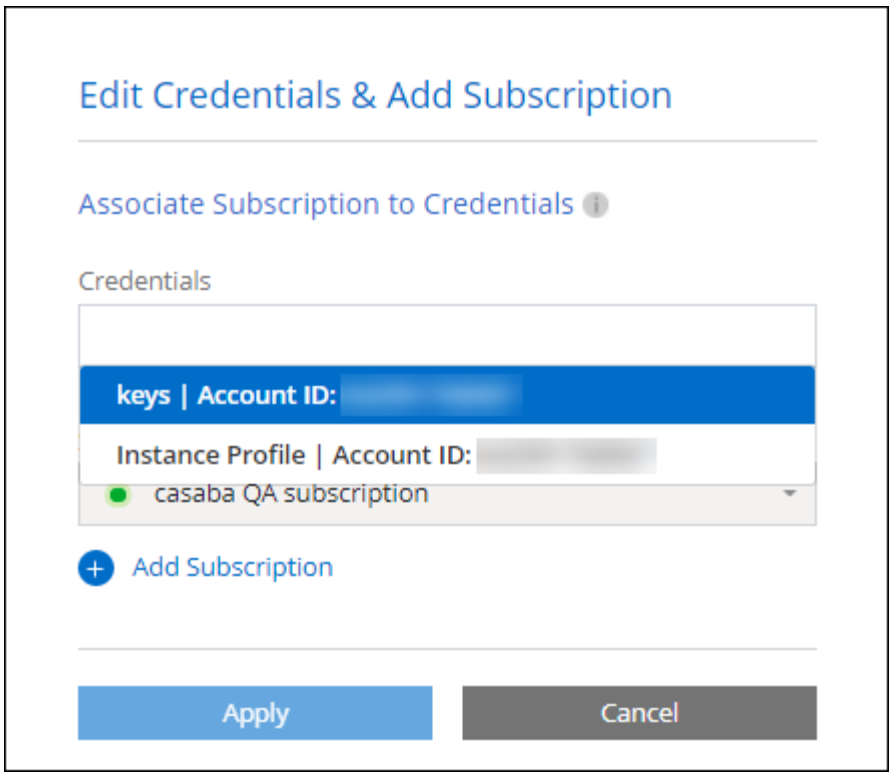

3. Na página **credenciais da organização** ou **credenciais da conta**, selecione **Adicionar credenciais** e siga as etapas no assistente.
   a. **Localização das credenciais**: Selecione **Amazon Web Services > Connector**.
   b. **Definir credenciais**: Forneça o ARN (Amazon Resource Name) de uma função IAM confiável ou insira uma chave de acesso e chave secreta da AWS.
   c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.

      Para pagar por serviços da BlueXP  por uma taxa horária (PAYGO) ou com um contrato anual, as credenciais da AWS precisam estar associadas a uma assinatura do AWS Marketplace.

   d. **Revisão**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

**Resultado**

Agora você pode alternar para um conjunto diferente de credenciais da página Detalhes e credenciais ao criar um novo ambiente de trabalho:




**Adicione credenciais ao BlueXP para criar um conetor**

Adicione credenciais da AWS ao BlueXP fornecendo o ARN de uma função do IAM que dá ao BlueXP as permissões necessárias para criar um conetor. Você pode escolher essas credenciais ao criar um novo conetor.

### Configure a função do IAM

Configure uma função do IAM que permita que a camada de software como serviço (SaaS) do BlueXP assuma a função.

**Passos**

1. Vá para o console do IAM na conta de destino.
2. Em Gerenciamento de Acesso, selecione **funções > criar função** e siga as etapas para criar a função.

   Certifique-se de fazer o seguinte:

   - Em **tipo de entidade confiável**, selecione **conta AWS**.
   - Selecione **outra conta da AWS** e insira o ID do SaaS do BlueXP : 952013314444
   - Crie uma política que inclua as permissões necessárias para criar um conetor.
     - "Veja as permissões necessárias para o FSX for ONTAP"
     - "Exibir a política de implantação do conetor"
3. Copie a função ARN da função IAM para que você possa colá-la no BlueXP na próxima etapa.

**Resultado**

A função do IAM agora tem as permissões necessárias. Agora você pode adicioná-lo ao BlueXP .

### Adicione as credenciais

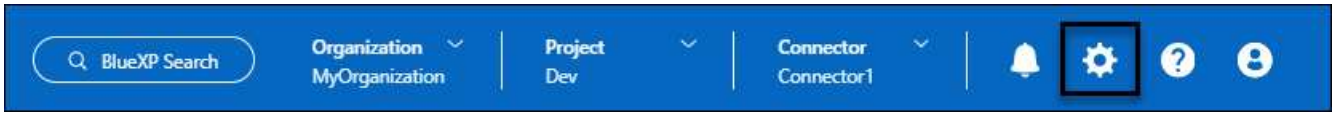
Depois de fornecer a função IAM com as permissões necessárias, adicione a função ARN ao BlueXP .

#### Antes de começar

Se você acabou de criar a função do IAM, pode levar alguns minutos até que eles estejam disponíveis para uso. Aguarde alguns minutos antes de adicionar as credenciais ao BlueXP .

#### Passos

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.




2. Na página **credenciais da organização** ou **credenciais da conta**, selecione **Adicionar credenciais** e siga as etapas no assistente.
   a. **Localização das credenciais**: Selecione **Serviços da Amazon Web > BlueXP** .
   b. **Definir credenciais**: Forneça o ARN (Amazon Resource Name) da função IAM.
   c. **Revisão**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

#### Resultado

Agora você pode usar as credenciais ao criar um novo conetor.

##### Adicione credenciais ao BlueXP  para o Amazon FSX for ONTAP

Para obter mais informações, consulte a. "Documentação do BlueXP  para o Amazon FSX for ONTAP"

##### Associar uma assinatura da AWS

Depois de adicionar suas credenciais da AWS ao BlueXP , você pode associar uma assinatura do AWS Marketplace a essas credenciais. A assinatura permite que você pague pelo Cloud Volumes ONTAP a uma taxa por hora (PAYGO) ou usando um contrato anual e use outros serviços da BlueXP .

Há dois cenários em que você pode associar uma assinatura do AWS Marketplace depois de já ter adicionado as credenciais ao BlueXP :

- Você não associou uma assinatura quando adicionou inicialmente as credenciais ao BlueXP .
- Você deseja alterar a assinatura do AWS Marketplace associada às credenciais da AWS.

  A substituição da assinatura atual do marketplace por uma nova assinatura altera a assinatura do marketplace para todos os ambientes de trabalho existentes da Cloud Volumes ONTAP e todos os novos ambientes de trabalho.

#### Antes de começar

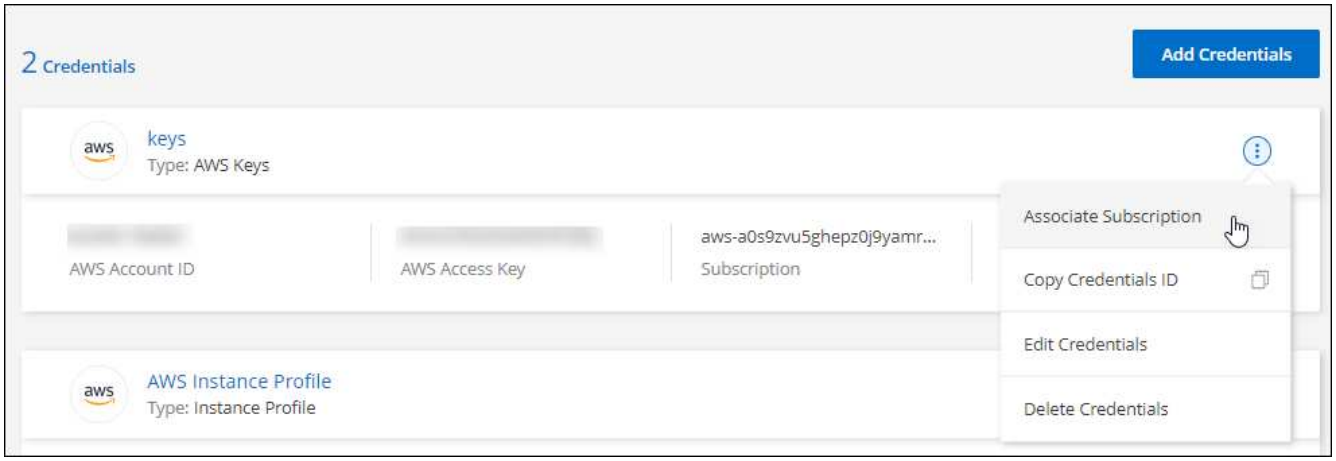
Você precisa criar um conetor antes de poder alterar as configurações do BlueXP . "Saiba como criar um conetor".

#### Passos

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Selecione o menu de ação para um conjunto de credenciais e, em seguida, selecione **assinatura**

**associada**.

Você deve selecionar credenciais associadas a um conetor. Não é possível associar uma assinatura do marketplace a credenciais associadas ao BlueXP .




3. Para associar as credenciais a uma assinatura existente, selecione a assinatura na lista suspensa e selecione **Associate**.
4. Para associar as credenciais a uma nova assinatura, selecione **Adicionar assinatura > continuar** e siga as etapas no AWS Marketplace:

   a. Selecione **Ver opções de compra**.

   b. Selecione **Subscribe**.

   c. Selecione **Configurar a sua conta**.

   Você será redirecionado para o site da BlueXP .

   d. Na página **atribuição de assinatura**:

   - Selecione as organizações ou contas do BlueXP às quais você deseja associar essa assinatura.
   - No campo **Substituir subscrição existente**, escolha se pretende substituir automaticamente a subscrição existente de uma organização ou conta por esta nova subscrição.

     O BlueXP substitui a assinatura existente para todas as credenciais na organização ou conta por essa nova assinatura. Se um conjunto de credenciais nunca foi associado a uma assinatura, essa nova assinatura não será associada a essas credenciais.

   Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo estas etapas.

   - Selecione **Guardar**.

     O vídeo a seguir mostra as etapas para se inscrever no AWS Marketplace:

Inscreva-se no BlueXP no AWS Marketplace

#### Associe uma assinatura existente à sua organização ou conta

Quando você se inscreve no BlueXP no AWS Marketplace, a última etapa do processo é associar a assinatura às suas contas do BlueXP Organizations ou BlueXP no site da BlueXP . Se você não concluiu

esta etapa, não poderá usar a assinatura com sua organização ou conta do BlueXP .

> Se você estiver usando o BlueXP no modo padrão, você terá uma organização *BlueXP* , que você gerencia usando o gerenciamento de identidade e acesso (IAM) do BlueXP . Mas se você estiver usando o BlueXP no modo restrito ou no modo privado, então você terá uma conta *BlueXP* .

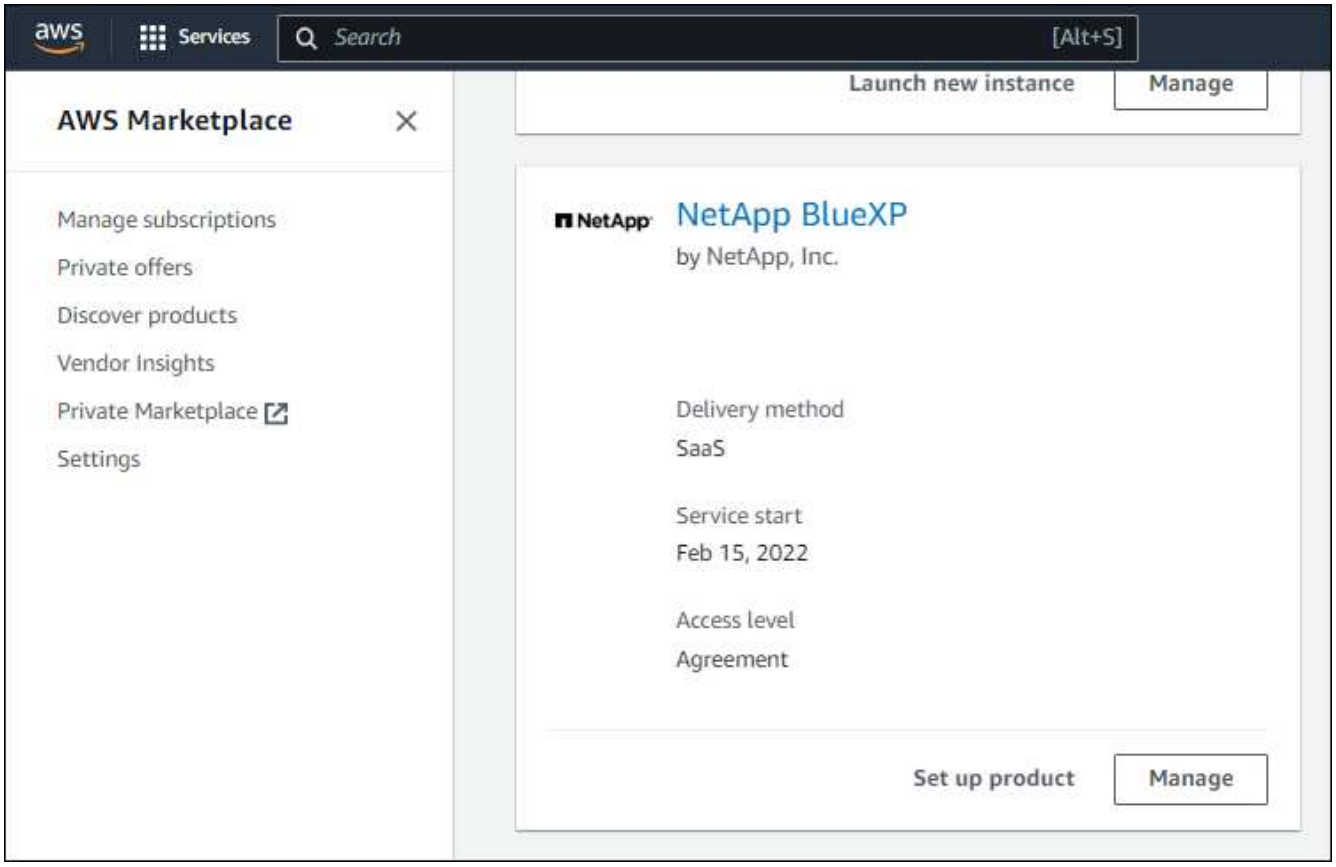
- "Saiba mais sobre os modos de implantação do BlueXP"
- "Saiba mais sobre o gerenciamento de identidades e acesso do BlueXP "
- "Saiba mais sobre as contas do BlueXP "

Siga as etapas abaixo se você se inscreveu no BlueXP no AWS Marketplace, mas não conseguiu associar a assinatura à sua conta.

**Passos**

1. Aceda à carteira digital da BlueXP para confirmar que não associou a sua subscrição à sua organização ou conta BlueXP .
   a. No menu de navegação BlueXP , selecione **Governança > carteira digital**.
   b. Selecione **Subscrições**.
   c. Verifique se sua assinatura do BlueXP não é exibida.

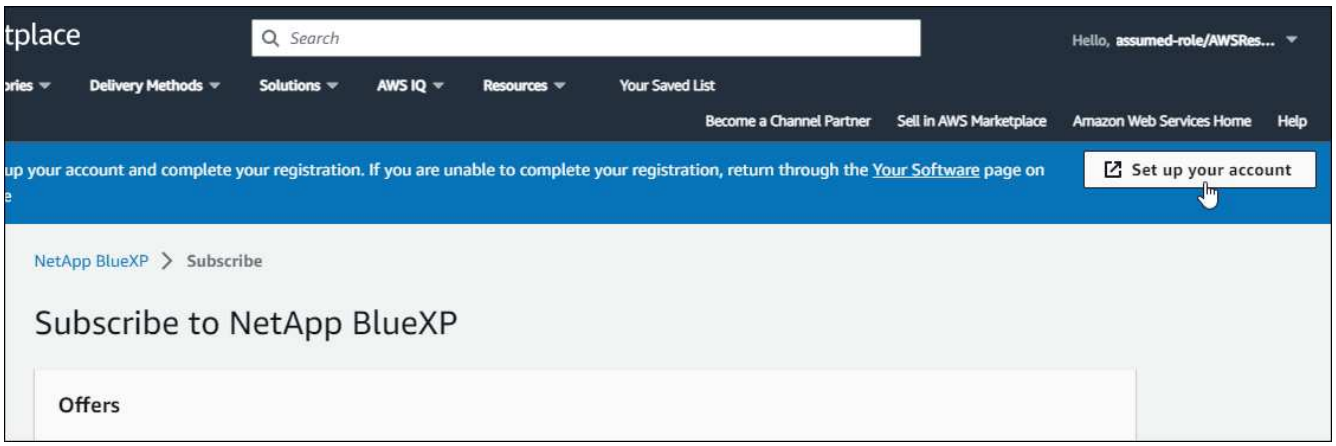
      Você verá apenas as assinaturas associadas à organização ou à conta que você está visualizando no momento. Se você não vir sua assinatura, prossiga com as etapas a seguir.
2. Faça login no Console da AWS e navegue até **assinaturas do AWS Marketplace**.
3. Encontre a assinatura do NetApp BlueXP .




4. Selecione **Configurar produto**.

   A página de oferta de assinatura deve ser carregada em uma nova guia ou janela do navegador.

5. Selecione **Configurar a sua conta**.




   A página **atribuição de assinatura** no NetApp.com deve ser carregada em uma nova guia ou janela do navegador.

   Observe que você pode ser solicitado a fazer login no BlueXP  primeiro.

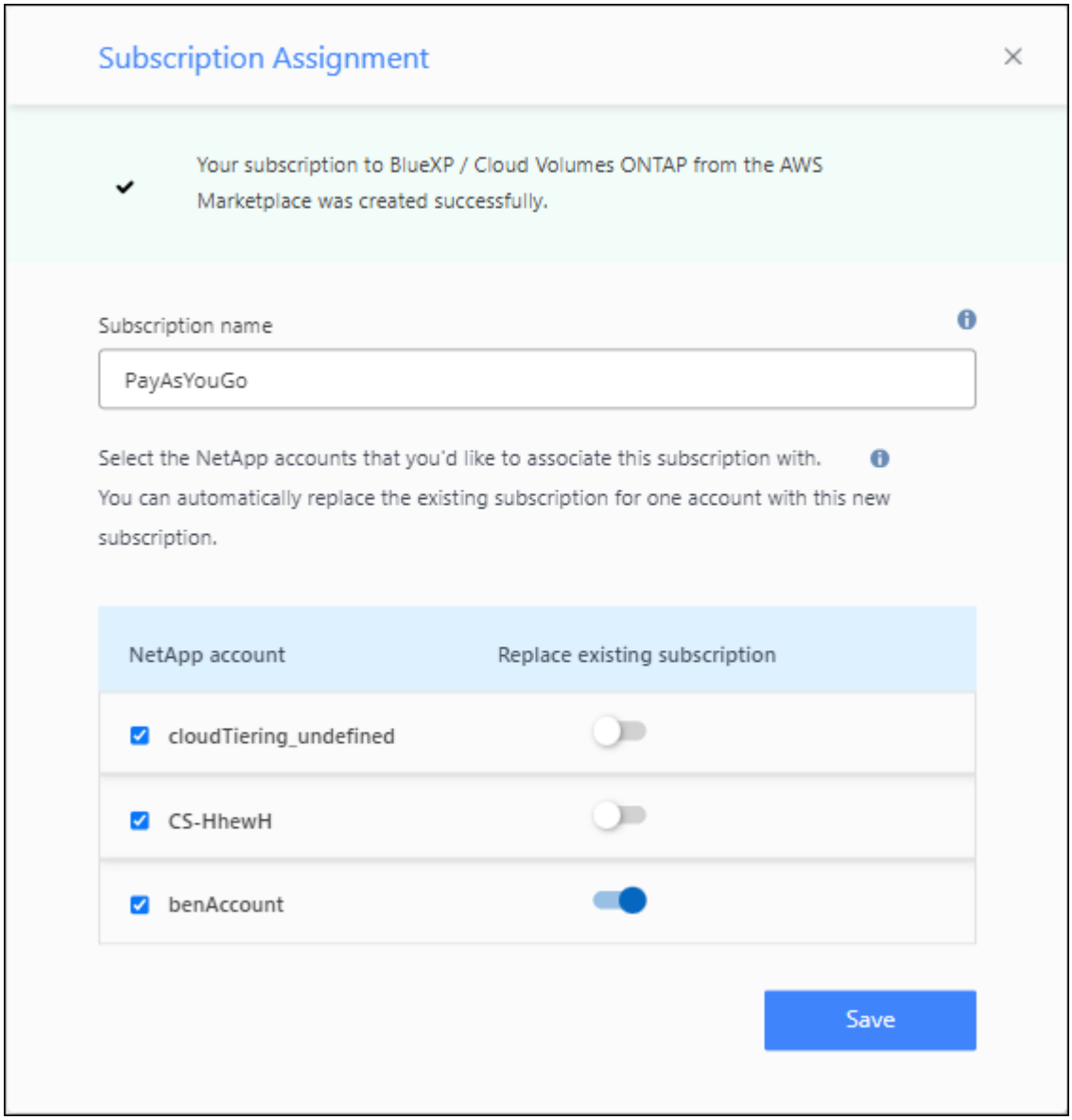
6. Na página **atribuição de assinatura**:

   - Selecione as organizações ou contas do BlueXP  às quais você deseja associar essa assinatura.

- No campo **Substituir subscrição existente**, escolha se pretende substituir automaticamente a subscrição existente de uma organização ou conta por esta nova subscrição.

  O BlueXP  substitui a assinatura existente para todas as credenciais na organização ou conta por essa nova assinatura. Se um conjunto de credenciais nunca foi associado a uma assinatura, essa nova assinatura não será associada a essas credenciais.

  Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo estas etapas.

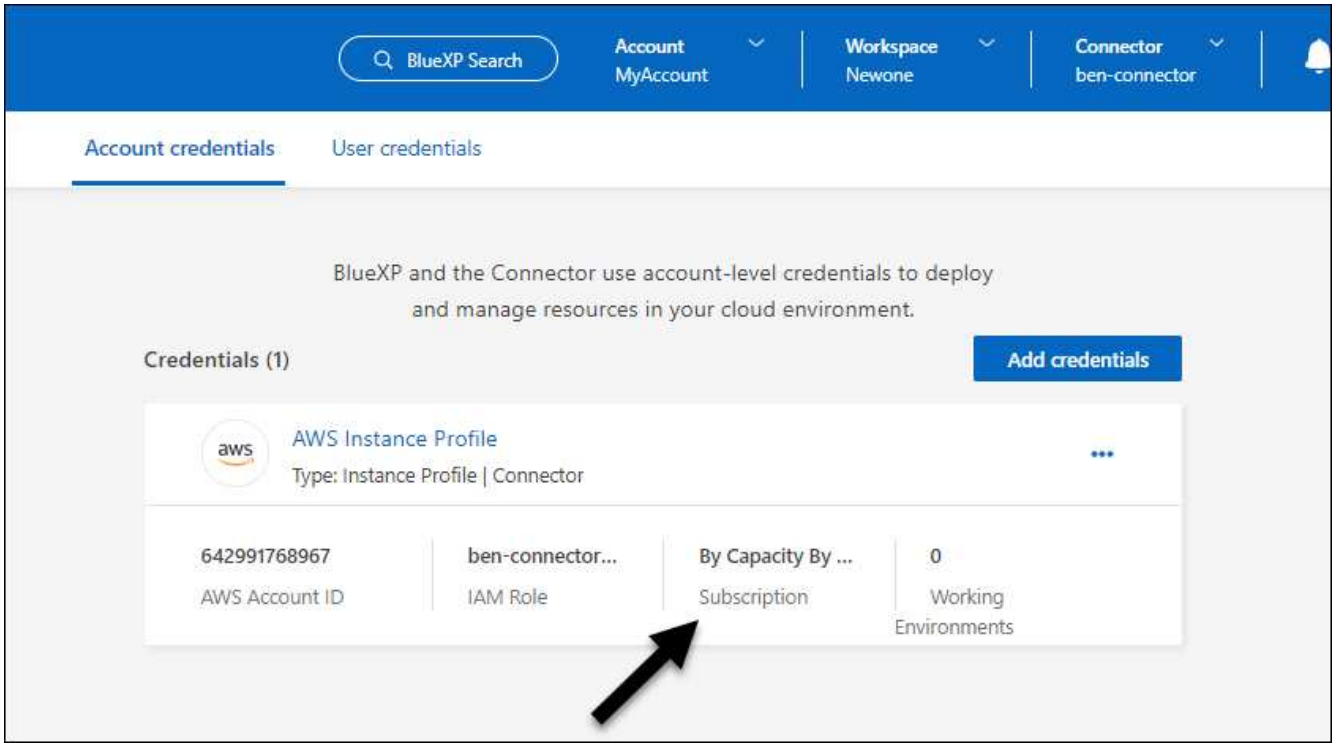



7. Aceda à carteira digital BlueXP  para confirmar que a subscrição está associada à sua organização ou conta BlueXP .
   a. No menu de navegação BlueXP , selecione **Governança > carteira digital**.
   b. Selecione **Subscrições**.
   c. Verifique se sua assinatura do BlueXP  é exibida.
8. Confirme se a assinatura está associada às suas credenciais da AWS.

a. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.

b. Na página **credenciais da organização** ou **credenciais da conta**, verifique se a assinatura está associada às credenciais da AWS.

   Aqui está um exemplo.




#### Editar credenciais

Edite suas credenciais da AWS no BlueXP  alterando o tipo de conta (chaves da AWS ou assumir função), editando o nome ou atualizando as próprias credenciais (as chaves ou a função ARN).

Não é possível editar as credenciais de um perfil de instância associado a uma instância de conetor.

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Na página **credenciais da organização** ou **credenciais da conta**, selecione o menu de ação para um conjunto de credenciais e, em seguida, selecione **Editar credenciais**.
3. Faça as alterações necessárias e selecione **aplicar**.

#### Eliminar credenciais

Se você não precisar mais de um conjunto de credenciais, poderá excluí-las do BlueXP . Você só pode excluir credenciais que não estão associadas a um ambiente de trabalho.

Não é possível excluir as credenciais de um perfil de instância associado a uma instância de conetor.

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Na página **credenciais da organização** ou **credenciais da conta**, selecione o menu de ação para um conjunto de credenciais e, em seguida, selecione **Excluir credenciais**.
3. Selecione **Eliminar** para confirmar.

## Azure

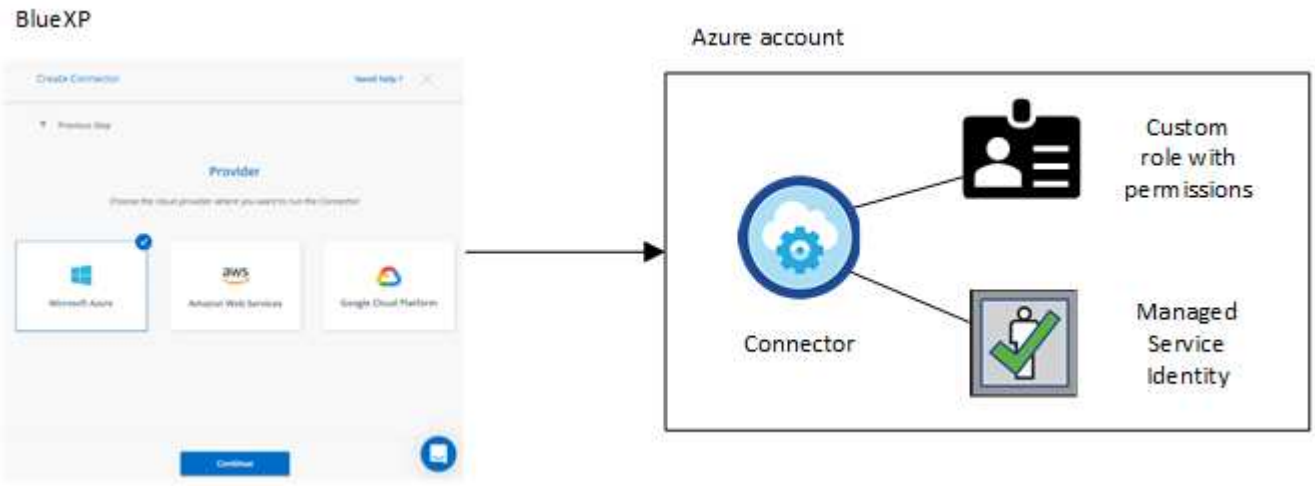
### Saiba mais sobre as credenciais e permissões do Azure

Saiba como o BlueXP  usa as credenciais do Azure para executar ações em seu nome e como essas credenciais estão associadas às assinaturas do marketplace. Entender esses detalhes pode ser útil ao gerenciar as credenciais de uma ou mais assinaturas do Azure. Por exemplo, você pode querer saber quando adicionar credenciais adicionais do Azure ao BlueXP .

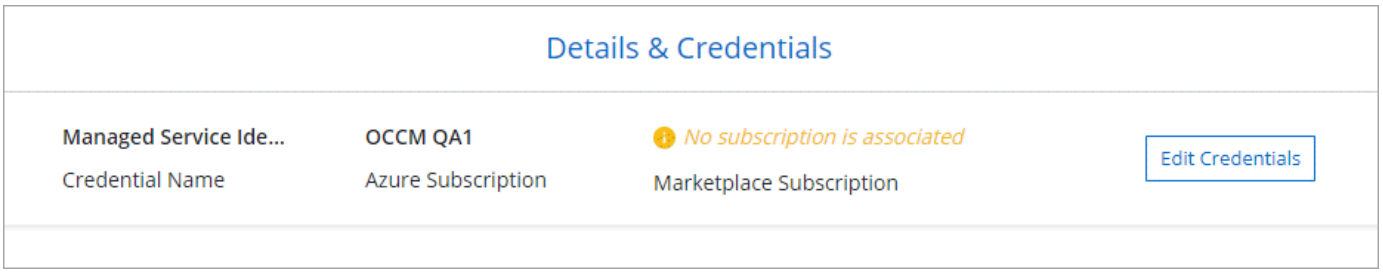
#### Credenciais iniciais do Azure

Ao implantar um conetor do BlueXP , você precisa usar uma conta do Azure ou um responsável de serviço que tenha permissões para implantar a máquina virtual do Connector. As permissões necessárias estão listadas no "Política de implantação do Connector para Azure".

Quando o BlueXP  implanta a máquina virtual Connector no Azure, ele ativa uma "identidade gerenciada atribuída ao sistema" máquina virtual on, cria uma função personalizada e a atribui à máquina virtual. A função fornece ao BlueXP  as permissões necessárias para gerenciar recursos e processos dentro dessa assinatura do Azure. "Veja como o BlueXP  usa as permissões".




Se você criar um novo ambiente de trabalho para o Cloud Volumes ONTAP, o BlueXP  selecionará essas credenciais do Azure por padrão:



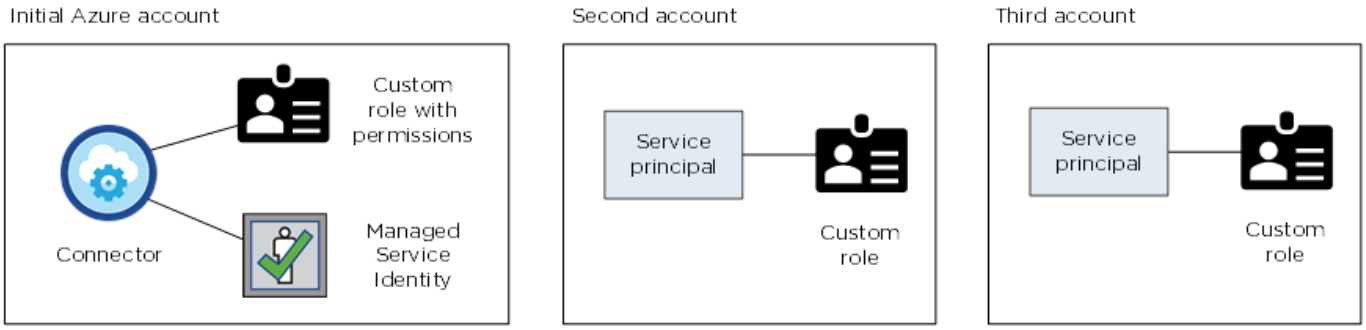

Você pode implantar todos os seus sistemas Cloud Volumes ONTAP usando as credenciais iniciais do Azure ou adicionar credenciais adicionais.

#### Subscrições adicionais do Azure para uma identidade gerida

A identidade gerenciada atribuída ao sistema atribuída à VM do conetor está associada à assinatura na qual você iniciou o conetor. Se você quiser selecionar uma assinatura diferente do Azure, precisará "associe a identidade gerenciada a essas assinaturas"do .

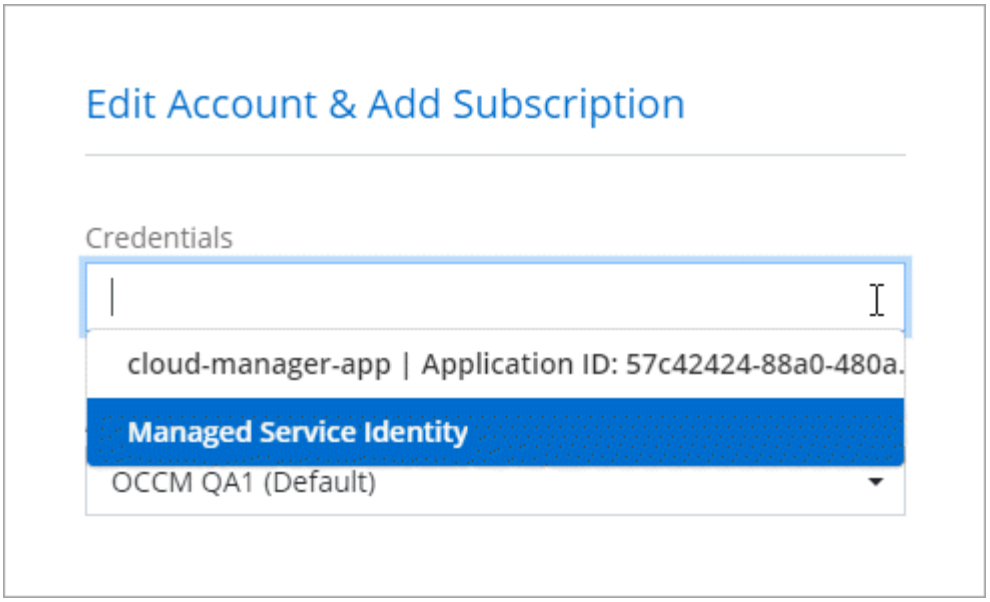
#### Credenciais adicionais do Azure

Se você quiser usar diferentes credenciais do Azure com o BlueXP , você deve conceder as permissões necessárias para "Criação e configuração de um responsável de serviço no Microsoft Entra ID"cada conta do Azure. A imagem a seguir mostra duas contas adicionais, cada uma configurada com uma função principal de serviço e personalizada que fornece permissões:




Em seguida, você "Adicione as credenciais da conta ao BlueXP "forneceria detalhes sobre o diretor de serviço do AD.

Por exemplo, você pode alternar entre credenciais ao criar um novo ambiente de trabalho do Cloud Volumes ONTAP:




#### Credenciais e assinaturas de mercado

As credenciais que você adicionar a um conetor devem estar associadas a uma assinatura do Azure Marketplace para que você possa pagar pelo Cloud Volumes ONTAP a uma taxa por hora (PAYGO) ou por meio de um contrato anual e usar outros serviços da BlueXP .

"Saiba como associar uma assinatura do Azure".

Observe o seguinte sobre as credenciais do Azure e as assinaturas do marketplace:

- Você pode associar apenas uma assinatura do Azure Marketplace a um conjunto de credenciais do Azure
- Você pode substituir uma assinatura existente do mercado por uma nova

#### FAQ

A pergunta a seguir está relacionada a credenciais e assinaturas.

**Posso alterar a assinatura do Azure Marketplace para ambientes de trabalho do Cloud Volumes ONTAP?**

Sim, você pode. Quando você altera a assinatura do Azure Marketplace associada a um conjunto de credenciais do Azure, todos os ambientes de trabalho do Cloud Volumes ONTAP existentes e novos serão cobrados com a nova assinatura.

"Saiba como associar uma assinatura do Azure".

**Posso adicionar várias credenciais do Azure, cada uma com diferentes assinaturas do marketplace?**

Todas as credenciais do Azure que pertencem à mesma assinatura do Azure serão associadas à mesma assinatura do Azure Marketplace.

Se você tiver várias credenciais do Azure que pertencem a diferentes assinaturas do Azure, essas credenciais podem ser associadas à mesma assinatura do Azure Marketplace ou a diferentes assinaturas do marketplace.

### Posso mover os ambientes de trabalho existentes do Cloud Volumes ONTAP para uma assinatura diferente do Azure?

Não, não é possível mover os recursos do Azure associados ao seu ambiente de trabalho do Cloud Volumes ONTAP para uma assinatura diferente do Azure.

### Como as credenciais funcionam para implantações no mercado e implantações locais?

As seções acima descrevem o método de implantação recomendado para o conetor, que é da BlueXP . Você também pode implantar um conetor no Azure a partir do Azure Marketplace, e você pode instalar o software Connector em seu próprio host Linux.

Se você usar o Marketplace, poderá fornecer permissões atribuindo uma função personalizada à VM do conetor e a uma identidade gerenciada atribuída ao sistema, ou você pode usar um responsável de serviço do Microsoft Entra.

Para implantações locais, não é possível configurar uma identidade gerenciada para o conetor, mas você pode fornecer permissões usando um princípio de serviço.

Para saber como configurar permissões, consulte as seguintes páginas:

- Modo padrão
  - "Configurar permissões para uma implantação do Azure Marketplace"
  - "Configurar permissões para implantações locais"
- "Configurar permissões para o modo restrito"
- "Configurar permissões para o modo privado"

## Gerencie as credenciais do Azure e as assinaturas do marketplace para o BlueXP

Adicione e gerencie credenciais do Azure para que o BlueXP  tenha as permissões necessárias para implantar e gerenciar recursos de nuvem em suas assinaturas do Azure. Se você gerenciar várias assinaturas do Azure Marketplace, poderá atribuir cada uma delas a diferentes credenciais do Azure na página credenciais.

Siga as etapas nesta página se precisar usar várias credenciais do Azure ou várias assinaturas do Azure Marketplace para o Cloud Volumes ONTAP.

#### Visão geral

Há duas maneiras de adicionar assinaturas e credenciais adicionais do Azure no BlueXP .

1. Associe subscrições adicionais do Azure à identidade gerenciada do Azure.
2. Se você quiser implantar o Cloud Volumes ONTAP usando diferentes credenciais do Azure, conceda permissões do Azure usando um princípio de serviço e adicione suas credenciais ao BlueXP .

#### Associe subscrições adicionais do Azure a uma identidade gerida

O BlueXP  permite que você escolha as credenciais do Azure e a assinatura do Azure na qual você deseja implantar o Cloud Volumes ONTAP. Não é possível selecionar uma assinatura diferente do Azure para o perfil de identidade gerenciado, a menos que você associe a "identidade gerenciada" essas assinaturas.

### Sobre esta tarefa

Uma identidade gerenciada é "A conta inicial do Azure" quando você implementa um conetor do BlueXP . Quando você implantou o conetor, o BlueXP  criou a função Operador do BlueXP  e atribuiu-a à máquina virtual do conetor.

**Passos**

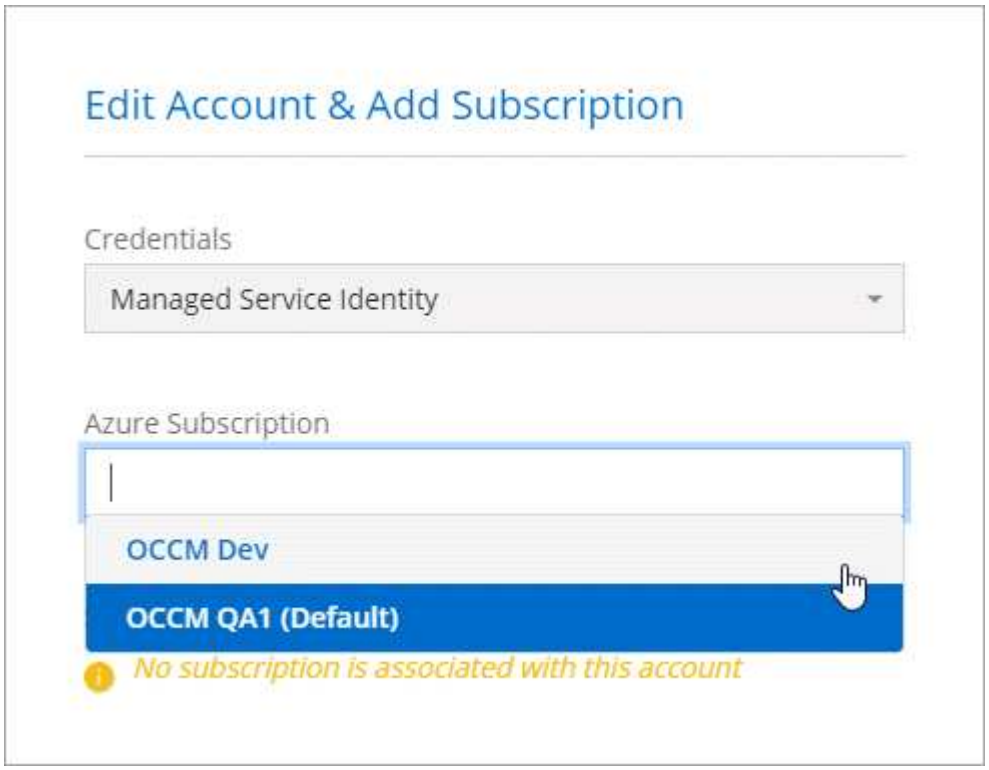
1. Faça login no portal do Azure.
2. Abra o serviço **assinaturas** e selecione a assinatura na qual deseja implantar o Cloud Volumes ONTAP.
3. Selecione **Access Control (IAM)**.
   a. Selecione **Adicionar** > **Adicionar atribuição de função** e adicione as permissões:
      - Selecione a função **Operador BlueXP** .

        Operador BlueXP  é o nome padrão fornecido na política de conetores. Se você escolher um nome diferente para a função, selecione esse nome em vez disso.

      - Atribua acesso a uma **Máquina Virtual**.
      - Selecione a assinatura na qual a máquina virtual do conetor foi criada.
      - Selecione a máquina virtual do conetor.
      - Selecione **Guardar**.
4. Repita estes passos para subscrições adicionais.

**Resultado**

Ao criar um novo ambiente de trabalho, agora você deve ter a capacidade de selecionar entre várias assinaturas do Azure para o perfil de identidade gerenciado.



#### Adicione credenciais adicionais do Azure ao BlueXP

Quando você implementa um conetor do BlueXP , o BlueXP  ativa uma identidade gerenciada atribuída ao sistema na máquina virtual que tem as permissões necessárias. O BlueXP  seleciona essas credenciais do Azure por padrão quando você cria um novo ambiente de trabalho para o Cloud Volumes ONTAP.

Um conjunto inicial de credenciais não é adicionado se você instalou manualmente o software Connector em um sistema existente. "Saiba mais sobre as credenciais e permissões do Azure".

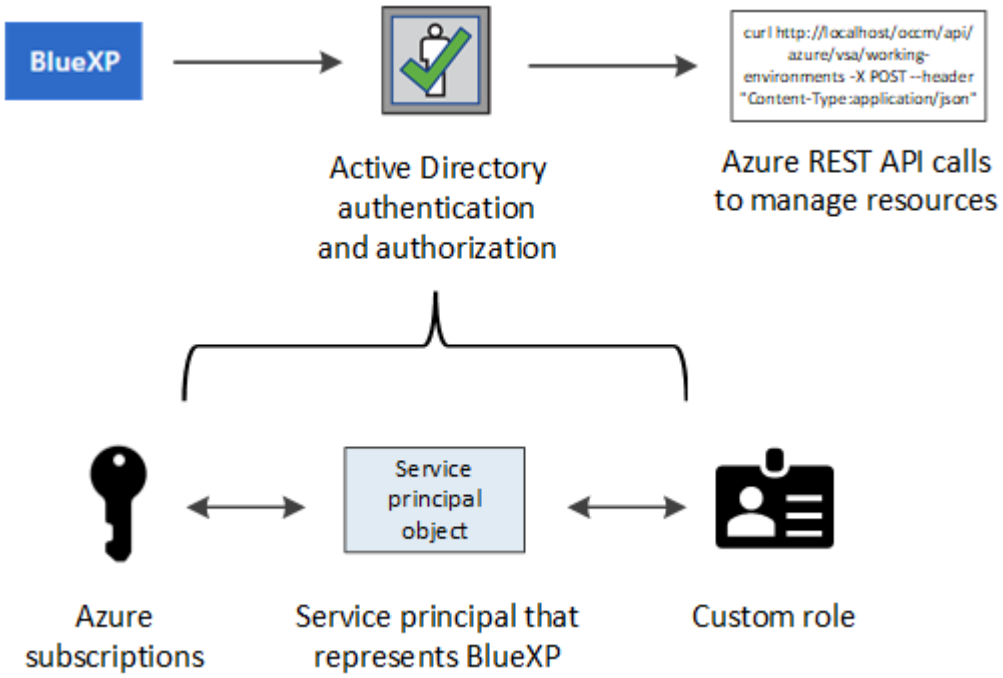
Se você quiser implantar o Cloud Volumes ONTAP usando *diferentes* credenciais do Azure, você deve conceder as permissões necessárias criando e configurando um responsável de serviço no Microsoft Entra ID para cada conta do Azure. Em seguida, você pode adicionar as novas credenciais ao BlueXP .

##### Conceda permissões do Azure usando um princípio de serviço

O BlueXP  precisa de permissões para executar ações no Azure. Você pode conceder as permissões necessárias a uma conta do Azure criando e configurando um responsável de serviço no Microsoft Entra ID e obtendo as credenciais do Azure de que o BlueXP  precisa.

###### Sobre esta tarefa

A imagem a seguir mostra como o BlueXP  obtém permissões para executar operações no Azure. Um objeto principal de serviço, que está vinculado a uma ou mais assinaturas do Azure, representa o BlueXP  no Microsoft Entra ID e é atribuído a uma função personalizada que permite as permissões necessárias.




###### Passos

1. Crie uma aplicação Microsoft Entra.
2. Atribua a aplicação a uma função.
3. Adicione permissões da API de Gerenciamento de Serviços do Windows Azure.
4. Obtenha o ID do aplicativo e o ID do diretório.
5. Crie um segredo de cliente.

### Crie uma aplicação Microsoft Entra

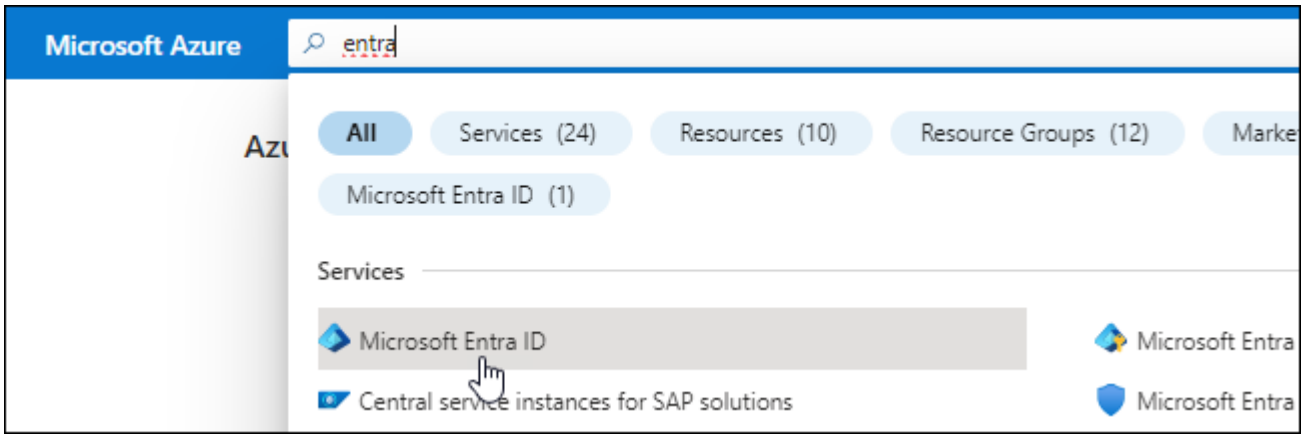
Crie um aplicativo e um responsável de serviço do Microsoft Entra que o BlueXP  pode usar para controle de acesso baseado em funções.

#### Passos

1. Certifique-se de ter permissões no Azure para criar um aplicativo do ative Directory e atribuir o aplicativo a uma função.

   Para obter mais informações, consulte "Documentação do Microsoft Azure: Permissões necessárias"

2. No portal do Azure, abra o serviço **Microsoft Entra ID**.




3. No menu, selecione **inscrições de aplicativos**.
4. Selecione **novo registo**.
5. Especifique detalhes sobre o aplicativo:
   - **Nome**: Insira um nome para o aplicativo.
   - **Tipo de conta**: Selecione um tipo de conta (qualquer funcionará com o BlueXP ).
   - * URI de redirecionamento*: Você pode deixar este campo em branco.
6. Selecione **Registe-se**.

   Você criou o aplicativo AD e o principal de serviço.

#### Resultado

Você criou o aplicativo AD e o principal de serviço.

### Atribua a aplicação a uma função

Você deve vincular o principal de serviço a uma ou mais assinaturas do Azure e atribuir-lhe a função personalizada "Operador do BlueXP " para que o BlueXP  tenha permissões no Azure.

#### Passos

1. Crie uma função personalizada:

   Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se você preferir usar um método diferente, consulte "Documentação do Azure"

a. Copie o conteúdo do "Permissões de função personalizadas para o conetor" e salve-o em um arquivo JSON.

b. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

   Você deve adicionar o ID para cada assinatura do Azure a partir da qual os usuários criarão sistemas Cloud Volumes ONTAP.

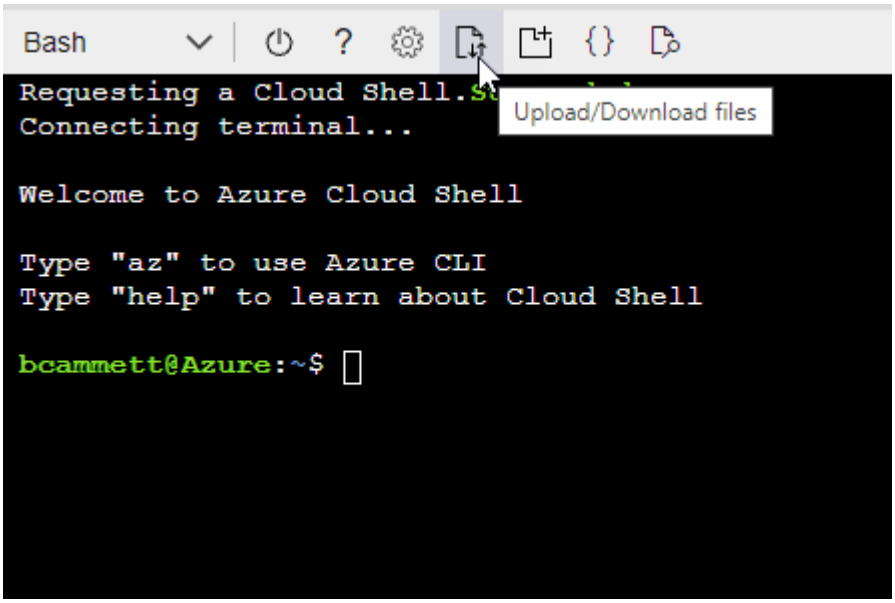
   **Exemplo**

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

c. Use o arquivo JSON para criar uma função personalizada no Azure.

   As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

   - Comece "Azure Cloud Shell" e escolha o ambiente Bash.
   - Carregue o arquivo JSON.




   - Use a CLI do Azure para criar a função personalizada:

```
az role definition create --role-definition Connector_Policy.json
```

   Agora você deve ter uma função personalizada chamada Operador BlueXP  que você pode atribuir à máquina virtual do conetor.

2. Atribua o aplicativo à função:

   a. No portal do Azure, abra o serviço **Subscrições**.

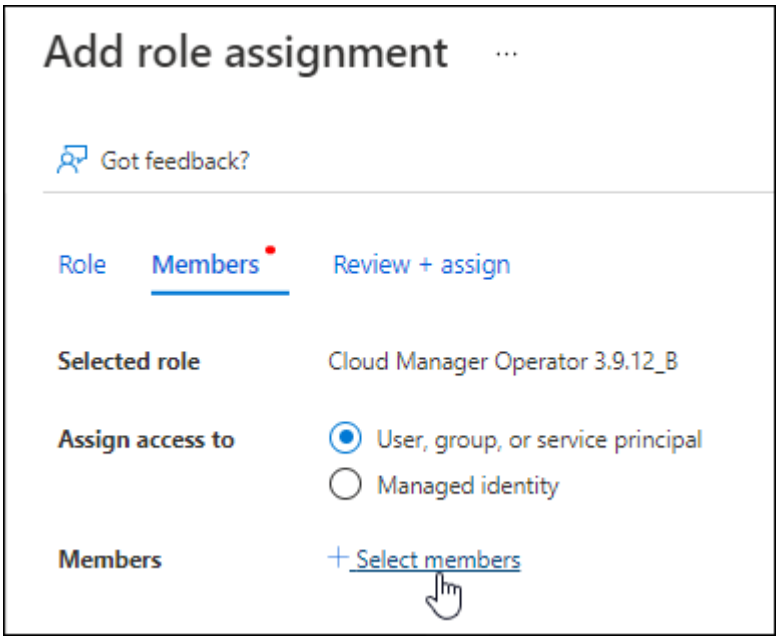
b. Selecione a subscrição.

c. Selecione **Access Control (IAM) > Add > Add > Add Role assignment** (Adicionar controlo de acesso).

d. Na guia **função**, selecione a função **Operador BlueXP** e selecione **seguinte**.

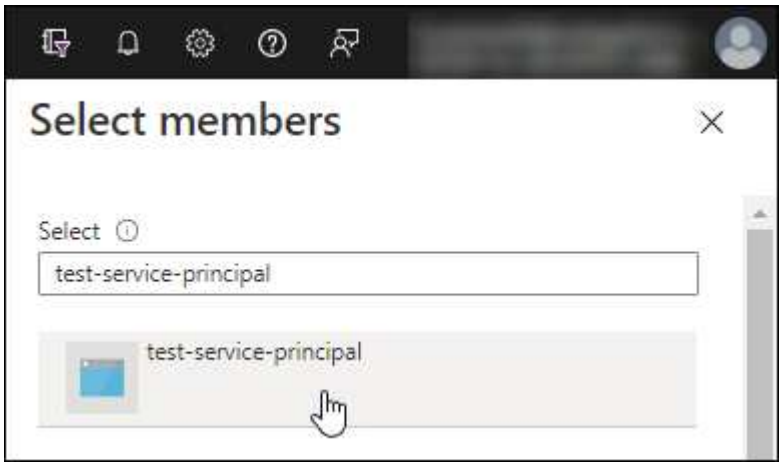
e. Na guia **Membros**, execute as seguintes etapas:

- Mantenha **Usuário, grupo ou responsável do serviço** selecionado.
- Selecione **Selecionar membros**.




- Procure o nome da aplicação.

  Aqui está um exemplo:




- Selecione a aplicação e selecione **Select**.
- Selecione **seguinte**.

f. Selecione **Rever e atribuir**.

O principal de serviço agora tem as permissões necessárias do Azure para implantar o conetor.

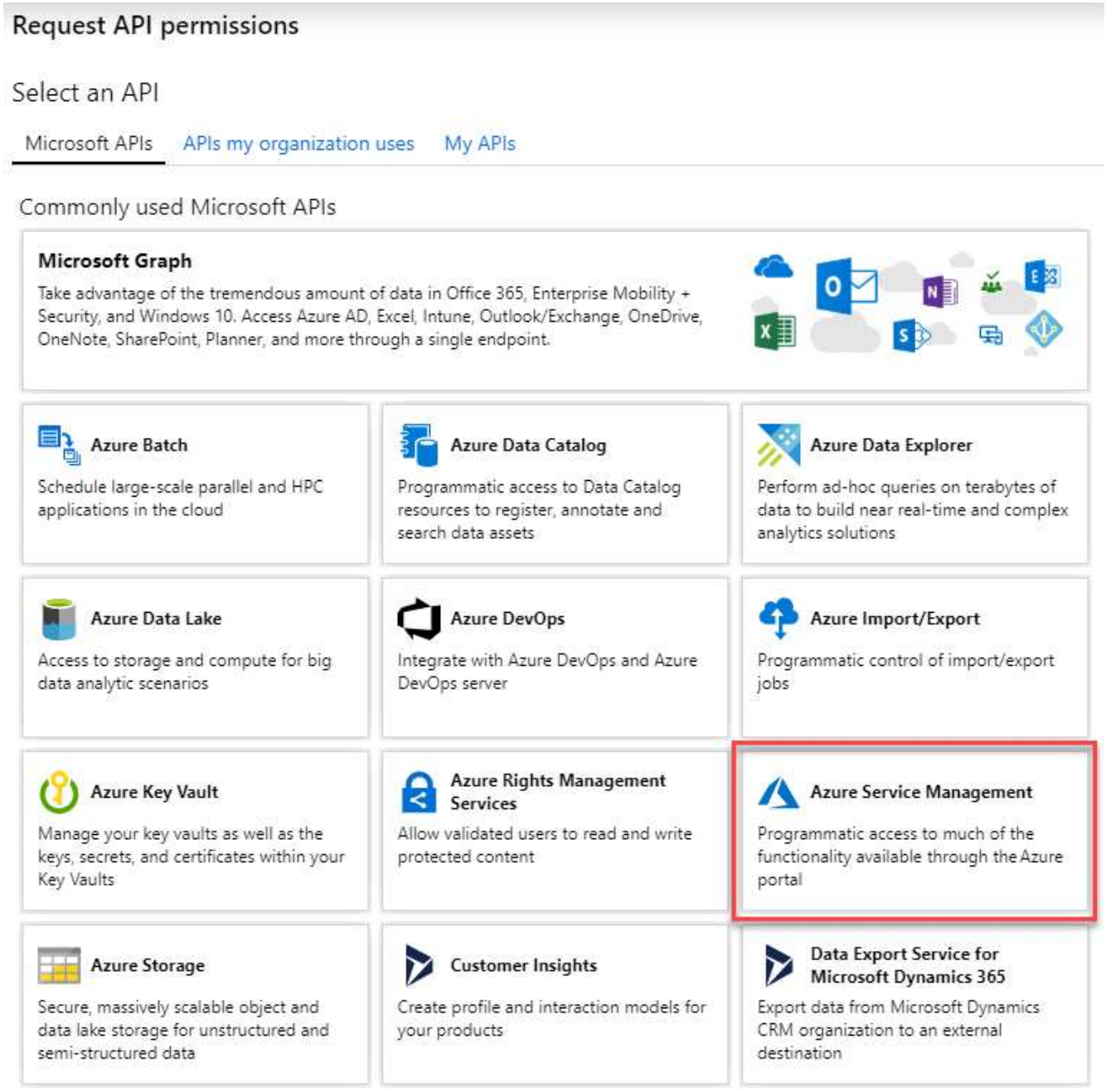
Se você quiser implantar o Cloud Volumes ONTAP a partir de várias assinaturas do Azure, então você deve vincular o principal de serviço a cada uma dessas assinaturas. O BlueXP  permite que você selecione a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

### Adicione permissões da API de Gerenciamento de Serviços do Windows Azure

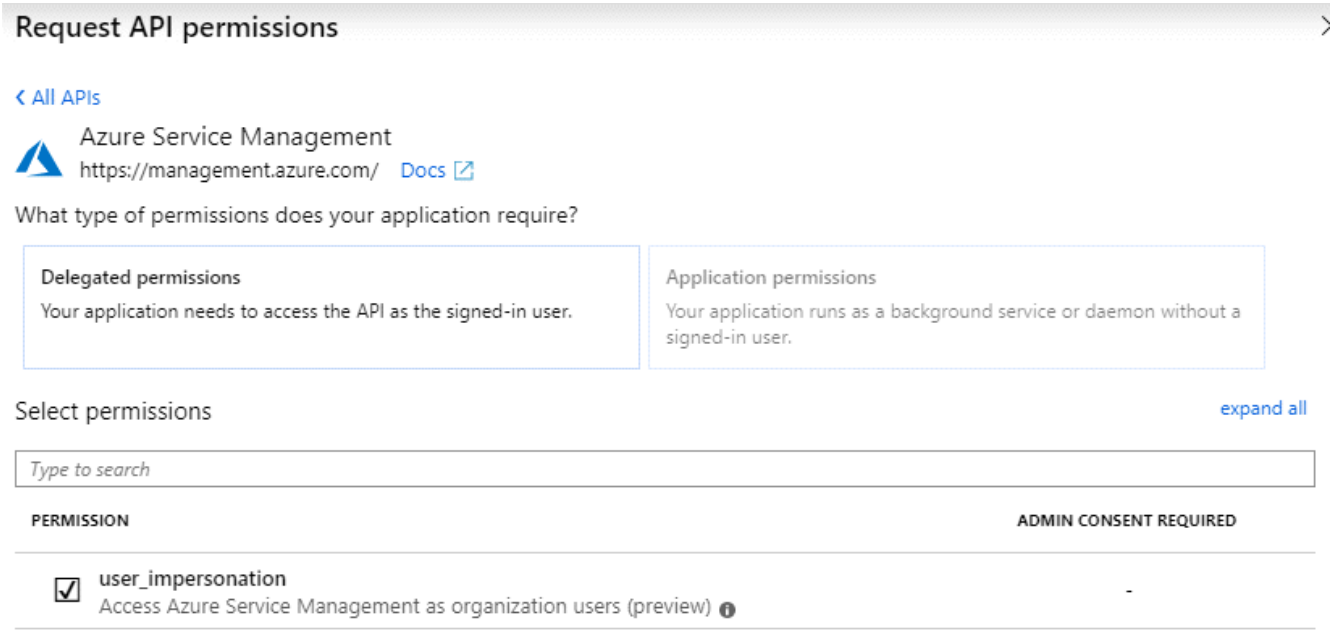
O responsável do serviço deve ter permissões "Windows Azure Service Management API".

**Passos**

1. No serviço **Microsoft Entra ID**, selecione **inscrições de aplicativos** e selecione o aplicativo.
2. Selecione **permissões de API > Adicionar uma permissão**.
3. Em **Microsoft APIs**, selecione **Azure Service Management**.



4. Selecione **Acesse o Gerenciamento de Serviços do Azure como usuários da organização** e selecione **Adicionar permissões**.

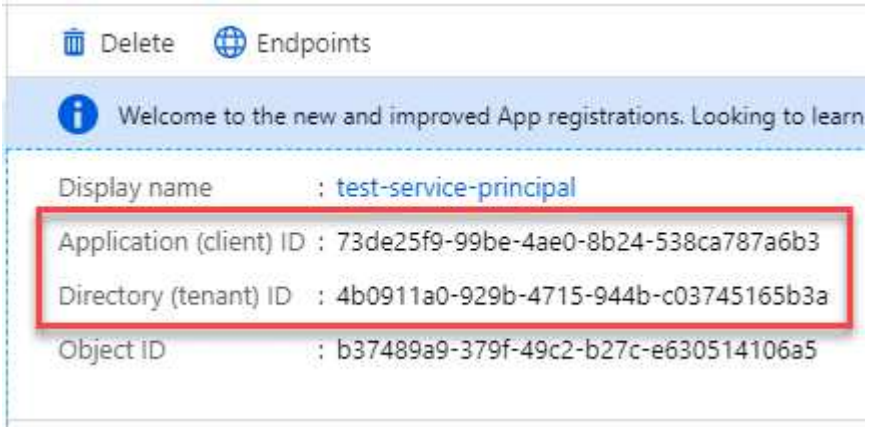



### Obtenha o ID do aplicativo e o ID do diretório

Quando você adiciona a conta do Azure ao BlueXP , você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O BlueXP  usa os IDs para fazer login programaticamente.

**Passos**

1. No serviço **Microsoft Entra ID**, selecione **inscrições de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.




Quando você adiciona a conta do Azure ao BlueXP , você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O BlueXP  usa os IDs para fazer login programaticamente.

### Crie um segredo de cliente

Você precisa criar um segredo de cliente e, em seguida, fornecer ao BlueXP  o valor do segredo para que o BlueXP  possa usá-lo para autenticar com o Microsoft Entra ID.

**Passos**

1. Abra o serviço **Microsoft Entra ID**.
2. Selecione **inscrições de aplicativos** e selecione sua inscrição.
3. Selecione **certificados e segredos > segredo de novo cliente**.
4. Forneça uma descrição do segredo e uma duração.
5. Selecione **Adicionar**.
6. Copie o valor do segredo do cliente.


Agora você tem um segredo de cliente que o BlueXP  pode usá-lo para autenticar com o Microsoft Entra ID.

**Resultado**

Seu responsável de serviço está configurado e você deve ter copiado o ID do aplicativo (cliente), o ID do diretório (locatário) e o valor do segredo do cliente. Você precisa inserir essas informações no BlueXP  ao adicionar uma conta do Azure.

### Adicione as credenciais ao BlueXP

Depois de fornecer uma conta do Azure com as permissões necessárias, você pode adicionar as credenciais dessa conta ao BlueXP . A conclusão desta etapa permite que você inicie o Cloud Volumes ONTAP usando diferentes credenciais do Azure.

**Antes de começar**

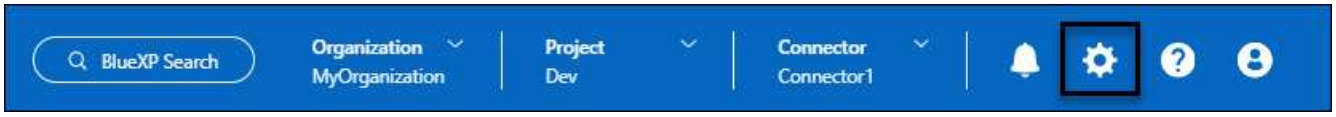
Se você acabou de criar essas credenciais no seu provedor de nuvem, talvez demore alguns minutos até que elas estejam disponíveis para uso. Aguarde alguns minutos antes de adicionar as credenciais ao BlueXP .

**Antes de começar**

Você precisa criar um conetor antes de poder alterar as configurações do BlueXP . "Saiba como criar um conetor".

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.

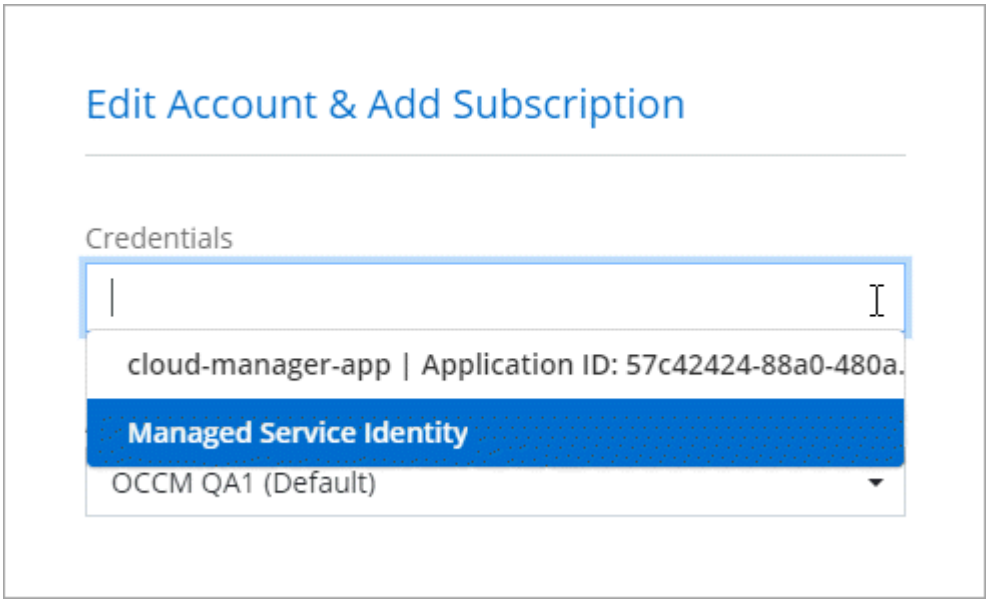



2. Selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Credentials Location**: Selecione **Microsoft Azure > Connector**.

b. **Definir credenciais**: Insira informações sobre o responsável do serviço Microsoft Entra que concede as permissões necessárias:
   - ID da aplicação (cliente)
   - ID do diretório (locatário)
   - Segredo Cliente
c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.
d. **Revisão**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

**Resultado**

Agora você pode alternar para diferentes conjuntos de credenciais na página Detalhes e credenciais "ao criar um novo ambiente de trabalho"




#### Gerenciar credenciais existentes

Gerencie as credenciais do Azure que você já adicionou ao BlueXP  associando uma assinatura do Marketplace, editando credenciais e excluindo-as.

### Associe uma assinatura do Azure Marketplace às credenciais

Depois de adicionar suas credenciais do Azure ao BlueXP , você pode associar uma assinatura do Azure Marketplace a essas credenciais. A assinatura permite que você crie um sistema Cloud Volumes ONTAP com pagamento conforme o uso e use outros serviços do BlueXP .

Há dois cenários em que você pode associar uma assinatura do Azure Marketplace depois de já ter adicionado as credenciais ao BlueXP :

- Você não associou uma assinatura quando adicionou inicialmente as credenciais ao BlueXP .
- Você deseja alterar a assinatura do Azure Marketplace associada às credenciais do Azure.

  A substituição da assinatura atual do marketplace por uma nova assinatura altera a assinatura do marketplace para todos os ambientes de trabalho existentes da Cloud Volumes ONTAP e todos os novos ambientes de trabalho.

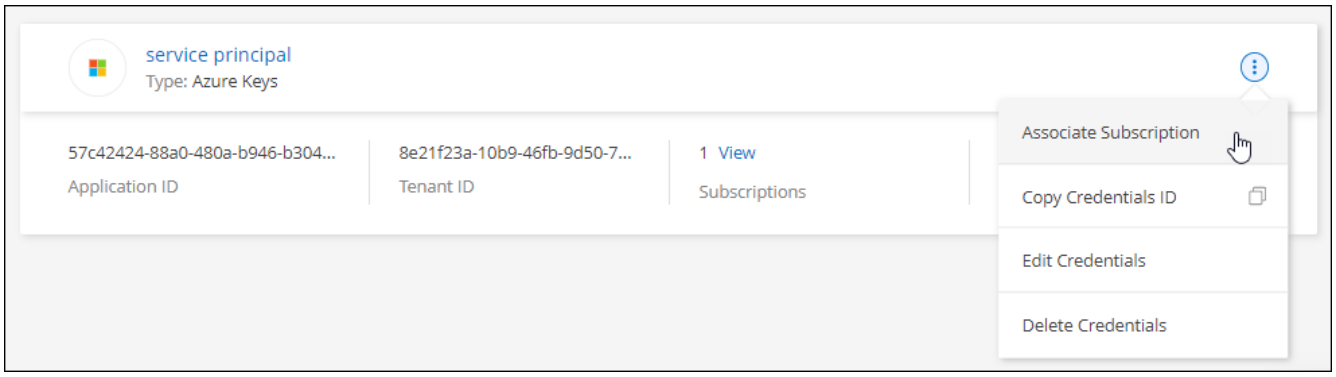
**Antes de começar**

Você precisa criar um conetor antes de poder alterar as configurações do BlueXP . "Saiba como".

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Selecione o menu de ação para um conjunto de credenciais e, em seguida, selecione **assinatura associada**.

   Você deve selecionar credenciais associadas a um conetor. Não é possível associar uma assinatura do marketplace a credenciais associadas ao BlueXP .




3. Para associar as credenciais a uma assinatura existente, selecione a assinatura na lista suspensa e selecione **Associate**.
4. Para associar as credenciais a uma nova assinatura, selecione **Adicionar assinatura > continuar** e siga as etapas no Azure Marketplace:

   a. Se solicitado, faça login na sua conta do Azure.

   b. Selecione **Subscribe**.

   c. Preencha o formulário e selecione **Subscribe**.

   d. Depois que o processo de assinatura estiver concluído, selecione **Configurar conta agora**.

      Você será redirecionado para o site da BlueXP .

   e. Na página **atribuição de assinatura**:

      - Selecione as organizações ou contas do BlueXP às quais você deseja associar essa assinatura.
      - No campo **Substituir subscrição existente**, escolha se pretende substituir automaticamente a subscrição existente de uma organização ou conta por esta nova subscrição.

        O BlueXP substitui a assinatura existente para todas as credenciais na organização ou conta por essa nova assinatura. Se um conjunto de credenciais nunca foi associado a uma assinatura, essa nova assinatura não será associada a essas credenciais.

   Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo estas etapas.

      - Selecione **Guardar**.

        O vídeo a seguir mostra as etapas para se inscrever no Azure Marketplace:

Inscreva-se no BlueXP  a partir do Azure Marketplace

#### Editar credenciais

Edite suas credenciais do Azure no BlueXP  modificando os detalhes sobre suas credenciais de serviço do Azure. Por exemplo, você pode precisar atualizar o segredo do cliente se um novo segredo foi criado para o aplicativo principal do serviço.

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Na página **credenciais da organização** ou **credenciais da conta**, selecione o menu de ação para um conjunto de credenciais e, em seguida, selecione **Editar credenciais**.
3. Faça as alterações necessárias e selecione **aplicar**.

#### Eliminar credenciais

Se você não precisar mais de um conjunto de credenciais, poderá excluí-las do BlueXP . Você só pode excluir credenciais que não estão associadas a um ambiente de trabalho.

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Na página **credenciais da organização** ou **credenciais da conta**, selecione o menu de ação para um conjunto de credenciais e, em seguida, selecione **Excluir credenciais**.
3. Selecione **Eliminar** para confirmar.

## Google Cloud

#### Saiba mais sobre os projetos e permissões do Google Cloud

Saiba como o BlueXP  usa as credenciais do Google Cloud para executar ações em seu nome e como essas credenciais estão associadas às assinaturas do marketplace. Entender esses detalhes pode ser útil ao gerenciar as credenciais de um ou mais projetos do Google Cloud. Por exemplo, você pode querer saber mais sobre a conta de serviço associada à VM do conetor.

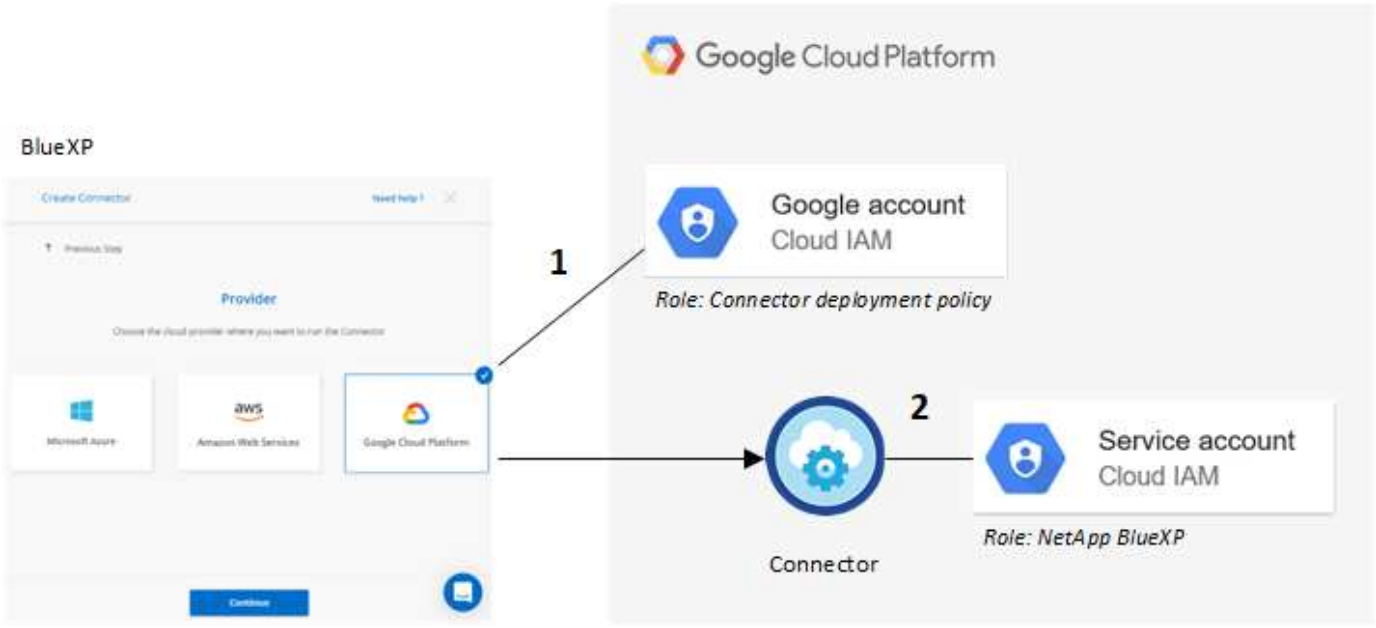
##### Projeto e permissões para BlueXP

Antes de usar o BlueXP  para gerenciar recursos em seu projeto do Google Cloud, primeiro é necessário implantar um conetor. O conetor não pode ser executado em suas instalações ou em um provedor de nuvem diferente.

Dois conjuntos de permissões devem estar em vigor antes de implantar um conetor diretamente do BlueXP :

1. Você precisa implantar um conetor usando uma conta do Google que tenha permissões para iniciar a instância de VM Connector do BlueXP .
2. Ao implantar o conetor, você será solicitado a selecionar um "conta de serviço" para a instância de VM. O BlueXP  obtém permissões da conta de serviço para criar e gerenciar sistemas Cloud Volumes ONTAP, gerenciar backups usando backup e recuperação do BlueXP  e muito mais. As permissões são fornecidas anexando uma função personalizada à conta de serviço.

A imagem a seguir mostra os requisitos de permissão descritos nos números 1 e 2 acima:




Para saber como configurar permissões, consulte as seguintes páginas:

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

#### Credenciais e assinaturas de mercado

Ao implantar um conetor no Google Cloud, o BlueXP  cria um conjunto padrão de credenciais para a conta de serviço do Google Cloud no projeto em que o conetor reside. Essas credenciais devem estar associadas a uma assinatura do Google Cloud Marketplace para que você possa pagar pelo Cloud Volumes ONTAP por uma taxa por hora (PAYGO) e usar outros serviços da BlueXP .

"Saiba como associar uma assinatura do Google Cloud Marketplace".

Observe o seguinte sobre as credenciais do Google Cloud e as assinaturas de mercado:

- Apenas um conjunto de credenciais do Google Cloud pode ser associado a um conetor
- Você pode associar apenas uma assinatura do Google Cloud Marketplace às credenciais
- Você pode substituir uma assinatura existente do mercado por uma nova

#### Projeto para Cloud Volumes ONTAP

O Cloud Volumes ONTAP pode residir no mesmo projeto que o conetor, ou em um projeto diferente. Para implantar o Cloud Volumes ONTAP em um projeto diferente, você precisa primeiro adicionar a conta de serviço do Connector e a função a esse projeto.

- "Saiba como configurar a conta de serviço"
- "Saiba como implantar o Cloud Volumes ONTAP no Google Cloud e selecione um projeto"

## Gerenciar credenciais e assinaturas do Google Cloud para o BlueXP

Você pode gerenciar as credenciais do Google Cloud associadas à instância da VM Connector associando uma assinatura do marketplace e solucionando problemas no processo de assinatura. Ambas as tarefas garantem que você use a assinatura do mercado para pagar pelos serviços da BlueXP .

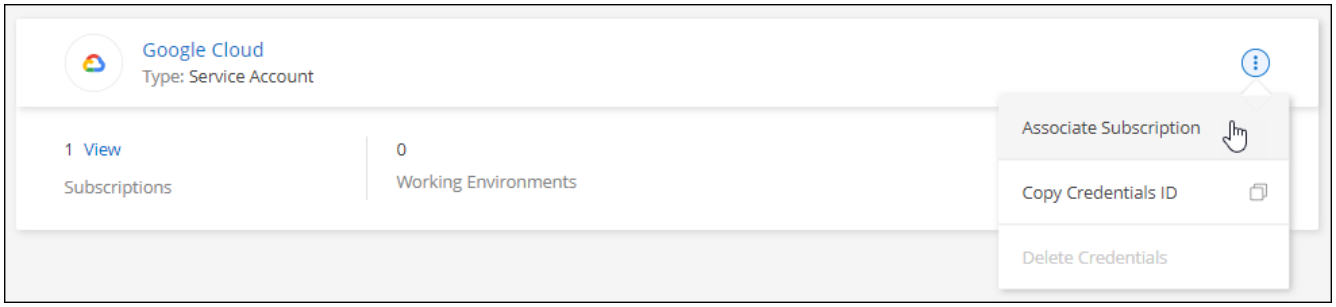
### Associar uma assinatura do Marketplace às credenciais do Google Cloud

Ao implantar um conetor no Google Cloud, o BlueXP  cria um conjunto padrão de credenciais associadas à instância de VM do Connector. A qualquer momento, você pode alterar a assinatura do Google Cloud Marketplace associada a essas credenciais. A assinatura permite que você crie um sistema Cloud Volumes ONTAP com pagamento conforme o uso e use outros serviços do BlueXP .

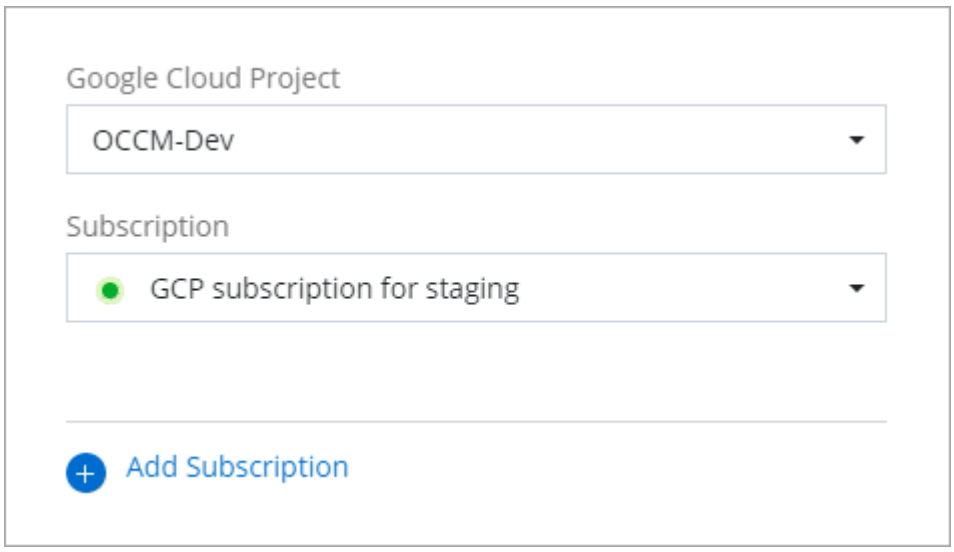
A substituição da assinatura atual do marketplace por uma nova assinatura altera a assinatura do marketplace para todos os ambientes de trabalho existentes da Cloud Volumes ONTAP e todos os novos ambientes de trabalho.

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Selecione o menu de ação para um conjunto de credenciais e, em seguida, selecione **assinatura associada**.



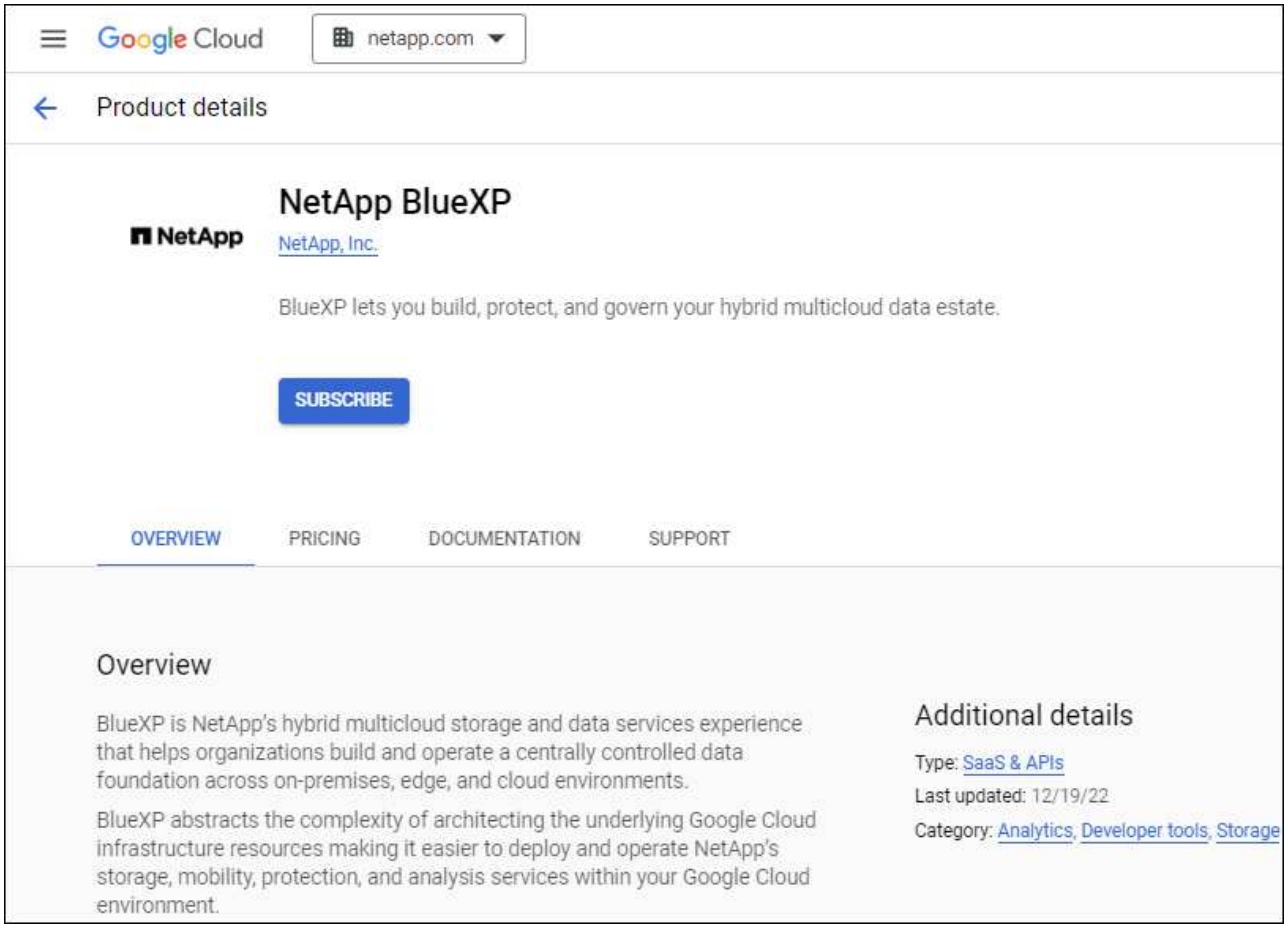

3. Para associar as credenciais a uma assinatura existente, selecione um projeto e assinatura do Google Cloud na lista suspensa e, em seguida, selecione **Associate**.



4. Se você ainda não tiver uma assinatura, selecione **Adicionar assinatura > continuar** e siga as etapas no Google Cloud Marketplace.

   Antes de concluir as etapas a seguir, certifique-se de que você tenha o Privileges de Administração de faturamento na sua conta do Google Cloud, bem como um login no BlueXP .

   a. Depois de ser redirecionado para o "Página do NetApp BlueXP  no Google Cloud Marketplace", certifique-se de que o projeto correto está selecionado no menu de navegação superior.




   b. Selecione **Subscribe**.

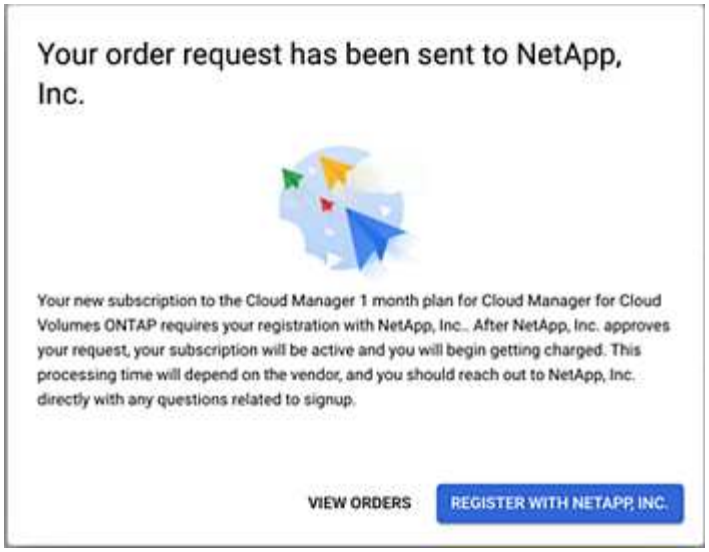
   c. Selecione a conta de faturamento apropriada e concorde com os termos e condições.

   d. Selecione **Subscribe**.

      Esta etapa envia sua solicitação de transferência para o NetApp.

   e. Na caixa de diálogo pop-up, selecione **Register with NetApp, Inc.**

      Essa etapa deve ser concluída para vincular a assinatura do Google Cloud à sua organização ou conta do BlueXP . O processo de vinculação de uma assinatura não está concluído até que você seja redirecionado desta página e, em seguida, entre no BlueXP .




f. Conclua as etapas na página **atribuição de assinatura**:

> Se alguém da sua organização já se inscreveu na assinatura do NetApp BlueXP da sua conta de faturamento, então você será redirecionado para "A página Cloud Volumes ONTAP no site da BlueXP ". Se isso for inesperado, entre em Contato com sua equipe de vendas da NetApp. O Google ativa apenas uma assinatura por conta de faturamento do Google.

- Selecione as organizações ou contas do BlueXP às quais você deseja associar essa assinatura.
- No campo **Substituir subscrição existente**, escolha se pretende substituir automaticamente a subscrição existente de uma organização ou conta por esta nova subscrição.

  O BlueXP substitui a assinatura existente para todas as credenciais na organização ou conta por essa nova assinatura. Se um conjunto de credenciais nunca foi associado a uma assinatura, essa nova assinatura não será associada a essas credenciais.

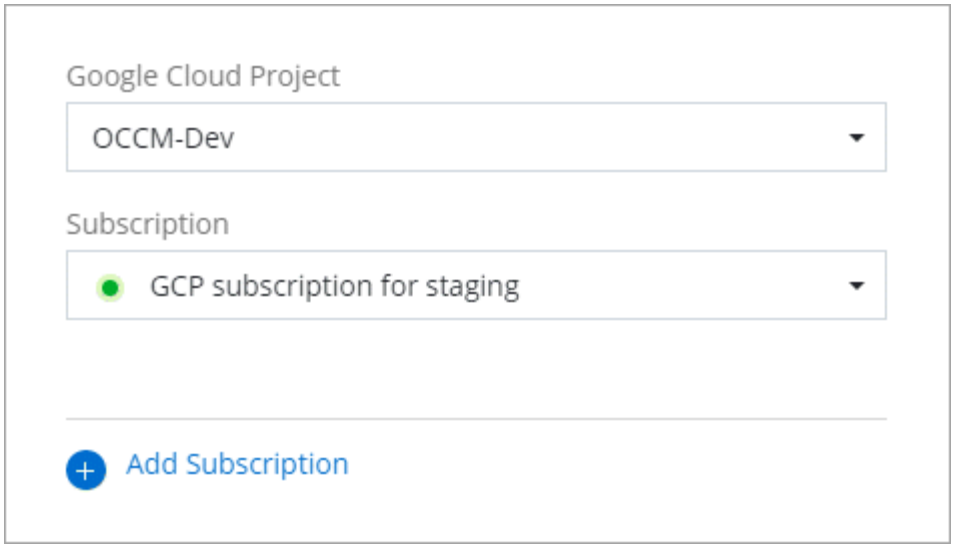
Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo estas etapas.

- Selecione **Guardar**.

  O vídeo a seguir mostra as etapas para se inscrever no Google Cloud Marketplace:

Inscreva-se no BlueXP no Google Cloud Marketplace

a. Quando esse processo estiver concluído, navegue de volta para a página credenciais no BlueXP e selecione essa nova assinatura.




**Solucionar problemas do processo de assinatura do Marketplace**

Às vezes, a assinatura do BlueXP  através do Google Cloud Marketplace pode se tornar fragmentada devido a permissões incorretas ou acidentalmente não seguir o redirecionamento para o site do BlueXP . Se isso acontecer, siga as etapas a seguir para concluir o processo de assinatura.

**Passos**

1. Navegue até a "Página do NetApp BlueXP  no Google Cloud Marketplace" para verificar o estado da encomenda. Se a página indicar **Gerenciar no provedor**, role para baixo e selecione **Gerenciar pedidos**.


   - Se o pedido mostrar uma marca de verificação verde e isso for inesperado, outra pessoa da organização que usa a mesma conta de faturamento pode já estar subscrita. Se isso for inesperado ou você precisar dos detalhes dessa assinatura, entre em Contato com sua equipe de vendas da NetApp.


   - Se o pedido mostrar um relógio e status **pendente**, volte para a página do mercado e escolha **Gerenciar no provedor** para concluir o processo conforme documentado acima.

## Gerencie credenciais NSS associadas a uma organização ou conta do BlueXP

Associe uma conta do site de suporte da NetApp à sua organização ou conta do BlueXP para ativar os principais fluxos de trabalho do Cloud Volumes ONTAP. Essas credenciais do NSS estão associadas a toda a organização ou conta do BlueXP .

O BlueXP  também suporta a associação de uma conta NSS por conta de usuário do BlueXP . "Saiba como gerenciar credenciais de nível de usuário".

Se você estiver usando o BlueXP  no modo padrão, você terá uma organização *BlueXP* , que você gerencia usando o gerenciamento de identidade e acesso (IAM) do BlueXP . Mas se você estiver usando o BlueXP  no modo restrito ou no modo privado, então você terá uma conta *BlueXP* .

- "Saiba mais sobre os modos de implantação do BlueXP"
- "Saiba mais sobre o gerenciamento de identidades e acesso do BlueXP "
- "Saiba mais sobre as contas do BlueXP "

### Visão geral

A associação das credenciais do site de suporte da NetApp com o número de série específico da sua conta BlueXP  é necessária para ativar as seguintes tarefas no BlueXP :

- Implantando o Cloud Volumes ONTAP quando você traz sua própria licença (BYOL)

  É necessário fornecer a sua conta NSS para que o BlueXP  possa carregar a sua chave de licença e ativar a subscrição para o período que adquiriu. Isso inclui atualizações automáticas para renovações de prazo.

- Registar sistemas Cloud Volumes ONTAP de pagamento conforme o uso

  Fornecer sua conta NSS é necessário para ativar o suporte para o seu sistema e para obter acesso aos recursos de suporte técnico da NetApp.

- Atualizar o software Cloud Volumes ONTAP para a versão mais recente

Essas credenciais estão associadas ao número de série específico da sua conta BlueXP . Os usuários que pertencem à organização ou conta do BlueXP  podem acessar essas credenciais a partir de **suporte > Gerenciamento do NSS**.

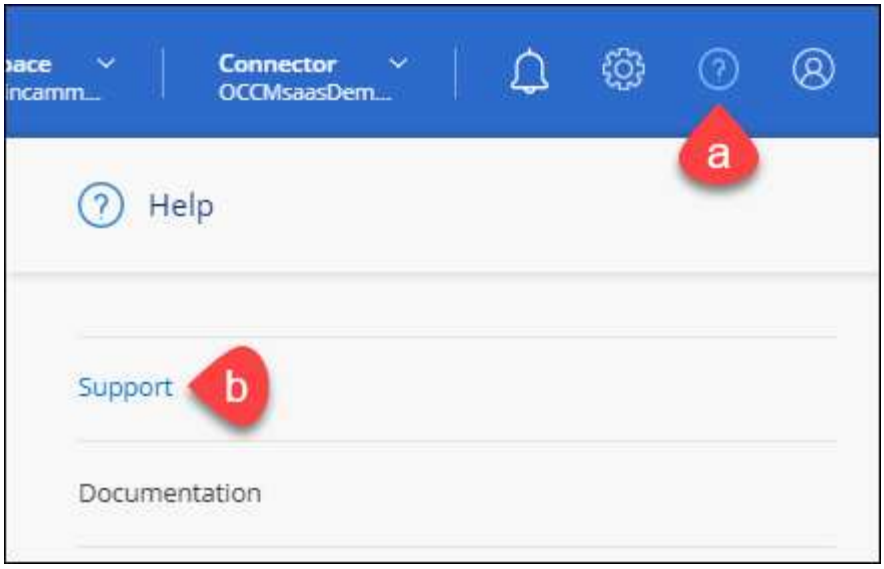
### Adicione uma conta NSS

O Painel de suporte permite que você adicione e gerencie suas contas do site de suporte da NetApp para uso com o BlueXP  no nível da organização ou da conta da BlueXP .

- Se você tiver uma conta no nível do cliente, pode adicionar uma ou mais contas NSS.
- Se você tiver uma conta de parceiro ou revendedor, você pode adicionar uma ou mais contas NSS, mas elas não podem ser adicionadas ao lado de contas de nível de cliente.

#### Passos

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda e selecione **suporte**.




2. Selecione **NSS Management > Add NSS Account** (Gestão NSS > Adicionar conta NSS*).
3. Quando for solicitado, selecione **continuar** para ser redirecionado para uma página de login da Microsoft.

   O NetApp usa o Microsoft Entra ID como provedor de identidade para serviços de autenticação específicos para suporte e licenciamento.

4. Na página de login, forneça seu endereço de e-mail e senha registrados no site de suporte da NetApp para executar o processo de autenticação.

   Essas ações permitem que o BlueXP  use sua conta NSS para tarefas como downloads de licenças, verificação de atualização de software e futuros Registros de suporte.

   Observe o seguinte:

   - A conta NSS tem de ser uma conta ao nível do cliente (não uma conta de convidado ou temporária). Você pode ter várias contas NSS no nível do cliente.
   - Só pode haver uma conta NSS se essa conta for uma conta de nível de parceiro. Se você tentar adicionar contas NSS no nível do cliente e existir uma conta no nível do parceiro, você receberá a seguinte mensagem de erro:

     "O tipo de cliente NSS não é permitido para esta conta, uma vez que já existem utilizadores NSS de tipo diferente."

   O mesmo acontece se você tiver contas NSS pré-existentes no nível do cliente e tentar adicionar uma conta no nível do parceiro.

   - Após o login bem-sucedido, o NetApp armazenará o nome de usuário do NSS.

     Este é um ID gerado pelo sistema que mapeia para o seu e-mail. Na página **NSS Management**, você pode exibir seu e-mail no ••• menu.

   - Se você precisar atualizar seus tokens de credenciais de login, há também uma opção **Atualizar credenciais** ••• no menu.

     Usando esta opção, você solicita que você faça login novamente. Observe que o token para essas contas expira após 90 dias. Uma notificação será postada para alertá-lo sobre isso.

**O que se segue?**

Os usuários agora podem selecionar a conta ao criar novos sistemas Cloud Volumes ONTAP e ao Registrar sistemas Cloud Volumes ONTAP existentes.

- "Iniciando o Cloud Volumes ONTAP na AWS"
- "Iniciar o Cloud Volumes ONTAP no Azure"
- "Lançamento do Cloud Volumes ONTAP no Google Cloud"
- "Registar sistemas de pagamento conforme o uso"

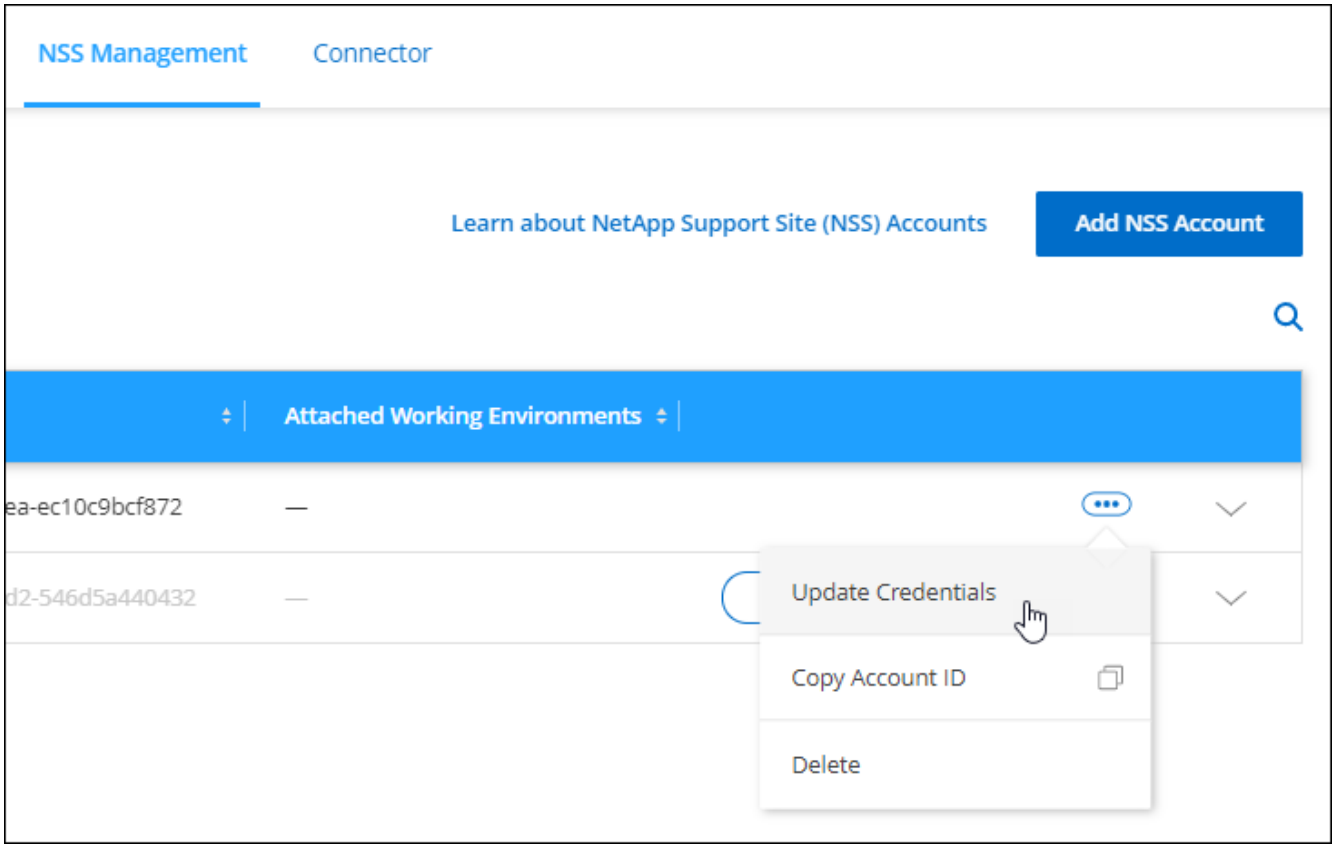
### Atualizar credenciais NSS

Você precisará atualizar as credenciais para suas contas NSS no BlueXP  quando uma das seguintes situações acontecer:

- Você altera as credenciais da conta
- O token de atualização associado à sua conta expira após 3 meses

**Passos**

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda e selecione **suporte**.
2. Selecione **NSS Management**.
3. Para a conta NSS que você deseja atualizar, •••selecione e selecione **Atualizar credenciais**.




4. Quando for solicitado, selecione **continuar** para ser redirecionado para uma página de login da Microsoft.

   O NetApp usa o Microsoft Entra ID como provedor de identidade para serviços de autenticação específicos para suporte e licenciamento.

5. Na página de login, forneça seu endereço de e-mail e senha registrados no site de suporte da NetApp para executar o processo de autenticação.

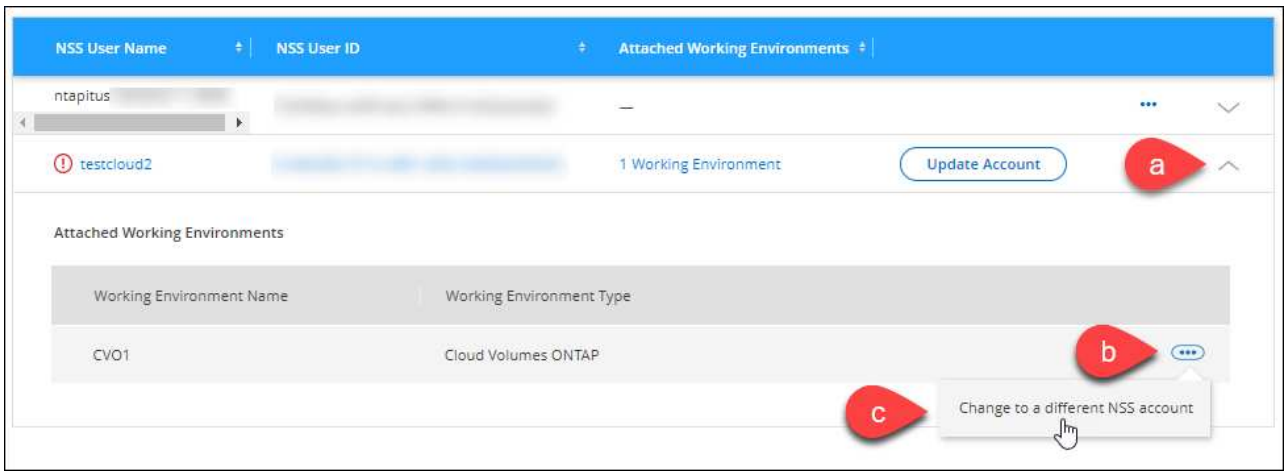
### Anexe um ambiente de trabalho a uma conta NSS diferente

Se a sua organização tiver várias contas do site de suporte da NetApp, você poderá alterar qual conta está associada a um sistema Cloud Volumes ONTAP.

Este recurso é suportado apenas com contas NSS que estão configuradas para usar o Microsoft Entra ID adotado pelo NetApp para gerenciamento de identidades. Antes de poder utilizar esta funcionalidade, é necessário selecionar **Adicionar conta NSS** ou **Atualizar conta**.

**Passos**

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda e selecione **suporte**.
2. Selecione **NSS Management**.
3. Execute as seguintes etapas para alterar a conta do NSS:
   a. Expanda a linha para a conta do site de suporte da NetApp à qual o ambiente de trabalho está atualmente associado.
   b. Para o ambiente de trabalho para o qual você deseja alterar a associação, selecione •••
   c. Selecione **alterar para uma conta NSS diferente**.




   d. Selecione a conta e, em seguida, selecione **Salvar**.

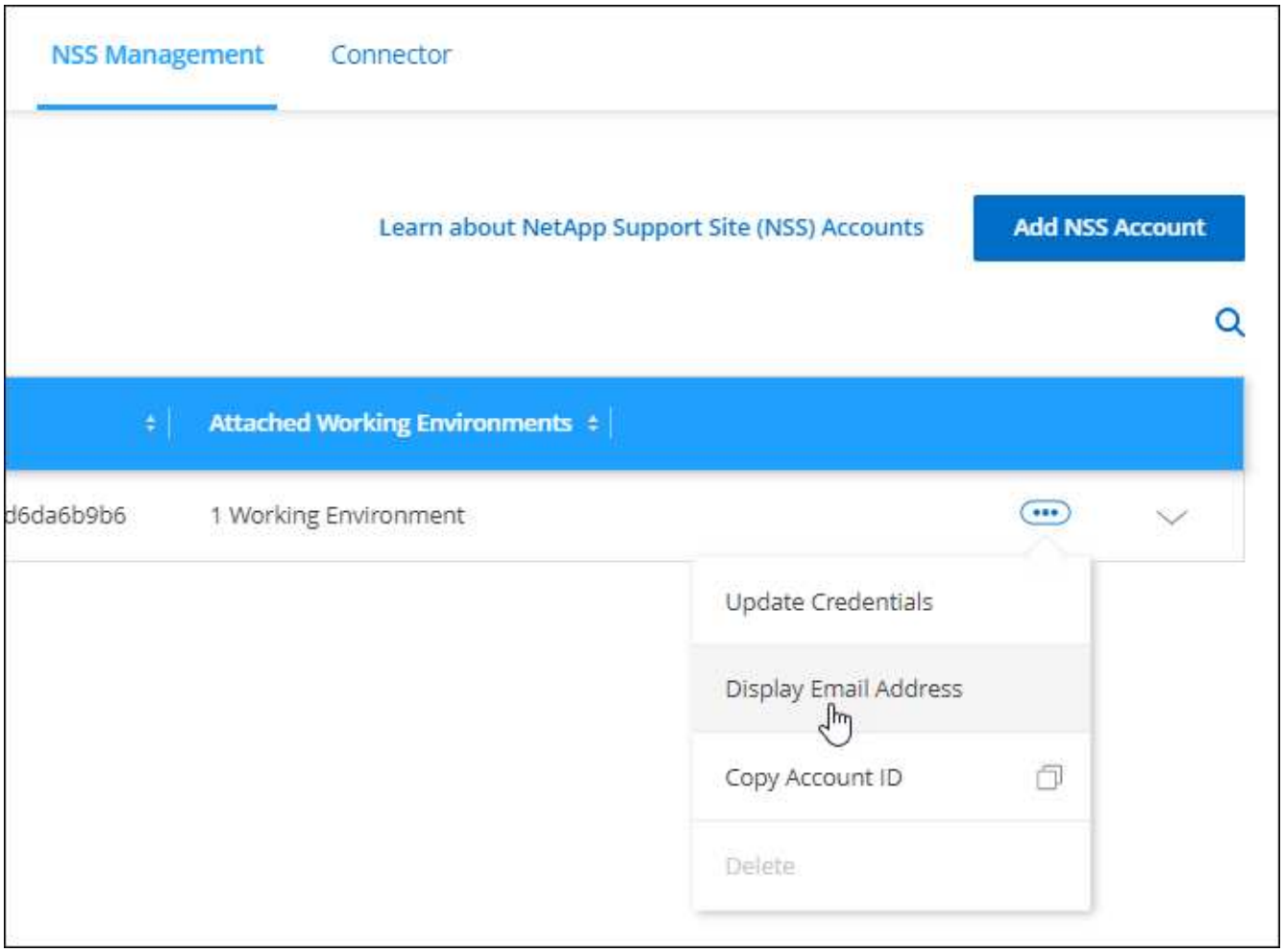
### Exibir o endereço de e-mail de uma conta NSS

Agora que as contas do site de suporte da NetApp usam o ID do Microsoft Entra para serviços de autenticação, o nome de usuário do NSS que é exibido no BlueXP  é normalmente um identificador gerado pelo Microsoft Entra. Como resultado, você pode não saber imediatamente o endereço de e-mail associado a essa conta. Mas o BlueXP  tem uma opção para mostrar o endereço de e-mail associado.

Quando você acessa a página Gerenciamento do NSS, o BlueXP  gera um token para cada conta na tabela. Esse token inclui informações sobre o endereço de e-mail associado. O token é então removido quando você sai da página. As informações nunca são armazenadas em cache, o que ajuda a proteger sua privacidade.

**Passos**

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda e selecione **suporte**.
2. Selecione **NSS Management**.
3. Para a conta NSS que você deseja atualizar, ••• selecione e selecione **Exibir endereço de e-mail**.




**Resultado**

O BlueXP  exibe o nome de usuário do site de suporte da NetApp e o endereço de e-mail associado. Você pode usar o botão copiar para copiar o endereço de e-mail.

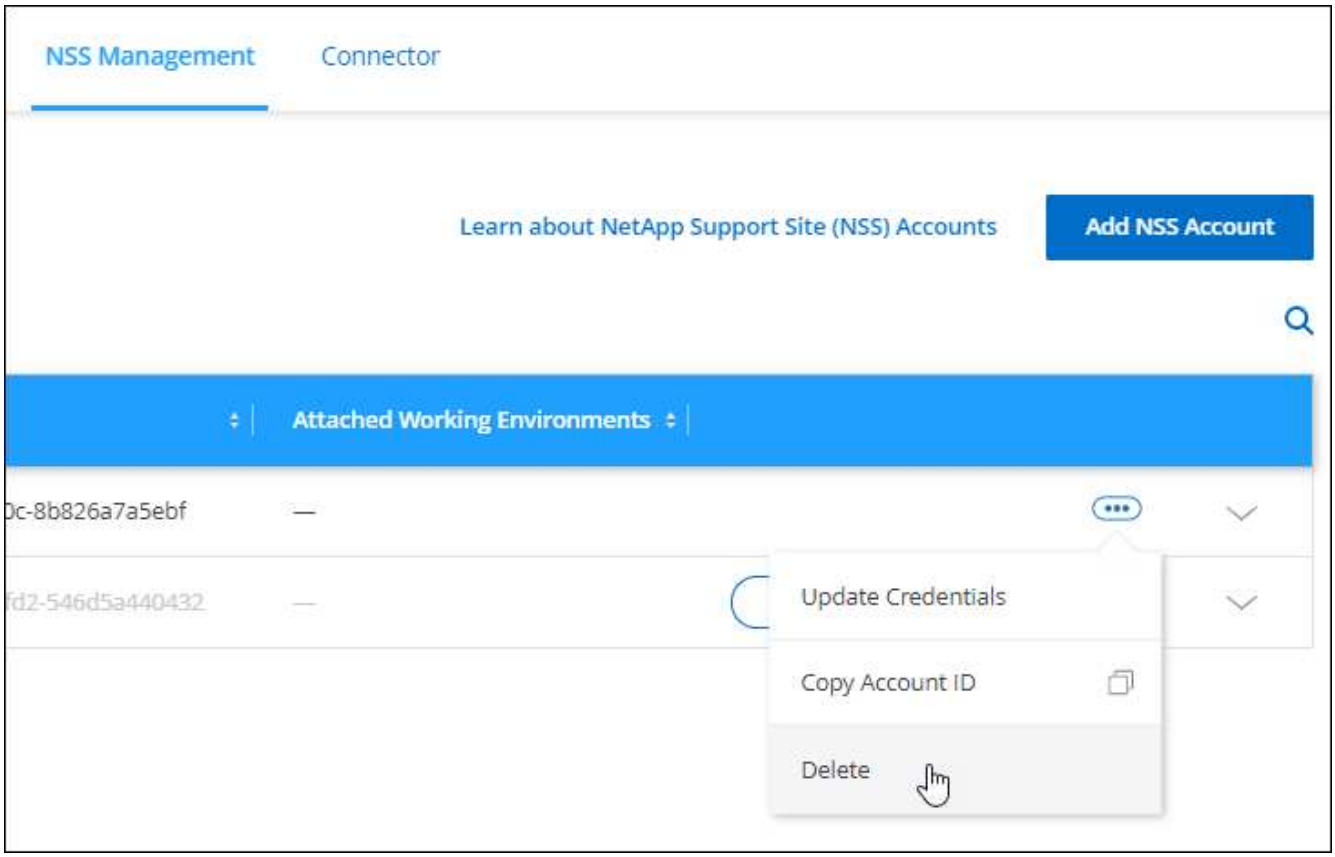
### Remover uma conta NSS

Exclua qualquer uma das contas NSS que você não deseja mais usar com o BlueXP .

Observe que não é possível excluir uma conta que esteja atualmente associada a um ambiente de trabalho do Cloud Volumes ONTAP. Primeiro você precisa Anexe esses ambientes de trabalho a uma conta NSS diferente.

**Passos**

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda e selecione **suporte**.
2. Selecione **NSS Management**.
3. Para a conta NSS que você deseja excluir, ••• selecione e selecione **Excluir**.




4. Selecione **Eliminar** para confirmar.

## Gerencie credenciais associadas ao seu login no BlueXP

Dependendo das ações realizadas no BlueXP , talvez você tenha associado credenciais do ONTAP e credenciais do site de suporte da NetApp (NSS) ao login de usuário do BlueXP . Você pode exibir e gerenciar essas credenciais no BlueXP  depois de associá-las. Por exemplo, se você alterar a senha dessas credenciais, precisará atualizar a senha no BlueXP .

### Credenciais ONTAP

Quando você descobre diretamente um cluster do ONTAP no local sem usar um conetor, será solicitado a inserir credenciais do ONTAP para o cluster. Essas credenciais são gerenciadas no nível do usuário, o que significa que elas não são visíveis por outros usuários que fazem login.

### Credenciais NSS

As credenciais do NSS associadas ao login do BlueXP  permitem o Registro de suporte, o gerenciamento de casos e o acesso ao consultor digital.

- Quando você acessa **suporte > recursos** e se Registra para obter suporte, será solicitado que você associe credenciais NSS ao seu login no BlueXP .

  Esta ação Registra a organização ou conta do BlueXP  para obter suporte e ativa o direito ao suporte. Somente um usuário em sua organização ou conta do BlueXP  deve associar uma conta do site de suporte da NetApp ao login do BlueXP  para se Registrar para obter suporte e ativar o direito de suporte.

Depois que isso for concluído, a página **recursos** mostra que sua conta está registrada para suporte.

"Saiba como se inscrever para obter suporte"

- Quando aceder a **suporte > Gestão de casos**, ser-lhe-á pedido que introduza as suas credenciais NSS, se ainda não o tiver feito. Esta página permite-lhe criar e gerir os casos de suporte associados à sua conta NSS e à sua empresa.
- Quando você acessa o consultor digital no BlueXP , você será solicitado a fazer login no consultor digital inserindo suas credenciais do NSS.

Observe o seguinte sobre a conta NSS associada ao seu login no BlueXP :

- A conta é gerenciada no nível do usuário, o que significa que não é visível por outros usuários que fazem login.
- Só pode haver uma conta NSS associada ao Digital Advisor e ao gerenciamento de casos de suporte, por usuário.
- Se você estiver tentando associar uma conta do site de suporte da NetApp a um ambiente de trabalho da Cloud Volumes ONTAP, você só poderá escolher entre as contas NSS que foram adicionadas à organização ou à conta da BlueXP  da qual você é membro.

  As credenciais no nível da conta NSS são diferentes da conta NSS associada ao seu login no BlueXP . As credenciais de nível de conta do NSS permitem que você implante o Cloud Volumes ONTAP quando você traz sua própria licença (BYOL), Registra sistemas PAYGO e atualiza o software Cloud Volumes ONTAP.

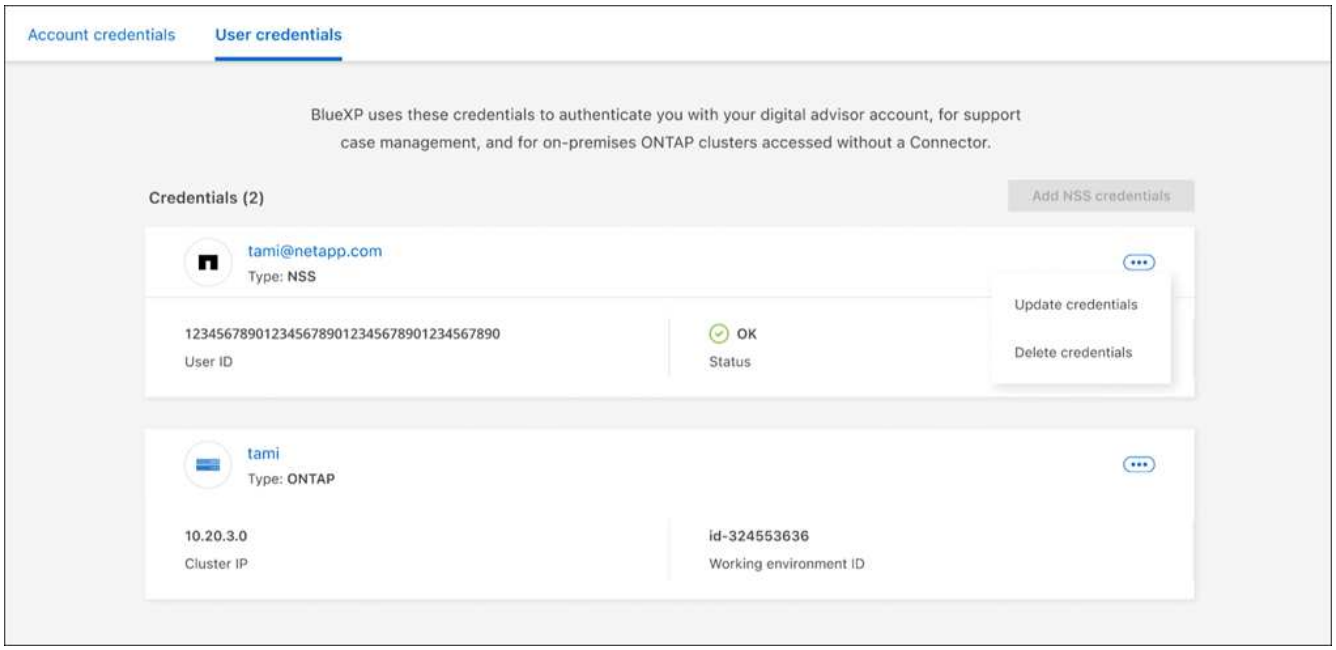
  "Saiba mais sobre como usar credenciais NSS com sua organização ou conta do BlueXP ".

### Gerencie suas credenciais de usuário

Gerencie suas credenciais de usuário atualizando o nome de usuário e a senha ou excluindo as credenciais.

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Selecione **credenciais do usuário**.
3. Se ainda não tiver quaisquer credenciais de utilizador, pode selecionar **Adicionar credenciais NSS** para adicionar a sua conta no site de suporte da NetApp.
4. Gerencie credenciais existentes escolhendo as seguintes opções:
   - **Atualizar credenciais**: Atualize o nome de usuário e a senha da conta.
   - **Excluir credenciais**: Remova a conta associada à sua conta de usuário do BlueXP .




**Resultado**

O BlueXP  atualiza suas credenciais. As alterações serão refletidas quando você acessar o cluster do ONTAP, o consultor digital ou a página Gerenciamento de casos.

# Monitorar operações do BlueXP

Você pode monitorar o status das operações que o BlueXP  está executando para ver se há algum problema que você precisa resolver. Você pode exibir o status na linha do tempo, na Central de notificações ou ter notificações enviadas para seu e-mail.

A tabela a seguir fornece uma comparação entre a linha do tempo e a Central de notificações para que você possa entender o que cada um tem a oferecer.

| Centro de notificações | Linha do tempo |
| --- | --- |
| Mostra o status de alto nível para eventos e ações | Fornece detalhes para cada evento ou ação para investigação adicional |
| Mostra o status da sessão de login atual (as informações não aparecerão no Centro de notificações após o logout) | Mantém o status do último mês |
| Mostra apenas ações iniciadas na interface do usuário | Mostra todas as ações da IU ou APIs |
| Mostra ações iniciadas pelo usuário | Mostra todas as ações, iniciadas pelo usuário ou iniciadas pelo sistema |
| Filtrar resultados por importância | Filtre por serviço, ação, usuário, status e muito mais |
| Fornece a capacidade de enviar notificações por e-mail para usuários e para outros | Sem capacidade de e-mail |

## Auditar a atividade do usuário a partir da linha do tempo do BlueXP

A linha do tempo no BlueXP  mostra as ações que os usuários concluíram para gerenciar sua organização ou conta. Isso inclui ações de gerenciamento, como associar usuários, criar ambientes de trabalho, criar conetores e muito mais.

Verificar a linha do tempo pode ser útil se você precisar identificar quem executou uma ação específica ou se precisar identificar o status de uma ação.

**Passos**

1. No canto superior direito do console BlueXP , selecione > **linha do tempo**.
2. Use os filtros acima da tabela para alterar as ações exibidas na tabela.

   Por exemplo, você pode usar o filtro **Serviço** para mostrar ações relacionadas a um serviço BlueXP específico ou usar o filtro **Usuário** para mostrar ações relacionadas a uma conta de usuário específica.

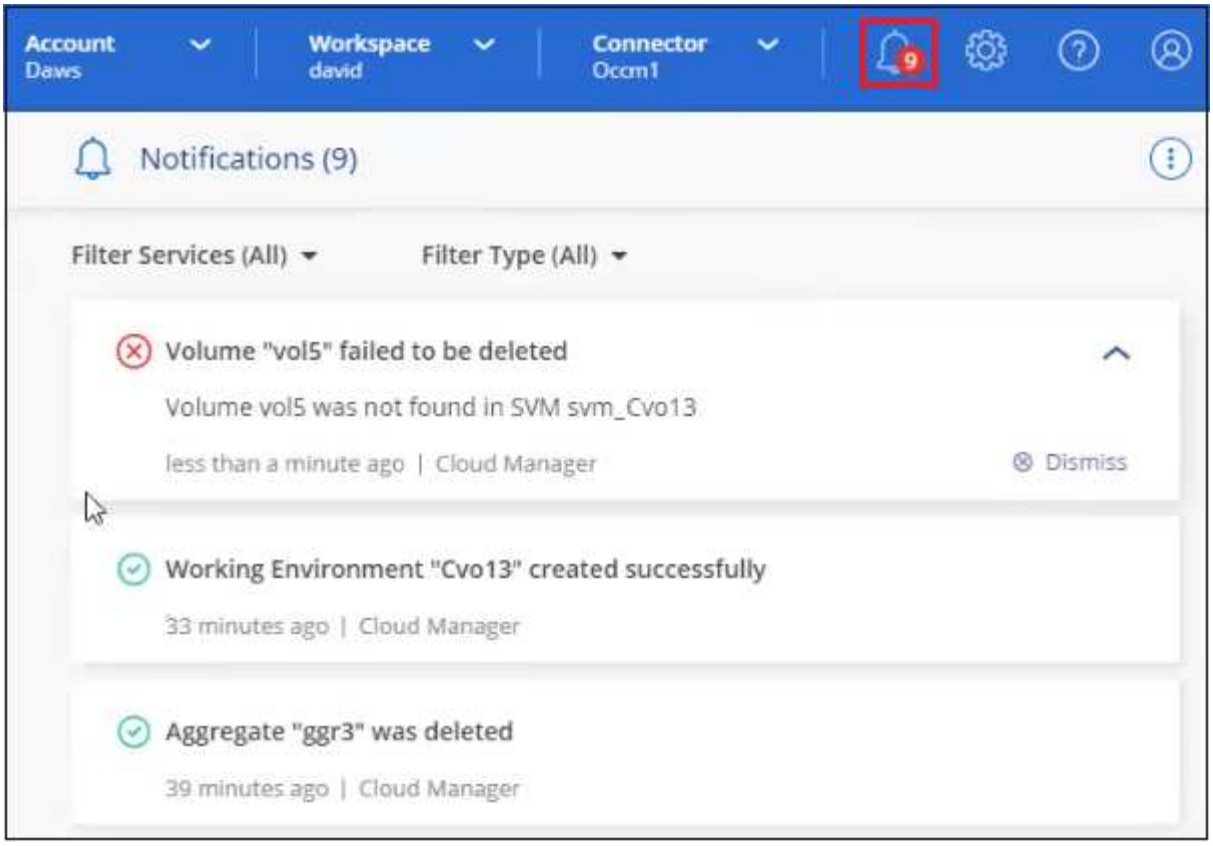
**Resultado**

A linha do tempo é atualizada para mostrar as ações de gerenciamento concluídas.

## Monitore atividades usando o Centro de notificações

As notificações rastreiam o progresso das operações iniciadas no BlueXP  para que você possa verificar se a operação foi bem-sucedida ou não. Eles permitem que você visualize o status de muitas ações do BlueXP iniciadas durante sua sessão de login atual. Neste momento, nem todos os serviços BlueXP  reportam informações na Central de notificações.

É possível exibir as notificações selecionando o sino de notificação ( ) na barra de menus. A cor da pequena bolha no sino indica a notificação de gravidade de nível mais alto que está ativa. Então, se você vir uma bolha vermelha, isso significa que há uma notificação importante que você deve olhar.




Você também pode configurar o BlueXP  para enviar certos tipos de notificações por e-mail, para que você possa ser informado sobre atividades importantes do sistema, mesmo quando não estiver conetado ao sistema. Os e-mails podem ser enviados a qualquer usuário que faça parte da sua organização ou conta do BlueXP  ou a qualquer outro destinatário que precise estar ciente de certos tipos de atividade do sistema. Consulte como defina as configurações de notificação por e-mail.

### Comparação da Central de notificações com alertas do BlueXP

A Central de notificações permite visualizar o status das operações iniciadas pelo BlueXP  e configurar notificações de alerta para determinados tipos de atividades do sistema. Enquanto isso, os alertas do BlueXP permitem visualizar problemas ou riscos potenciais no ambiente de storage do ONTAP relacionados à capacidade, disponibilidade, desempenho, proteção e segurança.

"Saiba mais sobre os alertas do BlueXP "

### Tipos de notificação

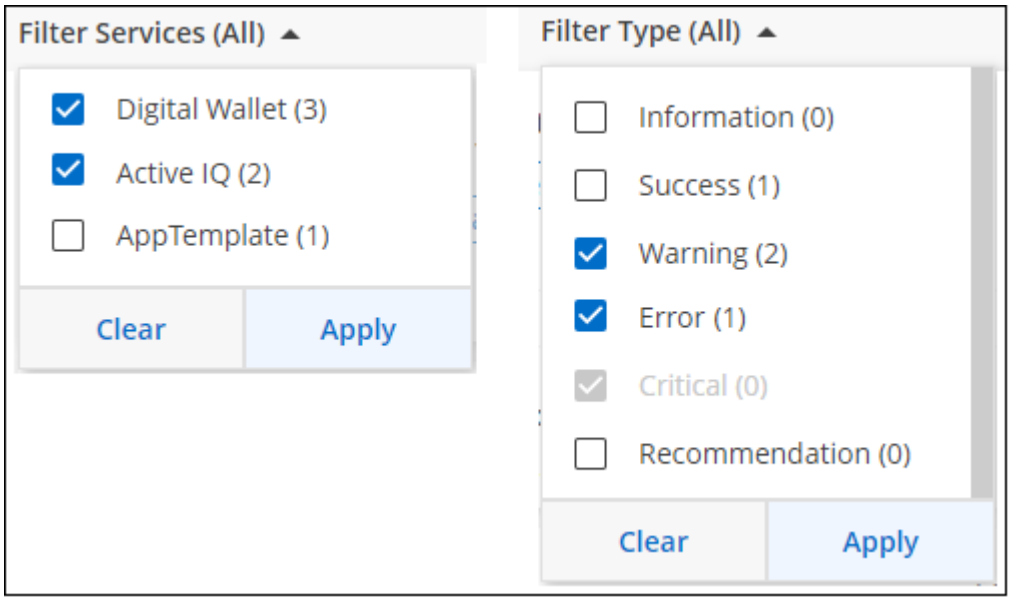
As notificações são classificadas nas seguintes categorias:

| Tipo de notificação | Descrição |
| --- | --- |
| Crítico | Ocorreu um problema que pode levar à interrupção do serviço se não forem tomadas medidas corretivas imediatamente. |
| Erro | Uma ação ou processo terminou com falha, ou pode levar à falha se não for tomada uma ação corretiva. |
| Aviso | Um problema que você deve estar ciente para se certificar de que ele não atinge a gravidade crítica. As notificações desta gravidade não causam interrupções no serviço e podem não ser necessárias ações corretivas imediatas. |

| Tipo de notificação | Descrição |
| --- | --- |
| Recomendação | Uma recomendação do sistema para que você tome uma ação para melhorar o sistema ou um determinado serviço; por exemplo: Economia de custos, sugestão de novos serviços, configuração de segurança recomendada, etc. |
| Informações | Uma mensagem que fornece informações adicionais sobre uma ação ou processo. |
| Sucesso | Uma ação ou processo concluído com sucesso. |

### Filtrar notificações

Por padrão, você verá todas as notificações ativas no Centro de notificações. Você pode filtrar as notificações que você vê para mostrar apenas as notificações que são importantes para você. Você pode filtrar por BlueXP "Serviço" e por notificação "tipo".




Por exemplo, se você quiser ver apenas notificações de "erro" e "Aviso" para operações do BlueXP , selecione essas entradas e você verá apenas esses tipos de notificações.

### Ignorar notificações

Você pode remover notificações da página se não precisar mais vê-las. Você pode ignorar todas as notificações de uma só vez ou ignorar notificações individuais.

Para ignorar todas as notificações, na Central de notificações, selecione e selecione **Descartar tudo**.


Para ignorar notificações individuais, passe o cursor sobre a notificação e selecione **Dismiss**.


### Defina as configurações de notificação por e-mail

Você pode enviar tipos específicos de notificações por e-mail para que você possa ser informado sobre atividades importantes do sistema, mesmo quando não estiver conetado ao BlueXP . Os e-mails podem ser enviados a qualquer usuário que faça parte da sua organização ou conta do BlueXP  ou a qualquer outro destinatário que precise estar ciente de certos tipos de atividade do sistema.

- As notificações são enviadas por e-mail para os seguintes recursos e serviços do BlueXP : Conetor, carteira digital BlueXP , cópia e sincronização do BlueXP  e backup e recuperação do BlueXP .
- O envio de notificações por e-mail não é suportado quando o conetor é instalado em um site sem acesso à Internet.

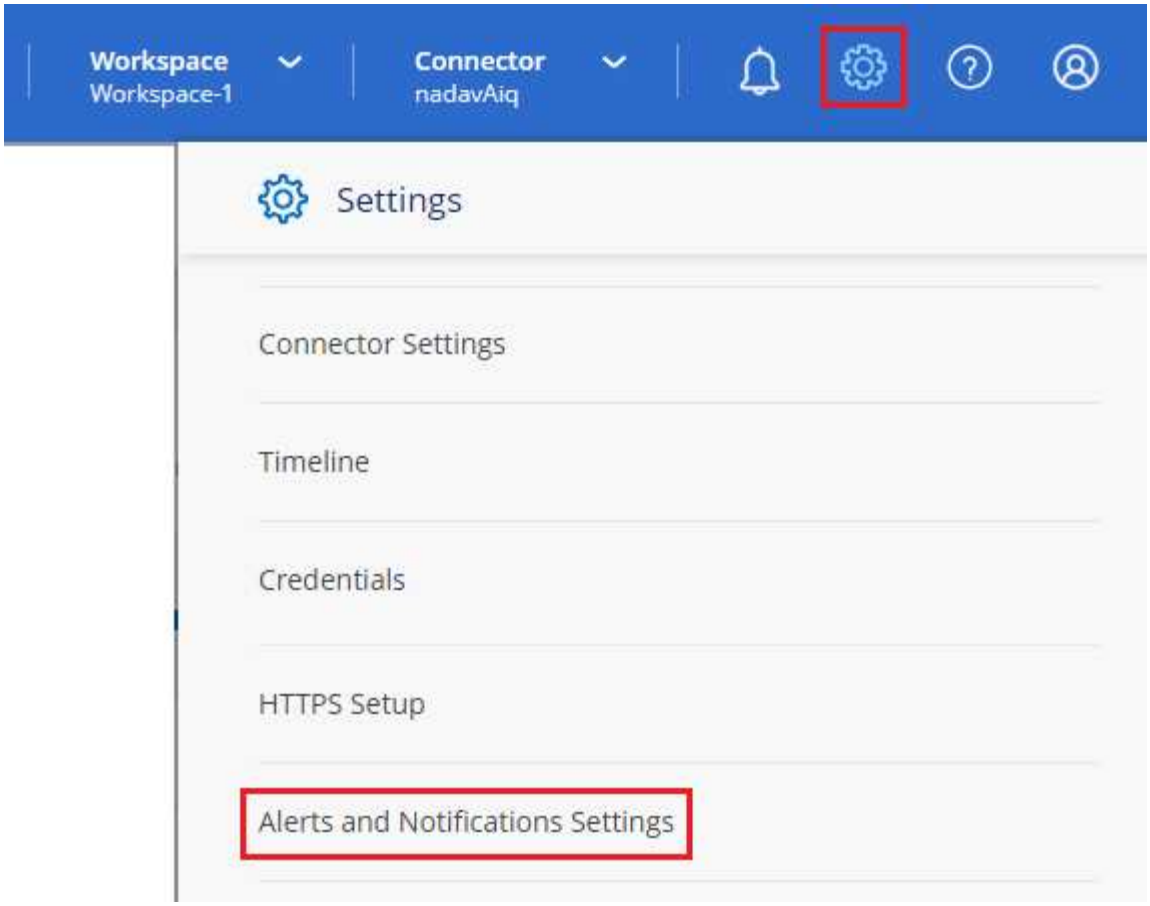
Os filtros definidos na Central de notificações não determinam os tipos de notificações que você receberá por e-mail. Por padrão, qualquer administrador do BlueXP  receberá e-mails para todas as notificações "críticas" e "Recomendação". Essas notificações estão em todos os serviços - você não pode optar por receber notificações apenas para determinados serviços, por exemplo, conetores ou backup e recuperação do BlueXP .

Todos os outros usuários e destinatários estão configurados para não receber nenhum e-mail de notificação - portanto, você precisará configurar as configurações de notificação para quaisquer usuários adicionais.

Você deve ser um administrador do BlueXP  para personalizar as configurações de notificações.

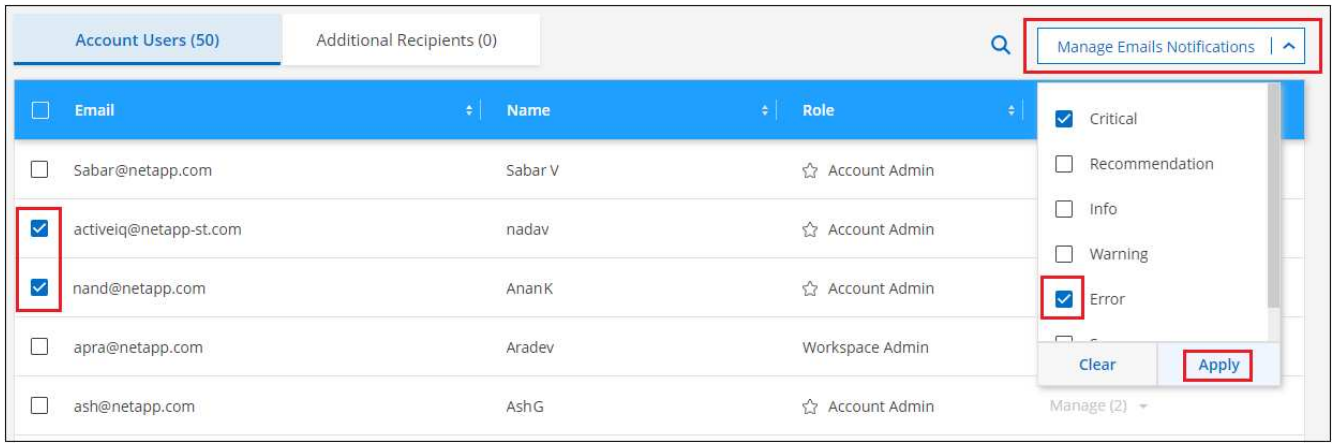
**Passos**

1. Na barra de menus do BlueXP , selecione **Definições > Definições de alertas e notificações**.




2. Selecione um usuário ou vários usuários na guia *Users* ou *Additional Recipients* e escolha o tipo de notificações a serem enviadas:

   - Para fazer alterações para um único usuário, selecione o menu na coluna notificações para esse usuário, verifique os tipos de notificações a serem enviadas e selecione **aplicar**.
   - Para fazer alterações para vários usuários, marque a caixa para cada usuário, selecione **Gerenciar notificações por e-mail**, marque os tipos de notificações a serem enviadas e selecione **aplicar**.



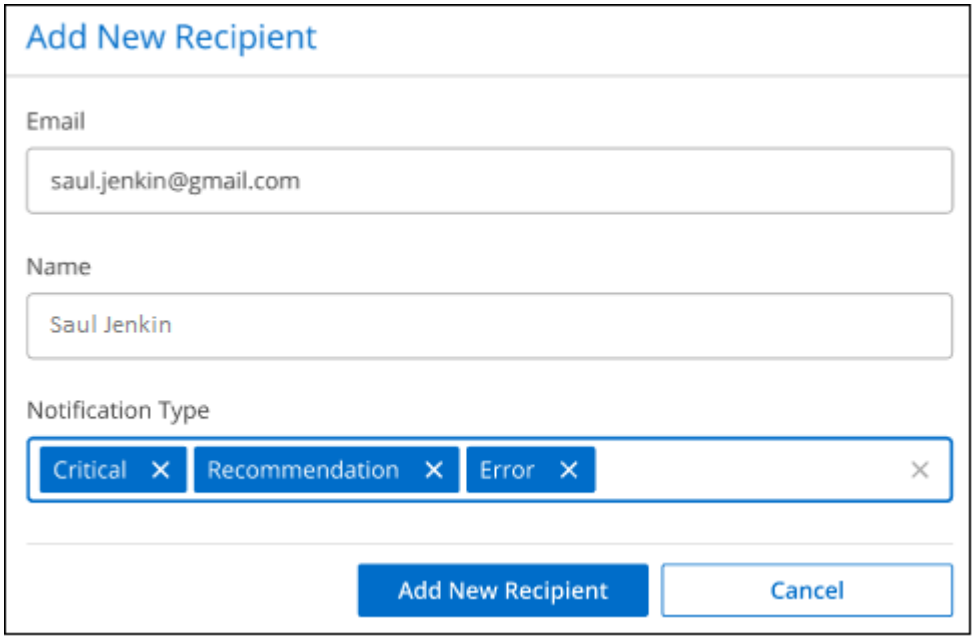

### Adicionar destinatários de e-mail adicionais

Os usuários que aparecem na guia *Users* são preenchidos automaticamente a partir dos usuários na sua organização ou conta do BlueXP . Você pode adicionar endereços de e-mail na guia *destinatários adicionais* para outras pessoas, ou grupos, que não têm acesso ao BlueXP , mas que precisam ser notificados sobre

certos tipos de alertas e notificações.

**Passos**

1. Na página Configurações de alertas e notificações, selecione **Adicionar novos destinatários**.




2. Digite o nome, o endereço de e-mail e selecione os tipos de notificações que o destinatário receberá e selecione **Adicionar novo destinatário**.

# Referência

# Permissões

## Resumo de permissões para o BlueXP

Para usar os recursos e serviços do BlueXP , você precisará fornecer permissões para que o BlueXP  possa executar operações em seu ambiente de nuvem. Use os links nesta página para acessar rapidamente as permissões que você precisa com base em seu objetivo.

### Permissões da AWS

O BlueXP  requer permissões da AWS para o conetor e para serviços individuais.

#### Conetores

| Meta | Descrição | Link |
|---|---|---|
| Implante o conetor do BlueXP | O usuário que cria um conetor do BlueXP  precisa de permissões específicas para implantar a instância na AWS. | "Configurar permissões da AWS" |
| Forneça permissões para o conetor | Quando o BlueXP  inicia o conetor, ele anexa uma política à instância que fornece as permissões necessárias para gerenciar recursos e processos em sua conta da AWS. Você precisa configurar a política por conta própria se iniciar um conetor no AWS Marketplace, se você instalar manualmente o conetor ou se você "Adicione mais credenciais da AWS a um conetor". Você também precisa garantir que a política esteja atualizada à medida que novas permissões forem adicionadas em versões subsequentes. | "Permissões da AWS para o conetor" |

#### Backup e recuperação

| Meta | Descrição | Link |
|---|---|---|
| Fazer backup de clusters ONTAP on-premises para o Amazon S3 | Ao ativar backups em seus volumes do ONTAP, o backup e a recuperação do BlueXP  solicita que você insira uma chave de acesso e um segredo para um usuário do IAM com permissões específicas. | "Configurar permissões S3 para backups" |

#### Cloud Volumes ONTAP

| Meta | Descrição | Link |
|---|---|---|
| Fornecer permissões para nós do Cloud Volumes ONTAP | Uma função do IAM deve ser anexada a cada nó do Cloud Volumes ONTAP na AWS. O mesmo se aplica ao mediador da HA. A opção padrão é permitir que o BlueXP  crie as funções do IAM para você, mas você pode usar as suas ao criar o ambiente de trabalho. | "Saiba como configurar as funções do IAM sozinho" |

#### Copiar e sincronizar

| Meta | Descrição | Link |
| --- | --- | --- |
| Implante o agente de dados na AWS | A conta de usuário da AWS que você usa para implantar o agente de dados deve ter permissões específicas. | "Permissões necessárias para implantar o agente de dados na AWS" |
| Forneça permissões para o agente de dados | Quando o BlueXP  copy and Sync implanta o agente de dados, ele cria uma função do IAM para a instância do agente de dados. Você pode implantar o agente de dados usando sua própria função do IAM, se preferir. | "Requisitos para usar sua própria função do IAM com o agente de dados da AWS" |
| Ative o AWS Access para um agente de dados instalado manualmente | Se você usar o agente de dados com uma relação de sincronização que inclui um bucket do S3, então você deve preparar o host Linux para o AWS Access. Ao instalar o data broker, você precisará fornecer chaves da AWS para um usuário do IAM com acesso programático e permissões específicas. | "Habilitando o acesso à AWS" |

#### FSX para ONTAP

| Meta | Descrição | Link |
| --- | --- | --- |
| Crie e gerencie o FSX para ONTAP | Para criar ou gerenciar um ambiente de trabalho do Amazon FSX for NetApp ONTAP, você precisa adicionar credenciais da AWS ao BlueXP  fornecendo o ARN de uma função do IAM que dá ao BlueXP  as permissões necessárias para criar o ambiente de trabalho. | "Saiba como configurar as credenciais da AWS para o FSX" |

#### Disposição em camadas

| Meta | Descrição | Link |
| --- | --- | --- |
| Categorize clusters ONTAP on-premises no Amazon S3 | Quando você ativa a disposição em camadas do BlueXP  na AWS, o assistente solicita que você insira uma chave de acesso e uma chave secreta. Essas credenciais são passadas para o cluster do ONTAP para que o ONTAP possa categorizar dados no bucket do S3. | "Configurar permissões S3 para disposição em camadas" |

### Permissões do Azure

O BlueXP  requer permissões do Azure para o conetor e para serviços individuais.

#### Conetores

| Meta | Descrição | Link |
| --- | --- | --- |
| Implante o conetor do BlueXP | Ao implantar um conetor do BlueXP , você precisa usar uma conta do Azure ou um responsável de serviço que tenha permissões para implantar a VM do Connector no Azure. | "Configurar permissões do Azure" |

| Meta | Descrição | Link |
| --- | --- | --- |
| Forneça permissões para o conetor | Quando o BlueXP  implanta a VM Connector no Azure, ele cria uma função personalizada que fornece as permissões necessárias para gerenciar recursos e processos dentro dessa assinatura do Azure.<br><br>Você precisa configurar a função personalizada sozinho se você iniciar um conetor do mercado, se você instalar manualmente o conetor ou se você "Adicione mais credenciais do Azure a um conetor".<br><br>Você também precisa garantir que a política esteja atualizada à medida que novas permissões forem adicionadas em versões subsequentes. | "Permissões do Azure para o conetor" |

#### Copiar e sincronizar

| Meta | Descrição | Link |
| --- | --- | --- |
| Implante o agente de dados no Azure | A conta de usuário do Azure que você usa para implantar o agente de dados deve ter as permissões necessárias. | "Permissões necessárias para implantar o agente de dados no Azure" |

### Permissões do Google Cloud

O BlueXP  requer permissões do Google Cloud para o conetor e para serviços individuais.

#### Conetores

| Meta | Descrição | Link |
| --- | --- | --- |
| Implante o conetor do BlueXP | O usuário do Google Cloud que implanta um conetor do BlueXP precisa de permissões específicas para implantar o conetor no Google Cloud. | "Configure permissões para criar o conetor" |
| Forneça permissões para o conetor | A conta de serviço da instância de VM Connector deve ter permissões específicas para operações diárias. Você precisa associar a conta de serviço ao conetor durante a implantação. Você também precisa garantir que a política esteja atualizada à medida que novas permissões forem adicionadas em versões subsequentes. | "Configure permissões para o conetor" |

#### Backup e recuperação

| Meta | Descrição | Link |
| --- | --- | --- |
| Faça backup do Cloud Volumes ONTAP para o Google Cloud | Ao usar o backup e a recuperação do BlueXP para fazer backup do Cloud Volumes ONTAP, você precisa adicionar permissões ao conetor nos seguintes cenários:<br>• Pretende utilizar a funcionalidade "Procurar e Restaurar"<br>• Você deseja usar chaves de criptografia gerenciadas pelo cliente (CMEK) | • "Permissões para a funcionalidade Procurar Restaurar"<br>• "Permissões para CMEKs" |
| Fazer backup de clusters do ONTAP no local no Google Cloud | Ao usar o backup e a recuperação do BlueXP para fazer backup de clusters ONTAP locais, você precisa adicionar permissões ao conetor para usar a funcionalidade "pesquisar e restaurar". | "Permissões para a funcionalidade Procurar Restaurar" |

#### Cloud Volumes Service para Google Cloud

| Meta | Descrição | Link |
| --- | --- | --- |
| Descubra o Cloud Volumes Service para Google Cloud | O BlueXP precisa de acesso à API do Cloud Volumes Service e às permissões certas por meio de uma conta de serviço do Google Cloud. | "Configure uma conta de serviço" |

#### Copiar e sincronizar

| Meta | Descrição | Link |
| --- | --- | --- |
| Implante o agente de dados no Google Cloud | Certifique-se de que o usuário do Google Cloud que implanta o agente de dados tenha as permissões necessárias. | "Permissões necessárias para implantar o agente de dados no Google Cloud" |
| Ative o Google Cloud Access para um agente de dados instalado manualmente | Se você planeja usar o agente de dados com uma relação de sincronização que inclua um bucket do Google Cloud Storage, prepare o host Linux para o Google Cloud Access. Ao instalar o corretor de dados, você precisará fornecer uma chave para uma conta de serviço que tenha permissões específicas. | "Habilitando o acesso ao Google Cloud" |

### Permissões do StorageGRID

O BlueXP requer permissões StorageGRID para dois serviços.

#### Backup e recuperação

| Meta | Descrição | Link |
| --- | --- | --- |
| Fazer backup de clusters ONTAP on-premises para o StorageGRID | Quando você prepara o StorageGRID como destino de backup para clusters do ONTAP, o backup e a recuperação do BlueXP solicitará que você insira uma chave de acesso e um segredo para um usuário do IAM com permissões específicas. | "Prepare o StorageGRID como destino do backup" |

**Disposição em camadas**

| Meta | Descrição | Link |
| --- | --- | --- |
| Colocar clusters ONTAP on-premises em categorias no StorageGRID | Ao configurar a disposição em camadas do BlueXP no StorageGRID, você precisa fornecer a disposição em camadas do BlueXP com uma chave de acesso S3 e uma chave secreta. A disposição em camadas do BlueXP usa as chaves para acessar seus buckets. | "Preparar a disposição em camadas no StorageGRID" |

## Permissões da AWS para o conetor

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

### Políticas do IAM

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

Observe o seguinte:

- Se você criar um conetor em uma região padrão da AWS diretamente do BlueXP , o BlueXP aplicará automaticamente políticas ao conetor.
- Você precisa configurar as políticas por conta própria se você implantar o conetor no AWS Marketplace, se você instalar manualmente o conetor em um host Linux ou se quiser adicionar credenciais adicionais da AWS ao BlueXP .
- Em ambos os casos, você precisa garantir que as políticas estejam atualizadas à medida que novas permissões são 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 elemento IAM `Condition`. "Documentação da AWS: Elemento condição"
- Para ver instruções passo a passo para utilizar estas políticas, consulte as seguintes páginas:
  - "Configurar permissões para uma implantação do AWS Marketplace"
  - "Configurar permissões para implantações locais"
  - "Configurar permissões para o modo restrito"
  - "Configurar permissões para o modo privado"

Selecione sua região para exibir as políticas necessárias:

**Regiões padrão**

Para regiões padrão, as permissões são distribuídas em duas políticas. Duas políticas são necessárias devido a um limite máximo de tamanho de caractere 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:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "fsx:Describe*",
                "fsx:List*",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "cvoServicePolicy"
        },
        {
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "kms:List*",
                "kms:Describe*",
                "ec2:DescribeVpcEndpoints",
                "kms:ListAliases",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
                "glue:BatchDeletePartition"
```

```
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "backupPolicy"
        },
        {
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketAcl",
                "s3:PutBucketPublicAccessBlock",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",
                "s3:DeleteBucket",
                "s3:GetObjectVersionTagging",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:PutObjectVersionTagging",
                "s3:PutObjectRetention",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketVersioning",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:PutBucketPolicy",
                "s3:PutBucketOwnershipControls"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
```

```
            ],
            "Effect": "Allow",
            "Sid": "backupS3Policy"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:DeleteBucket"
            ],
            "Resource": [
                "arn:aws:s3:::fabric-pool*"
            ],
            "Effect": "Allow",
            "Sid": "fabricPoolS3Policy"
        },
        {
            "Action": [
                "ec2:DescribeRegions"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "fabricPoolPolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/netapp-adc-manager": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
```

```
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume",
                "ec2:StopInstances",
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        }
    ]
```

```
}
```

**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:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
```

```
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::fabric-pool*"
            ]
        },
        {
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::netapp-backup-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
```

```
                "arn:aws-us-gov:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-us-gov:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

**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",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

**Top 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",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

### Como as permissões da AWS são usadas

As seções a seguir descrevem como as permissões são usadas para cada serviço BlueXP . Essas informações podem ser úteis se suas políticas corporativas determinarem que as permissões são fornecidas somente conforme necessário.

#### Amazon FSX para ONTAP

O conetor faz as seguintes solicitações de API para gerenciar um sistema de arquivos do Amazon FSX for ONTAP:

- EC2: DescribeInstances
- EC2:DescribeInstanceStatus
- EC2:DescribeInstanceAttribute
- EC2:DescribeRouteTables
- EC2: DescribeImages
- EC2:CreateTags
- EC2:DescribeVolumes
- EC2:DescribeSecurityGroups
- EC2:DescribeNetworkInterfaces

- EC2: DescribeSubnets
- EC2: DescribeVPCs
- EC2: DescribeDhcpOptions
- EC2:DescribeSnapshots
- EC2: DescribeKeyPairs
- EC2:DescribeRegiões
- EC2: DescribeTags
- EC2:DescribeIamInstanceProfileAssociations
- EC2:DescribeReservedInstancesOferings
- EC2:DescribeVpcEndpoints
- EC2: DescribeVPCs
- EC2:DescribeVolumesModificações
- EC2:DescribePlacementGroups
- Kms:Lista*
- Kms: Descrever*
- Kms:CreateGrant
- Kms:ListAliases
- fsx:descrever*
- fsx:Lista*

#### Descoberta de bucket do Amazon S3

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

S3:GetEncryptionConfiguration

#### Backup e recuperação

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

- S3:GetBucketLocation
- S3:ListAllMyBuckets
- S3: ListBucket
- S3:CreateBucket
- S3:GetLifecycleConfiguration
- S3:PutLifecycleConfiguration
- S3:PutBucketTagging
- S3:ListBucketVersions
- S3:GetBucketAcl
- S3:PutBucketPublicAccessBlock
- Kms:Lista*

- Kms: Descrever*
- S3:GetObject
- EC2:DescribeVpcEndpoints
- Kms:ListAliases
- S3:PutEncryptionConfiguration

O conetor faz as seguintes solicitações de API quando você usa o método de pesquisa e restauração para restaurar volumes e arquivos:

- S3:CreateBucket
- S3:DeleteObject
- S3:DeleteObjectVersion
- S3:GetBucketAcl
- S3: ListBucket
- S3:ListBucketVersions
- S3:ListBucketMultipartUploads
- S3:PutObject
- S3:PutBucketAcl
- S3:PutLifecycleConfiguration
- S3:PutBucketPublicAccessBlock
- S3:AbortMultipartUpload
- S3:ListMultipartUploadParts
- atena:StartQueryExecution
- atena:GetQueryResults
- atena:GetQueryExecution
- Athena:StopQueryExecution
- Cola: CreateDatabase
- Cola: CreateTable
- Cola: BatchDeletePartition

O conetor faz as seguintes solicitações de API quando você usa a proteção DataLock e ransomware para seus backups de volume:

- S3:GetObjectVersionTagging
- S3:GetBucketObjectLockConfiguration
- S3:GetObjectVersionAcl
- S3:PutObjectTagging
- S3:DeleteObject
- S3:DeleteObjectTagging
- S3:GetObjectRetention

- S3:DeleteObjectVersionTagging
- S3:PutObject
- S3:GetObject
- S3:PutBucketObjectLockConfiguration
- S3:GetLifecycleConfiguration
- S3:ListBucketByTags
- S3:GetBucketTagging
- S3:DeleteObjectVersion
- S3:ListBucketVersions
- S3: ListBucket
- S3:PutBucketTagging
- S3:GetObjectTagging
- S3:PutBucketControle de versão
- S3:PutObjectVersionTagging
- S3:GetBucketControle de versão
- S3:GetBucketAcl
- S3:BypassGovernanceretenção
- S3:retenção de objetos Put
- S3:GetBucketLocation
- S3:GetObjectVersion

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

- S3:PutBucketPolicy
- S3:PutBucketOwnershipControls

#### Classificação

O conetor faz as seguintes solicitações de API para implantar a instância de classificação do BlueXP :

- EC2: DescribeInstances
- EC2:DescribeInstanceStatus
- EC2:RunInstances
- EC2:TerminateInstances
- EC2:CreateTags
- EC2:Createvolume
- EC2: Attachvolume
- EC2:CreateSecurityGroup
- EC2:DeleteSecurityGroup
- EC2:DescribeSecurityGroups

- EC2: CreateNetworkInterface
- EC2:DescribeNetworkInterfaces
- EC2:DeleteNetworkInterface
- EC2: DescribeSubnets
- EC2: DescribeVPCs
- EC2:CreateSnapshot
- EC2:DescribeRegiões
- Formação de nuvens: CreateStack
- Cloudformation:DeleteStack
- Cloudformation:DescribeStacks
- Cloudformation:DescribeStackEvents
- IAM:AddRoleToInstanceProfile
- EC2:AssociateIamInstanceProfile
- EC2:DescribeIamInstanceProfileAssociations

O conetor faz as seguintes solicitações de API para verificar buckets do S3 quando você usa a classificação do BlueXP :

- IAM:AddRoleToInstanceProfile
- EC2:AssociateIamInstanceProfile
- EC2:DescribeIamInstanceProfileAssociations
- S3:GetBucketTagging
- S3:GetBucketLocation
- S3:ListAllMyBuckets
- S3: ListBucket
- S3:GetBucketPolicyStatus
- S3:GetBucketPolicy
- S3:GetBucketAcl
- S3:GetObject
- IAM: GetRole
- S3:DeleteObject
- S3:DeleteObjectVersion
- S3:PutObject
- STS:AssumeRole

#### Cloud Volumes ONTAP

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

| Finalidade | Ação | Usado para implantação? | Usado para operações diárias? | Usado para exclusão? |
|---|---|---|---|---|
| Crie e gerencie funções e perfis de instâncias do IAM para instâncias do Cloud Volumes ONTAP | IAM:ListInstanceProfiles | Sim | Sim | Não |
| | IAM:CreateRole | Sim | Não | Não |
| | IAM:DeleteRole | Não | Sim | Sim |
| | IAM:PutRolePolicy | Sim | Não | Não |
| | IAM:CreateInstanceProfile | Sim | Não | Não |
| | IAM:DeleteRolePolicy | Não | Sim | Sim |
| | IAM:AddRoleToInstanceProfile | Sim | Não | Não |
| | IAM:RemoveRoleFromInstanceProfile | Não | Sim | Sim |
| | IAM:DeleteInstanceProfile | Não | Sim | Sim |
| | IAM:PassRole | Sim | Não | Não |
| | EC2:AssociateIamInstanceProfile | Sim | Sim | Não |
| | EC2:DescribeIamInstanceProfileAssociations | Sim | Sim | Não |
| | EC2:DesassociateIamInstanceProfile | Não | Sim | Não |
| Decodificar mensagens de status de autorização | STS:DecodeAuthorizationMessage | Sim | Sim | Não |
| Descrever as imagens especificadas (AMIS) disponíveis para a conta | EC2: DescribeImages | Sim | Sim | Não |
| Descrever as tabelas de rota em uma VPC (necessário apenas para pares de HA) | EC2:DescribeRouteTables | Sim | Não | Não |

| Finalidade | Ação | Usado para implantação? | Usado para operações diárias? | Usado para exclusão? |
|---|---|---|---|---|
| Parar, iniciar e monitorar instâncias | EC2: StartInstances | Sim | Sim | Não |
| | EC2:StopInstances | Sim | Sim | Não |
| | EC2: DescribeInstances | Sim | Sim | Não |
| | EC2:DescribeInstanceStatus | Sim | Sim | Não |
| | EC2:RunInstances | Sim | Não | Não |
| | EC2:TerminateInstances | Não | Não | Sim |
| | EC2:ModifyInstanceAttribute | Não | Sim | Não |
| Verifique se a rede aprimorada está ativada para tipos de instâncias compatíveis | EC2:DescribeInstanceAttribute | Não | Sim | Não |
| Marque recursos com as tags "WorkingEnvironment" e "WorkingEnvironmentId" que são usadas para manutenção e alocação de custos | EC2:CreateTags | Sim | Sim | Não |
| Gerenciar volumes do EBS que o Cloud Volumes ONTAP usa como armazenamento back-end | EC2:Createvolume | Sim | Sim | Não |
| | EC2:DescribeVolumes | Sim | Sim | Sim |
| | EC2:ModifyVolumeAtributo | Não | Sim | Sim |
| | EC2: Attachvolume | Sim | Sim | Não |
| | EC2:Deletevolume | Não | Sim | Sim |
| | EC2: Detachvolume | Não | Sim | Sim |

| Finalidade | Ação | Usado para implantação? | Usado para operações diárias? | Usado para exclusão? |
|---|---|---|---|---|
| Crie e gerencie grupos de segurança para o Cloud Volumes ONTAP | EC2:CreateSecurityGroup | Sim | Não | Não |
| | EC2:DeleteSecurityGroup | Não | Sim | Sim |
| | EC2:DescribeSecurityGroups | Sim | Sim | Sim |
| | EC2:RevokeSecurityGroupEgress | Sim | Não | Não |
| | EC2:AutorizeSecurityGroupEgress | Sim | Não | Não |
| | EC2:AutorizeSecurityGroupIngress | Sim | Não | Não |
| | EC2:RevokeSecurityGroupIngress | Sim | Sim | Não |
| Crie e gerencie interfaces de rede para Cloud Volumes ONTAP na sub-rede de destino | EC2:CreateNetworkInterface | Sim | Não | Não |
| | EC2:DescribeNetworkInterfaces | Sim | Sim | Não |
| | EC2:DeleteNetworkInterface | Não | Sim | Sim |
| | EC2:ModifyNetworkInterfaceAttribute | Não | Sim | Não |
| Obtenha a lista de sub-redes de destino e grupos de segurança | EC2:DescribeSubnets | Sim | Sim | Não |
| | EC2: DescribeVPCs | Sim | Sim | Não |
| Obtenha servidores DNS e o nome de domínio padrão para instâncias Cloud Volumes ONTAP | EC2:DescribeDhcpOptions | Sim | Não | Não |
| Tire instantâneos de volumes do EBS para Cloud Volumes ONTAP | EC2:CreateSnapshot | Sim | Sim | Não |
| | EC2:DeleteSnapshot | Não | Sim | Sim |
| | EC2:DescribeSnapshots | Não | Sim | Não |

| Finalidade | Ação | Usado para implantação? | Usado para operações diárias? | Usado para exclusão? |
|---|---|---|---|---|
| Capture o console do Cloud Volumes ONTAP, que está conetado às mensagens do AutoSupport | EC2:GetConsoleOutput | Sim | Sim | Não |
| Obtenha a lista de pares de chaves disponíveis | EC2: DescribeKeyPairs | Sim | Não | Não |
| Obtenha a lista de regiões da AWS disponíveis | EC2:DescribeRegiões | Sim | Sim | Não |
| Gerenciar tags para recursos associados às instâncias do Cloud Volumes ONTAP | EC2:DeleteTags | Não | Sim | Sim |
| | EC2: DescribeTags | Não | Sim | Não |
| Crie e gerencie stacks para modelos do AWS CloudFormation | Formação de nuvens: CreateStack | Sim | Não | Não |
| | Cloudformation:DeleteStack | Sim | Não | Não |
| | Cloudformation:DescribeStacks | Sim | Sim | Não |
| | Cloudformation:DescribeStackEvents | Sim | Não | Não |
| | Cloudformation:ValidateTemplate | Sim | Não | Não |

| Finalidade | Ação | Usado para implantação? | Usado para operações diárias? | Usado para exclusão? |
|---|---|---|---|---|
| Crie e gerencie um bucket do S3 usado pelo sistema Cloud Volumes ONTAP como uma categoria de capacidade para categorização de dados | S3:CreateBucket | Sim | Sim | Não |
| | S3:DeleteBucket | Não | Sim | Sim |
| | S3:GetLifecycleConfiguration | Não | Sim | Não |
| | S3:PutLifecycleConfiguration | Não | Sim | Não |
| | S3:PutBucketTagging | Não | Sim | Não |
| | S3:ListBucketVersions | Não | Sim | Não |
| | S3:GetBucketPolicyStatus | Não | Sim | Não |
| | S3:GetBucketPublicAccessBlock | Não | Sim | Não |
| | S3:GetBucketAcl | Não | Sim | Não |
| | S3:GetBucketPolicy | Não | Sim | Não |
| | S3:PutBucketPublicAccessBlock | Não | Sim | Não |
| | S3:GetBucketTagging | Não | Sim | Não |
| | S3:GetBucketLocation | Não | Sim | Não |
| | S3:ListAllMyBuckets | 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:Lista* | Sim | Sim | Não |
| | Kms: Recriptografar* | Sim | Não | Não |
| | Kms: Descrever* | Sim | Sim | Não |
| | Kms:CreateGrant | Sim | Sim | Não |
| | Kms:GenerateDataKeyWithoutPlaxt | Sim | Sim | Não |
| 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:CreatePlacementGroup | Sim | Não | Não |
| | EC2:DeletePlacementGroup | Não | Sim | Sim |

| Finalidade | Ação | Usado para implantação? | Usado para operações diárias? | Usado para exclusão? |
|---|---|---|---|---|
| Crie relatórios | fsx:descrever* | Não | Sim | Não |
| | fsx:Lista* | Não | Sim | Não |
| Criar e gerenciar agregados que suportam o recurso volumes elásticos do Amazon EBS | EC2:DescribeVolumesModificações | Não | Sim | Não |
| | EC2:Modifyvolume | Não | Sim | Não |
| Verifique se a zona de disponibilidade é uma zona local da AWS e valida que todos os parâmetros de implementação são compatíveis | EC2:DescribeDisabilityZones | Sim | Não | Sim |

### Alterar registo

À medida que as permissões são adicionadas e removidas, vamos anotá-las nas seções abaixo.

#### 9 de setembro de 2024

As permissões foram removidas da política nº 2 para regiões padrão porque o BlueXP  não oferece mais suporte ao armazenamento em cache na borda do BlueXP , além de detecção e gerenciamento de clusters do Kubernetes.

**Exibir 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**

As seguintes permissões agora são necessárias para o Cloud Volumes ONTAP:

EC2:DescribeDisabilityZones

#### 6 de junho de 2023

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

Kms:GenerateDataKeyWithoutPlaxt

#### 14 de fevereiro de 2023

A seguinte permissão agora é necessária para a disposição em camadas do BlueXP :

EC2:DescribeVpcEndpoints

## Permissões do Azure para o conetor

Quando o BlueXP  inicia a VM Connector no Azure, ele atribui uma função personalizada à VM que fornece ao conetor permissões para gerenciar recursos e processos dentro dessa assinatura do Azure. O conetor usa as permissões para fazer chamadas de API para vários serviços do Azure.

### Permissões de função personalizadas

A função personalizada mostrada abaixo fornece as permissões que um conetor precisa para gerenciar recursos e processos na sua rede Azure.

Observe o seguinte:

- Quando você cria um conetor diretamente do BlueXP , o BlueXP  aplica automaticamente essa função personalizada ao conetor.
- Se você implantar o conetor a partir do Azure Marketplace ou instalar manualmente o conetor em um host Linux, precisará configurar a função personalizada por conta própria.
- Em ambos os casos, você precisa garantir que a função esteja atualizada à medida que novas permissões são adicionadas em versões subsequentes. Se novas permissões forem necessárias, elas serão listadas nas notas de versão.
- Para ver instruções passo a passo para utilizar estas políticas, consulte as seguintes páginas:
  - "Configurar permissões para uma implantação do Azure Marketplace"
  - "Configurar permissões para implantações locais"
  - "Configurar permissões para o modo restrito"
  - "Configurar permissões para o modo privado"

```
{
    "Name": "BlueXP Operator",
    "Actions": [
                    "Microsoft.Compute/disks/delete",
                    "Microsoft.Compute/disks/read",
                    "Microsoft.Compute/disks/write",
                    "Microsoft.Compute/locations/operations/read",
```

```
                    "Microsoft.Compute/locations/vmSizes/read",
                    "Microsoft.Resources/subscriptions/locations/read",
                    "Microsoft.Compute/operations/read",
                    "Microsoft.Compute/virtualMachines/instanceView/read",
                    "Microsoft.Compute/virtualMachines/powerOff/action",
                    "Microsoft.Compute/virtualMachines/read",
                    "Microsoft.Compute/virtualMachines/restart/action",
                    "Microsoft.Compute/virtualMachines/deallocate/action",
                    "Microsoft.Compute/virtualMachines/start/action",
                    "Microsoft.Compute/virtualMachines/vmSizes/read",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/images/read",
                    "Microsoft.Network/locations/operationResults/read",
                    "Microsoft.Network/locations/operations/read",
                    "Microsoft.Network/networkInterfaces/read",
                    "Microsoft.Network/networkInterfaces/write",
                    "Microsoft.Network/networkInterfaces/join/action",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/networkSecurityGroups/write",
                    "Microsoft.Network/networkSecurityGroups/join/action",
                    "Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
                    "Microsoft.Network/virtualNetworks/subnets/read",
                    "Microsoft.Network/virtualNetworks/subnets/write",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",

"Microsoft.Network/virtualNetworks/virtualMachines/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
                    "Microsoft.Resources/deployments/operations/read",
                    "Microsoft.Resources/deployments/read",
                    "Microsoft.Resources/deployments/write",
                    "Microsoft.Resources/resources/read",

"Microsoft.Resources/subscriptions/operationresults/read",

"Microsoft.Resources/subscriptions/resourceGroups/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",
                    "Microsoft.Storage/checknameavailability/read",
```

```
                    "Microsoft.Storage/operations/read",
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Storage/storageAccounts/read",
                    "Microsoft.Storage/storageAccounts/delete",
                    "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/listAccountSas/action",
                    "Microsoft.Storage/usages/read",
                    "Microsoft.Compute/snapshots/write",
                    "Microsoft.Compute/snapshots/read",
                    "Microsoft.Compute/availabilitySets/write",
                    "Microsoft.Compute/availabilitySets/read",
                    "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write",
                    "Microsoft.Network/loadBalancers/read",
                    "Microsoft.Network/loadBalancers/write",
                    "Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/backendAddressPools/join/action",

"Microsoft.Network/loadBalancers/loadBalancingRules/read",
                    "Microsoft.Network/loadBalancers/probes/read",
                    "Microsoft.Network/loadBalancers/probes/join/action",
                    "Microsoft.Authorization/locks/*",
                    "Microsoft.Network/routeTables/join/action",
                    "Microsoft.NetApp/netAppAccounts/read",
                    "Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
                    "Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acti
on",
```

```
"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
                    "Microsoft.Network/privateEndpoints/read",
                    "Microsoft.Network/privateDnsZones/write",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
                    "Microsoft.Network/virtualNetworks/join/action",
                    "Microsoft.Network/privateDnsZones/A/write",
                    "Microsoft.Network/privateDnsZones/read",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
                    "Microsoft.Insights/Metrics/Read",
                    "Microsoft.Compute/virtualMachines/extensions/write",
                    "Microsoft.Compute/virtualMachines/extensions/delete",
                    "Microsoft.Compute/virtualMachines/extensions/read",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Network/networkInterfaces/delete",
                    "Microsoft.Network/networkSecurityGroups/delete",
                    "Microsoft.Resources/deployments/delete",
                    "Microsoft.Compute/diskEncryptionSets/read",
                    "Microsoft.Compute/snapshots/delete",
                    "Microsoft.Network/privateEndpoints/delete",
                    "Microsoft.Compute/availabilitySets/delete",
                    "Microsoft.KeyVault/vaults/read",
                    "Microsoft.KeyVault/vaults/accessPolicies/write",
                    "Microsoft.Compute/diskEncryptionSets/write",
                    "Microsoft.KeyVault/vaults/deploy/action",
                    "Microsoft.Compute/diskEncryptionSets/delete",
                    "Microsoft.Resources/tags/read",
                    "Microsoft.Resources/tags/write",
                    "Microsoft.Resources/tags/delete",
                    "Microsoft.Network/applicationSecurityGroups/write",
                    "Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

"Microsoft.Network/networkSecurityGroups/securityRules/write",
                    "Microsoft.Network/applicationSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/securityRules/delete",
```

```
                    "Microsoft.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": "BlueXP Permissions",
    "IsCustom": "true"
}
```

### Como as permissões do Azure são usadas

As seções a seguir descrevem como as permissões são usadas para cada serviço BlueXP . Essas informações podem ser úteis se suas políticas corporativas determinarem que as permissões são fornecidas somente conforme necessário.

#### Azure NetApp Files

O conetor faz as seguintes solicitações de API quando você usa a classificação BlueXP  para verificar dados do Azure NetApp Files:

- Microsoft.NetApp/netAppAccounts/read
- Microsoft.NetApp/netAppAccount/capacityPools/read
- Microsoft.NetApp/netAppAccount/capacityPools/volumes/write
- Microsoft.NetApp/netAppAccount/capacityPools/volumes/read
- Microsoft.NetApp/netAppAccount/capacityPools/volumes/delete

#### Backup e recuperação

O conetor faz as seguintes solicitações de API para backup e recuperação do BlueXP :

- 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.KeyVault/vaults/read
- Microsoft.KeyVault/vaults/accessPolicies/write
- Microsoft.Network/networkInterfaces/read
- Microsoft.resources/assinaturas/localizações/leitura
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.resources/assinaturas/resourceGroups/read
- Microsoft.resources/assinaturas/resourcegroups/resources/read
- Microsoft.resources/assinaturas/resourceGroups/write
- Microsoft.Authorization/Locks/*
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/privateEndpoints/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/write
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Network/privateDnsZones/A/write
- Microsoft.Network/privateDnsZones/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/read
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.resources/deployments/delete
- Microsoft.ManagedIdentity/userAssignedIdentities/Assign/action

O conetor faz as seguintes solicitações de API quando você usa a funcionalidade pesquisar e Restaurar:

- Microsoft.Synapse/workspaces/write
- Microsoft.Synapse/workspaces/read
- Microsoft.Synapse/workspaces/delete
- Microsoft.Synapse/register/action
- Microsoft.Synapse/checkNameDisponibilidade/ação
- 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

#### Classificação

O conetor faz as seguintes solicitações de API quando você usa a classificação BlueXP .

| Ação | Usado para configurar? | Usado para operações diárias? |
|---|---|---|
| Microsoft.Compute/locations/operations/read | Sim | Sim |
| Microsoft.Compute/locations/vmSizes/read | Sim | Sim |
| Microsoft.Compute/operations/read | Sim | Sim |
| Microsoft.Compute/virtualMachines/instanceView/read | Sim | Sim |
| Microsoft.Compute/virtualMachines/powerOff/action | Sim | Não |
| Microsoft.Compute/virtualMachines/read | Sim | Sim |
| Microsoft.Compute/virtualMachines/restart/action | Sim | Não |
| Microsoft.Compute/virtualMachines/start/action | Sim | Não |
| Microsoft.Compute/virtualMachines/vmSizes/read | Não | Sim |
| Microsoft.Compute/virtualMachines/write | Sim | Não |
| Microsoft.Compute/images/read | Sim | Sim |
| Microsoft.Compute/disks/delete | Sim | Não |
| Microsoft.Compute/disks/read | Sim | Sim |
| Microsoft.Compute/disks/write | Sim | Não |
| Microsoft.Storage/checknameavailability/read | Sim | Sim |
| Microsoft.Storage/operations/read | Sim | Sim |
| Microsoft.Storage/storageAccounts/listkeys/action | Sim | Não |
| Microsoft.Storage/storageAccounts/read | Sim | Sim |
| Microsoft.Storage/storageAccounts/write | Sim | Não |
| Microsoft.Storage/storageAccounts/blobServices/containers/read | Sim | Sim |

| Ação | Usado para configurar? | Usado para operações diárias? |
| --- | --- | --- |
| Microsoft.Network/networkInterfaces/read | Sim | Sim |
| Microsoft.Network/networkInterfaces/write | Sim | Não |
| Microsoft.Network/networkInterfaces/join/action | Sim | Não |
| Microsoft.Network/networkSecurityGroups/read | Sim | Sim |
| Microsoft.Network/networkSecurityGroups/write | Sim | Não |
| Microsoft.resources/assinaturas/localizações/leitura | Sim | Sim |
| Microsoft.Network/locations/operationResults/read | Sim | Sim |
| Microsoft.Network/locations/operations/read | Sim | Sim |
| Microsoft.Network/virtualNetworks/read | Sim | Sim |
| Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read | Sim | Sim |
| Microsoft.Network/virtualNetworks/subnets/read | Sim | Sim |
| Microsoft.Network/virtualNetworks/subnets/virtualMachines/read | Sim | Sim |
| Microsoft.Network/virtualNetworks/virtualMachines/read | Sim | Sim |
| Microsoft.Network/virtualNetworks/subnets/join/action | Sim | Não |
| Microsoft.Network/virtualNetworks/subnets/write | Sim | Não |
| Microsoft.Network/routeTables/join/action | Sim | Não |
| Microsoft.resources/implantações/operações/leitura | Sim | Sim |
| Microsoft.resources/implantações/leitura | Sim | Sim |
| Microsoft.resources/implantações/gravação | Sim | Não |
| Microsoft.resources/resources/read | Sim | Sim |

| Ação | Usado para configurar? | Usado para operações diárias? |
| --- | --- | --- |
| Microsoft.resources/assinaturas/operationresults/read | Sim | Sim |
| Microsoft.resources/assinaturas/resourceGroups/delete | Sim | Não |
| Microsoft.resources/assinaturas/resourceGroups/read | Sim | Sim |
| Microsoft.resources/assinaturas/resourcegroups/resources/read | Sim | Sim |
| Microsoft.resources/assinaturas/resourceGroups/write | Sim | Não |

#### Cloud Volumes ONTAP

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

| Finalidade | Ação | Usado para implantação? | Usado para operações diárias? | Usado para exclusão? |
|---|---|---|---|---|
| Criar e gerenciar VMs | Microsoft.Compute/locations/operations/read | Sim | Sim | Não |
| | Microsoft.Compute/locations/vmSizes/read | Sim | Sim | Não |
| | Microsoft.resources/assinaturas/localizações/leitura | Sim | Não | Não |
| | Microsoft.Compute/operations/read | Sim | Sim | Não |
| | Microsoft.Compute/virtualMachines/instanceView/read | Sim | Sim | Não |
| | Microsoft.Compute/virtualMachines/powerOff/action | Sim | Sim | Não |
| | Microsoft.Compute/virtualMachines/read | Sim | Sim | Não |
| | Microsoft.Compute/virtualMachines/restart/action | Sim | Sim | Não |
| | Microsoft.Compute/virtualMachines/start/action | Sim | Sim | Não |
| | Microsoft.Compute/virtualMachines/deallocate/action | Não | Sim | Sim |
| | Microsoft.Compute/virtualMachines/vmSizes/read | Não | Sim | Não |
| | Microsoft.Compute/virtualMachines/write | Sim | Sim | Não |
| | Microsoft.Compute/virtualMachines/delete | Sim | Sim | Sim |
| | Microsoft.resources/deployments/delete | Sim | Não | Não |
| Ativar a implementação a partir de um VHD | Microsoft.Compute/images/read | Sim | Não | Não |
| | Microsoft.Compute/images/write | Sim | Não | Não |

| Finalidade | Ação | Usado para implantação? | Usado para operações diárias? | Usado para exclusão? |
|---|---|---|---|---|
| Crie e gerencie interfaces de rede na sub-rede de destino | Microsoft.Network/networkInterfaces/read | Sim | Sim | Não |
| | Microsoft.Network/networkInterfaces/write | Sim | Sim | Não |
| | Microsoft.Network/networkInterfaces/join/action | Sim | Sim | Não |
| | Microsoft.Network/networkInterfaces/delete | Sim | Sim | Não |
| Criar e gerenciar grupos de segurança de rede | Microsoft.Network/networkSecurityGroups/read | Sim | Sim | Não |
| | Microsoft.Network/networkSecurityGroups/write | Sim | Sim | Não |
| | Microsoft.Network/networkSecurityGroups/join/action | Sim | Não | Não |
| | Microsoft.Network/networkSecurityGroups/delete | Não | Sim | Sim |

| Finalidade | Ação | Usado para implantação? | Usado para operações diárias? | Usado para exclusão? |
|---|---|---|---|---|
| Obtenha informações de rede sobre regiões, VNet de destino e sub-rede e adicione as VMs aos VNets | Microsoft.Network/locations/operationResults/read | Sim | Sim | Não |
| | Microsoft.Network/locations/operations/read | Sim | Sim | Não |
| | Microsoft.Network/virtualNetworks/read | Sim | Não | Não |
| | Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read | Sim | Não | Não |
| | Microsoft.Network/virtualNetworks/subnets/read | Sim | Sim | Não |
| | Microsoft.Network/virtualNetworks/subnets/virtualMachines/read | Sim | Sim | Não |
| | Microsoft.Network/virtualNetworks/virtualMachines/read | Sim | Sim | Não |
| | Microsoft.Network/virtualNetworks/subnets/join/action | Sim | Sim | Não |

| Finalidade | Ação | Usado para implantação? | Usado para operações diárias? | Usado para exclusão? |
|---|---|---|---|---|
| Criar e gerenciar grupos de recursos | Microsoft.resources/implantações/operações/leitura | Sim | Sim | Não |
| | Microsoft.resources/implantações/leitura | Sim | Sim | Não |
| | Microsoft.resources/implantações/gravação | Sim | Sim | Não |
| | Microsoft.resources/resources/read | Sim | Sim | Não |
| | Microsoft.resources/assinaturas/operationresults/read | Sim | Sim | Não |
| | Microsoft.resources/assinaturas/resourceGroups/delete | Sim | Sim | Sim |
| | Microsoft.resources/assinaturas/resourceGroups/read | Não | Sim | Não |
| | Microsoft.resources/assinaturas/resourcegroups/resources/read | Sim | Sim | Não |
| | Microsoft.resources/assinaturas/resourceGroups/write | Sim | Sim | Não |

| Finalidade | Ação | Usado para implantação? | Usado para operações diárias? | Usado para exclusão? |
|---|---|---|---|---|
| Gerenciar contas e discos de storage do Azure | Microsoft.Compute/disks/read | Sim | Sim | Sim |
| | Microsoft.Compute/disks/write | Sim | Sim | Não |
| | Microsoft.Compute/disks/delete | Sim | Sim | Sim |
| | Microsoft.Storage/checknameavailability/read | Sim | Sim | Não |
| | Microsoft.Storage/operations/read | Sim | Sim | Não |
| | Microsoft.Storage/storageAccounts/listkeys/action | Sim | Sim | Não |
| | Microsoft.Storage/storageAccounts/read | 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 o armazenamento de Blob e a criptografia de contas de storage | Microsoft.Storage/storageAccounts/blobServices/containers/read | Sim | Sim | Não |
| | Microsoft.KeyVault/vaults/read | Sim | Sim | Não |
| | Microsoft.KeyVault/vaults/accessPolicies/write | Sim | Sim | Não |
| Habilite pontos de extremidade do serviço VNet para disposição em camadas de dados | Microsoft.Network/virtualNetworks/subnets/write | Sim | Sim | Não |
| | Microsoft.Network/routeTables/join/action | Sim | Sim | Não |

| Finalidade | Ação | Usado para implantação? | Usado para operações diárias? | Usado para exclusão? |
|---|---|---|---|---|
| Crie e gerencie snapshots gerenciados do Azure | Microsoft.Compute/snapshots/write | Sim | Sim | Não |
| | Microsoft.Compute/snapshots/read | Sim | Sim | Não |
| | Microsoft.Compute/snapshots/delete | Não | Sim | Sim |
| | Microsoft.Compute/disks/beginGetAccess/action | Não | Sim | Não |
| Criar e gerenciar conjuntos de disponibilidade | Microsoft.Compute/availabilitySets/write | Sim | Não | Não |
| | Microsoft.Compute/availabilitySets/read | Sim | Não | Não |
| Habilite implantações programáticas no marketplace | Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read | Sim | Não | Não |
| | Microsoft.MarketplaceOrdering/offertypes/publishers/offerments/offerments/offertyes | Sim | Sim | Não |

| Finalidade | Ação | Usado para implantação? | Usado para operações diárias? | Usado para exclusão? |
|---|---|---|---|---|
| Gerenciar um balanceador de carga para pares de HA | Microsoft.Network/loadBalancers/read | Sim | Sim | Não |
| | Microsoft.Network/loadBalancers/write | Sim | Não | Não |
| | Microsoft.Network/loadBalancers/delete | Não | Sim | Sim |
| | Microsoft.Network/loadBalancers/backendAddressPools/read | Sim | Não | Não |
| | Microsoft.Network/loadBalancers/backendAddressPools/join/action | Sim | Não | Não |
| | Microsoft.Network/loadBalancers/frontendIPConfigurations/read | Sim | Sim | Não |
| | Microsoft.Network/loadBalancers/loadBalancingRules/read | Sim | Não | Não |
| | Microsoft.Network/loadBalancers/probes/read | Sim | Não | Não |
| | Microsoft.Network/loadBalancers/probes/join/action | Sim | Não | Não |
| Habilite o gerenciamento de bloqueios em discos Azure | Microsoft.Authorization/Locks/* | Sim | Sim | Não |

| Finalidade | Ação | Usado para implantação? | Usado para operações diárias? | Usado para exclusão? |
|---|---|---|---|---|
| Ative endpoints privados para pares de HA quando não houver conetividade fora da sub-rede | Microsoft.Network/privateEndpoints/write | Sim | Sim | Não |
| | Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action | Sim | Não | Não |
| | Microsoft.Storage/storageAccounts/privateEndpointConnections/read | Sim | Sim | Sim |
| | Microsoft.Network/privateEndpoints/read | Sim | Sim | Sim |
| | Microsoft.Network/privateDnsZones/write | Sim | Sim | Não |
| | Microsoft.Network/privateDnsZones/virtualNetworkLinks/write | Sim | Sim | Não |
| | Microsoft.Network/virtualNetworks/join/action | Sim | Sim | Não |
| | Microsoft.Network/privateDnsZones/A/write | Sim | Sim | Não |
| | Microsoft.Network/privateDnsZones/read | Sim | Sim | Não |
| | Microsoft.Network/privateDnsZones/virtualNetworkLinks/read | Sim | Sim | Não |
| Necessário para algumas implantações de VM, dependendo do hardware físico subjacente | Microsoft.resources/deployments/operationStatuses/read | Sim | Sim | Não |
| Remover recursos de um grupo de recursos em caso de falha ou exclusão da implantação | Microsoft.Network/privateEndpoints/delete | Sim | Sim | Não |
| | Microsoft.Compute/availabilitySets/delete | Sim | Sim | Não |

| Finalidade | Ação | Usado para implantação? | Usado para operações diárias? | Usado para exclusão? |
|---|---|---|---|---|
| Ative o uso de chaves de criptografia gerenciadas pelo cliente ao usar a API | Microsoft.Compute/diskEncryptionSets/read | Sim | Sim | Sim |
| | Microsoft.Compute/diskEncryptionSets/write | Sim | Sim | Não |
| | Microsoft.KeyVault/vaults/deploy/action | Sim | Não | Não |
| | Microsoft.Compute/diskEncryptionSets/delete | Sim | Sim | Sim |
| Configure um grupo de segurança de aplicativos para um par de HA para isolar a interconexão de HA e as NICs de rede de cluster | Microsoft.Network/applicationSecurityGroups/write | Não | Sim | Não |
| | Microsoft.Network/applicationSecurityGroups/read | Não | Sim | Não |
| | Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action | Não | Sim | Não |
| | Microsoft.Network/networkSecurityGroups/securityRules/write | Sim | Sim | Não |
| | Microsoft.Network/applicationSecurityGroups/delete | Não | Sim | Sim |
| | Microsoft.Network/networkSecurityGroups/securityRules/delete | Não | Sim | Sim |
| Leia, escreva e exclua tags associadas aos recursos do Cloud Volumes ONTAP | Microsoft.resources/tags/read | Não | Sim | Não |
| | Microsoft.resources/tags/write | Sim | Sim | Não |
| | Microsoft.resources/tags/delete | Sim | Não | Não |
| Criptografe contas de storage durante a criação | Microsoft.ManagedIdentity/userAssignedIdentities/Assign/action | Sim | Sim | Não |

| Finalidade | Ação | Usado para implantação? | Usado para operações diárias? | Usado para exclusão? |
|---|---|---|---|---|
| Use conjuntos de escala de máquinas virtuais no modo de orquestração flexível para especificar zonas específicas para o Cloud Volumes ONTAP | Microsoft.Compute/virtualMachineScaleSets/write | Sim | Não | Não |
| | Microsoft.Compute/virtualMachineScaleSets/read | Sim | Não | Não |
| | Microsoft.Compute/virtualMachineScaleSets/delete | Não | Não | Sim |

#### Disposição em camadas

O conetor faz as seguintes solicitações de API quando você configura a disposição em camadas do BlueXP .

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.resources/assinaturas/resourceGroups/read
- Microsoft.resources/assinaturas/localizações/leitura

O conetor faz as seguintes solicitações de API para operações diárias.

- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/managemPolicies/read
- Microsoft.Storage/storageAccounts/managemPolicies/write
- Microsoft.Storage/storageAccounts/read

### Alterar registo

À medida que as permissões são adicionadas e removidas, vamos anotá-las nas seções abaixo.

#### 9 de setembro de 2024

As permissões a seguir foram removidas da política JSON porque o BlueXP  não suporta mais a descoberta e o gerenciamento de clusters do Kubernetes:

- Microsoft.ContainerService/managedclusters/listClusterUserCredential/action
- Microsoft.ContainerService/managedclusters/leitura

#### 22 de agosto de 2024

As permissões a seguir foram adicionadas à política JSON porque são necessárias para o suporte do Cloud Volumes ONTAP de conjuntos de escala de máquinas virtuais:

- Microsoft.Compute/virtualMachineScaleSets/write
- Microsoft.Compute/virtualMachineScaleSets/read
- Microsoft.Compute/virtualMachineScaleSets/delete

#### 5 de dezembro de 2023

As permissões a seguir não são mais necessárias para backup e recuperação do BlueXP  ao fazer backup de dados de volume para o storage Blob do Azure:

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

Essas permissões são necessárias para outros serviços de storage da BlueXP , portanto, continuarão na função personalizada do conetor se você estiver usando esses outros serviços de storage.

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

As permissões a seguir foram removidas da política JSON porque elas não são mais necessárias:

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

#### 23 de março de 2023

A permissão "Microsoft.Storage/storageAccounts/DELETE" não é mais necessária para a classificação BlueXP .

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/action
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

  Essas permissões são necessárias para backup e recuperação do BlueXP .

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

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

## Permissões do Google Cloud para o conetor

O BlueXP  requer permissões para executar ações no Google Cloud. Essas permissões estão incluídas em uma função personalizada fornecida pelo NetApp. Você pode querer

entender o que o BlueXP  faz com essas permissões.

**Permissões da conta de serviço**

A função personalizada mostrada abaixo fornece as permissões que um conetor precisa para gerenciar recursos e processos em sua rede do Google Cloud.

Você precisará aplicar essa função personalizada a uma conta de serviço que seja anexada à VM Connector.

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

Você também precisa garantir que a função esteja atualizada à medida que novas permissões são adicionadas em versões subsequentes. Se novas permissões forem necessárias, elas serão listadas nas notas de versão.

```
title: NetApp BlueXP
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.addAccessConfig
- compute.instances.attachDisk
```

```
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
- compute.instanceGroups.get
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
```

```
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
```

**Como as permissões do Google Cloud são usadas**

| Ações | Finalidade |
| --- | --- |
| - Compute.disks.create - Compute.disks.createSnapshot - compute.disks.delete - Compute.disks.get - Compute.disks.list - compute.disks.setLabels - compute.disks.use. | Para criar e gerenciar discos para Cloud Volumes ONTAP. |
| - compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list | Para criar regras de firewall para o Cloud Volumes ONTAP. |
| - Compute.globalOperations.get | Para obter o status das operações. |
| - Compute.images.get - Compute.images.getFromFamily - Compute.images.list - compute.images.useReadOnly | Para obter imagens para instâncias de VM. |

| Ações | Finalidade |
| --- | --- |
| - compute.instances.attachDisk - compute.instances.detachDisk | Para anexar e desanexar discos ao Cloud Volumes ONTAP. |
| - compute.instances.create - compute.instances.delete | Para criar e excluir instâncias de VM do Cloud Volumes ONTAP. |
| - compute.instances.get | Para listar instâncias de VM. |
| - compute.instances.getSerialPortOutput | Para obter logs de console. |
| - compute.instances.list | Para recuperar a lista de instâncias em uma zona. |
| - compute.instances.setDeletionProtection | Para definir a proteção de exclusão na instância. |
| - compute.instances.setLabels | Para adicionar etiquetas. |
| - compute.instances.setMachineType - compute.instances.setMinCpuPlatform | Para alterar o tipo de máquina para Cloud Volumes ONTAP. |
| - compute.instances.setMetadata | Para adicionar metadados. |
| - compute.instances.setTags | Para adicionar etiquetas para regras de firewall. |
| - compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice | Para iniciar e parar o Cloud Volumes ONTAP. |
| - Compute.machineTypes.get | Para obter os números de núcleos para verificar qoutas. |
| - compute.projects.get | Para apoiar multi-projetos. |
| - Compute.snapshots.create - compute.snapshots.delete - Compute.snapshots.get - Compute.snapshots.list - compute.snapshots.setLabels | Para criar e gerenciar snapshots persistentes em disco. |
| - compute.networks.get - compute.networks.list - Compute.regions.get - Compute.regions.list - Compute.subnetworks.get - Compute.subnetworks.list - Compute.zoneOperations.get - Compute.zones.get - Compute.zones.list | Para obter as informações de rede necessárias para criar uma nova instância de máquina virtual Cloud Volumes ONTAP. |
| - 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 | Para implantar a instância de máquina virtual do Cloud Volumes ONTAP usando o Gerenciador de implantação do Google Cloud. |
| - LogEntries.list - logging.privateLogEntries.list | Para obter unidades de log de pilha. |
| - resourcemanager.projects.get | Para apoiar multi-projetos. |
| - storage.buckets.create - storage.buckets.delete - storage.buckets.get - storage.buckets.list - storage.buckets.update | Para criar e gerenciar um bucket do Google Cloud Storage para categorização de dados. |

| Ações | Finalidade |
| --- | --- |
| - cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.list - cloudkms.keyrings.list | Para usar chaves de criptografia gerenciadas pelo cliente a partir do Serviço de gerenciamento de chaves na nuvem com o Cloud Volumes ONTAP. |
| - compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - storage.objects.get - storage.objects.list | Para definir uma conta de serviço na instância do Cloud Volumes ONTAP. Essa conta de serviço fornece permissões para categorização de dados em um bucket do Google Cloud Storage. |
| - compute.addresses.list | Para recuperar os endereços em uma região ao implantar um par de HA. |
| - Compute.backendServices.create - Compute.regionBackendServices.create - Compute.regionBackendServices.get - Compute.regionBackendServices.list | Para configurar um serviço de back-end para distribuir tráfego em um par de HA. |
| - compute.networks.updatePolicy | Para aplicar regras de firewall nos VPCs e sub-redes para um par de HA. |
| - compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig | Para ativar a classificação BlueXP . |
| - compute.instanceGroups.get - Compute.Addresses.get - compute.instances.updateNetworkInterface | Para criar e gerenciar VMs de storage em pares de HA do Cloud Volumes ONTAP. |
| - Monitoring.timeseries.list - storage.buckets.getIamPolicy | Para descobrir informações sobre os buckets do Google Cloud Storage. |
| - Cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.getIamPolicy - cloudkms.cryptoKeys.list - cloudkms.cryptoKeys.setIamPolicy - cloudkms.keyrings.get - cloudkms.keyrings.getIamPolicy - cloudkms.keyrings.list - cloudkms.keyRings.setIamPolicy | Para selecionar suas próprias chaves gerenciadas pelo cliente no assistente de ativação de backup e recuperação do BlueXP  em vez de usar as chaves de criptografia gerenciadas pelo Google padrão. |

### Alterar registo

À medida que as permissões são adicionadas e removidas, vamos anotá-las nas seções abaixo.

#### 6 de fevereiro de 2023

A seguinte permissão foi adicionada a esta política:

- compute.instances.updateNetworkInterface

Esta permissão é necessária para o Cloud Volumes ONTAP.

#### 27 de janeiro de 2023

As seguintes permissões foram adicionadas à política:

- Cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- Cloudkms.keyrings.get
- Cloudkms.keyrings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

Essas permissões são necessárias para backup e recuperação do BlueXP .

# Portas

## Regras do grupo de segurança do conetor na AWS

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

### Regras de entrada

| Protocolo | Porta | Finalidade |
|---|---|---|
| SSH | 22 | Fornece acesso SSH ao host do conetor |
| HTTP | 80 | • Fornece acesso HTTP a partir de navegadores da Web cliente para a interface de usuário local<br>• Usado durante o processo de atualização do Cloud Volumes ONTAP |
| HTTPS | 443 | Fornece acesso HTTPS a partir de navegadores da Web cliente para a interface de usuário local e conexões a partir da instância de classificação BlueXP |
| TCP | 3128 | Fornece ao Cloud Volumes ONTAP acesso à Internet para enviar mensagens AutoSupport para o suporte da NetApp. Você deve abrir manualmente essa porta após a implantação. "Saiba como o conetor é usado como proxy para mensagens AutoSupport" |

### Regras de saída

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

#### Regras básicas de saída

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

| Protocolo | Porta | Finalidade |
|---|---|---|
| Todo o TCP | Tudo | Todo o tráfego de saída |
| Todos os UDP | Tudo | Todo o tráfego de saída |

#### Regras de saída avançadas

Se você 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 conetor.

O endereço IP de origem é o host do conetor.

| Serviço | Protocolo | Porta | Destino | Finalidade |
|---|---|---|---|---|
| Chamadas de API e AutoSupport | HTTPS | 443 | LIF de gerenciamento de cluster de ONTAP e Internet de saída | Chamadas de API para AWS, ONTAP, classificação BlueXP  e envio de mensagens AutoSupport para NetApp |
| Chamadas de API | TCP | 3000 | Mediador do ONTAP HA | Comunicação com o mediador ONTAP HA |
| | TCP | 8080 | Classificação BlueXP | Sonda para a instância de classificação BlueXP  durante a implantação |
| DNS | UDP | 53 | DNS | Usado para resolução de DNS por BlueXP |

## Regras do grupo de segurança do conetor no Azure

O grupo de segurança do Azure para o conetor requer regras de entrada e saída. O BlueXP  cria automaticamente esse grupo de segurança quando você cria um conetor do BlueXP . Você precisa configurar este grupo de segurança para todas as outras opções de instalação.

#### Regras de entrada

| Protocolo | Porta | Finalidade |
|---|---|---|
| SSH | 22 | Fornece acesso SSH ao host do conetor |

| Protocolo | Porta | Finalidade |
| --- | --- | --- |
| HTTP | 80 | • Fornece acesso HTTP a partir de navegadores da Web cliente para a interface de usuário local<br>• Usado durante o processo de atualização do Cloud Volumes ONTAP |
| HTTPS | 443 | Fornece acesso HTTPS a partir de navegadores da Web cliente para a interface de usuário local e conexões a partir da instância de classificação BlueXP |
| TCP | 3128 | Fornece ao Cloud Volumes ONTAP acesso à Internet para enviar mensagens AutoSupport para o suporte da NetApp. Você deve abrir manualmente essa porta após a implantação. "Saiba como o conetor é usado como proxy para mensagens AutoSupport" |

### Regras de saída

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

#### Regras básicas de saída

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

| Protocolo | Porta | Finalidade |
| --- | --- | --- |
| Todo o TCP | Tudo | Todo o tráfego de saída |
| Todos os UDP | Tudo | Todo o tráfego de saída |

#### Regras de saída avançadas

Se você 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 conetor.

O endereço IP de origem é o host do conetor.

| Serviço | Protocolo | Porta | Destino | Finalidade |
|---|---|---|---|---|
| Chamadas de API e AutoSupport | HTTPS | 443 | LIF de gerenciamento de cluster de ONTAP e Internet de saída | Chamadas de API para Azure, ONTAP, classificação BlueXP  e envio de mensagens AutoSupport para o NetApp |
| Chamadas de API | TCP | 8080 | Classificação BlueXP | Sonda para a instância de classificação BlueXP  durante a implantação |
| DNS | UDP | 53 | DNS | Usado para resolução de DNS por BlueXP |

## Regras de firewall do conetor no Google Cloud

As regras de firewall do Google Cloud para o conetor exigem regras de entrada e saída. O BlueXP  cria automaticamente esse grupo de segurança quando você cria um conetor do BlueXP . Você precisa configurar este grupo de segurança para todas as outras opções de instalação.

### Regras de entrada

| Protocolo | Porta | Finalidade |
|---|---|---|
| SSH | 22 | Fornece acesso SSH ao host do conetor |
| HTTP | 80 | • Fornece acesso HTTP a partir de navegadores da Web cliente para a interface de usuário local<br>• Usado durante o processo de atualização do Cloud Volumes ONTAP |
| HTTPS | 443 | Fornece acesso HTTPS a partir de navegadores da Web cliente para a interface de usuário local |
| TCP | 3128 | Fornece ao Cloud Volumes ONTAP acesso à Internet para enviar mensagens AutoSupport para o suporte da NetApp. Você deve abrir manualmente essa porta após a implantação. "Saiba como o conetor é usado como proxy para mensagens AutoSupport" |

### Regras de saída

As regras de firewall predefinidas para o conetor abrem todo o tráfego de saída. Se isso for aceitável, siga as regras básicas de saída. Se você precisar de regras mais rígidas, use as regras de saída avançadas.

#### Regras básicas de saída

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

| Protocolo | Porta | Finalidade |
|---|---|---|
| Todo o TCP | Tudo | Todo o tráfego de saída |
| Todos os UDP | Tudo | Todo o tráfego de saída |

#### Regras de saída avançadas

Se você 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 conetor.

O endereço IP de origem é o host do conetor.

| Serviço | Protocolo | Porta | Destino | Finalidade |
|---|---|---|---|---|
| Chamadas de API e AutoSupport | HTTPS | 443 | LIF de gerenciamento de cluster de ONTAP e Internet de saída | Chamadas de API para Google Cloud, ONTAP, classificação BlueXP e envio de mensagens AutoSupport para o NetApp |
| Chamadas de API | TCP | 8080 | Classificação BlueXP | Sonda para a instância de classificação BlueXP durante a implantação |
| DNS | UDP | 53 | DNS | Usado para resolução de DNS por BlueXP |

## Portas para o conetor on-premise

O conetor usa portas *inbound* quando instaladas manualmente em um host Linux local. Talvez seja necessário consultar essas portas para fins de Planejamento.

Essas regras de entrada se aplicam a todos os modelos de implantação do BlueXP .

| Protocolo | Porta | Finalidade |
|---|---|---|
| HTTP | 80 | • Fornece acesso HTTP a partir de navegadores da Web cliente para a interface de usuário local<br>• Usado durante o processo de atualização do Cloud Volumes ONTAP |
| HTTPS | 443 | Fornece acesso HTTPS a partir de navegadores da Web cliente para a interface de usuário local |

# Conhecimento e apoio

## Registre-se para obter suporte

O Registro de suporte é necessário para receber suporte técnico específico da BlueXP  e de suas soluções e serviços de storage. O Registro de suporte também é necessário para habilitar fluxos de trabalho importantes para sistemas Cloud Volumes ONTAP.

O Registro para suporte não ativa o suporte do NetApp para um serviço de arquivos de provedor de nuvem. Para obter suporte técnico relacionado a um serviço de arquivo de provedor de nuvem, sua infraestrutura ou qualquer solução usando o serviço, consulte "obter ajuda" na documentação do BlueXP  para esse produto.

- "Amazon FSX para ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service para Google Cloud"

### Visão geral do Registro de suporte

Existem duas formas de Registro para ativar o direito de suporte:

- Registar o número de série da sua conta BlueXP  (o número de série 960xxxxxxxx de 20 dígitos localizado na página recursos de suporte no BlueXP ).

  Isso serve como seu ID de assinatura de suporte único para qualquer serviço no BlueXP . Cada assinatura de suporte no nível de conta do BlueXP  deve ser registrada.

- Registrando os números de série do Cloud Volumes ONTAP associados a uma assinatura no mercado do seu provedor de nuvem (estes são números de série de 20 dígitos 909201xxxxxxxx).

  Esses números de série são comumente referidos como *PAYGO serial numbers* e são gerados pelo BlueXP  no momento da implantação do Cloud Volumes ONTAP.

Registrar ambos os tipos de números de série permite recursos como abrir tickets de suporte e geração automática de casos. O Registro é concluído adicionando contas do site de suporte da NetApp (NSS) ao BlueXP , conforme descrito abaixo.

### Registre o BlueXP  para obter suporte ao NetApp

Para se Registrar para obter suporte e ativar o direito de suporte, um usuário em sua organização (ou conta) do BlueXP  deve associar uma conta do site de suporte da NetApp ao login do BlueXP . A forma como você se Registra no suporte da NetApp depende se você já tem uma conta do site de suporte da NetApp (NSS).

#### Cliente existente com uma conta NSS

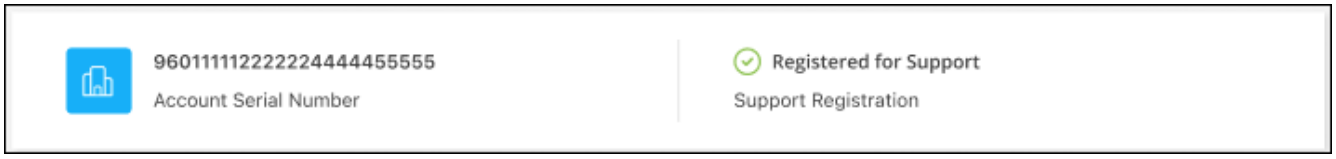
Se você é um cliente da NetApp com uma conta NSS, você simplesmente precisa se Registrar para obter suporte através do BlueXP .

**Passos**

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Selecione **credenciais do usuário**.

3. Selecione **Adicionar credenciais NSS** e siga o prompt de autenticação do site de suporte da NetApp (NSS).
4. Para confirmar que o processo de Registro foi bem-sucedido, selecione o ícone Ajuda e selecione **suporte**.

   A página **recursos** deve mostrar que sua organização do BlueXP  está registrada para suporte.




   Observe que outros usuários do BlueXP  não verão esse mesmo status de Registro de suporte se não tiverem associado uma conta do site de suporte da NetApp ao login do BlueXP . No entanto, isso não significa que sua organização do BlueXP  não esteja registrada para suporte. Desde que um usuário na organização tenha seguido esses passos, sua organização foi registrada.

### Cliente existente, mas sem conta NSS

Se você já é um cliente NetApp com licenças e números de série existentes, mas *no* conta NSS, você precisa criar uma conta NSS e associá-la ao seu login no BlueXP .

**Passos**

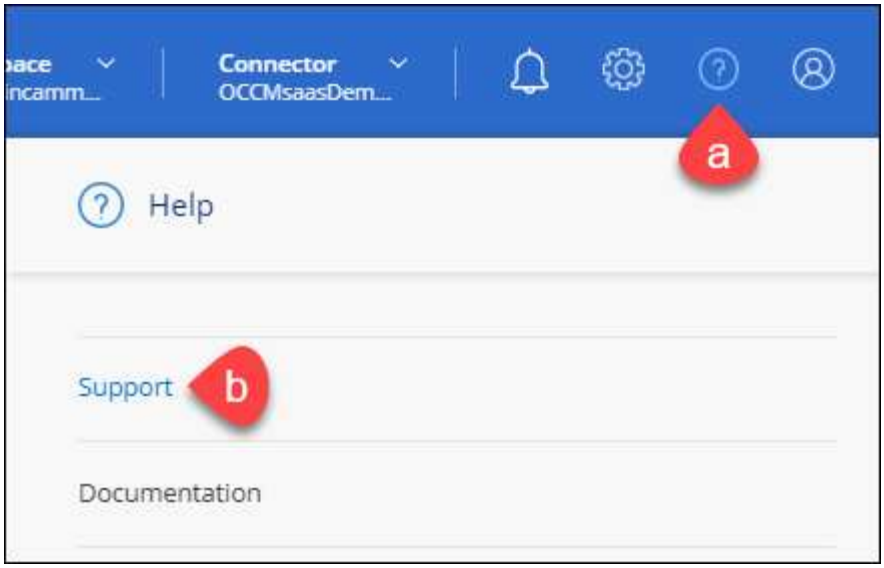
1. Crie uma conta do site de suporte da NetApp preenchendo o. "Formulário de Registro do usuário do site de suporte da NetApp"
   a. Certifique-se de selecionar o nível de usuário apropriado, que normalmente é **Cliente NetApp/Usuário final**.
   b. Certifique-se de copiar o número de série da conta BlueXP  (960xxxx) usado acima para o campo de número de série. Isto irá acelerar o processamento da conta.
2. Associe a sua nova conta NSS ao seu login no BlueXP  executando as etapas em Cliente existente com uma conta NSS.

### Novo na NetApp

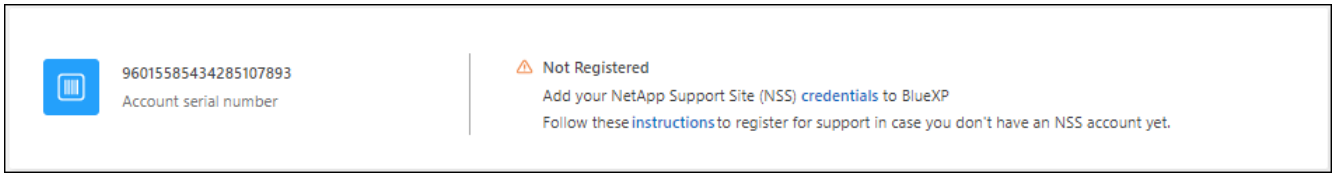
Se você é novo no NetApp e não tem uma conta NSS, siga cada passo abaixo.

**Passos**

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda e selecione **suporte**.




2. Localize o número de série da ID da conta na página Registro de suporte.




3. Navegue "Site de Registro de suporte da NetApp" e selecione **não sou um Cliente NetApp registado**.
4. Preencha os campos obrigatórios (aqueles com asteriscos vermelhos).
5. No campo **linha de produtos**, selecione **Cloud Manager** e, em seguida, selecione seu provedor de cobrança aplicável.
6. Copie o número de série da sua conta a partir da etapa 2 acima, complete a verificação de segurança e confirme se leu a Política de Privacidade de dados globais da NetApp.

   Um e-mail é enviado imediatamente para a caixa de correio fornecida para finalizar esta transação segura. Certifique-se de verificar suas pastas de spam se o e-mail de validação não chegar em poucos minutos.

7. Confirme a ação a partir do e-mail.

   A confirmação envia sua solicitação à NetApp e recomenda que você crie uma conta do site de suporte da NetApp.

8. Crie uma conta do site de suporte da NetApp preenchendo o. "Formulário de Registro do usuário do site de suporte da NetApp"
   a. Certifique-se de selecionar o nível de usuário apropriado, que normalmente é **Cliente NetApp/Usuário final**.
   b. Certifique-se de copiar o número de série da conta (960xxxx) usado acima para o campo de número de série. Isto irá acelerar o processamento.

**Depois de terminar**

O NetApp deve entrar em Contato com você durante esse processo. Este é um exercício de integração única para novos usuários.

Depois de ter sua conta do site de suporte da NetApp, associe a conta ao login do BlueXP , executando as

etapas em Cliente existente com uma conta NSS.

## Associar credenciais NSS para suporte ao Cloud Volumes ONTAP

A associação das credenciais do site de suporte da NetApp à sua organização do BlueXP  é necessária para ativar os seguintes fluxos de trabalho principais para o Cloud Volumes ONTAP:

- Registro de sistemas Cloud Volumes ONTAP de pagamento conforme o uso para suporte

  Fornecer sua conta NSS é necessário para ativar o suporte para o seu sistema e para obter acesso aos recursos de suporte técnico da NetApp.

- Implantando o Cloud Volumes ONTAP quando você traz sua própria licença (BYOL)

  É necessário fornecer a sua conta NSS para que o BlueXP  possa carregar a sua chave de licença e ativar a subscrição para o período que adquiriu. Isso inclui atualizações automáticas para renovações de prazo.

- Atualizar o software Cloud Volumes ONTAP para a versão mais recente

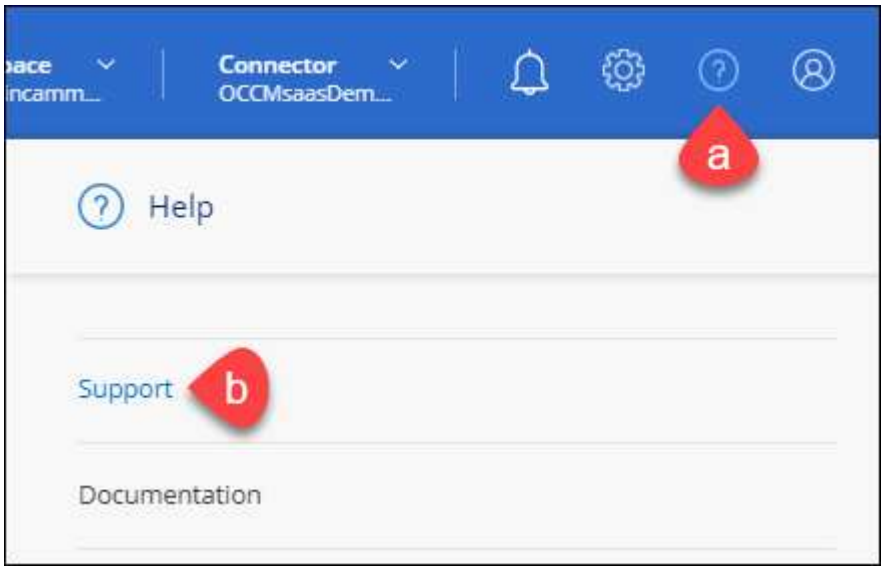
Associar credenciais NSS à sua organização do BlueXP  é diferente da conta NSS associada a um login de usuário do BlueXP .

Essas credenciais do NSS estão associadas ao ID específico da organização do BlueXP . Os utilizadores que pertencem à organização BlueXP  podem aceder a estas credenciais a partir de **suporte > Gestão NSS**.

- Se você tiver uma conta no nível do cliente, pode adicionar uma ou mais contas NSS.
- Se você tiver uma conta de parceiro ou revendedor, você pode adicionar uma ou mais contas NSS, mas elas não podem ser adicionadas ao lado de contas de nível de cliente.

**Passos**

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda e selecione **suporte**.




2. Selecione **NSS Management > Add NSS Account** (Gestão NSS > Adicionar conta NSS*).
3. Quando for solicitado, selecione **continuar** para ser redirecionado para uma página de login da Microsoft.

   O NetApp usa o Microsoft Entra ID como provedor de identidade para serviços de autenticação

específicos para suporte e licenciamento.

4. Na página de login, forneça seu endereço de e-mail e senha registrados no site de suporte da NetApp para executar o processo de autenticação.

   Essas ações permitem que o BlueXP  use sua conta NSS para tarefas como downloads de licenças, verificação de atualização de software e futuros Registros de suporte.

   Observe o seguinte:

   - A conta NSS tem de ser uma conta ao nível do cliente (não uma conta de convidado ou temporária). Você pode ter várias contas NSS no nível do cliente.
   - Só pode haver uma conta NSS se essa conta for uma conta de nível de parceiro. Se você tentar adicionar contas NSS no nível do cliente e existir uma conta no nível do parceiro, você receberá a seguinte mensagem de erro:

     "O tipo de cliente NSS não é permitido para esta conta, uma vez que já existem utilizadores NSS de tipo diferente."

   O mesmo acontece se você tiver contas NSS pré-existentes no nível do cliente e tentar adicionar uma conta no nível do parceiro.

   - Após o login bem-sucedido, o NetApp armazenará o nome de usuário do NSS.

     Este é um ID gerado pelo sistema que mapeia para o seu e-mail. Na página **NSS Management**, você pode exibir seu e-mail no ••• menu.

   - Se você precisar atualizar seus tokens de credenciais de login, há também uma opção **Atualizar credenciais** ••• no menu.

     Usando esta opção, você solicita que você faça login novamente. Observe que o token para essas contas expira após 90 dias. Uma notificação será postada para alertá-lo sobre isso.

# Obtenha ajuda

A NetApp oferece suporte ao BlueXP  e seus serviços de nuvem de várias maneiras. Amplas opções gratuitas de suporte autônomo estão disponíveis 24 horas por dia, 7 dias por semana, como artigos da base de conhecimento (KB) e um fórum da comunidade. O seu registo de suporte inclui suporte técnico remoto através de Bilheteira na Web.

## Obtenha suporte para um serviço de arquivos do provedor de nuvem

Para obter suporte técnico relacionado a um serviço de arquivo de provedor de nuvem, sua infraestrutura ou qualquer solução usando o serviço, consulte "obter ajuda" na documentação do BlueXP  para esse produto.

- "Amazon FSX para ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service para Google Cloud"

Para receber suporte técnico específico da BlueXP  e de suas soluções e serviços de storage, use as opções de suporte descritas abaixo.

## Use opções de suporte autônomo

Estas opções estão disponíveis gratuitamente, 24 horas por dia, 7 dias por semana:

- Documentação

  A documentação do BlueXP que você está visualizando no momento.

- "Base de conhecimento"

  PESQUISE na base de conhecimento do BlueXP para encontrar artigos úteis para solucionar problemas.

- "Comunidades"

  Junte-se à comunidade BlueXP para seguir as discussões em curso ou criar novas.

## Crie um caso com o suporte do NetApp

Além das opções de suporte autônomo acima, você pode trabalhar com um especialista de suporte da NetApp para resolver quaisquer problemas depois de ativar o suporte.

**Antes de começar**

- Para usar o recurso **criar um caso**, primeiro você deve associar suas credenciais do site de suporte da NetApp ao login do BlueXP . "Saiba como gerenciar credenciais associadas ao seu login no BlueXP".
- Se você estiver abrindo um caso para um sistema ONTAP com um número de série, sua conta NSS deve estar associada ao número de série desse sistema.

**Passos**

1. No BlueXP , selecione **Ajuda > suporte**.
2. Na página **recursos**, escolha uma das opções disponíveis em suporte técnico:

   a. Selecione **Ligue para nós** se quiser falar com alguém no telefone. Você será direcionado para uma página no NetApp.com que lista os números de telefone que você pode ligar.

   b. Selecione **criar um caso** para abrir um ticket com um especialista em suporte da NetApp:

      - **Serviço**: Selecione o serviço ao qual o problema está associado. Por exemplo, BlueXP quando específico para um problema de suporte técnico com fluxos de trabalho ou funcionalidade dentro do serviço.
      - **Ambiente de trabalho**: Se aplicável ao armazenamento, selecione **Cloud Volumes ONTAP** ou **no local** e, em seguida, o ambiente de trabalho associado.

        A lista de ambientes de trabalho está dentro do escopo da organização (ou conta) do BlueXP , do projeto (ou da área de trabalho) e do conetor que você selecionou no banner superior do serviço.

      - **Prioridade do caso**: Escolha a prioridade para o caso, que pode ser baixa, média, alta ou Crítica.

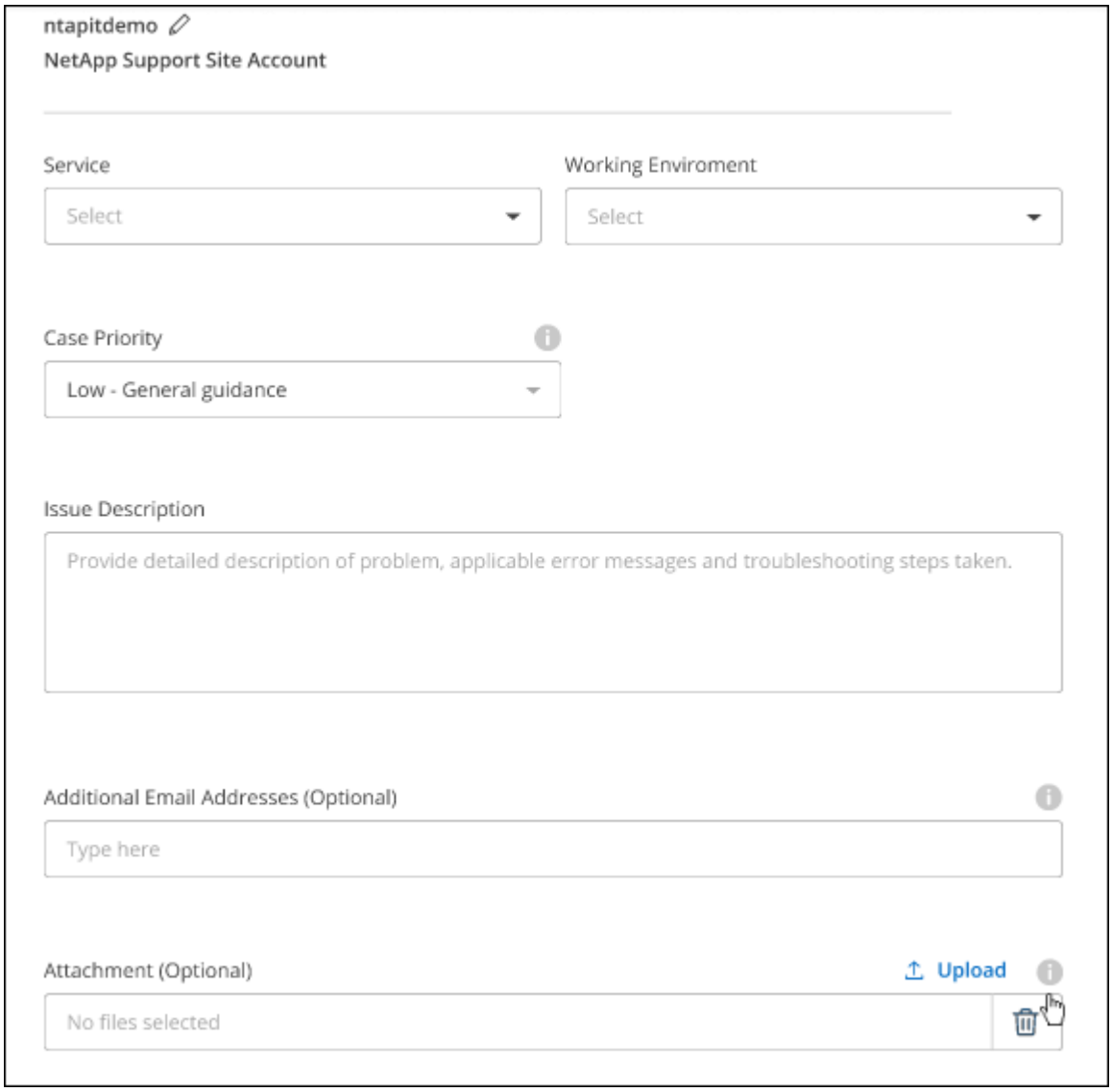
        Para saber mais detalhes sobre essas prioridades, passe o Mouse sobre o ícone de informações ao lado do nome do campo.

      - **Descrição do problema**: Forneça uma descrição detalhada do seu problema, incluindo quaisquer mensagens de erro aplicáveis ou etapas de solução de problemas que você executou.
      - **Endereços de e-mail adicionais**: Insira endereços de e-mail adicionais se você quiser que outra

pessoa saiba sobre esse problema.

- **Anexo (Opcional)**: Carregue até cinco anexos, um de cada vez.

  Os anexos estão limitados a 25 MB por ficheiro. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.




**Depois de terminar**

Um pop-up aparecerá com o número do seu caso de suporte. Um especialista em suporte da NetApp irá rever o seu caso e voltar para você em breve.

Para obter um histórico de seus casos de suporte, você pode selecionar **Configurações > linha do tempo** e procurar ações chamadas "criar caso de suporte". Um botão à direita permite expandir a ação para ver detalhes.

É possível que você encontre a seguinte mensagem de erro ao tentar criar um caso:

"Você não está autorizado a criar um caso contra o serviço selecionado"

Esse erro pode significar que a conta NSS e a empresa de Registro com a qual está associada não são a mesma empresa de Registro para o número de série da conta BlueXP  (ou seja. 960xxxx) ou o número de

série do ambiente de trabalho. Pode procurar assistência utilizando uma das seguintes opções:

- Use o chat no produto
- Envie um caso não técnico em https://mysupport.netapp.com/site/help

## Gerenciar seus casos de suporte (prévia)

Você pode visualizar e gerenciar casos de suporte ativos e resolvidos diretamente do BlueXP . Você pode gerenciar os casos associados à sua conta NSS e à sua empresa.

O gerenciamento de casos está disponível como uma prévia. Planejamos refinar essa experiência e adicionar melhorias nos próximos lançamentos. Por favor, envie-nos feedback usando o chat no produto.

Observe o seguinte:

- O painel de gerenciamento de casos na parte superior da página oferece duas visualizações:
  - A vista à esquerda mostra o total de casos abertos nos últimos 3 meses pela conta do usuário NSS que você forneceu.
  - A visualização à direita mostra o total de casos abertos nos últimos 3 meses ao nível da sua empresa com base na sua conta NSS de utilizador.

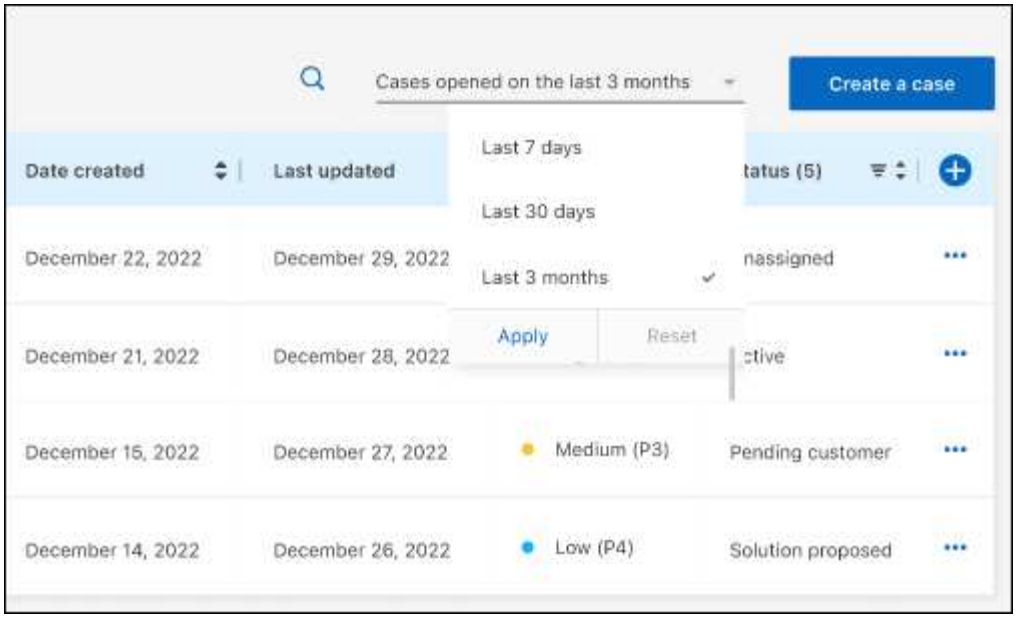
  Os resultados na tabela refletem os casos relacionados à exibição selecionada.
- Você pode adicionar ou remover colunas de interesse e pode filtrar o conteúdo de colunas como prioridade e Status. Outras colunas fornecem apenas capacidades de ordenação.

  Veja os passos abaixo para obter mais detalhes.
- Em um nível por caso, oferecemos a capacidade de atualizar notas de caso ou fechar um caso que ainda não esteja no status fechado ou pendente fechado.

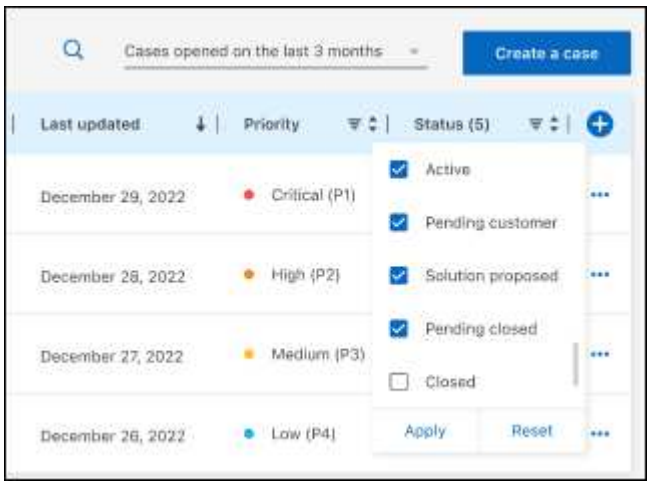
**Passos**

1. No BlueXP , selecione **Ajuda > suporte**.
2. Selecione **Gerenciamento de casos** e, se for solicitado, adicione sua conta NSS ao BlueXP .

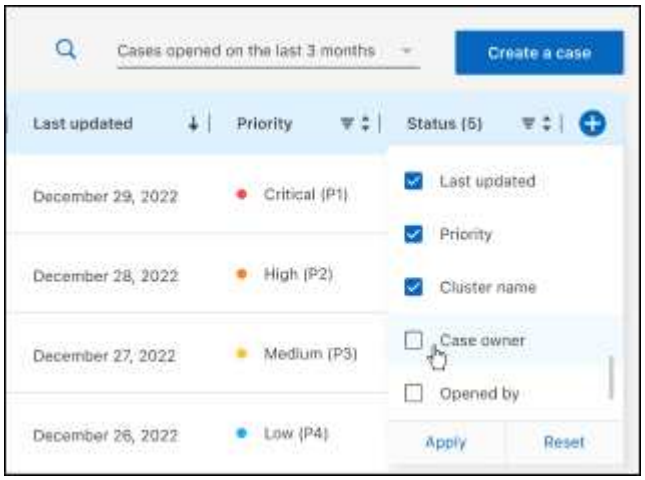
   A página **Gerenciamento de casos** mostra casos abertos relacionados à conta NSS associada à conta de usuário do BlueXP . Esta é a mesma conta NSS que aparece na parte superior da página **NSS Management**.
3. Opcionalmente, modifique as informações exibidas na tabela:
   - Em **casos da organização**, selecione **Exibir** para ver todos os casos associados à sua empresa.
   - Modifique o intervalo de datas escolhendo um intervalo de datas exato ou escolhendo um intervalo de tempo diferente.




- Filtre o conteúdo das colunas.




- Altere as colunas que aparecem na tabela selecionando e escolhendo as colunas que você deseja exibir.

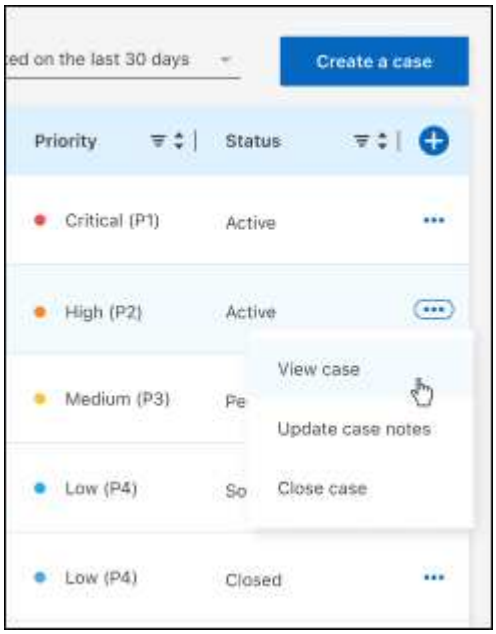


4. Gerencie um caso existente •••selecionando e selecionando uma das opções disponíveis:

   - **Ver caso**: Veja detalhes completos sobre um caso específico.
   - * Atualizar notas de caso*: Forneça detalhes adicionais sobre o seu problema ou selecione **carregar arquivos** para anexar até um máximo de cinco arquivos.

     Os anexos estão limitados a 25 MB por ficheiro. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.

   - * Fechar caso*: Forneça detalhes sobre por que você está fechando o caso e selecione **Fechar caso**.



# Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

## Direitos de autor

"https://www.netapp.com/company/legal/copyright/"

## Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respetivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

## Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

## Política de privacidade

"https://www.netapp.com/company/legal/privacy-policy/"

## Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais de terceiros e licenças usadas no software NetApp.

"Aviso para BlueXP"

## Informações sobre direitos autorais



## Informações sobre marcas comerciais