Começar

NetApp Console setup and administration

NetApp
January 27, 2026

Índice

Começar

Aprenda o básico

Saiba mais sobre o NetApp Console

O Console unifica o gerenciamento e a proteção de armazenamento em multinuvem híbrida com serviços de dados integrados para proteger e otimizar dados.

Está disponível como uma plataforma de serviço (SaaS) ou como uma opção auto-hospedada que você pode instalar em sua nuvem soberana. Oferece gerenciamento de armazenamento, mobilidade de dados, proteção de dados, análise e controle de dados. As funcionalidades de gestão são disponibilizadas através de uma consola baseada na Web e de APIs.

Gerenciamento de armazenamento centralizado

Descubra, implante e gerencie o armazenamento na nuvem e no local com o Console.

Armazenamento em nuvem e local com suporte

Você pode gerenciar os seguintes tipos de armazenamento no Console:

Soluções de armazenamento em nuvem

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Google Cloud NetApp Volumes

Armazenamento flash e de objetos no local

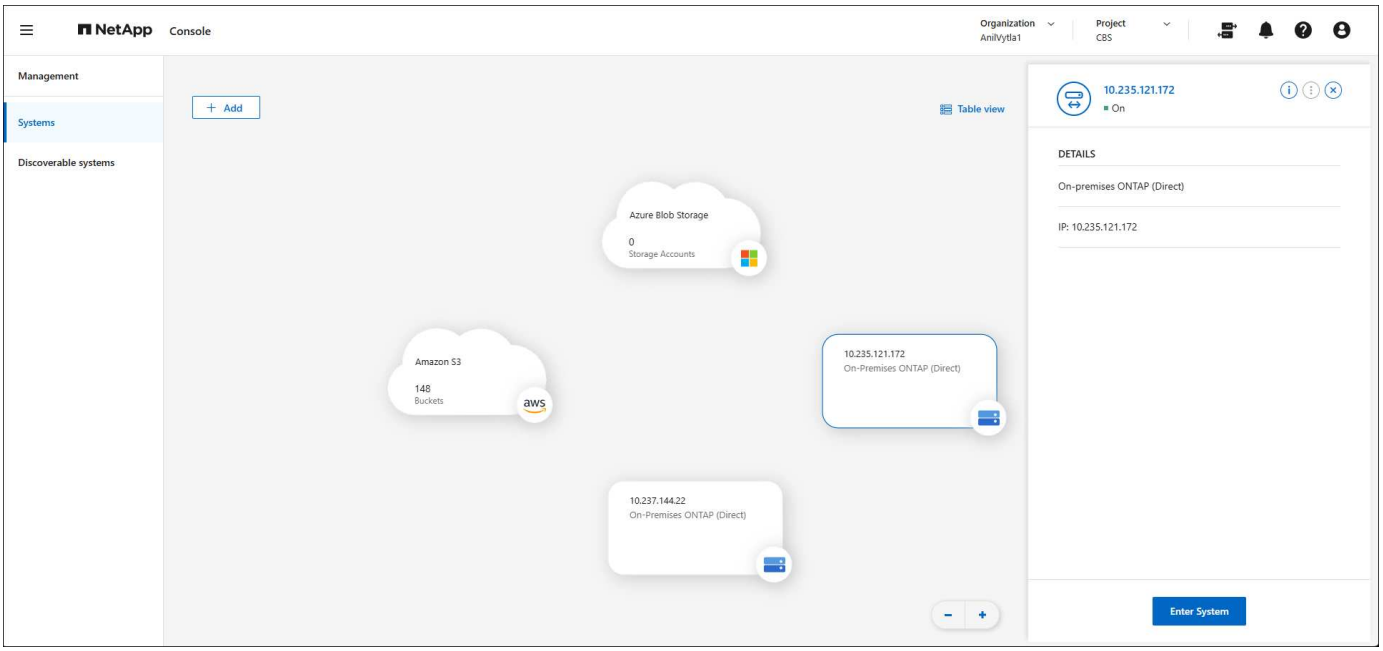
- Sistemas da série E
- Clusters ONTAP
- Sistemas StorageGRID

Armazenamento de objetos em nuvem

- Armazenamento Amazon S3
- Armazenamento de Blobs do Azure
- Armazenamento em nuvem do Google

Gerenciamento de armazenamento

No Console, *sistemas* representam armazenamento descoberto ou implantado. Você pode selecionar um *sistema* para integrá-lo aos serviços de dados da NetApp ou gerenciar o armazenamento, como adicionar volumes.



Serviços de dados integrados e gerenciamento de armazenamento para proteger, proteger e otimizar dados

O Console fornece serviços de dados para proteger e manter a disponibilidade do armazenamento.

Alertas de armazenamento

Visualize problemas relacionados à capacidade, disponibilidade, desempenho, proteção e segurança no seu ambiente ONTAP .

Centro de automação

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

NetApp Backup and Recovery

Faça backup e restaure dados na nuvem e no local.

NetApp Data Classification

Prepare a privacidade dos dados do seu aplicativo e dos ambientes de nuvem.

NetApp Copy and Sync

Sincronize dados entre armazenamentos de dados locais e na nuvem.

Consultor digital da NetApp (Active IQ)

Use análise preditiva e suporte proativo para otimizar sua infraestrutura de dados.

Licenses and subscriptions

Gerencie e monitore suas licenças e assinaturas.

NetApp Disaster Recovery

Proteja cargas de trabalho VMware locais usando o VMware Cloud no Amazon FSx para ONTAP como um site de recuperação de desastres.

Planejamento do ciclo de vida

Identifique clusters com baixa capacidade atual ou prevista e implemente recomendações de

hierarquização de dados ou capacidade adicional.

NetApp Ransomware Resilience
Detecte anomalias que podem resultar em ataques de ransomware. Proteja e recupere cargas de trabalho.

NetApp Replication
Replique dados entre sistemas de armazenamento para dar suporte a backup e recuperação de desastres.

Atualizações de software
Automatize a avaliação, o planejamento e a execução de atualizações do ONTAP .

Painel de sustentabilidade
Analise a sustentabilidade dos seus sistemas de armazenamento.

NetApp Cloud Tiering
Amplie seu armazenamento ONTAP local para a nuvem.

NetApp Volume Caching
Crie um volume de cache gravável para acelerar o acesso aos dados ou descarregar o tráfego de volumes muito acessados.

Cargas de trabalho da NetApp
Projete, configure e opere cargas de trabalho principais usando o Amazon FSx for NetApp ONTAP.

"Saiba mais sobre o NetApp Console e os serviços de dados disponíveis"

Provedores de nuvem suportados

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

Custo

Não há custo para o NetApp Console. Você incorrerá em custos se implantar agentes do Console na nuvem ou usar o modo Restrito implantado na nuvem. Há custos associados a alguns serviços de dados da NetApp .https://bluexp.netapp.com/pricing["Saiba mais sobre os preços dos serviços de dados da NetApp"^]

Como funciona o NetApp Console

O NetApp Console é um console baseado na Web fornecido por meio da camada SaaS, um sistema de gerenciamento de recursos e acesso, agentes de console que gerenciam sistemas de armazenamento e habilitam serviços de dados NetApp e diferentes modos de implantação para atender aos seus requisitos de negócios.

Software como serviço

Você acessa o Console através de um "interface baseada na web" e APIs. Essa experiência SaaS permite que você acesse automaticamente os recursos mais recentes assim que são lançados.

Gerenciamento de identidade e acesso (IAM)

O Console fornece gerenciamento de identidade e acesso (IAM) para gerenciamento de recursos e acesso. Este modelo de IAM fornece gerenciamento granular de recursos e permissões:

- Uma *organização* de nível superior permite que você gerencie o acesso em seus vários *projetos*
- *Pastas* permitem que você agrupe projetos relacionados
- O gerenciamento de recursos permite que você associe 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
- "Saiba mais sobre o IAM no NetApp Console"

Agentes de console

Um agente de console é necessário para alguns recursos adicionais e serviços de dados. Ele permite que você gerencie recursos e processos em seus ambientes locais e na nuvem. Você precisa dele para gerenciar alguns sistemas (por exemplo, Cloud Volumes ONTAP) e usar alguns serviços de dados da NetApp .

"Saiba mais sobre os agentes do Console" .

Implantação de SaaS versus nuvem soberana

Você pode começar a usar o NetApp Console inscrevendo-se na oferta SaaS ou implantando-o em sua nuvem soberana. Ao implementar o NetApp Console em uma nuvem soberana, a NetApp limita a conectividade de saída para atender aos requisitos de segurança e conformidade da sua organização. Nem todos os recursos e serviços estão disponíveis quando o Console é implantado em uma nuvem soberana.

A NetApp continua a oferecer o BlueXP para sites que não desejam conectividade de saída. O BlueXP pode ser instalado em sua rede sem necessidade de conectividade de saída. "Saiba mais sobre o BlueXP (modo privado) para sites sem conectividade com a internet."

"Saiba mais sobre os modos de implantação" .

Certificação SOC 2 Tipo 2

Uma empresa de contabilidade pública certificada independente e auditora de serviços examinou o Console e afirmou que ele obteve relatórios SOC 2 Tipo 2 com base nos critérios aplicáveis dos Serviços de Confiança.

"Ver relatórios SOC 2 da NetApp"

Saiba mais sobre os modos de implantação do NetApp Console

O NetApp Console oferece vários *modos de implantação* que permitem que você atenda aos seus requisitos comerciais e de segurança.

- O *modo padrão* utiliza uma camada de software como serviço (SaaS) para fornecer funcionalidade completa. Os usuários acessam o Console por meio de uma interface hospedada na web
- O *Modo restrito* está disponível para organizações com restrições de conectividade que desejam instalar o NetApp Console em sua própria nuvem pública. Os usuários acessam o Console por meio de uma interface baseada na Web hospedada em um agente do Console em seu ambiente de nuvem.

  O NetApp Console restringe o tráfego, a comunicação e os dados no modo restrito, e você deve garantir que seu ambiente (local e na nuvem) esteja em conformidade com as regulamentações necessárias.

Visão geral

Cada modo de implantação difere em conectividade de saída, localização, instalação, autenticação, serviços de dados e métodos de cobrança.

Modo padrão

Você usa um serviço SaaS do console baseado na web. Dependendo dos serviços e recursos de dados que você planeja usar, um administrador da organização do Console cria um ou mais agentes do Console para gerenciar dados no seu ambiente de nuvem híbrida.

Este modo usa transmissão de dados criptografados pela internet pública.

Modo restrito

Você instala um agente do Console na nuvem (em uma região governamental, soberana ou comercial) e ele tem conectividade de saída limitada à camada SaaS do NetApp Console .

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

Saiba mais sobre conectividade de saída para a camada SaaS .

Modo privado BlueXP (somente interface BlueXP legada)

O modo privado BlueXP (interface BlueXP legada) normalmente é usado com ambientes locais que não têm conexão com a Internet e com regiões de nuvem seguras, o que inclui AWS Secret Cloud, AWS Top Secret Cloud e Azure IL6. A NetApp continua a oferecer suporte a esses ambientes com a interface legada BlueXP ."Documentação em PDF para o modo privado do BlueXP"

A tabela a seguir fornece uma comparação do console NetApp .

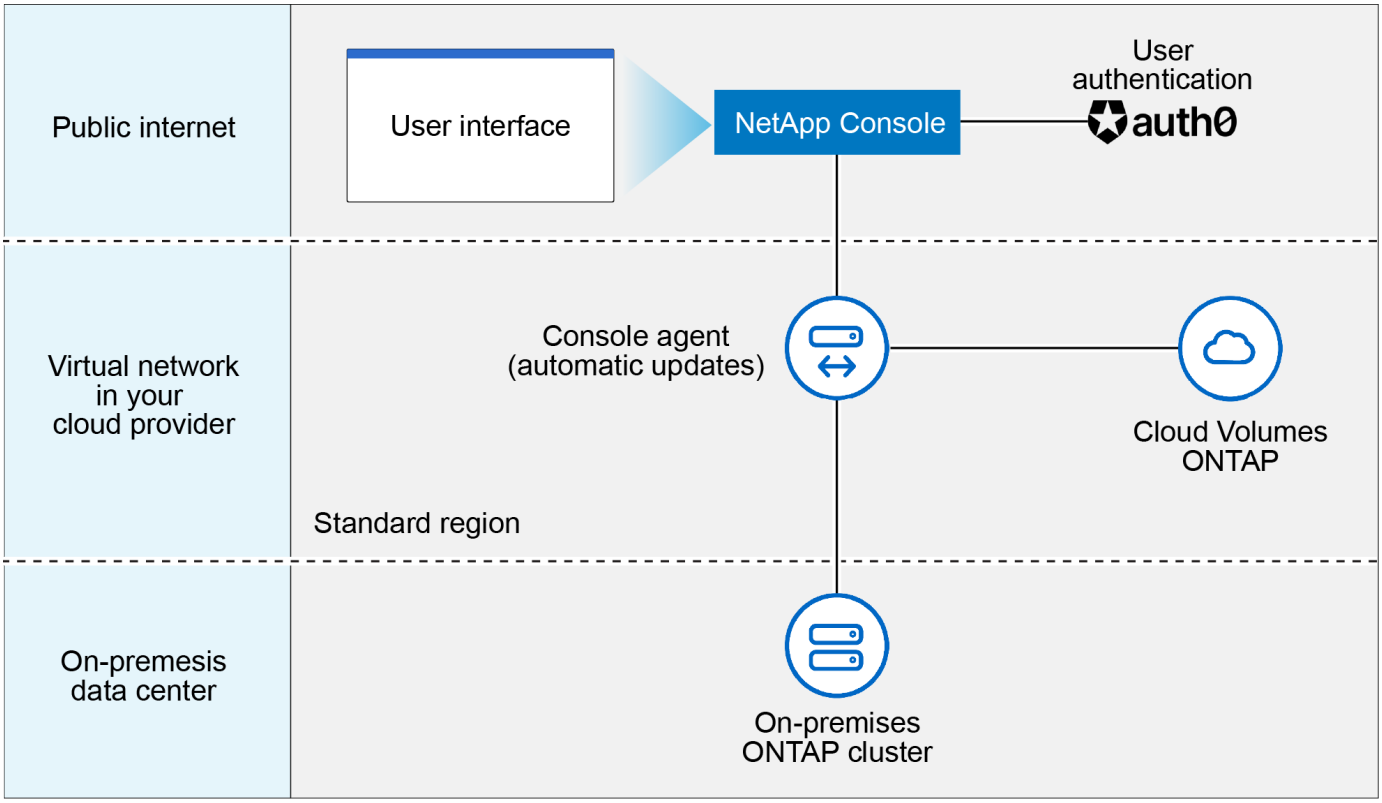
	Modo padrão	Modo restrito
Conexão necessária à camada SaaS do NetApp Console ?	Sim	Somente saída
É necessária conexão com seu provedor de nuvem?	Sim	Sim, dentro da região
Instalação do agente de console	Do Console, do marketplace na nuvem ou da instalação manual	Marketplace em nuvem ou instalação manual
Atualizações do agente do console	Atualizações automáticas	Atualizações automáticas
Acesso UI	Da camada SaaS do Console	Localmente de uma VM de agente
Ponto de extremidade da API	A camada SaaS do Console	Um agente de console
Autenticação	Por meio de SaaS usando auth0, login NSS ou federação de identidade	Por meio de SaaS usando auth0 ou federação de identidade
Autenticação multifator	Disponível para usuários locais	Não disponível
Serviços de armazenamento e dados	Todos são suportados	Muitos são suportados

	Modo padrão	Modo restrito
Opções de licenciamento de serviços de dados	Assinaturas de mercado e BYOL	Assinaturas de mercado e BYOL

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

Modo padrão

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



O Console funciona da seguinte maneira no modo padrão:

Comunicação de saída

É necessária conectividade de um agente do Console com a camada SaaS do Console, com os recursos disponíveis publicamente do seu provedor de nuvem e com outros componentes essenciais para as operações do dia a dia.

- "Endpoints que um agente contata na AWS"
- "Pontos de extremidade que um agente contata no Azure"
- "Pontos de extremidade que um agente contata no Google Cloud"

Localização com suporte para um agente

No modo padrão, um agente é suportado na nuvem ou em suas instalações.

Instalação do agente de console

Você pode instalar um agente usando um dos seguintes métodos:

- Do Console
- Do AWS ou Azure Marketplace
- Do Google Cloud SDK
- Usando manualmente um instalador em um host Linux em seu data center ou nuvem
- Use o OVA fornecido no seu ambiente VCenter.

Atualizações do agente do console

A NetApp atualiza automaticamente seu agente mensalmente.

Acesso à interface do usuário

A interface do usuário pode ser acessada pelo console baseado na web fornecido pela camada SaaS.

Ponto de extremidade da API

As chamadas de API são feitas para o seguinte endpoint: \ https://api.bluexp.netapp.com

Autenticação

Autenticação com logins auth0 ou NetApp Support Site (NSS). A federação de identidade está disponível.

Serviços de dados suportados

Todos os serviços de dados da NetApp são suportados. "Saiba mais sobre os serviços de dados da NetApp" .

Opções de licenciamento suportadas

Assinaturas do Marketplace e BYOL são suportadas no modo padrão; no entanto, as opções de licenciamento suportadas dependem do serviço de dados NetApp que você está usando. Revise a documentação de cada serviço para saber mais sobre as opções de licenciamento disponíveis.

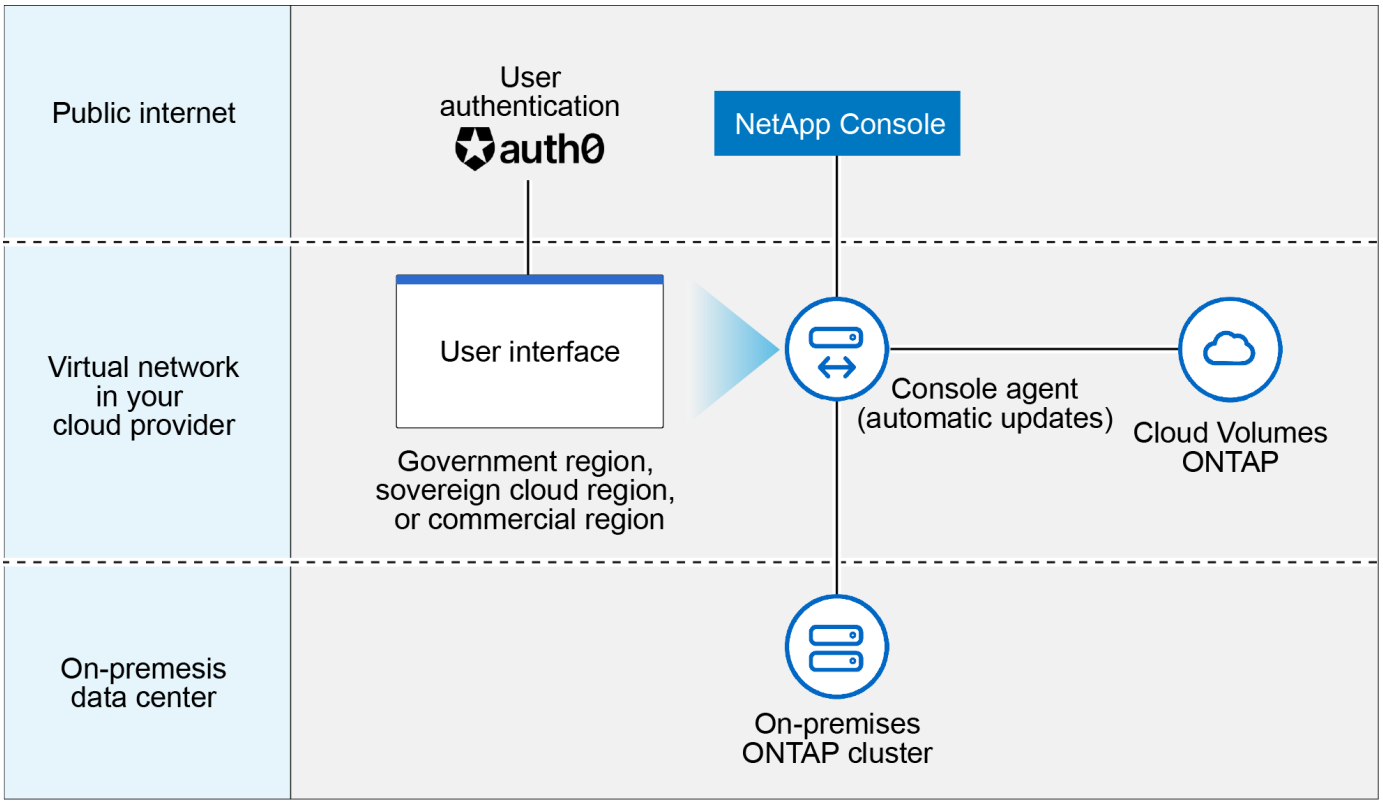
Como começar com o modo padrão

Vá para o "NetApp Console" e inscreva-se.

"Aprenda como começar com o modo padrão" .

Modo restrito

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



O Console funciona da seguinte maneira no modo restrito:

Comunicação de saída

Um agente requer conectividade de saída com a camada SaaS do Console para serviços de dados, atualizações de software, autenticação e transmissão de metadados.

A camada SaaS do Console não inicia a comunicação com um agente. Os agentes iniciam toda a comunicação com a camada SaaS do Console, extraindo ou enviando dados conforme necessário.

Também é necessária uma conexão com recursos do provedor de nuvem dentro da região.

Localização com suporte para um agente

No modo restrito, um agente é suportado na nuvem: em uma região governamental, região soberana ou região comercial.

Instalação do agente de console

Você pode instalar pelo AWS ou Azure Marketplace ou fazer uma instalação manual no seu próprio host Linux ou usar um OVA para download no seu ambiente VCenter.

Atualizações do agente do console

A NetApp atualiza automaticamente o software do seu agente com atualizações mensais.

Acesso à interface do usuário

A interface do usuário pode ser acessada a partir de uma máquina virtual de agente implantada na sua região de nuvem.

Ponto de extremidade da API

Chamadas de API são feitas para a máquina virtual do agente.

Autenticação

A autenticação é fornecida através de auth0. A federação de identidade também está disponível.

Gerenciamento de armazenamento e serviços de dados suportados

Os seguintes serviços de armazenamento e dados com modo restrito:

Serviços suportados	Notas
Azure NetApp Files	Suporte total
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 NetApp Backup and Recovery oferece suporte somente para backup e restauração de dados de volume ONTAP . "Veja a lista de destinos de backup suportados para dados ONTAP" O backup e a restauração de dados de aplicativos e dados de máquinas virtuais não são suportados.
NetApp Data Classification	Suportado em regiões governamentais com modo restrito. Não suportado em regiões comerciais ou em regiões soberanas com modo restrito.
Cloud Volumes ONTAP	Suporte total
Licenses and subscriptions	Você pode acessar informações de licença e assinatura com as opções de licenciamento suportadas listadas abaixo para o modo restrito.
Clusters ONTAP locais	A descoberta com um agente do Console e a descoberta sem um agente do Console (descoberta direta) são suportadas. Quando você descobre um cluster local sem um agente de console, a exibição Avançada (Gerenciador do Sistema) 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 Marketplace (contratos por hora e anuais)

  Observe o seguinte:

  - Para o Cloud Volumes ONTAP, somente o licenciamento baseado em capacidade é suportado.
  - No Azure, contratos anuais não são suportados com regiões governamentais.
- Traga sua própria bebida

  Para o Cloud Volumes ONTAP, tanto o licenciamento baseado em capacidade quanto o licenciamento baseado em nó são suportados com BYOL.

Como começar com o modo restrito

Você precisa habilitar o modo restrito ao criar sua organização do NetApp Console .

Se você ainda não tiver uma organização, será solicitado a criá-la e habilitar o modo restrito ao efetuar login no Console pela primeira vez a partir de um agente do Console instalado manualmente ou criado no marketplace do seu provedor de nuvem.

Não é possível alterar a configuração do modo restrito após criar a organização.

"Aprenda como começar com o modo restrito" .

Comparação de serviços e recursos

A tabela a seguir pode ajudar você a identificar rapidamente quais serviços e recursos são suportados no modo restrito.

Observe que alguns serviços podem ter suporte com limitações. Para mais detalhes sobre como esses serviços são suportados com o modo restrito, consulte as seções acima.

Área de produtos	Serviço ou recurso de dados NetApp	Modo restrito
Armazenamento Esta parte da tabela lista o suporte para gerenciamento de sistemas de armazenamento do Console. Não indica os destinos de backup suportados pelo NetApp Backup and Recovery.	Amazon FSx para ONTAP	Não
	Amazon S3	Não
	Blob do Azure	Não
	Azure NetApp Files	Sim
	Cloud Volumes ONTAP	Sim
	Google Cloud NetApp Volumes	Não
	Armazenamento em nuvem do Google	Não
	Clusters ONTAP locais	Sim
	Série E	Não
	StorageGRID	Não

Área de produtos	Serviço ou recurso de dados NetApp	Modo restrito
Serviços de Dados	Backup e recuperação da NetApp	Simhttps://docs.netapp.com/us-en/data-services-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-limited-internet-connectivity["Veja a lista de destinos de backup suportados para dados de volume ONTAP"^]
	NetApp Data Classification	Sim
	NetApp Copy and Sync	Não
	NetApp Disaster Recovery	Não
	NetApp Ransomware Resilience	Não
	NetApp Replication	Sim
	NetApp Cloud Tiering	Não
	Cache de volume do NetApp	Não
	Fábrica de carga de trabalho da NetApp	Não
Características	Alertas	Não
	Digital Advisor	Não
	Gerenciamento de licenças e assinaturas	Sim
	Gerenciamento de identidade e acesso	Sim
	Credenciais	Sim
	Federação	Sim
	Planejamento do ciclo de vida	Não
	Autenticação multifator	Sim
	Contas NSS	Sim
	Notificações	Sim
	Procurar	Sim
	Atualizações de software	Não
	Sustentabilidade	Não
	Auditoria	Sim

Gerenciar credenciais NSS associadas ao NetApp Console

Associe uma conta do NetApp Support Site à sua organização do Console para habilitar fluxos de trabalho importantes para gerenciamento de armazenamento. Essas credenciais do NSS estão associadas a toda a organização.

O Console também suporta a associação de uma conta NSS por conta de usuário. "Aprenda a gerenciar

credenciais em nível de usuário" .

Visão geral

É necessário associar as credenciais do site de suporte da NetApp ao número de série específico da sua conta do Console para habilitar as seguintes tarefas:

- Implantando o Cloud Volumes ONTAP quando você traz sua própria licença (BYOL)

  É necessário fornecer sua conta NSS para que o Console possa carregar sua chave de licença e habilitar a assinatura para o período que você comprou. Isso inclui atualizações automáticas para renovações de prazo.

- Registrando sistemas Cloud Volumes ONTAP de pagamento conforme o uso

  É necessário fornecer sua conta NSS para ativar o suporte para seu sistema e obter acesso aos recursos de suporte técnico da NetApp .

- Atualizando o software Cloud Volumes ONTAP para a versão mais recente

Essas credenciais estão associadas ao número de série específico da sua conta do Console. Os usuários podem acessar essas credenciais em **Suporte > Gerenciamento NSS**.

Adicionar uma conta NSS

Você pode adicionar e gerenciar suas contas do Site de Suporte NetApp para uso com o Console no Painel de Suporte do Console.

Depois de adicionar sua conta NSS, o Console usa essas informações para coisas como downloads de licenças, verificação de atualização de software e registros de suporte futuros.

Você pode associar várias contas NSS à sua organização; no entanto, não é possível ter contas de clientes e contas de parceiros na mesma organização.

A NetApp usa o Microsoft Entra ID como provedor de identidade para serviços de autenticação específicos para suporte e licenciamento.

Passos

1. Em **Administração > Suporte**.
2. Selecione **Gerenciamento NSS**.
3. Selecione **Adicionar conta NSS**.
4. Selecione **Continuar** para ser redirecionado para uma página de login da Microsoft.
5. Na página de login, forneça seu endereço de e-mail e senha registrados no Site de Suporte da NetApp .

   Após o login bem-sucedido, o NetApp armazenará o nome de usuário do NSS.

   Este é um ID gerado pelo sistema que mapeia para seu e-mail. Na página **NSS Management**, você pode exibir seu e-mail do ••• menu.

   - Se você precisar atualizar seus tokens de credenciais de login, também há uma opção **Atualizar credenciais** no ••• menu.

     Usar esta opção solicitará que você faça login novamente. Observe que o token para essas contas

expira após 90 dias. Uma notificação será publicada para alertá-lo sobre isso.

O que vem a seguir?

Os usuários agora podem selecionar a conta ao criar novos sistemas Cloud Volumes ONTAP e ao registrar sistemas Cloud Volumes ONTAP existentes.

- "Lançamento do Cloud Volumes ONTAP na AWS"
- "Iniciando o Cloud Volumes ONTAP no Azure"
- "Lançamento do Cloud Volumes ONTAP no Google Cloud"
- "Registrando sistemas de pagamento conforme o uso"

Atualizar credenciais NSS

Por motivos de segurança, você deve atualizar suas credenciais do NSS a cada 90 dias. Você será notificado no centro de notificações do Console se sua credencial NSS tiver expirado. "Saiba mais sobre o Centro de Notificações" .

Credenciais expiradas podem interromper o seguinte, mas não estão limitadas a:

- Atualizações de licença, o que significa que você não poderá aproveitar a capacidade recém-adquirida.
- Capacidade de enviar e rastrear casos de suporte.

Além disso, você pode atualizar as credenciais do NSS associadas à sua organização se quiser alterar a conta do NSS associada à sua organização. Por exemplo, se a pessoa associada à sua conta NSS saiu da sua empresa.

Passos

1. Em **Administração > Suporte**.
2. Selecione **Gerenciamento NSS**.
3. Para a conta NSS que você deseja atualizar, selecione ••• e então selecione **Atualizar credenciais**.
4. Quando solicitado, selecione **Continuar** para ser redirecionado para uma página de login da Microsoft.

   A NetApp usa o Microsoft Entra ID como provedor de identidade para serviços de autenticação relacionados a suporte e licenciamento.

5. Na página de login, forneça seu endereço de e-mail e senha registrados no Site de Suporte da NetApp .

Anexar um sistema a uma conta NSS diferente

Se sua organização tiver várias contas do NetApp Support Site, você poderá alterar qual conta está associada a um sistema Cloud Volumes ONTAP .

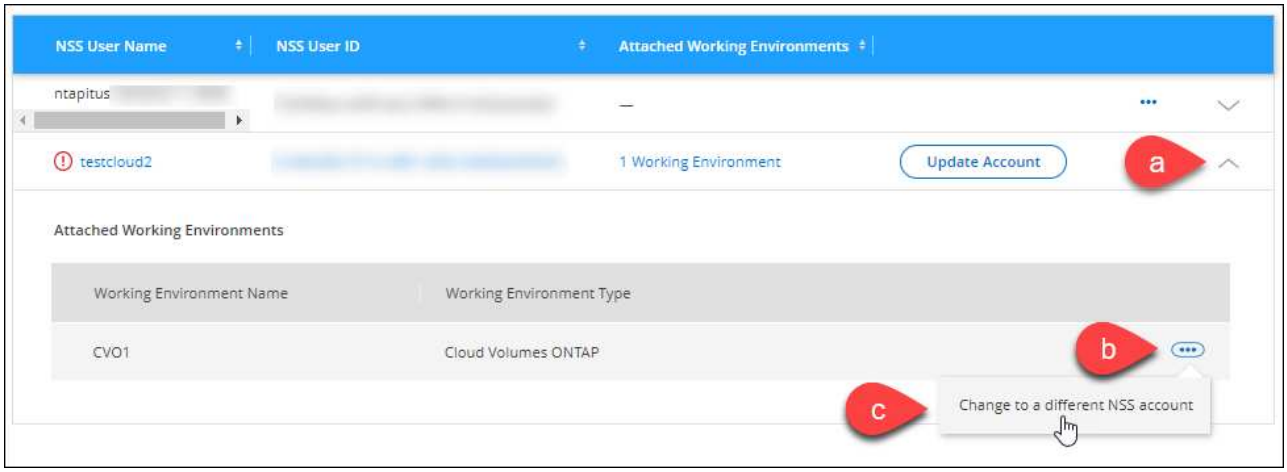
Primeiro você deve associar a conta ao Console.

Passos

1. Em **Administração > Suporte**.
2. Selecione **Gerenciamento NSS**.
3. Conclua as seguintes etapas para alterar a conta NSS:
   a. Expanda a linha da conta do site de suporte da NetApp à qual o sistema está atualmente associado.

b. Para o sistema cuja associação você deseja alterar, selecione •••

c. Selecione **Alterar para uma conta NSS diferente**.



d. Selecione a conta e depois selecione **Salvar**.

Exibir o endereço de e-mail de uma conta NSS

Por segurança, o endereço de e-mail associado a uma conta NSS não é exibido por padrão. Você pode visualizar o endereço de e-mail e o nome de usuário associado a uma conta NSS.

Quando você acessa a página Gerenciamento do NSS, o Console gera um token para cada conta na tabela. Esse token inclui informações sobre o endereço de e-mail associado. O token é removido quando você sai da página. As informações nunca são armazenadas em cache, o que ajuda a proteger sua privacidade.

Passos

1. Em **Administração > Suporte**.
2. Selecione **Gerenciamento NSS**.
3. Para a conta NSS que você deseja atualizar, selecione ••• e então selecione **Exibir endereço de e-mail**. Você pode usar o botão copiar para copiar o endereço de e-mail.

Remover uma conta NSS

Exclua todas as contas NSS que você não deseja mais usar com o Console.

Não é possível excluir uma conta que esteja atualmente associada a um sistema Cloud Volumes ONTAP . Primeiro você precisaanexar esses sistemas a uma conta NSS diferente .

Passos

1. Em **Administração > Suporte**.
2. Selecione **Gerenciamento NSS**.
3. Para a conta NSS que você deseja excluir, selecione ••• e então selecione **Excluir**.
4. Selecione **Excluir** para confirmar.

Saiba mais sobre os agentes do NetApp Console

Você usa um agente do Console para conectar o NetApp Console à sua infraestrutura e orquestrar com segurança soluções de armazenamento em ambientes AWS, Azure, Google Cloud ou locais, além de usar serviços de proteção de dados.

Um agente de console permite que você:

- Orquestre tarefas de gerenciamento de armazenamento a partir do NetApp Console , como provisionamento do Cloud Volumes ONTAP, configuração de volumes de armazenamento, uso de classificação de dados e muito mais.
- Autentique-se usando as funções IAM do seu provedor de nuvem para integração de faturamento de assinaturas.
- Utilize serviços de dados avançados (NetApp Backup and Recovery, NetApp Disaster Recovery, NetApp Ransomware Resilience e NetApp Cloud Tiering).
- Utilize o console no modo restrito.

Se você não precisa de orquestração avançada ou proteção de dados, pode gerenciar centralmente clusters ONTAP locais e serviços de armazenamento nativos da nuvem sem implantar um agente. Ferramentas de monitoramento e mobilidade de dados também estão disponíveis.

A tabela a seguir mostra quais recursos e serviços você pode usar com e sem um agente do Console.

	Disponível com agente	**Disponível sem agente**
Sistemas de armazenamento suportados:		
Amazon FSx para ONTAP	Sim (recursos de descoberta e gerenciamento)	Sim (somente descoberta)
Armazenamento Amazon S3	Sim	Não
Armazenamento de Blobs do Azure	Sim	Sim
Azure NetApp Files	Sim	Sim
Cloud Volumes ONTAP	Sim	Não
Sistemas da série E	Sim	Não
Google Cloud NetApp Volumes	Sim	Sim
Buckets de armazenamento do Google Cloud	Sim	Não
Sistemas StorageGRID	Sim	Não
Cluster ONTAP local (gerenciamento e descoberta avançados)	Sim (gestão e descoberta avançadas)	Não (apenas descoberta básica)

	Disponível com agente	Disponível sem agente
Serviços de gestão de armazenamento disponíveis:		
Alertas	Sim	Não
Centro de automação	Sim	Sim
Digital Advisor (Active IQ)	Sim	Não
Gerenciamento de licenças e assinaturas	Sim	Não
Eficiência econômica	Sim	Não
Métricas do painel da página inicial	Sim[2]	Não
Planejamento do ciclo de vida	Sim	Não[1]
Sustentabilidade	Sim	Não
Atualizações de software	Sim	Sim
Cargas de trabalho da NetApp	Sim	Sim
Serviços de dados disponíveis:		
NetApp Backup and Recovery	Sim	Não
Classificação de Dados	Sim	Não
NetApp Cloud Tiering	Sim	Não
NetApp Copy and Sync	Sim	Não
NetApp Disaster Recovery	Sim	Não
NetApp Ransomware Resilience	Sim	Não
NetApp Volume Caching	Sim	Não

[1] É possível visualizar o planejamento do ciclo de vida sem um agente do console, mas um agente do console é necessário para iniciar ações.

[2] Métricas precisas na página inicial exigem agentes de console com tamanho e configuração adequados.

Os agentes do console devem estar operacionais o tempo todo

Os agentes de console são uma parte fundamental do NetApp Console. É sua responsabilidade (o cliente)

garantir que os agentes relevantes estejam sempre ativos, operacionais e acessíveis. O Console pode lidar com pequenas interrupções do agente, mas você deve corrigir falhas de infraestrutura rapidamente.

Esta documentação é regida pelo CLUF. Operar o produto fora da documentação pode afetar sua funcionalidade e seus direitos de EULA.

Locais suportados

Você pode instalar agentes nos seguintes locais:

- Serviços Web da Amazon
- Microsoft Azure

  Implante um agente de console no Azure na mesma região que os sistemas Cloud Volumes ONTAP que ele gerencia. Alternativamente, implante-o no "Par de regiões do Azure" . Isso garante que uma conexão do Azure Private Link seja usada entre o Cloud Volumes ONTAP e suas contas de armazenamento associadas. "Saiba como o Cloud Volumes ONTAP usa um Azure Private Link"

- Google Cloud

  Para usar o Console e os serviços de dados com o Google Cloud, implante seu agente no Google Cloud.

- Nas suas instalações

Comunicação com provedores de nuvem

O agente usa TLS 1.3 para todas as comunicações com AWS, Azure e Google Cloud.

Modo restrito

Para usar o Console no modo restrito, instale um agente do Console e acesse a interface do Console que está sendo executada localmente no agente do Console.

"Saiba mais sobre os modos de implantação do NetApp Console" .

Como instalar um agente de console

Você pode instalar um agente do Console diretamente do Console, do marketplace do seu provedor de nuvem ou instalando manualmente o software no seu próprio host Linux ou no seu ambiente VCenter.

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

Permissões do provedor de nuvem

Você precisa de permissões específicas para criar o agente do Console diretamente do NetApp Console e outro conjunto de permissões para o próprio agente do Console. Se você criar o agente do Console na AWS ou no Azure diretamente do Console, o Console criará o agente do Console com as permissões necessárias.

Ao usar o Console no modo padrão, a maneira como você fornece permissões depende de como você planeja criar o agente do Console.

Para saber como configurar permissões, consulte o seguinte:

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

Para visualizar as permissões exatas que o agente do Console precisa para operações diárias, consulte as seguintes páginas:

- "Aprenda como o agente do Console usa as permissões da AWS"
- "Aprenda como o agente do Console usa as permissões do Azure"
- "Saiba como o agente do Console usa as permissões do Google Cloud"

É sua responsabilidade atualizar as políticas do agente do Console à medida que novas permissões são adicionadas em versões subsequentes. As notas de versão listam novas permissões.

Atualizações de agentes

A NetApp atualiza o software do agente mensalmente para adicionar recursos e melhorar a estabilidade. Alguns recursos do Console, como o Cloud Volumes ONTAP e o gerenciamento de cluster ONTAP local, dependem da versão e das configurações do agente do Console.

Ao instalar o agente na nuvem, o agente do Console é atualizado automaticamente, desde que tenha acesso à internet.

Manutenção de sistema operacional e VM

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

Observe que você (cliente) não precisa interromper nenhum serviço no host do Console Gent ao aplicar pequenas atualizações de segurança.

Se você (cliente) precisar parar e iniciar a VM do agente do Console, faça isso no console do seu provedor de nuvem ou usando os procedimentos padrão para gerenciamento local.

O agente do Console deve estar operacional o tempo todo .

Vários sistemas e agentes

Um agente pode gerenciar vários sistemas e dar suporte a serviços de dados no Console. Você pode usar um único agente para gerenciar vários sistemas com base no tamanho da implantação e nos serviços de dados que você usa.

Para implantações em larga escala, trabalhe com seu representante da NetApp para dimensionar seu ambiente. Entre em contato com o Suporte da NetApp se tiver problemas.

Aqui estão alguns exemplos de implantações de agentes:

- Você tem um ambiente multicloud (por exemplo, AWS e Azure) e prefere ter um agente na AWS e outro no Azure. Cada um gerencia os sistemas Cloud Volumes ONTAP em execução nesses ambientes.
- Um provedor de serviços pode usar uma organização do Console para fornecer serviços aos seus clientes, enquanto usa outra organização para fornecer recuperação de desastres para uma de suas unidades de negócios. Cada organização precisa de seu próprio agente.

Saiba mais sobre o gerenciamento de identidade e acesso do NetApp Console

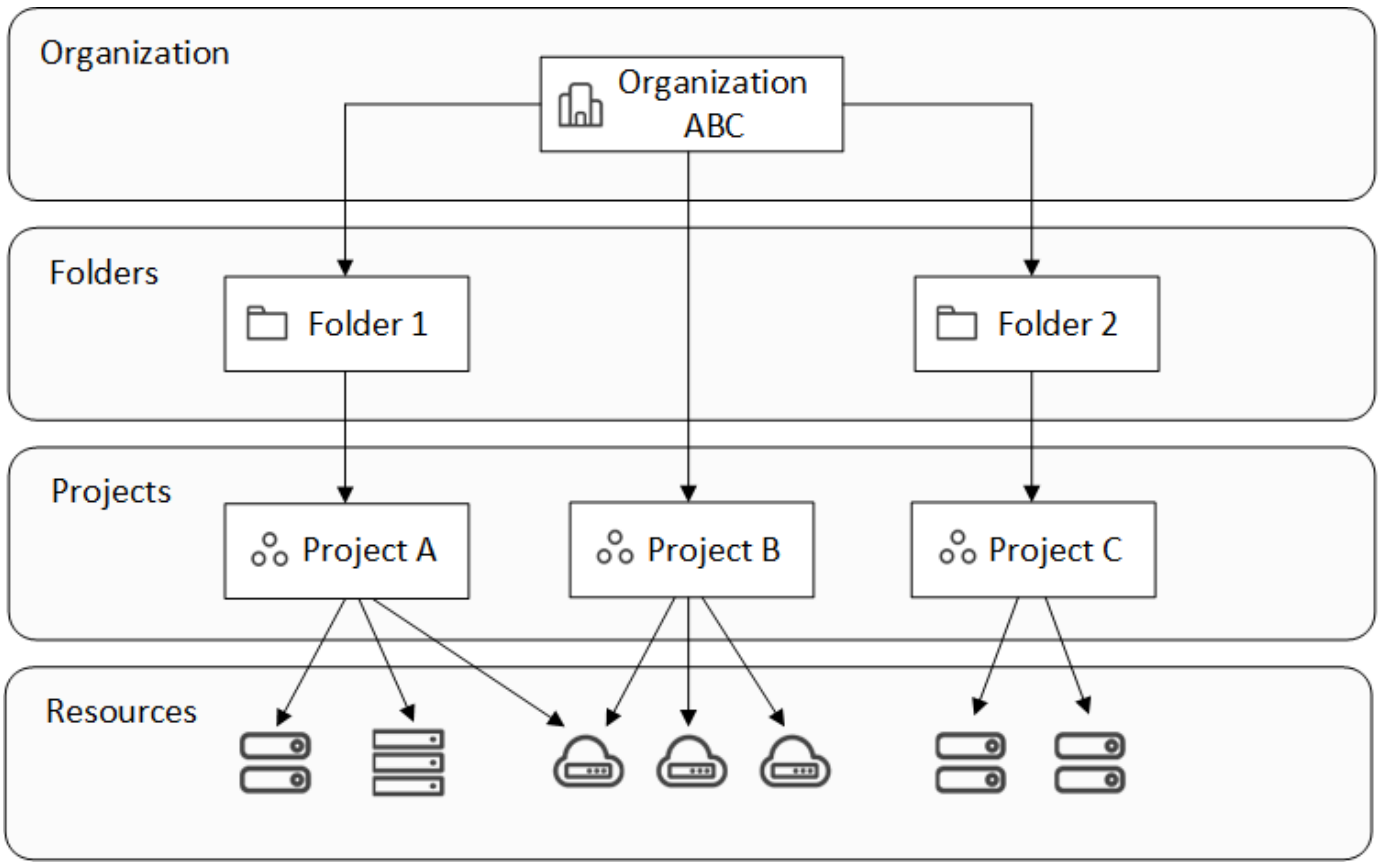
Utilize o Gerenciamento de Identidade e Acesso (IAM) do NetApp Console para organizar seus recursos NetApp e controlar o acesso de acordo com a estrutura da sua empresa — por local, departamento ou projeto.

Os recursos são organizados hierarquicamente: a organização está no topo, seguida pelas pastas (que podem conter outras pastas ou projetos) e, em seguida, pelos projetos, que contêm sistemas de armazenamento, cargas de trabalho e agentes.

Atribua permissões de controle de acesso baseado em funções (RBAC) aos membros no nível da organização, pasta ou projeto para garantir que os usuários tenham o acesso apropriado aos recursos.

Você precisa ter as funções de *Superadministrador*, *Administrador da organização* ou *Administrador de pasta ou projeto* para gerenciar o IAM no NetApp Console.

A imagem a seguir ilustra essa hierarquia em um nível básico.



]

Componentes de gerenciamento de identidade e acesso

No NetApp Console, você organiza seus recursos de armazenamento usando três componentes principais: componentes organizacionais, componentes de recursos e componentes de acesso do usuário.

Projetos e pastas dentro da sua organização

Dentro da sua estrutura IAM, você trabalha com três componentes organizacionais: organizações, projetos e pastas. Você pode conceder acesso aos usuários atribuindo-lhes funções em qualquer um desses níveis.

Organização

Uma *organização* é o nível superior do sistema Console IAM e normalmente representa sua empresa. Sua organização consiste em pastas, projetos, membros, funções e recursos. Os agentes estão associados a projetos específicos na organização.

Projetos

Um *projeto* é usado para fornecer acesso a um recurso de armazenamento. Você precisa atribuir recursos ao projeto antes que alguém possa acessá-los. Você pode atribuir vários recursos a um único projeto e também pode ter vários projetos. Em seguida, você atribui permissões de usuário ao projeto para dar a eles acesso aos recursos contidos nele.

Por exemplo, você pode associar um sistema ONTAP local a um único projeto ou a todos os projetos da sua organização, dependendo das suas necessidades.

"Aprenda como adicionar projetos à sua organização."

Pastas

Agrupe projetos relacionados em *pastas* para organizá-los por local, unidade ou negócio. Não é possível associar recursos diretamente a pastas, mas atribuir uma função a um usuário no nível da pasta dá a ele acesso a todos os projetos dessa pasta.

"Aprenda como adicionar pastas à sua organização."

Recursos

Os recursos incluem sistemas de armazenamento, assinaturas do Keystone , bem como agentes do Console.

+ Você precisa associar um recurso a um projeto antes que alguém possa acessá-lo.

+

Por exemplo, você pode associar um sistema Cloud Volumes ONTAP a um projeto ou a todos os projetos da sua organização. A forma como você associa um recurso depende das necessidades da sua organização.

+

"Aprenda como associar recursos a projetos."

Sistemas de armazenamento e assinaturas Keystone

Os sistemas de armazenamento são os principais recursos que você gerencia no NetApp Console. O NetApp Console oferece suporte ao gerenciamento de sistemas de armazenamento locais e em nuvem. Você precisa adicionar um sistema de armazenamento a um projeto antes que alguém possa acessá-lo.

Os sistemas de armazenamento são associados automaticamente ao projeto em que são adicionados, mas você também pode associá-los a outros projetos ou pastas na página **Recursos**.

As assinaturas do Keystone também são recursos que você pode associar a projetos para conceder aos usuários acesso à assinatura no NetApp Console.

Agentes de console

Os administradores da organização criam agentes do Console para gerenciar sistemas de armazenamento e habilitar os serviços de dados da NetApp . Inicialmente, os agentes são vinculados ao projeto em que são criados, mas os administradores podem adicioná-los a outros projetos ou pastas na página Agentes.

Associar um agente a um projeto permite o gerenciamento de recursos nesse projeto, enquanto associar um agente a uma pasta permite que os administradores da pasta ou do projeto decidam quais projetos devem usar o agente. Os agentes devem estar vinculados a projetos específicos para fornecerem capacidades de gestão.

"Aprenda como associar agentes a projetos."

Membros e funções

Membros

Os membros da sua organização são contas de usuário ou contas de serviço. Uma conta de serviço normalmente é usada por um aplicativo para concluir tarefas específicas sem intervenção humana.

Você precisa adicionar membros à sua organização depois que eles se inscreverem no NetApp Console. Depois de adicionados, você pode atribuir funções a eles para fornecer acesso a recursos. Você pode adicionar contas de serviço manualmente no Console ou automatizar a criação e o gerenciamento delas por meio da API IAM do NetApp Console .

"Aprenda como adicionar membros à sua organização."

Funções de acesso

O Console fornece funções de acesso que você pode atribuir aos membros da sua organização.

Ao associar um membro a uma função, você pode conceder essa função para toda a organização, uma pasta específica ou um projeto específico. A função que você selecionar concede permissões a um membro para acessar os recursos na parte selecionada da hierarquia.

O NetApp Console oferece funções granulares que seguem o princípio do "privilégio mínimo", o que significa que as funções de acesso são projetadas para conceder aos usuários acesso somente ao que eles precisam.

Isso significa que os usuários podem ter várias funções atribuídas a eles à medida que suas responsabilidades aumentam.

"Saiba mais sobre funções de acesso" .

Exemplos de estratégia IAM

Estratégia para pequenas organizações

Para organizações com menos de 50 usuários e gerenciamento de armazenamento centralizado, considere uma abordagem simplificada usando as funções de Superadministrador e Supervisualizador.

Exemplo: ABC Corporation (equipe de 5 pessoas)

- **Estrutura:** Organização única com 3 projetos (Produção, Desenvolvimento, Backup)

- **Funções:**
  - 2 membros seniores: Função de **Superadministrador** com acesso administrativo completo.
  - 3 membros da equipe: Função de **Supervisor** para monitoramento sem direitos de modificação.
- **Estratégia de agente:** Um único agente associado a todos os projetos para acesso a recursos compartilhados.
- **Benefícios:** Administração simplificada, complexidade de funções reduzida, adequado para equipes que necessitam de amplo acesso.

Estratégia empresarial multirregional

Para grandes organizações com operações regionais e equipes especializadas, implemente uma abordagem hierárquica com pastas representando limites geográficos ou de unidades de negócios.

Exemplo: Corporação XYZ (empresa multinacional)

- **Estrutura:** Organização > Pastas regionais (América do Norte, Europa, Ásia-Pacífico) > Pastas de projetos por região
- **Funções da plataforma:**
  - 1 **Administração organizacional**: Supervisão global e gestão de políticas
  - 3 **Administradores de pastas ou projetos**: Controle regional (um por região)
  - 1 **Administração da Federação**: Integração do provedor de identidade corporativa
- **Funções de armazenamento por região:**
  - 9 **Administrador de armazenamento**: Descobrir e gerenciar sistemas de armazenamento em regiões atribuídas.
  - 2 **Visualizador de armazenamento**: Monitore os recursos de armazenamento em diferentes regiões.
  - 1 **Especialista em integridade do sistema**: Gerencie a integridade do armazenamento sem modificações no sistema
- **Funções do serviço de dados:**
  - **Administrador de Backup e Recuperação**: Cobrança por projeto, com base nas responsabilidades de backup.
  - **Administrador de Resiliência a Ransomware**: Monitoramento da equipe de segurança em todos os projetos
- **Estratégia de agentes:** Agentes regionais associados a projetos geográficos relevantes.
- **Benefícios:** Segurança reforçada por meio da segregação de funções, autonomia regional e conformidade com as regulamentações locais.

Estratégia de especialização departamental

Para organizações com equipes especializadas que necessitam de acesso a serviços de dados específicos, utilize atribuições de funções direcionadas com base nas responsabilidades funcionais.

Exemplo: TechCorp (empresa de tecnologia de médio porte)

- **Estrutura:** Organização > Pastas de departamento (TI, Segurança, Desenvolvimento) > Recursos específicos do projeto
- **Funções especializadas:**

    - Equipe de segurança: funções de **Administrador de Resiliência a Ransomware** e **Visualizador de Classificações**.
    - Equipe de backup: **Superadministrador de backup e recuperação** para operações de backup abrangentes.
    - Equipe de desenvolvimento: **Administrador de armazenamento** para gerenciamento de ambiente de teste
    - Equipe de Compliance: **Analista de suporte operacional** para monitoramento e gerenciamento de casos de suporte.
- **Estratégia de agentes:** Agentes vinculados a projetos departamentais com base na propriedade dos recursos.
- **Benefícios:** Controle de acesso personalizado, maior eficiência operacional e responsabilidade clara por tarefas especializadas.

Próximos passos com o IAM no NetApp Console

- "Introdução ao IAM no NetApp Console"
- "Monitorar ou auditar a atividade do IAM"
- "Saiba mais sobre a API para NetApp Console IAM"

Comece a usar o NetApp Console (SaaS)

Fluxo de trabalho de primeiros passos (SaaS)

Comece a usar o NetApp Console (SaaS) preparando a rede para o Console, inscrevendo-se e criando uma conta e usando o assistente do Console para configurar as funcionalidades iniciais.

Você acessa um console baseado na web que é hospedado como um produto de Software como Serviço (SaaS) da NetApp. Você pode usar o Console para gerenciar seu ambiente de armazenamento em nuvem híbrida e usar os serviços de dados da NetApp .

"Preparar a rede para usar o console NetApp"

Certifique-se de que os computadores que acessam o console NetApp tenham acesso à rede nos endpoints necessários.

"Aprenda como preparar a rede para o console NetApp ."

"Cadastre-se e crie uma organização"

Vá para o "Console NetApp" e inscreva-se. Se for solicitado que você crie uma organização e você achar que já existe uma organização para sua empresa, feche a caixa de diálogo e informe o administrador da sua organização. Se não houver atualmente um administrador da organização para sua empresa, você pode reivindicar essa função. "Aprenda como entrar em contato com um administrador da organização."

Neste ponto, você já está conectado e pode usar o assistente da NetApp para começar a configurar o Console. Para começar, associe sua conta de suporte da NetApp a um agente de console para habilitar todas as funcionalidades.

Se optar por não usar o assistente da NetApp ou instalar um agente de console, você pode começar a gerenciar o armazenamento e usar serviços como Digital Advisor, Amazon FSx para ONTAP, Azure NetApp Files e muito mais. "Aprenda o que você pode fazer sem um agente de console".

3 Associe sua conta do NetApp Support Site (NSS).

Associar sua conta do NetApp Support Site (NSS) ao Console permite que você gerencie suas licenças e assinaturas com mais facilidade, além de acessar recursos de suporte diretamente do Console.

4 Criar um agente de console

Recursos avançados de gerenciamento de armazenamento e alguns serviços de dados do NetApp exigem que você instale um agente do Console. O agente do Console permite que o Console gerencie recursos e processos dentro do seu ambiente de nuvem híbrida.

Você pode criar um agente do Console na sua rede local ou na nuvem.

- "Saiba mais sobre quando os agentes do Console são necessários e como eles funcionam"
- "Aprenda a criar um agente de console na AWS"
- "Aprenda a criar um agente de console no Azure"
- "Aprenda a criar um agente de console no Google Cloud"
- "Aprenda a criar um agente de console no local"

5 Adicionar um sistema de armazenamento ao console

No NetApp Console, você pode adicionar ou descobrir sistemas de armazenamento para gerenciar seu ambiente de armazenamento em nuvem híbrida. Utilize o assistente da NetApp para adicionar seu primeiro sistema de armazenamento.

Se você instalar um agente do Console na AWS, Microsoft Azure ou Google Cloud, o Console descobrirá automaticamente informações sobre os buckets do Amazon S3, do Azure Blob Storage ou do Google Cloud Storage no local onde o agente está instalado. Esses sistemas são adicionados automaticamente à página **Sistemas**.

- "Aprenda como descobrir um sistema ONTAP"
- "Aprenda como descobrir um sistema StorageGRID"
- "Aprenda como descobrir um sistema da Série E"

6 "Assine o NetApp Intelligent Services (opcional)"

Cadastre-se no NetApp Intelligent Services por meio do seu provedor de nuvem para faturamento por hora (PAYGO) ou anual. A assinatura inclui NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience, NetApp Disaster Recovery e NetApp Data Classification.

Preparar o acesso à rede para o NetApp Console

O NetApp Console, o agente do NetApp Console e os serviços de dados do NetApp

exigem acesso de saída à Internet e a capacidade de entrar em contato com os endpoints necessários.

Você precisará configurar o acesso à rede para o seguinte:

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

> Com a versão 4.0.0, a NetApp reduziu os pontos de extremidade de rede necessários para o Console e os agentes do Console, aumentando a segurança e simplificando a implantação. É importante ressaltar que todas as implantações anteriores à versão 4.0.0 continuam com suporte total. Embora os endpoints anteriores permaneçam disponíveis para os agentes existentes, a NetApp recomenda fortemente atualizar as regras de firewall para os endpoints atuais após confirmar as atualizações bem-sucedidas dos agentes."Aprenda como atualizar sua lista de endpoints."

Endpoints contatados pelo NetApp Console e agentes do Console

Cada agente implantado e cada computador que acessa o NetApp Console deve ter conexões com os endpoints listados abaixo.

Os agentes de console implantados no seu provedor de nuvem precisam acessar os endpoints respectivos a esse provedor de nuvem.

Pontos finais	Propósito
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://signin.b2c.netapp.com	Para atualizar as credenciais do NetApp Support Site (NSS) ou adicionar novas credenciais do NSS ao NetApp Console.
\ https://support.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp , bem como receber atualizações de software para o Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Para fornecer recursos e serviços no NetApp Console.

Pontos finais	Propósito
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. • Quando você implanta um novo agente, a verificação de validação testa a conectividade com os endpoints atuais. Se você usar"pontos finais anteriores" , a verificação de validação falha. Para evitar essa falha, pule a verificação de validação. Embora os endpoints anteriores ainda sejam suportados, a NetApp recomenda atualizar suas regras de firewall para os endpoints atuais o mais rápido possível. "Aprenda como atualizar sua lista de endpoints" . • Quando você atualiza os endpoints atuais no seu firewall, seus agentes existentes continuarão funcionando.

Os endpoints do provedor de nuvem contataram o agente do Console

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

Configure o acesso ao ponto de extremidade da rede do provedor de nuvem antes de instalar o agente do Console.

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

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

Alguns serviços de dados da NetApp , bem como o Cloud Volumes ONTAP, exigem que o agente tenha acesso adicional à Internet de saída.

Pontos de extremidade para Cloud Volumes ONTAP

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

Pontos finais para cargas de trabalho

O agente do console deve ser capaz de acessar o seguinte endpoint para cargas de trabalho do NetApp .

Pontos finais	Propósito
https://api.workloads.netapp.com	O console baseado na web contata este endpoint para interagir com as APIs do Workload Factory, a fim de gerenciar e operar cargas de trabalho baseadas no FSx para ONTAP.

Inscreva-se ou faça login no NetApp Console

Para usar o Console, inscreva-se ou faça login com suas credenciais do Site de Suporte da NetApp ou crie um login no NetApp Console . Se você for o primeiro da sua empresa a se cadastrar, você criará uma nova organização como administrador. Se sua empresa já possui uma organização, inscreva-se ou faça login com suas credenciais existentes do Site de Suporte da NetApp ou com o login único (SSO) da empresa.

Cadastre-se no NetApp Console como administrador inicial da organização.

Se sua empresa não possui uma organização NetApp Console , inscreva-se para criar uma. O primeiro usuário se torna o administrador da organização e gerencia as contas de usuário e as permissões. Você poderá atualizar as funções e adicionar mais administradores posteriormente.

Passos

1. Abra um navegador da web e vá para o "NetApp Console"
2. Se você possui uma conta no site de suporte da NetApp , insira o endereço de e-mail associado à sua conta diretamente na página de **login**.

   O Console realiza o seu cadastro como parte deste login inicial, utilizando as suas credenciais do Site de Suporte da NetApp .

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

      Somente caracteres em inglês são permitidos no formulário de inscrição.

   b. Verifique sua caixa de entrada para ver se recebeu um e-mail da NetApp com instruções para verificar seu endereço de e-mail.

      Verifique seu endereço de e-mail para concluir o cadastro.

4. Após efetuar o login, revise e aceite o Contrato de Licença do Usuário Final.
5. Na página **Boas-vindas**, crie uma organização.
6. Selecione **Vamos começar**.

+ Como usuário iniciante e administrador da organização, você segue um processo guiado para adicionar recursos de armazenamento, criar um agente do Console e muito mais. "Aprenda a usar o Assistente do Console."

Próximos passos

Como administrador, após concluir as etapas incluídas no Assistente do Console, você deve planejar sua estratégia de identidade e acesso, adicionar usuários à sua organização e atribuir funções. "Saiba mais sobre

gerenciamento de identidade e acesso para o NetApp Console."

Cadastre-se ou faça login no NetApp Console se já existir uma organização.

Se sua empresa já possui uma organização NetApp Console , inscreva-se ou faça login para acessá-la. O método de cadastro ou login depende se sua empresa utiliza federação de identidades ou possui credenciais do site de suporte da NetApp . Caso contrário, crie um login no NetApp Console .

Passos

1. Abra um navegador da web e vá para o "NetApp Console"
2. Se você possui uma conta no site de suporte da NetApp ou se sua empresa configurou o login único (SSO), insira seu endereço de e-mail associado ou suas credenciais de SSO na página **Entrar**. Siga as instruções para concluir o login.

   Em ambos os casos, você se inscreve no Console como parte desse login inicial.

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

      Somente caracteres em inglês são permitidos no formulário de inscrição.

   b. Verifique sua caixa de entrada para ver se recebeu um e-mail da NetApp com instruções para verificar seu endereço de e-mail.

      Verifique seu endereço de e-mail para concluir o cadastro.

4. Após efetuar o login, revise e aceite o Contrato de Licença do Usuário Final.
5. Se o sistema solicitar que você crie uma organização, feche a caixa de diálogo e informe um administrador do Console para que ele possa adicioná-lo à sua organização do Console e conceder-lhe acesso. "Aprenda como entrar em contato com um administrador da organização."

Próximos passos

Após receber acesso à sua organização, você poderá começar a gerenciar o armazenamento e usar os serviços de dados que lhe forem atribuídos.

Comece a usar o assistente do NetApp Console

Se você estiver usando o NetApp Console (SaaS) pela primeira vez e tiver a função de administrador da organização, poderá usar o assistente do console para orientá-lo no processo de configuração inicial. O assistente ajuda você a adicionar uma conta do NetApp Support Site (NSS), adicionar um agente de console, adicionar um cluster e adicionar uma licença ou assinatura, facilitando o início do gerenciamento de seus dados.

Funções necessárias para acessar o assistente do Console

O assistente do Console está disponível somente para usuários com a função de administrador da organização.

Por padrão, o NetApp Console exibe o assistente do Console na página inicial para usuários que acessam o sistema pela primeira vez e que possuem a função de administrador da organização. Ele permanecerá

disponível até que você conclua as tarefas obrigatórias de criação de um agente de console e adição de um sistema.

Utilize o assistente para concluir essas tarefas, que fornecem a configuração mínima para o seu ambiente NetApp Console :

- Adicione uma conta do NetApp Support Site (NSS).

  "Aprenda como adicionar uma conta NSS".

- Conecte-se ao seu ambiente de armazenamento implantando um agente de console.

  "Aprenda como instalar um agente de console localmente."

- Gerencie um sistema de armazenamento adicionando ou descobrindo um cluster.
- Adicione uma assinatura de mercado ou uma licença PAYGO.

  "Aprenda como adicionar licenças e assinaturas.".

- Analise as informações dos serviços de dados.

Comece a usar o NetApp Console (modo restrito)

Fluxo de trabalho de introdução (modo restrito)

Comece a usar o NetApp Console no modo restrito preparando seu ambiente e implantando o agente do Console.

O modo restrito é normalmente usado por governos estaduais e locais e empresas regulamentadas, incluindo implantações nas regiões AWS GovCloud e Azure Government. Antes de começar, certifique-se de ter uma compreensão de"Agentes de console" e"modos de implantação" .

"Preparar para implantação"

1. Prepare um host Linux dedicado que atenda aos requisitos de CPU, RAM, espaço em disco, ferramenta de orquestração de contêineres e muito mais.
2. Configure uma rede que forneça acesso às redes de destino, acesso de saída à Internet para instalações manuais e acesso de saída à Internet para acesso diário.
3. Configure permissões no seu provedor de nuvem para que você possa associá-las à instância do agente do Console após implantá-lo.

"Implantar o agente do Console"

1. Instale o agente do Console no marketplace do seu provedor de nuvem ou instalando manualmente o software no seu próprio host Linux.
2. Configure o NetApp Console abrindo um navegador da Web e inserindo o endereço IP do host Linux.
3. Forneça ao agente do Console as permissões que você configurou anteriormente.

3 **"Assine o NetApp Intelligent Services (opcional)"**

Opcional: assine o NetApp Intelligent Services no marketplace do seu provedor de nuvem para pagar por serviços de dados a uma taxa por hora (PAYGO) ou por meio de um contrato anual. Os NetApp Intelligent Services incluem NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience e NetApp Disaster Recovery. A NetApp Data Classification está incluída na sua assinatura sem custo adicional.

Preparar para implantação no modo restrito

Prepare seu ambiente antes de implantar o NetApp Console no modo restrito. Você precisa revisar os requisitos do host, preparar a rede, configurar permissões e muito mais.

Etapa 1: Entenda como funciona o modo restrito

Entenda como o NetApp Console funciona no modo restrito antes de começar.

Use a interface baseada em navegador disponível localmente no agente do NetApp Console instalado. Você não pode acessar o NetApp Console pelo console baseado na Web fornecido pela camada SaaS.

Além disso, nem todos os recursos do Console e serviços de dados do NetApp estão disponíveis.

"Aprenda como funciona o modo restrito" .

Etapa 2: Revise as opções de instalação

No modo restrito, você só pode instalar o agente do Console na nuvem. As seguintes opções de instalação estão disponíveis:

- Do AWS Marketplace
- Do Azure Marketplace
- Instalando manualmente o agente do Console em seu próprio host Linux em execução no AWS, Azure ou Google Cloud

Etapa 3: Revise os requisitos do host

Um host deve atender a requisitos específicos de sistema operacional, RAM e porta para executar o agente do Console.

Quando você implanta o agente do Console do AWS ou do Azure Marketplace, a imagem inclui o sistema operacional e os componentes de software necessários. Você só precisa escolher um tipo de instância que atenda aos requisitos de CPU e RAM.

Host dedicado

O agente do Console requer um host dedicado. Qualquer arquitetura é suportada, desde que atenda a estes requisitos de tamanho:

- CPU: 8 núcleos ou 8 vCPUs
- RAM: 32 GB
- Espaço em disco: 165 GB é recomendado para o host, com os seguintes requisitos de partição:

- `/opt`: 120 GiB de espaço devem estar disponíveis

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

- `/var`: 40 GiB de espaço devem estar disponíveis

  O agente do console requer este espaço em `/var` Porque o Podman ou o Docker são projetados para criar contêineres dentro deste diretório. Especificamente, eles criarão contêineres no `/var/lib/containers/storage` diretório e `/var/lib/docker` para Docker. Montagens externas ou links simbólicos não funcionam neste espaço.

Tipo de instância AWS EC2

Um tipo de instância que atende aos requisitos de CPU e RAM. A NetApp recomenda t3.2xlarge.

Tamanho da VM do Azure

Um tipo de instância que atende aos requisitos de CPU e RAM. A NetApp recomenda Standard_D8s_v3.

Tipo de máquina do Google Cloud

Um tipo de instância que atende aos requisitos de CPU e RAM. A NetApp recomenda o n2-standard-8.

O agente do Console é compatível com o Google Cloud em uma instância de VM com um sistema operacional compatível "Recursos de VM blindada"

Hipervisor

É necessário um hipervisor bare metal ou hospedado certificado para executar um sistema operacional compatível.

Requisitos do sistema operacional e do contêiner

O agente do Console é compatível com os seguintes sistemas operacionais ao usar o Console no modo padrão ou no modo restrito. Uma ferramenta de orquestração de contêineres é necessária antes de instalar o agente.

Sistema operacional	Versões de SO suportadas	Versões de agentes suportadas	Ferramenta de contêiner necessária	SELinux
Red Hat Enterprise Linux		9,6 • Somente versões em inglês. • O host deve ser registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar os repositórios para atualizar o software de terceiros necessário durante a instalação do agente.	4.0.0 ou posterior com o Console no modo padrão ou no modo restrito.	Podman versão 5.4.0 com podman-compose 1.5.0. Ver requisitos de configuração do Podman .
Suportado no modo de imposição ou no modo permissivo		9.1 a 9.4 • Somente versões em inglês. • O host deve ser registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar os repositórios para atualizar o software de terceiros necessário durante a instalação do agente.	3.9.50 ou posterior com o Console no modo padrão ou modo restrito	Podman versão 4.9.4 com podman-compose 1.5.0. Ver requisitos de configuração do Podman .

Sistema operacional	Versões de SO suportadas	Versões de agentes suportadas	Ferramenta de contêiner necessária	SELinux
Suportado no modo de imposição ou no modo permissivo		8,6 a 8,10 • Somente versões em inglês. • O host deve ser registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar os repositórios para atualizar o software de terceiros necessário durante a instalação do agente.	3.9.50 ou posterior com o Console no modo padrão ou modo restrito	Podman versão 4.6.1 ou 4.9.4 com podman-compose 1.0.6. Ver requisitos de configuração do Podman .
Suportado no modo de imposição ou no modo permissivo	Ubuntu		24,04 LTS	3.9.45 ou posterior com o NetApp Console no modo padrão ou restrito
Docker Engine 23.06 para 28.0.0.	Não suportado		22,04 LTS	3.9.50 ou posterior

Etapa 4: instalar o Podman ou o Docker Engine

Para instalar manualmente o agente do Console, prepare o host instalando o Podman ou o Docker Engine.

Dependendo do seu sistema operacional, o Podman ou o Docker Engine é necessário antes de instalar o agente.

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

  Veja as versões do Podman suportadas .

- O Docker Engine é necessário para o Ubuntu.

  Veja as versões suportadas do Docker Engine .

Exemplo 1. Passos

Podman

Siga estas etapas para instalar e configurar o Podman:

- Habilite e inicie o serviço podman.socket
- Instalar python3
- Instale o pacote podman-compose versão 1.0.6
- Adicione podman-compose à variável de ambiente PATH
- Se estiver usando o Red Hat Enterprise Linux, verifique se sua versão do Podman está usando o DNS Netavark Aardvark em vez do CNI

Ajuste a porta aardvark-dns (padrão: 53) após instalar o agente para evitar conflitos de porta DNS. Siga as instruções para configurar a porta.

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.

   Você pode obter o Podman nos repositórios oficiais do Red Hat Enterprise Linux.

   a. Para Red Hat Enterprise Linux 9,6:

   ```
   sudo dnf install podman-5:<version>
   ```

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

   b. Para Red Hat Enterprise Linux 9.1 a 9.4:

   ```
   sudo dnf install podman-4:<version>
   ```

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

   c. Para Red Hat Enterprise Linux 8:

   ```
   sudo dnf install podman-4:<version>
   ```

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

3. Habilite e inicie o serviço podman.socket.

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

4. Instale python3.

```
sudo dnf install python3
```

5. Instale o pacote do repositório EPEL se ele 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).

6. Se estiver usando o Red Hat Enterprise 9:

   a. Instale o pacote do repositório EPEL.

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

   +

   a. Instale o pacote podman-compose 1.5.0.

```
sudo dnf install podman-compose-1.5.0
```

7. Se estiver usando o Red Hat Enterprise Linux 8:

   a. Instale o pacote do repositório EPEL.

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

   b. Instale o pacote podman-compose 1.0.6.

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

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

   c. Se estiver usando o Red Hat Enterprise Linux 8, verifique se sua versão do Podman está usando o NetAvark com o DNS Aardvark em vez do CNI.

i. Verifique se o seu networkBackend está definido como CNI executando o seguinte comando:

```
podman info | grep networkBackend
```

ii. Se o networkBackend estiver definido como `CNI` , você precisará alterá-lo para `netavark` .

iii. Instalar `netavark` e `aardvark-dns` usando o seguinte comando:

```
dnf install aardvark-dns netavark
```

iv. Abra o `/etc/containers/containers.conf` arquivo e modifique a opção network_backend para usar "netavark" em vez de "cni".

Se `/etc/containers/containers.conf` não existe, faça as alterações de configuração para `/usr/share/containers/containers.conf` .

v. Reinicie o podman.

```
systemctl restart podman
```

vi. Confirme se networkBackend foi alterado para "netavark" usando o seguinte comando:

```
podman info | grep networkBackend
```

Motor Docker

Siga a documentação do Docker para instalar o Docker Engine.

Passos

1. "Ver instruções de instalação do Docker"

   Siga as etapas para instalar uma versão compatível do Docker Engine. Não instale a versão mais recente, pois ela não é suportada pelo Console.

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

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

Etapa 5: preparar o acesso à rede

Configure o acesso à rede para que o agente do Console possa gerenciar recursos na sua nuvem pública. Além de ter uma rede virtual e uma sub-rede para o agente do Console, você precisa garantir que os seguintes requisitos sejam atendidos.

Conexões com redes de destino

Certifique-se de que o agente do Console tenha uma conexão de rede com os locais de armazenamento. Por exemplo, a VPC ou VNet onde você planeja implantar o Cloud Volumes ONTAP ou o data center onde seus clusters ONTAP locais residem.

Preparar a rede para acesso do usuário ao NetApp Console

No modo restrito, os usuários acessam o Console a partir da VM do agente do Console. O agente do Console entra em contato com alguns endpoints para concluir tarefas de gerenciamento de dados. Esses endpoints são contatados pelo computador de um usuário ao concluir ações específicas do Console.

Agentes de console anteriores à versão 4.0.0 precisam de endpoints adicionais. Se você atualizou para 4.0.0 ou posterior, poderá remover os endpoints antigos da sua lista de permissões."Saiba mais sobre o acesso de rede necessário para versões anteriores à 4.0.0."

+

Pontos finais	Propósito
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Para fornecer recursos e serviços no NetApp Console.
\ https://cdn.auth0.com \ https://services.cloud.netapp.com	Seu navegador da Web se conecta a esses endpoints para autenticação centralizada do usuário por meio do NetApp Console.

Acesso de saída à Internet para operações diárias

O local de rede do agente do Console deve ter acesso de saída à Internet. Ele precisa ser capaz de alcançar os serviços SaaS do NetApp Console , bem como os endpoints dentro do seu respectivo ambiente de nuvem pública.

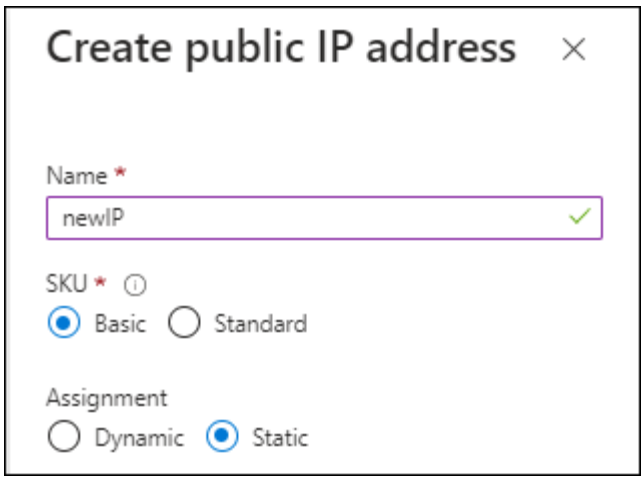
Pontos finais	Propósito
Ambientes AWS	Serviços da AWS (amazonaws.com): • CloudFormation • Nuvem de Computação Elástica (EC2) • Gerenciamento de Identidade e Acesso (IAM) • Serviço de Gerenciamento de Chaves (KMS) • Serviço de Token de Segurança (STS) • Serviço de Armazenamento Simples (S3)

Pontos finais	Propósito
Para gerenciar recursos da AWS. O ponto de extremidade depende da sua região da AWS. "Consulte a documentação da AWS para obter detalhes"	Amazon FSX para NetApp ONTAP: • api.workloads.netapp.com
O console baseado na web contata este endpoint para interagir com as APIs do Workload Factory, a fim de gerenciar e operar cargas de trabalho baseadas no FSx para ONTAP .	**Ambientes Azure**
\ 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 em regiões governamentais 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.
Ambientes do Google Cloud	\ 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://config.googleapis.com/v1/projects
Para gerenciar recursos no Google Cloud.	• Pontos de extremidade do NetApp Console *
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://signin.b2c.netapp.com	Para atualizar as credenciais do NetApp Support Site (NSS) ou adicionar novas credenciais do NSS ao NetApp Console.

Pontos finais	Propósito
\ https://support.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp , bem como receber atualizações de software para o Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Para fornecer recursos e serviços no NetApp Console.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. • Quando você implanta um novo agente, a verificação de validação testa a conectividade com os endpoints atuais. Se você usar"pontos finais anteriores" , a verificação de validação falha. Para evitar essa falha, pule a verificação de validação. Embora os endpoints anteriores ainda sejam suportados, a NetApp recomenda atualizar suas regras de firewall para os endpoints atuais o mais rápido possível. "Aprenda como atualizar sua lista de endpoints" . • Quando você atualiza os endpoints atuais no seu firewall, seus agentes existentes continuarão funcionando.

Endereço IP público no Azure

Se você quiser usar um endereço IP público com a VM do agente do Console no Azure, o endereço IP deverá usar um SKU básico para garantir que o Console use esse endereço IP público.



Se você usar um endereço IP de SKU padrão, o Console usará o endereço IP *privado* do agente do Console, em vez do IP público. Se a máquina que você está usando para acessar o Console não tiver acesso a esse endereço IP privado, as ações do Console falharão.

"Documentação do Azure: SKU de IP público"

Servidor proxy

O NetApp oferece suporte a configurações de proxy explícitas e transparentes. Se você estiver usando um proxy transparente, você só precisa fornecer o certificado para o servidor proxy. Se estiver usando um proxy explícito, você também precisará do endereço IP e das credenciais.

- Endereço IP
- Credenciais
- Certificado HTTPS

Portos

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

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

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

Habilitar NTP

Se você planeja usar o NetApp Data Classification para verificar suas fontes de dados corporativos, habilite um serviço Network Time Protocol (NTP) no agente do Console e no sistema NetApp Data Classification para que o horário seja sincronizado entre os sistemas. "Saiba mais sobre a classificação de dados da NetApp"

Se você estiver planejando criar um agente do Console no marketplace do seu provedor de nuvem, implemente este requisito de rede depois de criar o agente do Console.

Etapa 6: preparar permissões de nuvem

O agente do Console requer permissões do seu provedor de nuvem para implantar o Cloud Volumes ONTAP em uma rede virtual e usar os serviços de dados do NetApp . Você precisa configurar permissões no seu provedor de nuvem e então associá-las ao agente do Console.

Para visualizar as etapas necessárias, escolha a opção de autenticação a ser usada para seu provedor de nuvem.

Função do AWS IAM

Use uma função do IAM para fornecer permissões ao agente do Console.

Se estiver criando o agente do Console no AWS Marketplace, você será solicitado a selecionar essa função do IAM ao iniciar a instância do EC2.

Se você estiver instalando manualmente o agente do Console em seu próprio host Linux, anexe a função à instância do EC2.

Passos

1. Faça login no console da AWS e navegue até o serviço IAM.
2. Crie uma política:
   a. Selecione **Políticas > Criar política**.
   b. Selecione **JSON** e copie e cole o conteúdo do"Política do IAM para o agente do Console" .
   c. Conclua as etapas restantes para criar a política.
3. Crie uma função do IAM:
   a. Selecione **Funções > Criar função**.
   b. Selecione **Serviço AWS > 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 EC2 do agente do Console.

Chave de acesso AWS

Configure permissões e uma chave de acesso para um usuário do IAM. Você precisará fornecer ao Console a chave de acesso da AWS depois de instalar o agente do Console e configurar o Console.

Passos

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

      Dependendo dos serviços de dados da NetApp que você planeja usar, pode ser necessário criar uma segunda política.

   Para regiões padrão, as permissões são distribuídas em duas políticas. Duas políticas são necessárias devido ao limite máximo de tamanho de caracteres para políticas gerenciadas na AWS. "Saiba mais sobre as políticas do IAM para o agente do Console" .
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 usuário tenha uma chave de acesso que você possa adicionar ao NetApp Console após instalar o agente do Console.

Função do Azure

Crie uma função personalizada do Azure com as permissões necessárias. Você atribuirá essa função à VM do agente do Console.

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 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 pelo sistema na VM para que você possa fornecer as permissões necessárias do Azure por meio de uma função personalizada.

   "Documentação do Microsoft Azure: Configurar 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 Conector" e salvá-los em um arquivo JSON.
3. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

   Você deve adicionar o ID de cada assinatura do Azure que deseja usar com o NetApp Console.

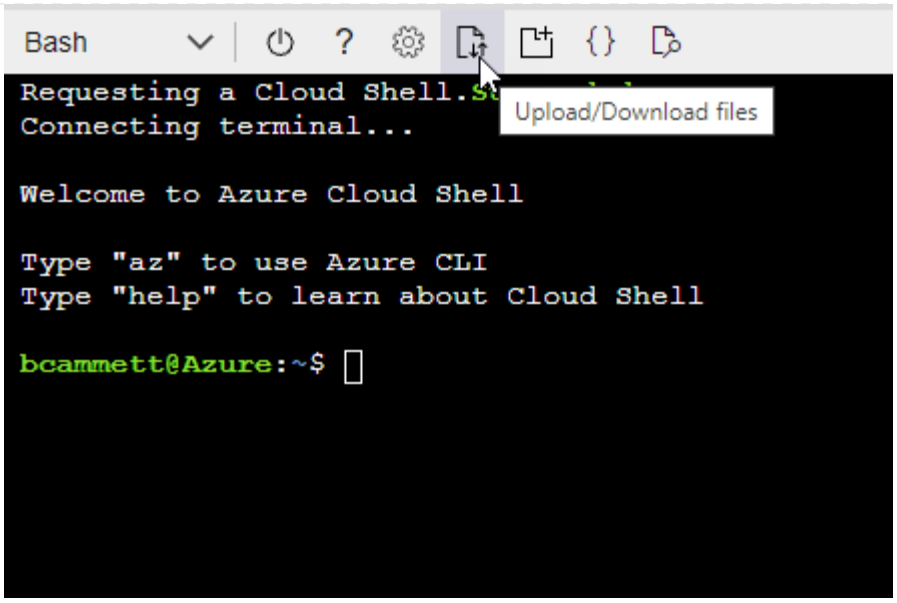
   Exemplo

   ```
   "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. Começar "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 agent_Policy.json
```

Principal de serviço do Azure

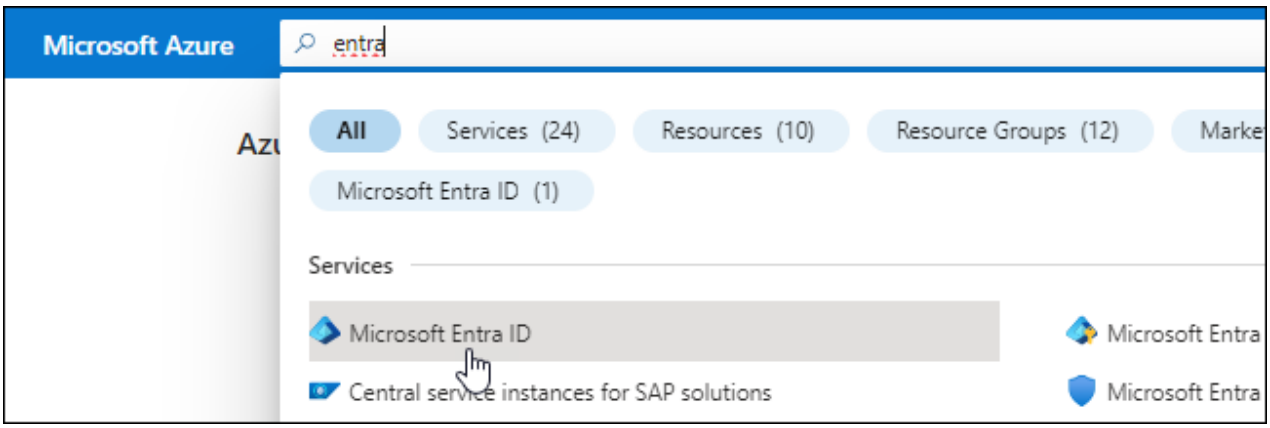
Crie e configure uma entidade de serviço no Microsoft Entra ID e obtenha as credenciais do Azure necessárias para o Console. Você precisa fornecer essas credenciais ao Console depois de instalar o agente do Console.

Crie um aplicativo Microsoft Entra para controle de acesso baseado em função

1. Verifique se você tem permissões no Azure para criar um aplicativo do Active Directory e atribuir o aplicativo a uma função.

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

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



3. No menu, selecione **Registros de aplicativos**.
4. Selecione **Novo registro**.

5. Especifique detalhes sobre o aplicativo:
   - **Nome**: Digite um nome para o aplicativo.
   - **Tipo de conta**: Selecione um tipo de conta (qualquer um funcionará com o NetApp Console).
   - **URI de redirecionamento**: Você pode deixar este campo em branco.
6. Selecione **Registrar**.

   Você criou o aplicativo AD e a entidade de serviço.

Atribuir o aplicativo 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 preferir usar um método diferente, consulte "Documentação do Azure"

   a. Copie o conteúdo do"permissões de função personalizadas para o agente do Console" e salvá-los em um arquivo JSON.

   b. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

      Você deve adicionar o ID de cada assinatura do Azure a partir da qual os usuários criarão sistemas Cloud Volumes ONTAP .

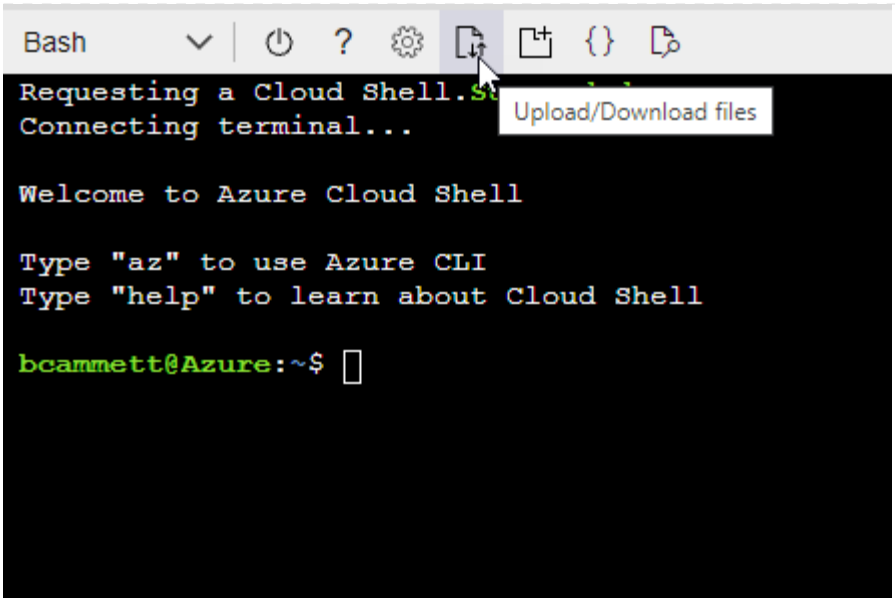
      Exemplo

      ```
      "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.

      - Começar "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 agent_Policy.json
```

Agora você deve ter uma função personalizada chamada Operador do Console que pode ser atribuída à máquina virtual do agente do Console.

2. Atribuir o aplicativo à função:

   a. No portal do Azure, abra o serviço **Assinaturas**.

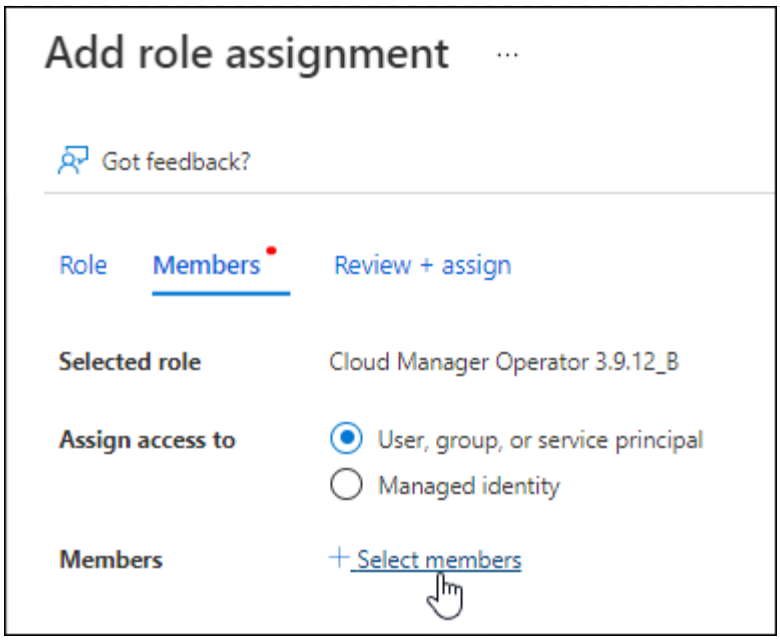
   b. Selecione a assinatura.

   c. Selecione **Controle de acesso (IAM) > Adicionar > Adicionar atribuição de função**.

   d. Na guia **Função**, selecione a função **Operador de console** e selecione **Avançar**.

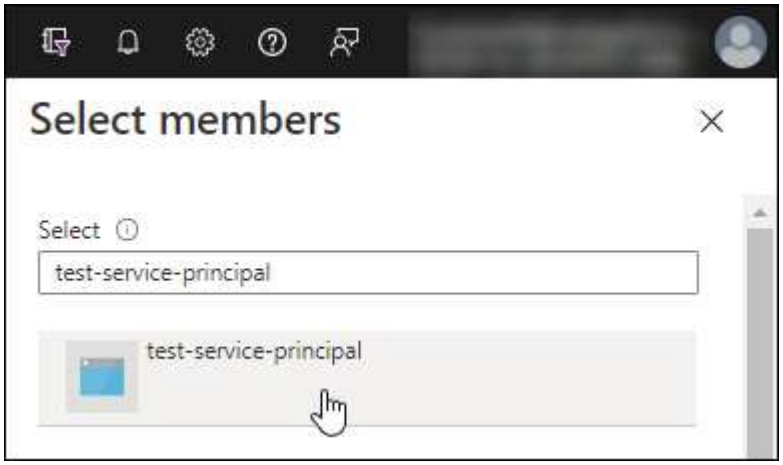
   e. Na aba **Membros**, complete os seguintes passos:

      - Mantenha **Usuário, grupo ou entidade de serviço** selecionado.
      - Selecione **Selecionar membros**.



- Pesquise o nome do aplicativo.

  Aqui está um exemplo:



- Selecione o aplicativo e selecione **Selecionar**.
- Selecione **Avançar**.

f. Selecione **Revisar + atribuir**.

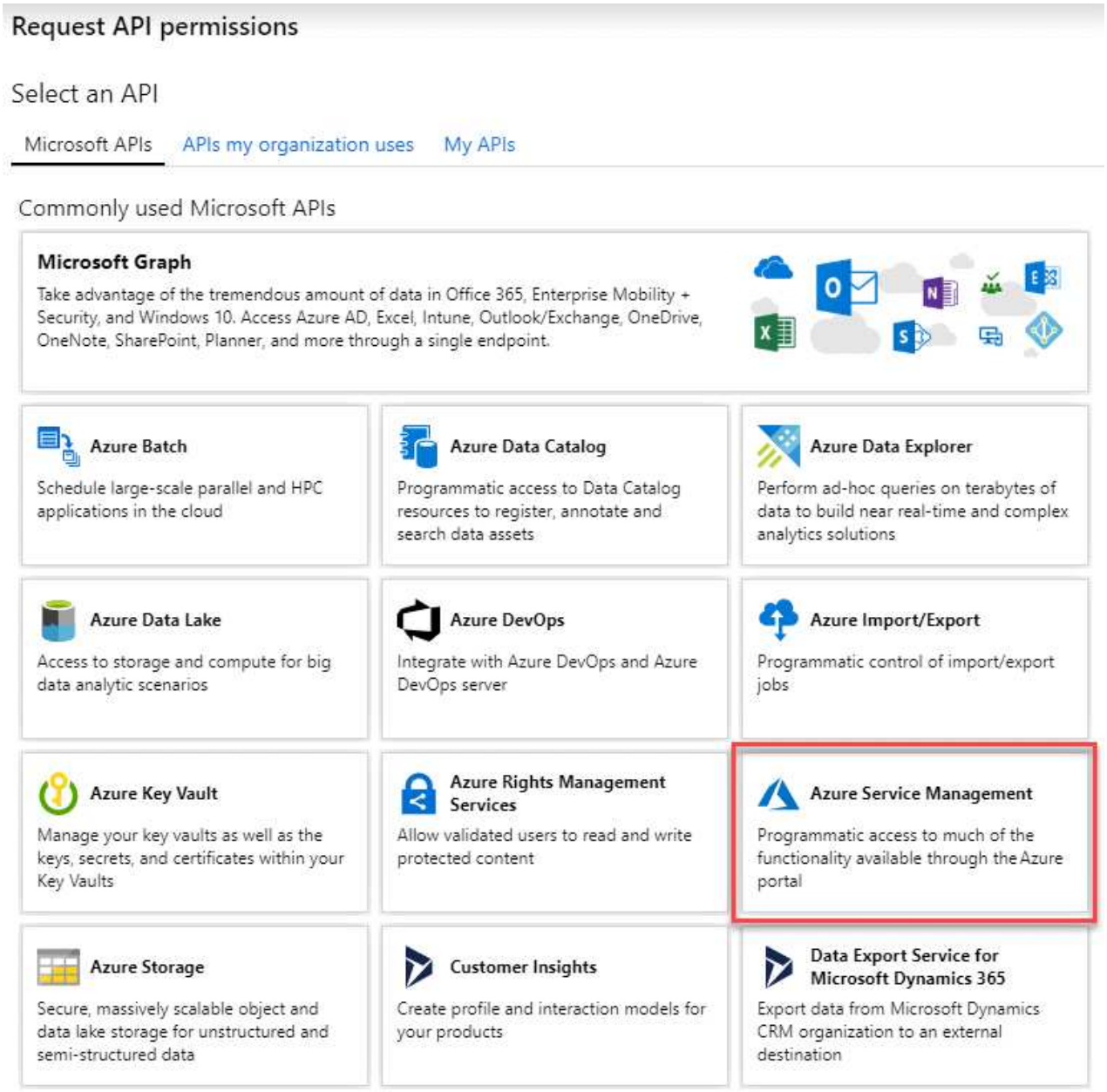
O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

Se você quiser implantar o Cloud Volumes ONTAP de várias assinaturas do Azure, será necessário vincular a entidade de serviço a cada uma dessas assinaturas. No NetApp Console, você pode selecionar a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

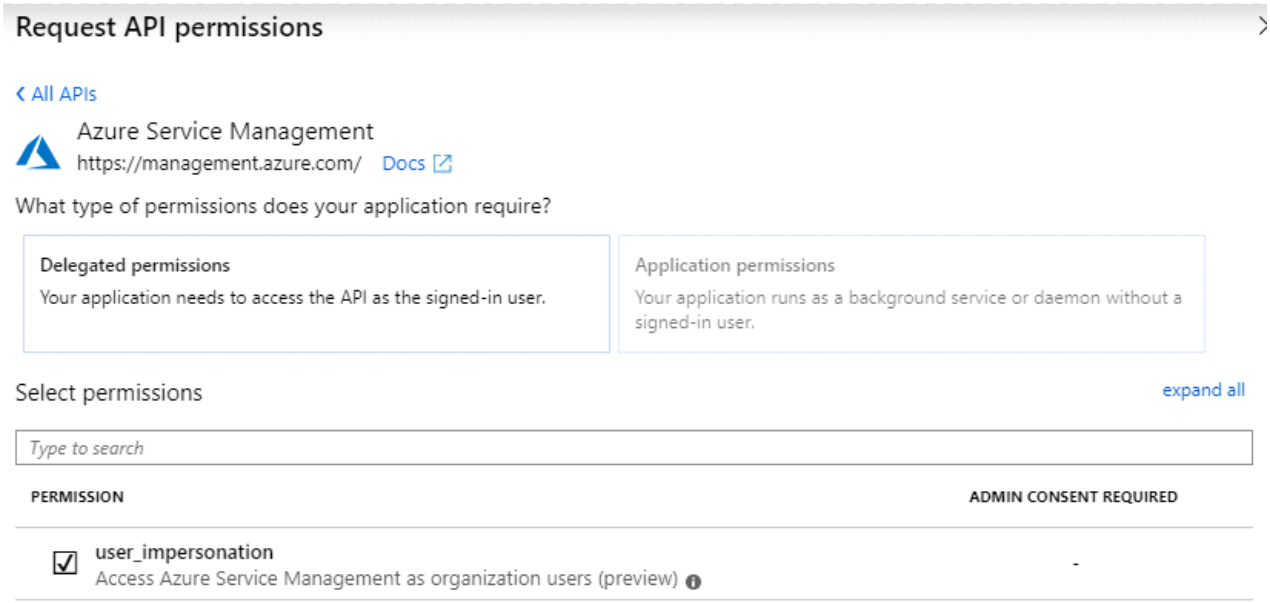
Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Selecione **Permissões de API > Adicionar uma permissão**.

3. Em **APIs da Microsoft**, selecione **Azure Service Management**.

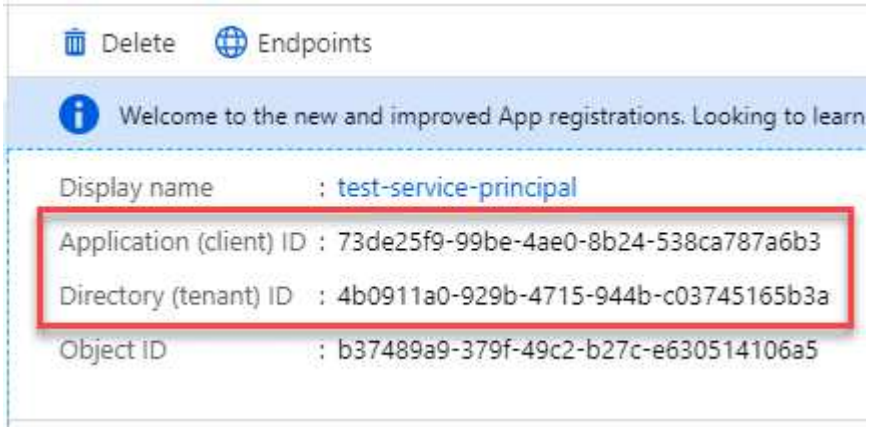


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



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

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



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

Criar um segredo do cliente

1. Abra o serviço **Microsoft Entra ID**.
2. Selecione **Registros de aplicativos** e selecione seu aplicativo.
3. Selecione **Certificados e segredos > Novo segredo do cliente**.
4. Forneça uma descrição do segredo e uma duração.
5. Selecione **Adicionar**.
6. Copie o valor do segredo do cliente.

Resultado

Seu principal serviço agora 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 Console 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 do agente do Console.

Passos

1. Crie uma função personalizada no Google Cloud:

   a. Crie um arquivo YAML que inclua as permissões definidas no"Política do agente do console para o Google Cloud" .

   b. No Google Cloud, ative o Cloud Shell.

   c. Carregue o arquivo YAML que inclui as permissões necessárias para o agente do Console.

   d. Crie uma função personalizada usando o `gcloud iam roles create` comando.

   O exemplo a seguir cria uma função chamada "agente" no nível do projeto:

```
gcloud iam roles create agent --project=myproject --file=agent.yaml
```

   +
   "Documentação do Google Cloud: Criação e gerenciamento de 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.

   "Documentação do Google Cloud: Criação de uma conta de serviço"

Etapa 7: habilitar as APIs do Google Cloud

Várias APIs são necessárias para implantar o Cloud Volumes ONTAP no Google Cloud.

Etapa

1. "Habilite as seguintes APIs do Google Cloud no seu projeto"
    - API do Cloud Infrastructure Manager
    - API do Gerenciador de Implantação em Nuvem V2
    - API de registro em nuvem
    - API do Gerenciador de Recursos de Nuvem
    - API do mecanismo de computação
    - API de gerenciamento de identidade e acesso (IAM)
    - API do Serviço de Gerenciamento de Chaves em Nuvem (KMS)

      (Obrigatório somente se você estiver planejando usar o NetApp Backup and Recovery com chaves de criptografia gerenciadas pelo cliente (CMEK))

Implantar o agente do Console no modo restrito

Implante o agente do Console no modo restrito para que você possa usar o NetApp Console com conectividade de saída limitada. Para começar, instale o agente do Console, configure o Console acessando a interface do usuário que está em execução no agente do Console e, em seguida, forneça as permissões de nuvem que você configurou anteriormente.

Etapa 1: instalar o agente do console

Instale o agente do Console no marketplace do seu provedor de nuvem ou manualmente em um host Linux.

Você precisa preparar seu ambiente antes de instalar o agente do console. Você pode instalar a partir do AWS Marketplace, do Azure Marketplace ou manualmente em seu próprio host Linux executado na AWS, Azure ou Google Cloud.

Marketplace comercial da AWS

Antes de começar

Tenha o seguinte:

- Uma VPC e uma 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 agente do Console.

  "Aprenda a configurar permissões da AWS"

- Permissões para assinar e cancelar a assinatura do AWS Marketplace para seu usuário do IAM.
- Uma compreensão dos requisitos de CPU e RAM para o agente.

  "Revisar requisitos do agente".

- Um par de chaves para a instância EC2.

Passos

1. Vá para o "Listagem do agente do NetApp Console no AWS Marketplace"
2. Na página Marketplace, selecione **Continuar assinando**.
3. Para assinar o software, selecione **Aceitar Termos**.

   O processo de assinatura pode levar alguns minutos.

4. Após a conclusão do processo de assinatura, selecione **Continuar para configuração**.
5. Na página **Configurar este software**, certifique-se de ter selecionado a região correta e selecione **Continuar para iniciar**.
6. Na página **Iniciar este software**, em **Escolher ação**, selecione **Iniciar pelo EC2** e depois selecione **Iniciar**.

   Use o Console do EC2 para iniciar a instância e anexar uma função do IAM. Isso não é possível com a ação **Iniciar do site**.

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 sistemas operacionais**: pule esta seção. O agente do console AMI 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 conectar 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 habilitam os métodos de conexão necessários para a instância do agente do Console: SSH, HTTP e HTTPS.

          "Exibir regras de grupo de segurança para AWS" .

    - **Configurar armazenamento**: Mantenha o tamanho e o tipo de disco padrão para o volume raiz.

      Se você quiser habilitar 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 agente do Console.
    - **Resumo**: Revise o resumo e selecione **Iniciar instância**.

Resultado

A AWS inicia o software com as configurações especificadas. O agente do Console é implantado em aproximadamente cinco minutos.

O que vem a seguir?

Configurar o NetApp Console.

Mercado governamental da AWS

Antes de começar

Tenha o seguinte:

- Uma VPC e uma sub-rede que atendem aos requisitos de rede.

  "Saiba mais sobre os requisitos de rede"

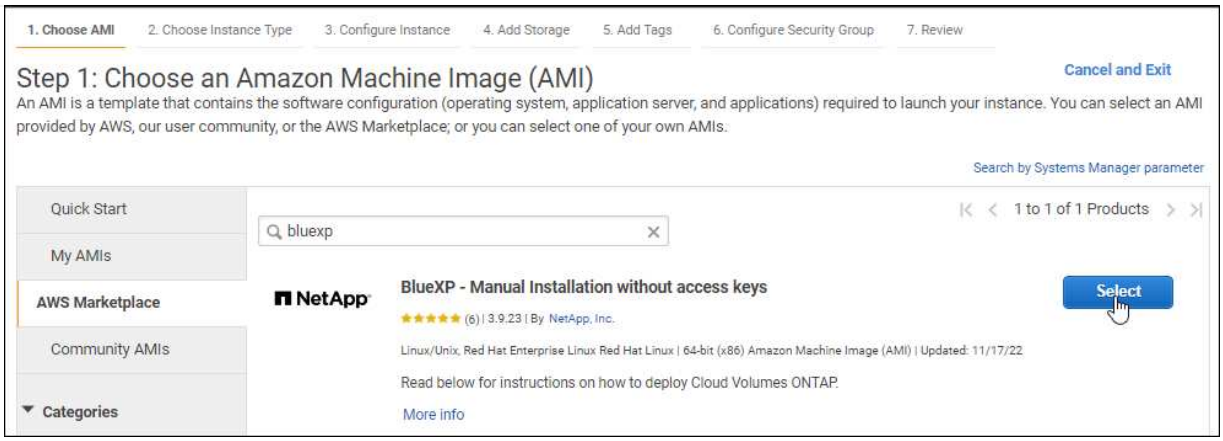
- Uma função do IAM com uma política anexada que inclui as permissões necessárias para o agente do Console.

  "Aprenda a configurar permissões da AWS"

- Permissões para assinar e cancelar a assinatura do AWS Marketplace para seu usuário do IAM.
- Um par de chaves para a instância EC2.

Passos

1. Acesse a oferta do agente do NetApp Console no AWS Marketplace.
    a. Abra o serviço EC2 e selecione **Iniciar instância**.
    b. Selecione **AWS Marketplace**.
    c. Pesquise por NetApp Console e selecione a oferta.



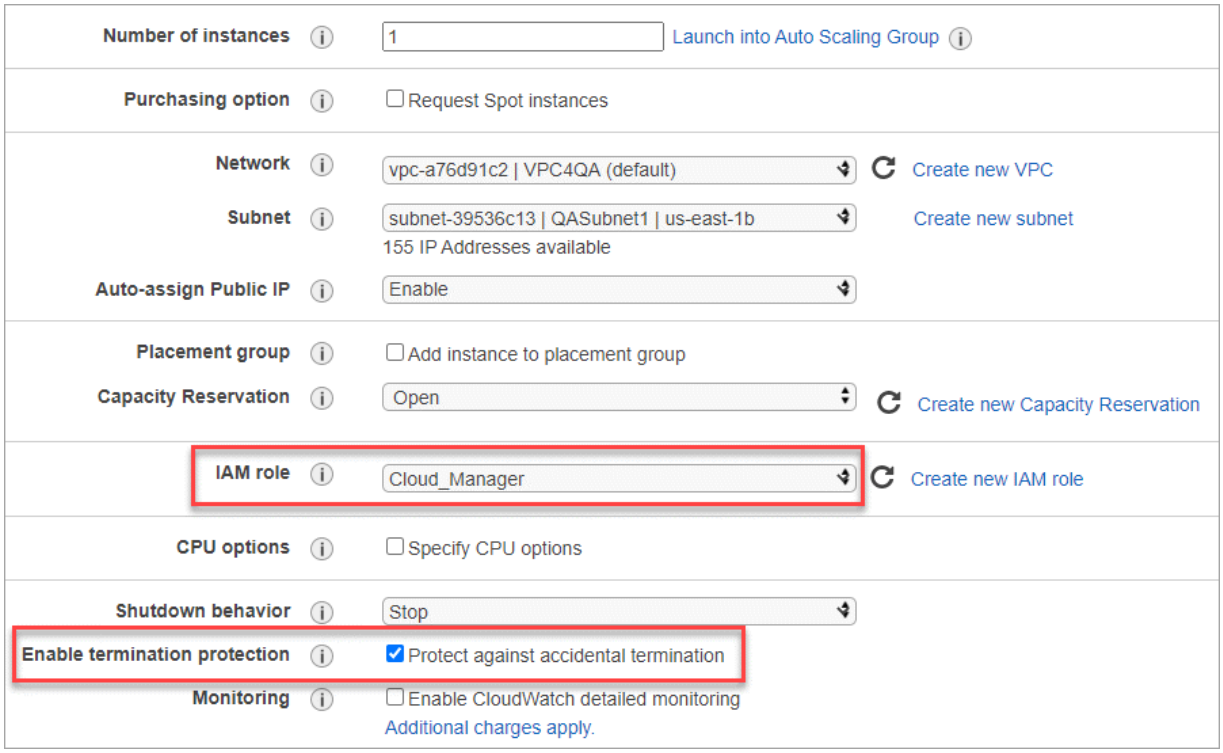
d. Selecione **Continuar**.

2. Siga as instruções para configurar e iniciar a instância:

   - **Escolha um tipo de instância**: Dependendo da disponibilidade da região, escolha um dos tipos de instância suportados (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, habilite a proteção de encerramento (recomendado) e escolha quaisquer outras opções de configuração que atendam aos seus requisitos.



   - **Adicionar armazenamento**: Mantenha as opções de armazenamento padrão.
   - **Adicionar tags**: insira tags para a instância, se desejar.
   - **Configurar grupo de segurança**: especifique os métodos de conexão necessários para a instância do agente do Console: SSH, HTTP e HTTPS.
   - **Revisar**: revise suas seleções e selecione **Iniciar**.

Resultado

A AWS inicia o software com as configurações especificadas. O agente do Console é implantado em aproximadamente cinco minutos.

O que vem a seguir?

Configurar o Console.

Mercado Azure Gov

Antes de começar

Você deve ter o seguinte:

- Uma VNet e uma sub-rede que atendem aos requisitos de rede.

  "Saiba mais sobre os requisitos de rede"

- Uma função personalizada do Azure que inclui as permissões necessárias para o agente do Console.

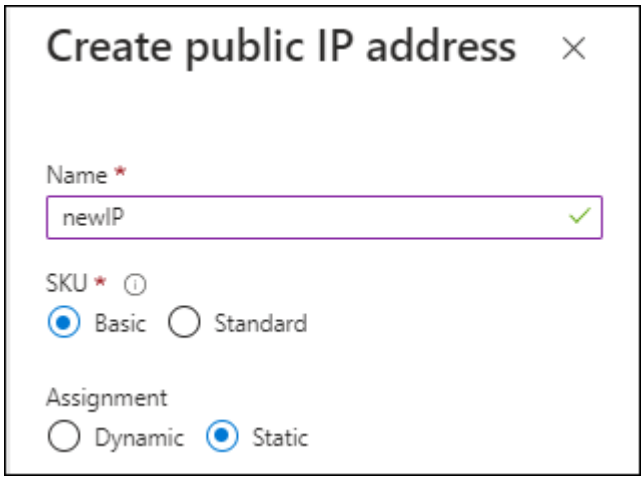
  "Aprenda a configurar permissões do Azure"

Passos

1. Acesse a página da VM do agente do NetApp Console no Azure Marketplace.
   - "Página do Azure Marketplace para regiões comerciais"
   - "Página do Azure Marketplace para regiões do Azure Government"
2. Selecione **Obter agora** e depois 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.
   - **Discos**: O agente do Console pode ter desempenho ideal com discos HDD ou SSD.
   - **IP público**: Para usar um endereço IP público com a VM do agente do Console, selecione uma SKU Básica.



   Se você usar um endereço IP de SKU padrão, o Console usará o endereço IP *privado* do agente do Console, em vez do IP público. Se o computador que você usa para acessar o Console não

conseguir alcançar o endereço IP privado, o Console não funcionará.

"Documentação do Azure: SKU de IP público"

- **Grupo de segurança de rede**: O agente do Console requer conexões de entrada usando SSH, HTTP e HTTPS.

  "Exibir regras de grupo de segurança para o Azure" .

- **Identidade**: Em **Gerenciamento**, selecione **Ativar identidade gerenciada atribuída pelo sistema**.

  Uma identidade gerenciada permite que a VM do agente do Console se identifique para o Microsoft Entra ID sem a necessidade de credenciais. "Saiba mais sobre identidades gerenciadas para recursos do Azure" .

4. Na página **Revisar + criar**, 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 agente do console devem estar em execução em aproximadamente cinco minutos.

O que vem a seguir?

Configurar o NetApp Console.

Instalação manual (obrigatória para o Google Cloud)

Você pode instalar o agente do Console manualmente em seu próprio host Linux em execução na AWS, Azure ou Google Cloud.

Antes de começar

Você deve ter o seguinte:

- Privilégios de root para instalar o agente do Console.
- Detalhes sobre um servidor proxy, caso um proxy seja necessário para acesso à Internet a partir do agente do Console.

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

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

  Não é possível definir um certificado para um servidor proxy transparente ao instalar manualmente o agente do Console. Se precisar definir um certificado para um servidor proxy transparente, você deverá usar o Console de Manutenção após a instalação. Saiba mais sobre o"Console de manutenção do agente" .

- Você precisa desabilitar a verificação de configuração que verifica a conectividade de saída durante a instalação. A instalação manual falhará se esta verificação não estiver desabilitada."Aprenda como desabilitar verificações de configuração para instalações manuais."
- Dependendo do seu sistema operacional, o Podman ou o Docker Engine será necessário antes de instalar o agente do Console.

Sobre esta tarefa

Após a instalação, o agente do Console 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. Baixe o software do agente do Console e copie-o para o host Linux. Você pode baixá-lo tanto do NetApp Console quanto do site de suporte da NetApp .
   - NetApp Console: Acesse **Agentes > Gerenciamento > Implantar agente > Local > Instalação manual**.

     Escolha baixar os arquivos de instalação do agente ou um URL para os arquivos.

   - Site de suporte da NetApp (necessário caso você ainda não tenha acesso ao Console) "Site de suporte da NetApp" ,

3. Atribua permissões para executar o script.

   ```
   chmod +x NetApp_Console_Agent_Cloud_<version>
   ```

   Onde <versão> é a versão do agente do Console que você baixou.

4. Se estiver instalando em um ambiente de nuvem governamental, desative as verificações de configuração."Aprenda como desabilitar verificações de configuração para instalações manuais."

5. Execute o script de instalação.

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

   Você precisará adicionar informações de proxy se sua rede exigir um proxy para acesso à internet. Você pode adicionar um proxy explícito durante a instalação. Os parâmetros `--proxy` e `--cacert` são opcionais e você não será solicitado a adicioná-los. Se você tiver um servidor proxy explícito, precisará inserir os parâmetros conforme mostrado.

   Se você deseja configurar um proxy transparente, pode fazê-lo após a instalação. "Saiba mais sobre o console de manutenção do agente."

+

Aqui está um exemplo de configuração de um servidor proxy explícito com um certificado assinado por uma CA:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

+
`--proxy` configura o agente do Console para usar um servidor proxy HTTP ou HTTPS usando um dos seguintes formatos:

+ * http://endereço:porta * http://nome-do-usuário:senha@endereço:porta * http://nome-do-domínio%92nome-do-usuário:senha@endereço:porta * https://endereço:porta * https://nome-do-usuário:senha@endereço:porta * https://nome-do-domínio%92nome-do-usuário:senha@endereço:porta

+ Observe o seguinte:

+ **O usuário pode ser um usuário local ou um usuário de domínio.** Para um usuário de domínio, você deve usar o código ASCII para uma \ conforme mostrado acima. **O agente do Console não oferece suporte a nomes de usuário ou senhas que incluam o caractere @.** Se a senha incluir algum dos seguintes caracteres especiais, você deve escapar esse caractere especial adicionando uma barra invertida antes dele: & ou !

+ Por exemplo:

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

1. Se você usou o Podman, precisará ajustar a porta aardvark-dns.

   a. SSH para a máquina virtual do agente do Console.

   b. Abra o arquivo podman */usr/share/containers/containers.conf* e modifique a porta escolhida para o serviço DNS do Aardvark. Por exemplo, altere para 54.

      ```
      vi /usr/share/containers/containers.conf
      ```

      Por exemplo:

   ```
   # Port to use for dns forwarding daemon with netavark in rootful
   bridge
   # mode and dns enabled.
   # Using an alternate port might be useful if other DNS services
   should
   # run on the machine.
   #
   dns_bind_port = 54
   ```

   a. Reinicie a máquina virtual do agente do Console.

Resultado

O agente do Console agora está instalado. No final da instalação, o serviço do agente do Console (occm) será reiniciado duas vezes se você tiver especificado um servidor proxy.

O que vem a seguir?

Configurar o NetApp Console.

Etapa 2: configurar o NetApp Console

Ao acessar o console pela primeira vez, você será solicitado a escolher uma organização para o agente do Console e precisará habilitar o modo restrito.

Antes de começar

A pessoa que configura o agente do Console deve fazer login no Console usando um login que ainda não pertença a uma organização do Console.

Se o seu login estiver associado a outra organização, você precisará se cadastrar com um novo login. Caso contrário, você não verá a opção para ativar o modo restrito na tela de configuração.

Passos

1. Abra um navegador da Web em um host que tenha uma conexão com a instância do agente do Console e insira a seguinte URL do agente do Console que você instalou.
2. Inscreva-se ou faça login no NetApp Console.
3. Após efetuar login, configure o Console:

    a. Digite um nome para o agente do Console.

    b. Insira um nome para uma nova organização do Console.

    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 a conta for criada. Você não poderá ativar o modo restrito mais tarde, nem desativá-lo mais tarde.

    Se você implantou o agente do Console em uma região governamental, a caixa de seleção já estará habilitada e não poderá ser alterada. Isso ocorre porque o modo restrito é o único modo suportado nas regiões governamentais.

    a. Selecione **Vamos começar**.

Resultado

O agente do Console agora está instalado e configurado com sua organização do Console. Todos os usuários precisam acessar o Console usando o endereço IP da instância do agente do Console.

O que vem a seguir?

Forneça ao Console as permissões que você configurou anteriormente.

Etapa 3: fornecer permissões ao agente do Console

Se você instalou o agente do Console a partir do Azure Marketplace ou manualmente, será necessário conceder as permissões que você configurou anteriormente.

Essas etapas não se aplicam se você implantou o agente do Console do AWS Marketplace porque escolheu a

função do IAM necessária durante a implantação.

"Aprenda a preparar permissões de nuvem" .

Função do AWS IAM

Anexe a função do IAM que você criou anteriormente à instância do EC2 onde instalou o agente do Console.

Estas etapas se aplicam somente se você instalou manualmente o agente do Console na AWS. Para implantações do AWS Marketplace, você já associou a instância do agente do Console a uma função do IAM que inclui as permissões necessárias.

Passos

1. Acesse o console do Amazon EC2.
2. Selecione **Instâncias**.
3. Selecione a instância do agente do Console.
4. Selecione **Ações > Segurança > Modificar função do IAM**.
5. Selecione a função do IAM e selecione **Atualizar função do IAM**.

Chave de acesso AWS

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

Passos

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

Função do Azure

Acesse o portal do Azure e atribua a função personalizada do Azure à máquina virtual do agente do Console para uma ou mais assinaturas.

Passos

1. No Portal do Azure, abra o serviço **Assinaturas** e selecione sua assinatura.

   É importante atribuir a função do serviço **Assinaturas** porque isso especifica o escopo da atribuição de função no nível da assinatura. O *escopo* 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 no NetApp Console será afetada.

   "Documentação do Microsoft Azure: Entenda o escopo do RBAC do Azure"

2. Selecione **Controle de acesso (IAM)** > **Adicionar** > **Adicionar atribuição de função**.
3. Na guia **Função**, selecione a função **Operador de console** e selecione **Avançar**.

Operador do console é o nome padrão fornecido na política. Se você escolheu um nome diferente para a função, selecione esse nome.

4. Na aba **Membros**, complete os seguintes passos:
   a. Atribuir acesso a uma **Identidade gerenciada**.
   b. Selecione **Selecionar membros**, selecione a assinatura na qual a máquina virtual do agente do Console foi criada, em **Identidade gerenciada**, escolha **Máquina virtual** e selecione a máquina virtual do agente do Console.
   c. Selecione **Selecionar**.
   d. Selecione **Avançar**.
   e. Selecione **Revisar + atribuir**.
   f. Se você quiser gerenciar recursos em assinaturas adicionais do Azure, alterne para essa assinatura e repita essas etapas.

Principal de serviço do Azure

Forneça ao NetApp Console as credenciais para a entidade de serviço do Azure que você configurou anteriormente.

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Localização das credenciais**: Selecione **Microsoft Azure > Agente**.
   b. **Definir credenciais**: insira informações sobre a entidade de serviço do Microsoft Entra que concede as permissões necessárias:
      - ID do aplicativo (cliente)
      - ID do diretório (inquilino)
      - Segredo do cliente
   c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.
   d. **Revisar**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

Resultado

O NetApp Console 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 agente do Console.

Passos

1. Acesse o portal do Google Cloud e atribua a conta de serviço à instância de VM do agente do Console.

   "Documentação do Google Cloud: Alterando a conta de serviço e os escopos de acesso de uma instância"

2. Se você quiser gerenciar recursos em outros projetos, conceda acesso adicionando a conta de serviço com a função de agente do Console a esse projeto. Você precisará repetir esta etapa para cada projeto.

Assine o NetApp Intelligent Services (modo restrito)

Assine o NetApp Intelligent Services no marketplace do seu provedor de nuvem para pagar por serviços de dados a uma taxa por hora (PAYGO) ou por meio de um contrato anual. Se você comprou uma licença da NetApp (BYOL), também precisa assinar a oferta do marketplace. Sua licença é sempre cobrada primeiro, mas você será cobrado pela taxa horária se exceder sua capacidade licenciada ou se o prazo da licença expirar.

Uma assinatura de mercado permite cobrar pelos seguintes serviços de dados com modo restrito:

- NetApp Backup and Recovery
- Cloud Volumes ONTAP
- NetApp Cloud Tiering
- NetApp Ransomware Resilience
- NetApp Disaster Recovery

A NetApp Data Classification é habilitada por meio de sua assinatura, mas não há cobrança pelo uso da classificação.

Antes de começar

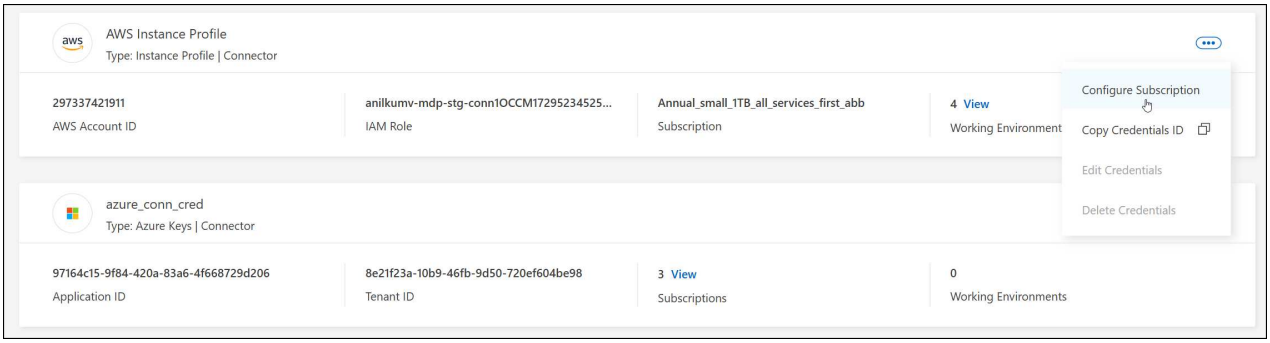
Você já deve ter implantado um agente do Console para assinar serviços de dados. Você precisa associar uma assinatura do marketplace às credenciais de nuvem conectadas a um agente do Console.

AWS

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Credenciais da organização**.
3. Selecione o menu de ação para um conjunto de credenciais associadas a um agente do Console e selecione **Configurar assinatura**.

   Você deve selecionar credenciais associadas a um agente do Console. Não é possível associar uma assinatura do marketplace a credenciais associadas ao NetApp Console.



4. Para associar as credenciais a uma assinatura existente, selecione a assinatura na lista suspensa e selecione **Configurar**.
5. 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 **Inscrever-se**.

   c. Selecione **Configurar sua conta**.

      Você será redirecionado para o NetApp Console.

   d. Na página **Atribuição de Assinatura**:

      - Selecione as organizações ou contas do Console às quais você gostaria de associar esta assinatura.
      - No campo **Substituir assinatura existente**, escolha se deseja substituir automaticamente a assinatura existente de uma organização ou conta por esta nova assinatura.

        O Console substitui a assinatura existente para todas as credenciais na organização ou conta por esta 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 essas etapas.

   - Selecione **Salvar**.

Azul

Passos

1. Selecione **Administração > Credenciais**.

2. Selecione **Credenciais da organização**.
3. Selecione o menu de ação para um conjunto de credenciais associadas a um agente do Console e selecione **Configurar assinatura**.

   Você deve selecionar credenciais associadas a um agente do Console. Não é possível associar uma assinatura do marketplace a credenciais associadas ao NetApp Console.

4. Para associar as credenciais a uma assinatura existente, selecione a assinatura na lista suspensa e selecione **Configurar**.
5. 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 **Inscrever-se**.

   c. Preencha o formulário e selecione **Inscrever-se**.

   d. Após a conclusão do processo de assinatura, selecione **Configurar conta agora**.

      Você será redirecionado para o NetApp Console.

   e. Na página **Atribuição de Assinatura**:

      - Selecione as organizações ou contas do Console às quais você gostaria de associar esta assinatura.
      - No campo **Substituir assinatura existente**, escolha se deseja substituir automaticamente a assinatura existente de uma organização ou conta por esta nova assinatura.

        O Console substitui a assinatura existente para todas as credenciais na organização ou conta por esta nova assinatura. Se um conjunto de credenciais nunca foi associado a uma assinatura, essa nova assinatura não será associada a essas credenciais.

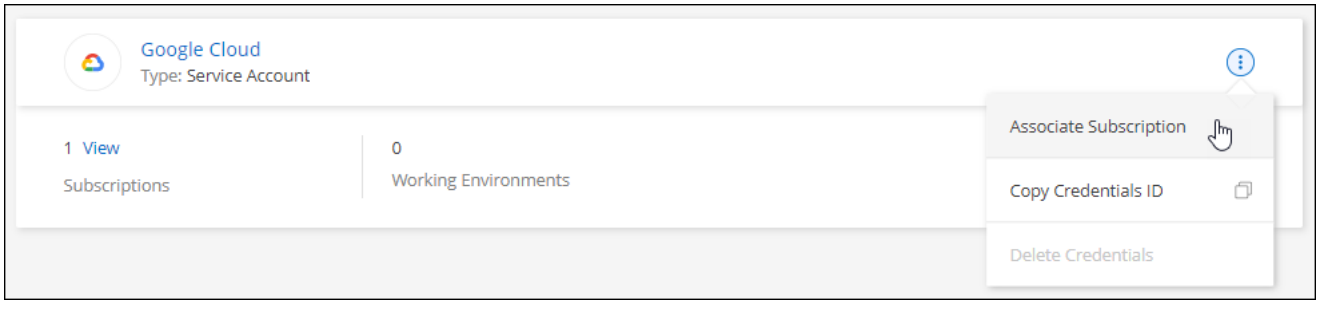
   Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo essas etapas.

   - Selecione **Salvar**.

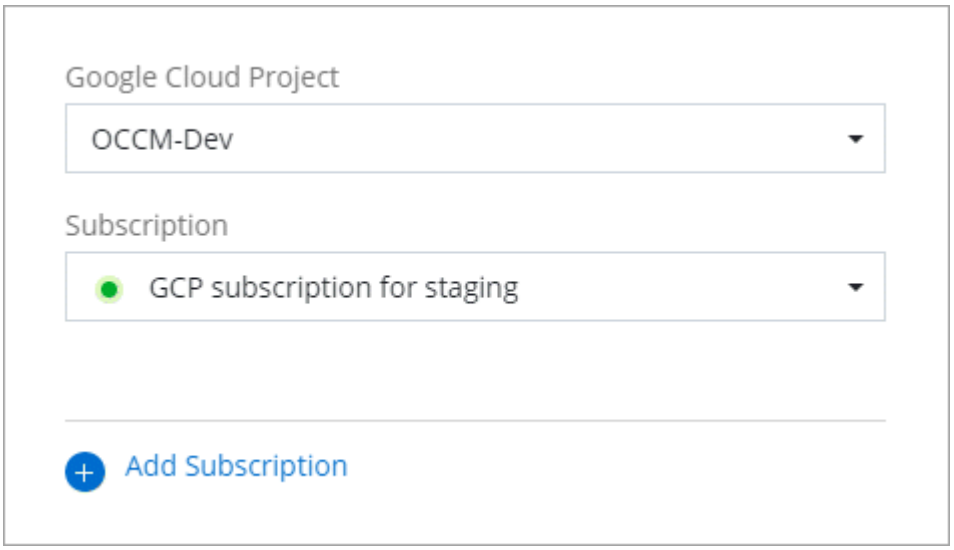
Google Cloud

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Credenciais da organização**.
3. Selecione o menu de ação para um conjunto de credenciais associadas a um agente do Console e selecione **Configurar assinatura**.



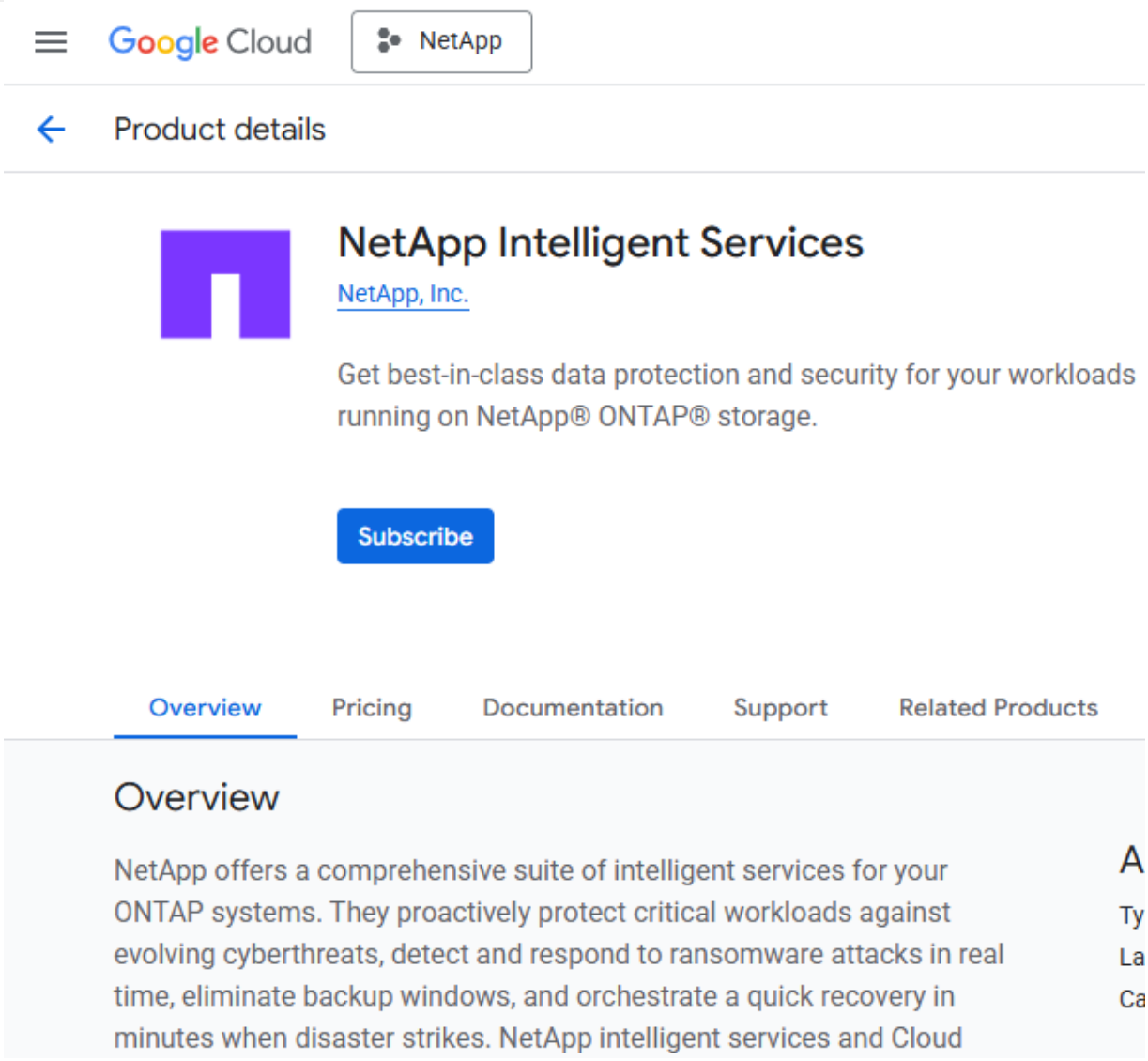
1. Para configurar uma assinatura existente com as credenciais selecionadas, selecione um projeto e uma assinatura do Google Cloud na lista suspensa e selecione **Configurar**.



2. 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, verifique se você tem privilégios de administrador de cobrança na sua conta do Google Cloud, bem como um login no NetApp Console .

   a. Depois de ser redirecionado para o "Página do NetApp Intelligent Services no Google Cloud Marketplace" , certifique-se de que o projeto correto esteja selecionado no menu de navegação superior.

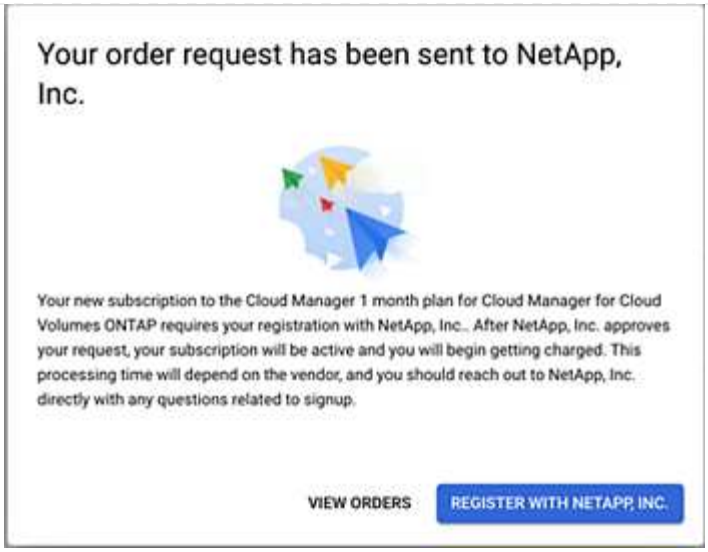


b. Selecione **Inscrever-se**.
c. Selecione a conta de cobrança apropriada e concorde com os termos e condições.
d. Selecione **Inscrever-se**.

   Esta etapa envia sua solicitação de transferência para a NetApp.

e. Na caixa de diálogo pop-up, selecione **Registrar-se na NetApp, Inc.**

   Esta etapa deve ser concluída para vincular a assinatura do Google Cloud à sua organização ou conta do Console. O processo de vinculação de uma assinatura não estará concluído até que você seja redirecionado desta página e faça login no Console.



f. Conclua as etapas na página **Atribuição de assinatura**:

> Se alguém da sua organização já tiver uma assinatura de mercado da sua conta de cobrança, você será redirecionado para "a página Cloud Volumes ONTAP no NetApp Console" em vez de. Se isso for inesperado, entre em contato com sua equipe de vendas da NetApp . O Google permite apenas uma assinatura por conta de cobrança do Google.

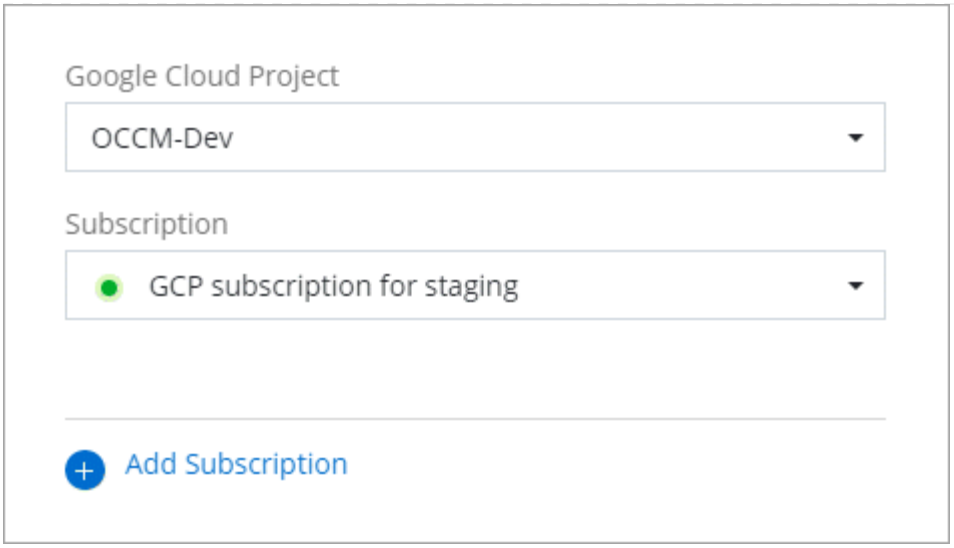
- Selecione a organização do Console à qual você gostaria de associar esta assinatura.
- No campo **Substituir assinatura existente**, escolha se deseja substituir automaticamente a assinatura existente de uma organização por esta nova assinatura.

  O Console substitui a assinatura existente para todas as credenciais na organização por esta 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 essas etapas.

- Selecione **Salvar**.

3. Quando esse processo estiver concluído, volte para a página Credenciais no Console e selecione esta nova assinatura.



Informações relacionadas

- "Gerenciar licenças baseadas em capacidade BYOL para Cloud Volumes ONTAP"
- "Gerenciar licenças BYOL para serviços de dados"
- "Gerenciar credenciais e assinaturas da AWS"
- "Gerenciar credenciais e assinaturas do Azure"
- "Gerenciar credenciais e assinaturas do Google Cloud"

O que você pode fazer a seguir (modo restrito)

Depois de começar a usar o NetApp Console no modo restrito, você poderá começar a usar os serviços suportados no modo restrito.

Para obter ajuda, consulte a documentação destes serviços:

- "Documentação do Azure NetApp Files"
- "Documentos de backup e recuperação"
- "Documentação de classificação"
- "Documentação do Cloud Volumes ONTAP"
- "Documentos de carteira digital"
- "Documentação do cluster ONTAP local"
- "Documentação de replicação"

Informações relacionadas

"Modos de implantação do NetApp Console"

Comece a usar o modo privado

Fluxo de trabalho de introdução (modo privado BlueXP)

O modo privado BlueXP (interface BlueXP legada) normalmente é usado com ambientes locais que não têm conexão com a Internet e com regiões de nuvem seguras, o que inclui AWS Secret Cloud, AWS Top Secret Cloud e Azure IL6. A NetApp continua a oferecer suporte a esses ambientes com a interface legada BlueXP .

"Documentação em PDF para o modo privado do BlueXP"

Recursos e serviços de dados suportados com o modo privado

A tabela a seguir pode ajudar você a identificar rapidamente quais serviços e recursos do BlueXP são suportados no modo privado.

Observe que alguns serviços podem ter suporte com limitações.

Área de produtos	Serviço ou recurso BlueXP	Modo privado
Ambientes de trabalho Esta parte da tabela lista o suporte para gerenciamento de ambientes de trabalho a partir da tela BlueXP . Não indica os destinos de backup suportados para BlueXP backup and recovery.	Amazon FSx para ONTAP	Não
	Amazon S3	Não
	Blob do Azure	Não
	Azure NetApp Files	Não
	Cloud Volumes ONTAP	Sim
	Google Cloud NetApp Volumes	Não
	Armazenamento em nuvem do Google	Não
	Clusters ONTAP locais	Sim
	Série E	Não
	StorageGRID	Não

Área de produtos	Serviço ou recurso BlueXP	Modo privado
Serviços	Alertas	Não
	Backup e recuperação	Simhttps://docs.netapp.com/us-en/data-services-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-no-internet-connectivity["Veja a lista de destinos de backup suportados para dados de volume ONTAP"^]
	Classificação	Sim
	Copiar e sincronizar	Não
	Consultor digital	Não
	carteira digital	Sim
	Recuperação de desastres	Não
	Eficiência econômica	Não
	Resiliência ao Ransomware	Não
	Replicação	Sim
	Atualizações de software	Não
	Sustentabilidade	Não
	Hierarquização	Não
	Cache de volume	Não
	Fábrica de carga de trabalho	Não
Características	Gerenciamento de identidade e acesso	Sim
	Credenciais	Sim
	Federação	Não
	Autenticação multifator	Não
	Contas NSS	Não
	Notificações	Não
	Procurar	Não
	Linha do tempo	Sim

Informações sobre direitos autorais

Informações sobre marcas comerciais