Documentação de configuração e administração do NetApp Console

NetApp Console setup and administration

NetApp
October 07, 2025

Índice

Documentação de configuração e administração do NetApp Console

Notas de lançamento

O que há de novo

Saiba o que há de novo nos recursos de administração do NetApp Console: gerenciamento de identidade e acesso (IAM), agentes do Console, credenciais do provedor de nuvem e muito mais.

6 de outubro de 2025

BlueXP agora é NetApp Console

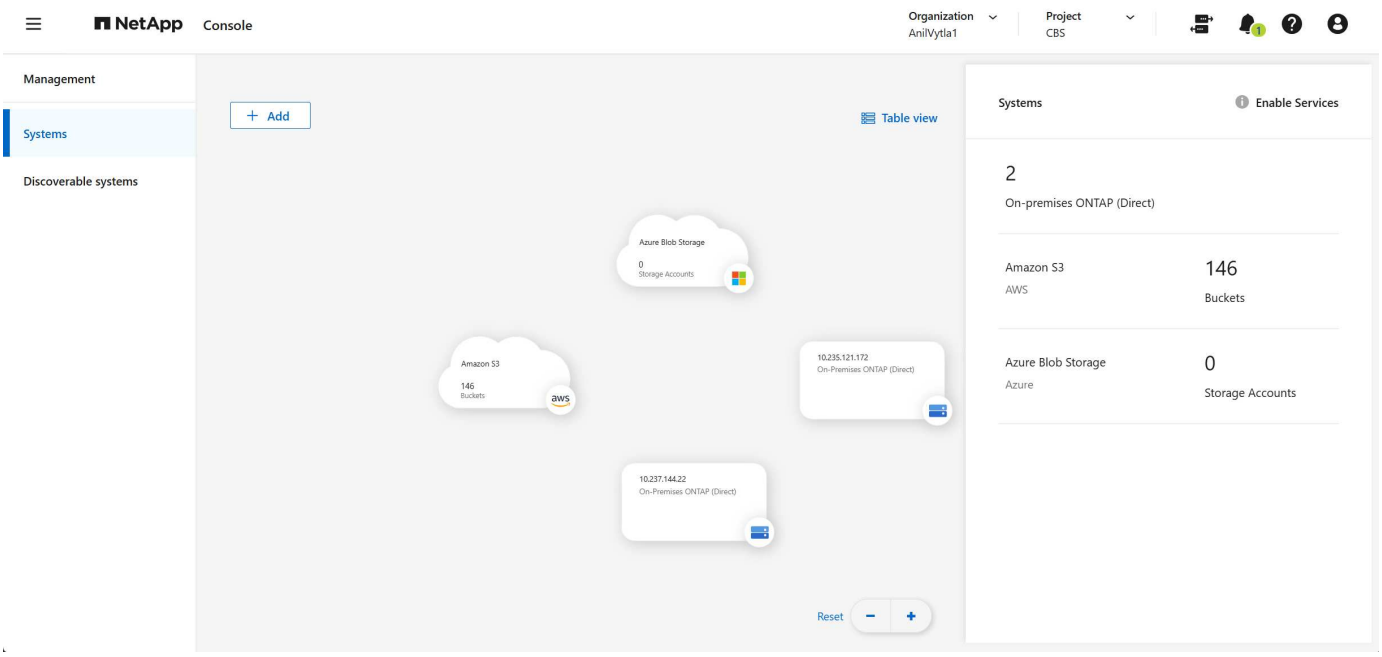
O NetApp Console, criado com base na base aprimorada e reestruturada do BlueXP , fornece gerenciamento centralizado do armazenamento NetApp e do NetApp Data Services em ambientes locais e na nuvem em nível empresarial, fornecendo insights em tempo real, fluxos de trabalho mais rápidos e administração simplificada, altamente segura e compatível.

Menus e páginas de navegação

A NetApp moveu a maioria das opções de menu para o painel de navegação esquerdo e reorganizou os menus para facilitar a navegação no NetApp Console.

A tela é substituída pela página Sistemas

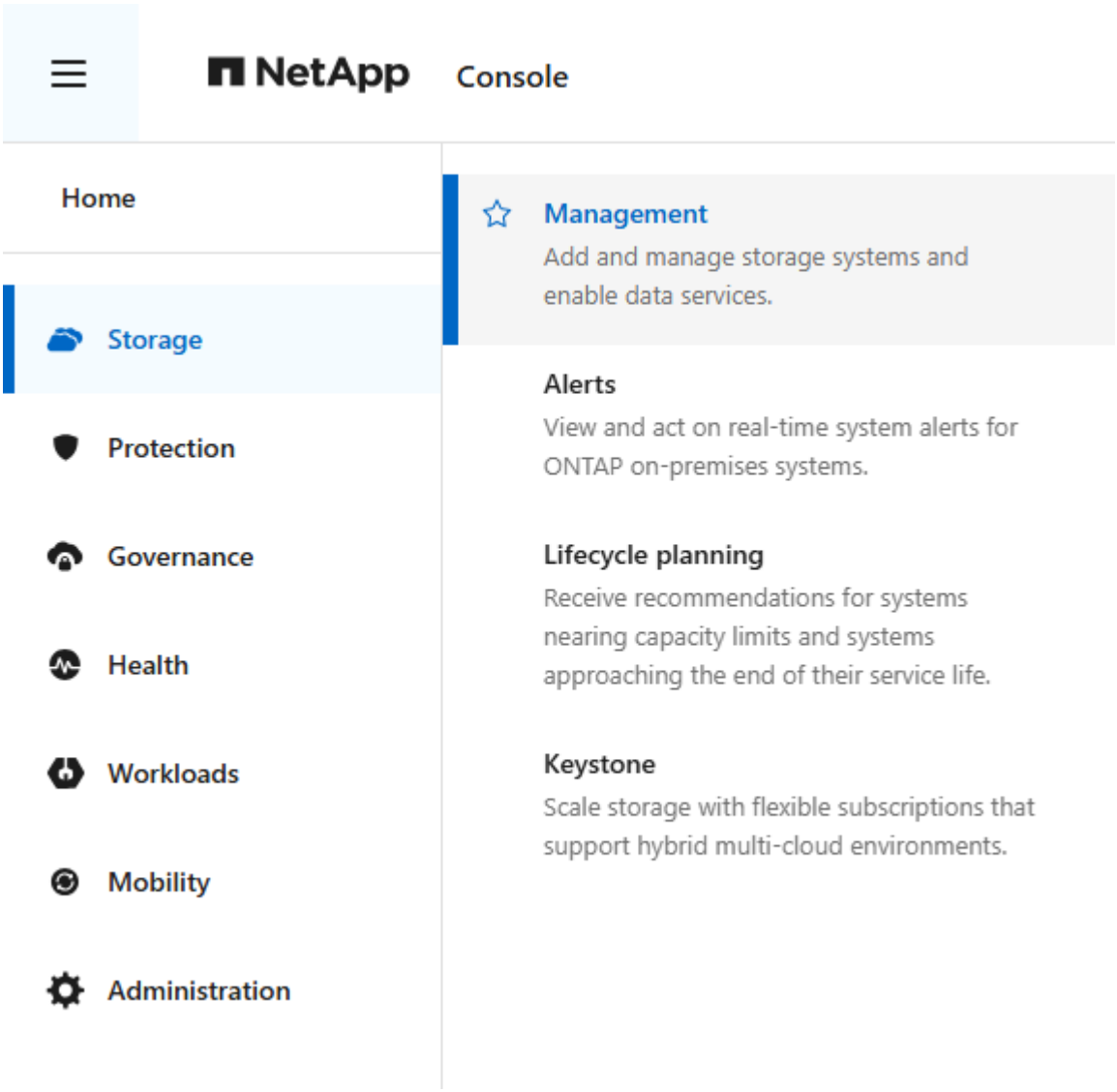
A NetApp renomeou o Canvas para a página **Sistemas**. Navegue até a página **Sistema** no menu **Armazenamento > Gerenciamento**.



Menu de armazenamento expandido

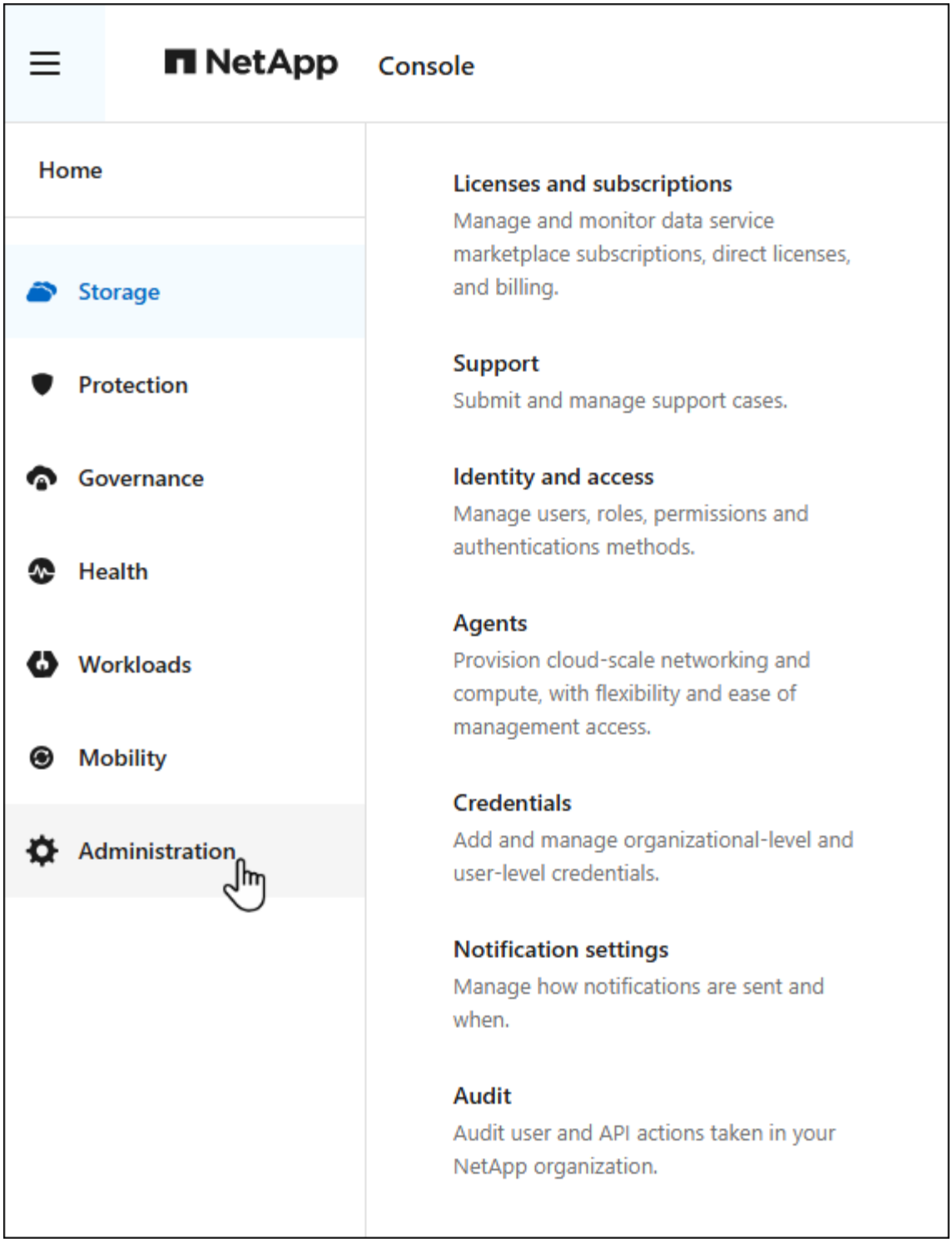
O menu **Armazenamento** inclui **Alertas** para visualizar alertas do sistema ONTAP e **Planejamento do ciclo de vida** (anteriormente **Eficiência econômica**) para identificar recursos não utilizados ou subutilizados.

A NetApp moveu o Keystone para o menu **Armazenamento**, onde você pode gerenciar suas assinaturas do NetApp Keystone e visualizar seu uso.



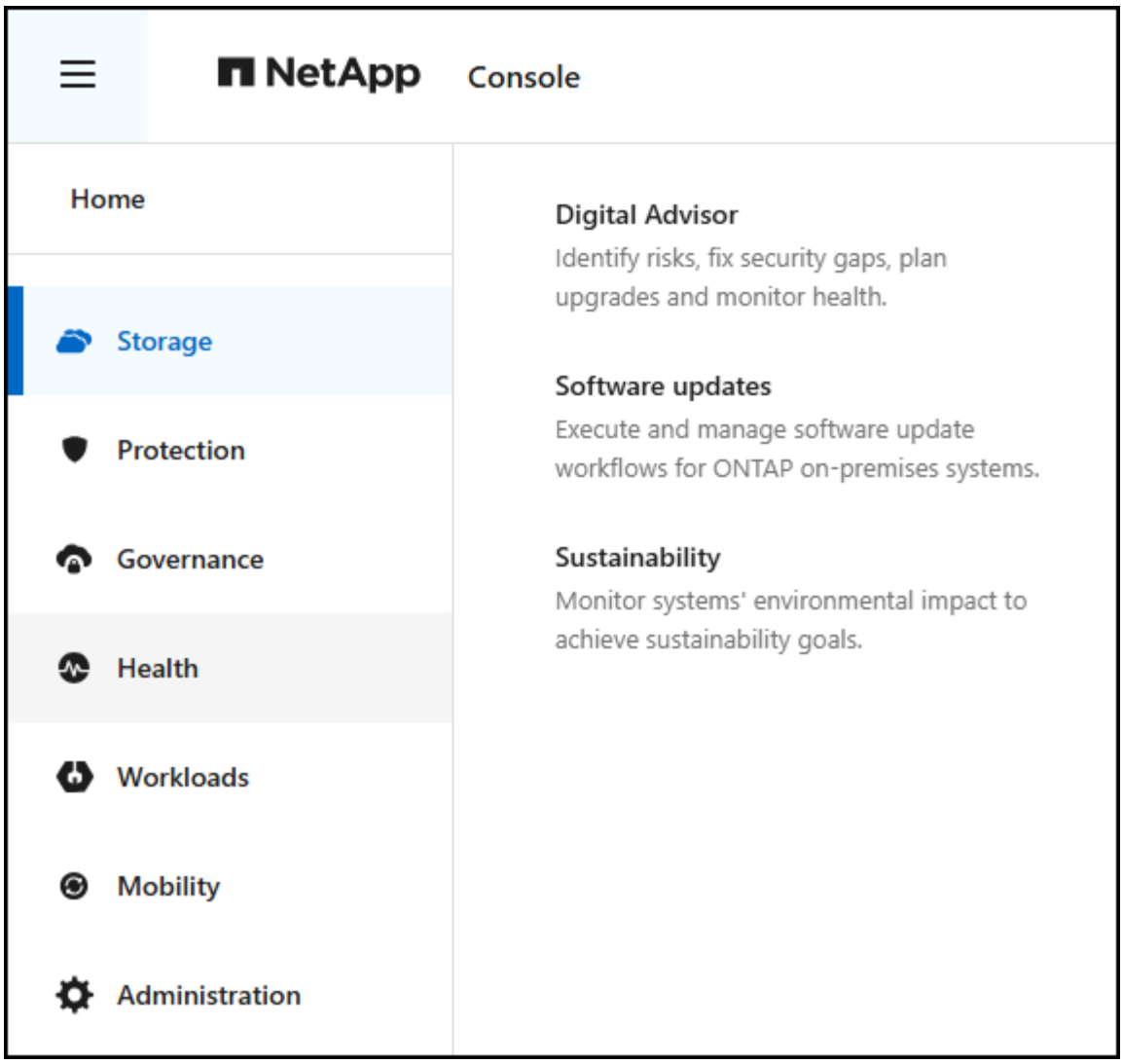
Menu de administração

Use o menu centralizado **Administração** para gerenciar o NetApp Console, casos de suporte, licenças e assinaturas (anteriormente chamado de carteira digital).



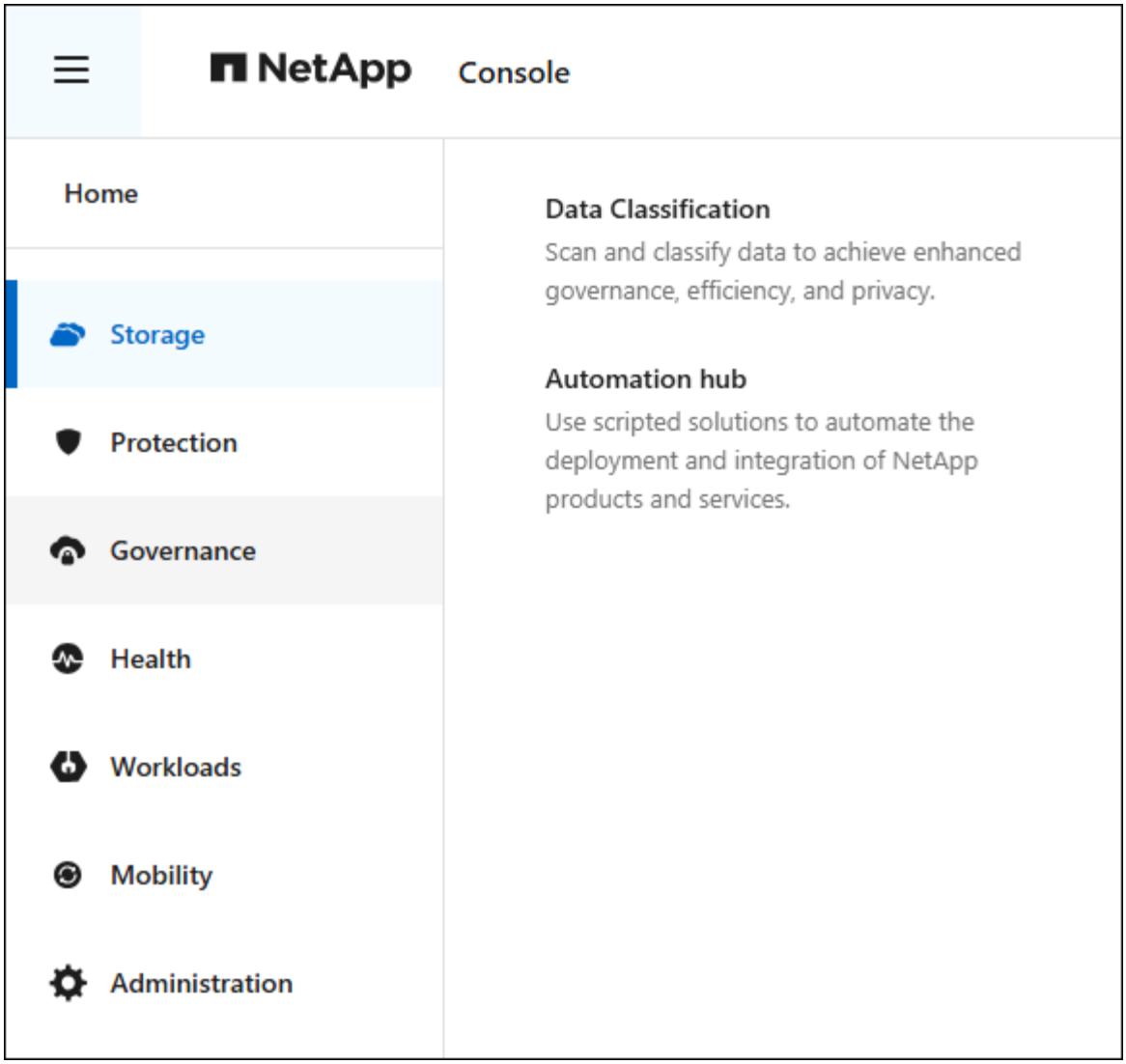
Cardápio de saúde

Um menu eficiente de **Saúde** inclui **Atualizações de software**, onde você pode gerenciar atualizações de software ONTAP , **Sustentabilidade**, onde você pode monitorar seu impacto ambiental, e * Digital Advisor*, onde você pode obter recomendações proativas para otimizar seu ambiente de armazenamento.



Menu de governança

O menu **Governança** inclui **Classificação de Dados**, onde você pode gerenciar a classificação e a conformidade de dados, e o **Hub de Automação**, onde você pode criar e gerenciar fluxos de trabalho de automação.



Nomenclatura mais intuitiva de elementos, serviços de dados e recursos

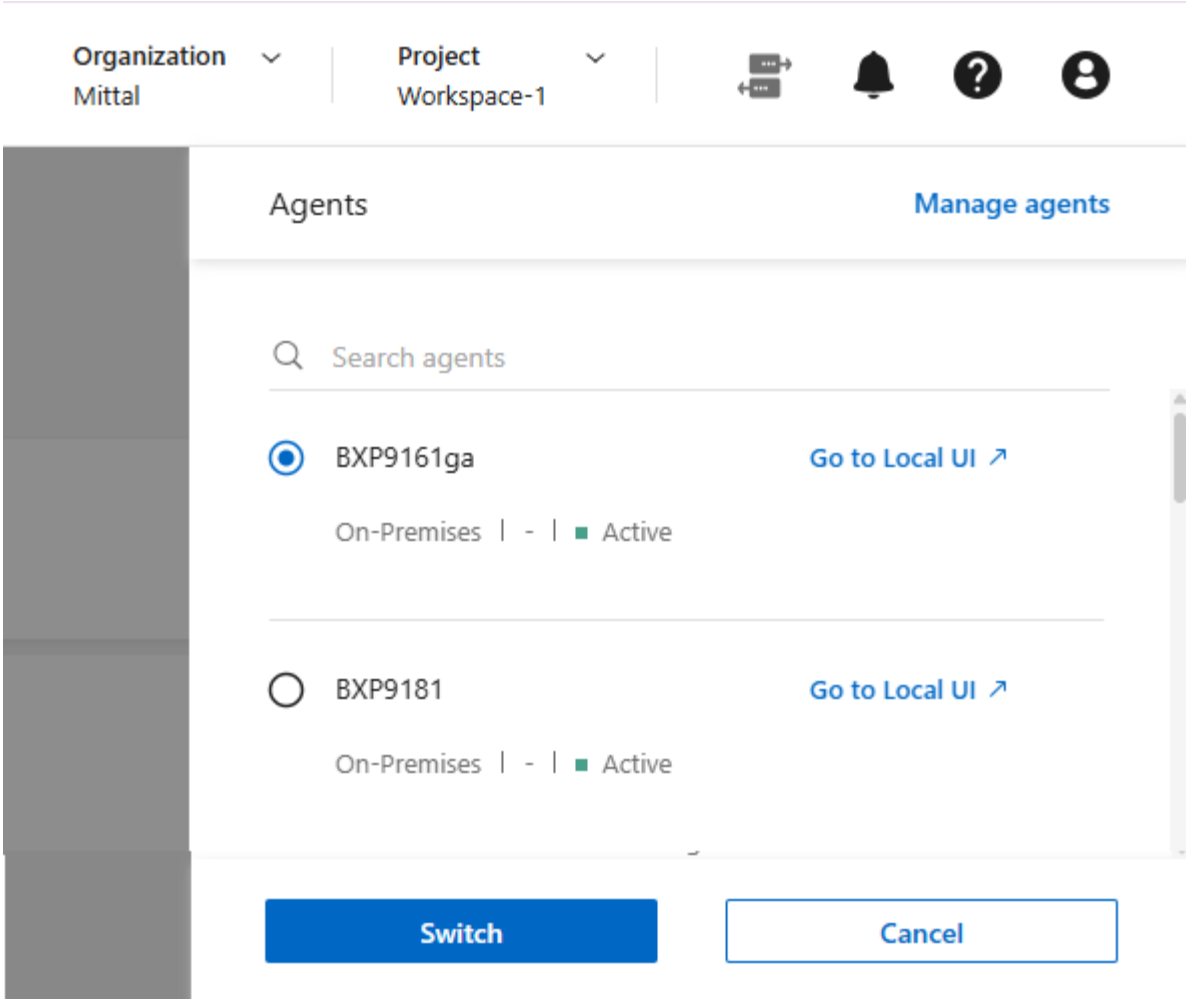
A NetApp renomeou vários elementos, serviços de dados e recursos para esclarecer sua finalidade. As principais mudanças incluem:

Nome anterior	* Nome do console NetApp *
Conectores	Agentes de console. Visualize, adicione e gerencie seus agentes no menu **Administração > Agentes**.
Página da linha do tempo	Página de auditoria Visualize a atividade do Console de auditoria no menu **Administração > Auditoria**.

Nome anterior	* Nome do console NetApp *
Ambientes de trabalho	Sistemas Visualize, adicione e gerencie seus sistemas no menu **Armazenamento > Gerenciamento**.
Proteção BlueXP Ransomware	Resiliência do NetApp Ransomware. O Ransomware Resilience ajuda você a proteger seus dados e se recuperar rapidamente de um ataque de ransomware.
Eficiência Econômica BlueXP	Planejamento do ciclo de vida. O planejamento do ciclo de vida ajuda você a otimizar seus custos de armazenamento identificando recursos não utilizados e subutilizados. Acesse o planejamento do ciclo de vida no menu **Armazenamento > Planejamento do ciclo de vida**.
BlueXP digital wallet	Licenças e assinaturas Acesse suas licenças e assinaturas no menu **Administração > Licenças e assinaturas**.

Agentes de console

Acesse e gerencie seus agentes do Console no menu **Administração > Agentes**. A NetApp mudou a forma de selecionar um agente de Console para a página **Sistemas** (antigamente Canvas). A NetApp substituiu o nome do menu Conector por um ícone  , permitindo que você selecione o agente do Console cujos sistemas você deseja visualizar.



Você também pode gerenciar seus agentes no menu **Administração > Agentes**.

Agente de console 4.0.0

Esta versão do agente do Console inclui melhorias de segurança, correções de bugs e os seguintes novos recursos.

A versão 4.0.0 está disponível para modo padrão e modo restrito.

Consolidação e redução de pontos de extremidade de rede necessários

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" .
- "Saiba mais sobre os pontos de extremidade necessários."

Suporte para implantação de agentes de console no VCenter

Você pode implantar agentes do Console em ambientes VMware usando um arquivo OVA. O arquivo OVA inclui uma imagem de VM pré-configurada com software de agente do Console e configurações para conectar

ao NetApp Console. Um download de arquivo ou implantação de URL está disponível diretamente no NetApp Console."Aprenda a implantar um agente de console em ambientes VMware."

O agente de console OVA para VMware oferece uma imagem de VM pré-configurada para implantação rápida.

Relatórios de validação para implantações de agentes com falha

Ao implantar um agente do Console a partir do NetApp Console, agora você tem a opção de validar a configuração do agente. Se o Console não conseguir implantar o agente, ele fornecerá um relatório para download para ajudar você a solucionar o problema.

Solução de problemas aprimorada para agentes do Console

O agente do Console melhorou as mensagens de erro que ajudam você a entender melhor os problemas."Aprenda a solucionar problemas de agentes do Console."

Console NetApp

A administração do NetApp Console inclui os seguintes novos recursos:

Painel da página inicial

O painel da página inicial do NetApp Console fornece visibilidade em tempo real da infraestrutura de armazenamento com métricas de integridade, capacidade, status da licença e serviços de dados."Saiba mais sobre a página inicial."

Assistente NetApp

Novos usuários com a função de administrador da organização podem usar o assistente do NetApp para configurar o Console, incluindo adicionar um agente, vincular uma conta de suporte do NetApp e adicionar um sistema de armazenamento."Saiba mais sobre o assistente NetApp ."

Autenticação de conta de serviço

O NetApp Console oferece suporte à autenticação de conta de serviço usando um ID de cliente gerado pelo sistema e JWTs secretos ou gerenciados pelo cliente, permitindo que as organizações selecionem a abordagem que melhor se adapta aos seus requisitos de segurança e fluxos de trabalho de integração. A autenticação de cliente JWT de chave privada usa criptografia assimétrica, fornecendo segurança mais forte do que métodos tradicionais de ID de cliente e segredo. A autenticação de cliente JWT de chave privada usa criptografia assimétrica, mantendo a chave privada segura no ambiente do cliente, reduzindo os riscos de roubo de credenciais e melhorando a segurança da sua pilha de automação e dos aplicativos do cliente."Saiba como adicionar uma conta de serviço."

Tempo limite de sessão

O sistema desconecta os usuários após 24 horas ou quando eles fecham o navegador.

Apoio a parcerias entre organizações

Você pode criar parcerias no NetApp Console que permitem que os parceiros gerenciem com segurança os recursos do NetApp em todos os limites organizacionais, facilitando a colaboração e fortalecendo a segurança. "Aprenda a gerir parcerias" .

Funções de superadministrador e supervisualizador

Adicionadas as funções **Superadministrador** e **Supervisualizador**. **Superadministrador** concede acesso de gerenciamento total aos recursos do Console, armazenamento e serviços de dados. **Super visualizador** fornece visibilidade somente leitura para auditores e partes interessadas. Essas funções são úteis para equipes menores de membros seniores, onde o amplo acesso é comum. Para maior segurança e capacidade de auditoria, as organizações são incentivadas a usar o acesso de **Superadministrador** com moderação e atribuir funções refinadas sempre que possível."Saiba mais sobre funções de acesso."

Função adicional para Resiliência de Ransomware

Adicionadas as funções **Administrador de comportamento do usuário de resiliência ao ransomware** e **Visualizador de comportamento do usuário de resiliência ao ransomware**. Essas funções permitem que os usuários configurem e visualizem o comportamento do usuário e os dados analíticos, respectivamente."Saiba mais sobre funções de acesso."

Chat de suporte removido

A NetApp removeu o recurso de chat de suporte do NetApp Console. Use a página **Administração > Suporte** para criar e gerenciar casos de suporte.

11 de agosto de 2025

Conector 3.9.55

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

A versão 3.9.55 está disponível para modo padrão e modo restrito.

Suporte ao idioma japonês

A interface do usuário do BlueXP agora está disponível em japonês. Se o idioma do seu navegador for japonês, o BlueXP será exibido em japonês. Para acessar a documentação em japonês, use o menu de idiomas no site de documentação.

Recurso de resiliência operacional

O recurso de resiliência operacional foi removido do BlueXP. Entre em contato com o suporte da NetApp se tiver problemas.

Gerenciamento de Identidade e Acesso (IAM) BlueXP

O Gerenciamento de Identidade e Acesso no BlueXP agora oferece o seguinte recurso.

Nova função de acesso para suporte operacional

O BlueXP agora oferece suporte à função de analista de suporte operacional. Esta função concede ao usuário permissões para monitorar alertas de armazenamento, visualizar o cronograma de auditoria do BlueXP e inserir e rastrear casos de suporte da NetApp .

"Saiba mais sobre o uso de funções de acesso."

31 de julho de 2025

Lançamento do modo privado (3.9.54)

Uma nova versão do modo privado já está disponível para download no "Site de suporte da NetApp"

A versão 3.9.54 inclui atualizações para os seguintes componentes e serviços do BlueXP .

Componente ou serviço	Versão incluída nesta versão	Mudanças desde o lançamento anterior do modo privado
Conector	3.9.54, 3.9.53	Vá para o "o que há de novo na página BlueXP" e consulte as alterações incluídas nas versões 3.9.54 e 3.9.53.
Backup e recuperação	28 de julho de 2025	Vá para o "o que há de novo na página de BlueXP backup and recovery" e consulte as alterações incluídas no comunicado de julho de 2025.
Classificação	14 de julho de 2025 (versão 1.45)	Vá para o "o que há de novo na página de BlueXP classification" .

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

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

21 Julho 2025

Suporte para Google Cloud NetApp Volumes

Agora você pode visualizar o Google Cloud NetApp Volumes no BlueXP."Saiba mais sobre o Google Cloud NetApp Volumes."

Gerenciamento de Identidade e Acesso (IAM) BlueXP

Nova função de acesso para o Google Cloud NetApp Volumes

O BlueXP agora oferece suporte ao uso de uma função de acesso para o seguinte sistema de armazenamento:

- Google Cloud NetApp Volumes

"Saiba mais sobre o uso de funções de acesso."

14 Julho 2025

Conector 3.9.54

Esta versão do BlueXP Connector inclui melhorias de segurança, correções de bugs e os seguintes novos recursos:

- Suporte para proxies transparentes para conectores dedicados ao suporte de serviços Cloud Volumes ONTAP ."Saiba mais sobre como configurar um proxy transparente."
- Capacidade de usar tags de rede para ajudar a rotear o tráfego do Connector quando o Connector é implantado em um ambiente do Google Cloud.
- Notificações adicionais no produto para monitoramento de integridade do Connector, incluindo uso de CPU e RAM.

No momento, a versão 3.9.54 está disponível para modo padrão e modo restrito.

Gerenciamento de Identidade e Acesso (IAM) BlueXP

O Gerenciamento de Identidade e Acesso no BlueXP agora oferece os seguintes recursos:

- Suporte para IAM no modo privado, permitindo que você gerencie o acesso do usuário e as permissões para serviços e aplicativos BlueXP .
- Gerenciamento simplificado de federações de identidade, incluindo navegação mais fácil, opções mais claras para configurar conexões federadas e melhor visibilidade das federações existentes.
- Funções de acesso para BlueXP backup and recovery, BlueXP disaster recovery e gerenciamento de federação.

Suporte para IAM no modo privado

O BlueXP agora oferece suporte ao IAM no modo privado, permitindo que você gerencie o acesso do usuário e as permissões para serviços e aplicativos do BlueXP . Esse aprimoramento permite que clientes do modo privado aproveitem o controle de acesso baseado em função (RBAC) para melhor segurança e conformidade.

"Saiba mais sobre o IAM no BlueXP."

Gestão simplificada de federações de identidade

O BlueXP agora oferece uma interface mais intuitiva para gerenciar a federação de identidades. Isso inclui navegação mais fácil, opções mais claras para configurar conexões federadas e melhor visibilidade das federações existentes.

Habilitar o logon único (SSO) por meio da federação de identidade permite que os usuários façam login no BlueXP com suas credenciais corporativas. Isso melhora a segurança, reduz o uso de senhas e simplifica a integração.

Você será solicitado a importar quaisquer conexões federadas existentes para a nova interface para obter acesso aos novos recursos de gerenciamento. Isso permite que você aproveite os aprimoramentos mais recentes sem precisar recriar suas conexões federadas."Saiba mais sobre como importar sua conexão federada existente para o BlueXP."

O gerenciamento aprimorado da federação permite que você:

- Adicione mais de um domínio verificado a uma conexão federada, permitindo que você use vários domínios com o mesmo provedor de identidade (IdP).
- Desabilite ou exclua conexões federadas quando necessário, dando a você controle sobre o acesso e a

segurança do usuário.

- Controle o acesso ao gerenciamento da federação com funções do IAM.

"Saiba mais sobre federação de identidade no BlueXP."

Novas funções de acesso para BlueXP backup and recovery, BlueXP disaster recovery e gerenciamento de federação

O BlueXP agora oferece suporte ao uso de funções do IAM para os seguintes recursos e serviços de dados:

- BlueXP backup and recovery
- BlueXP disaster recovery
- Federação

"Saiba mais sobre o uso de funções de acesso."

9 de junho de 2025

Conector 3.9.53

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

A versão 3.9.53 está disponível para modo padrão e modo restrito.

Alertas de uso de espaço em disco

O Centro de Notificações agora inclui alertas para uso de espaço em disco no Conector."Saber mais."

Melhorias de auditoria

A Linha do tempo agora inclui eventos de login e logout para usuários. Você pode ver a atividade de login, o que pode ajudar na auditoria e no monitoramento de segurança. Os usuários da API que têm a função de administrador da organização podem visualizar o endereço de e-mail do usuário que efetuou login, incluindo o `includeUserData=true` parâmetro como no seguinte: `/audit/<account_id>?includeUserData=true` .

Gerenciamento de assinaturas Keystone disponível no BlueXP

Você pode gerenciar sua assinatura do NetApp Keystone pelo BlueXP.

"Saiba mais sobre o gerenciamento de assinaturas do Keystone no BlueXP."

Gerenciamento de Identidade e Acesso (IAM) BlueXP

Autenticação multifator (MFA)

Usuários não federados podem habilitar o MFA para suas contas BlueXP para melhorar a segurança. Os administradores podem gerenciar as configurações do MFA, incluindo redefinir ou desabilitar o MFA para usuários, conforme necessário. Isso é suportado apenas no modo padrão.

"Saiba mais sobre como configurar a autenticação multifator para você." "Saiba mais sobre como administrar a autenticação multifator para usuários."

Cargas de trabalho

Agora você pode visualizar e excluir credenciais do Amazon FSx for NetApp ONTAP na página Credenciais no BlueXP.

29 de maio de 2025

Lançamento do modo privado (3.9.52)

Uma nova versão do modo privado já está disponível para download no "Site de suporte da NetApp"

A versão 3.9.52 inclui atualizações para os seguintes componentes e serviços do BlueXP .

Componente ou serviço	Versão incluída nesta versão	Mudanças desde o lançamento anterior do modo privado
Conector	3.9.52, 3.9.51	Vá para o "o que há de novo na página do conector BlueXP" e consulte as alterações incluídas nas versões 3.9.52 e 3.9.50.
Backup e recuperação	12 de maio de 2025	Vá para o "o que há de novo na página de BlueXP backup and recovery" e consulte as alterações incluídas no comunicado de maio de 2025.
Classificação	12 de maio de 2025 (versão 1.43)	Vá para o "o que há de novo na página de BlueXP classification" e consulte as alterações incluídas nas versões 1.38 a 1.371.41.

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

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

12 de maio de 2025

Conector 3.9.52

Esta versão do BlueXP Connector inclui pequenas melhorias de segurança e correções de bugs, bem como algumas atualizações adicionais.

No momento, a versão 3.9.52 está disponível para modo padrão e modo restrito.

Suporte para Docker 27 e Docker 28

O Docker 27 e o Docker 28 agora são suportados pelo Connector.

Cloud Volumes ONTAP

Os nós do Cloud Volumes ONTAP não desligam mais quando o Conector não está em conformidade ou fica

inativo por mais de 14 dias. O Cloud Volumes ONTAP ainda envia mensagens de gerenciamento de eventos quando perde o acesso ao conector. Essa alteração garante que o Cloud Volumes ONTAP possa continuar operando mesmo se o Conector ficar inativo por um longo período. Isso não altera os requisitos de conformidade do Conector.

Administração Keystone disponível no BlueXP

A versão beta do NetApp Keystone no BlueXP adicionou acesso à administração do Keystone . Você pode acessar a página de inscrição para o NetApp Keystone beta na barra de navegação esquerda do BlueXP.

Gerenciamento de Identidade e Acesso (IAM) BlueXP

Novas funções de gerenciamento de armazenamento

As funções de administrador de armazenamento, especialista em integridade do sistema e visualizador de armazenamento estão disponíveis e podem ser atribuídas aos usuários.

Essas funções permitem que você gerencie quem na sua organização pode descobrir e gerenciar recursos de armazenamento, bem como visualizar informações de integridade do armazenamento e executar atualizações de software.

Essas funções são suportadas para controlar o acesso aos seguintes recursos de armazenamento:

- Sistemas da série E
- Sistemas StorageGRID
- Sistemas ONTAP locais

Você também pode usar essas funções para controlar o acesso aos seguintes serviços BlueXP :

- Atualizações de software
- Consultor digital
- Resiliência operacional
- Eficiência econômica
- Sustentabilidade

As seguintes funções foram adicionadas:

- **Administrador de armazenamento**

  Administrar a integridade do armazenamento, a governança e a descoberta dos recursos de armazenamento na organização. Essa função também pode executar atualizações de software em recursos de armazenamento.

- **Especialista em saúde do sistema**

  Administrar a integridade e a governança do armazenamento para os recursos de armazenamento na organização. Essa função também pode executar atualizações de software em recursos de armazenamento. Esta função não pode modificar ou excluir ambientes de trabalho.

- **Visualizador de armazenamento**

  Visualize informações sobre integridade do armazenamento e dados de governança.

"Saiba mais sobre funções de acesso."

14 de abril de 2025

Conector 3.9.51

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

No momento, a versão 3.9.51 está disponível para modo padrão e modo restrito.

Pontos de extremidade seguros para downloads do Connector agora são suportados para backup e recuperação e proteção contra ransomware

Se você estiver usando backup e recuperação ou proteção contra ransomware, agora poderá usar endpoints seguros para downloads do Connector."Saiba mais sobre endpoints seguros para downloads do Connector."

Gerenciamento de Identidade e Acesso (IAM) BlueXP

- Usuários sem a função de administrador da organização, pasta ou projeto devem receber uma função de proteção contra ransomware para ter acesso à proteção contra ransomware. Você pode atribuir a um usuário uma das duas funções: administrador de proteção contra ransomware ou visualizador de proteção contra ransomware.
- Usuários sem a função de administrador da organização, pasta ou projeto devem receber uma função Keystone para ter acesso ao Keystone. Você pode atribuir a um usuário uma das duas funções: administrador do Keystone ou visualizador do Keystone .

  "Saiba mais sobre funções de acesso."

- Se você tiver a função de administrador da organização, de administrador de pasta ou de projeto, agora poderá associar uma assinatura do Keystone a um projeto do IAM. Associar uma assinatura do Keystone a um projeto do IAM permite que você controle o acesso ao Keystone dentro do BlueXP.

28 de março de 2025

Lançamento do modo privado (3.9.50)

Uma nova versão do modo privado já está disponível para download no "Site de suporte da NetApp"

A versão 3.9.50 inclui atualizações para os seguintes componentes e serviços do BlueXP .

Componente ou serviço	Versão incluída nesta versão	Mudanças desde o lançamento anterior do modo privado
Conector	3.9.50, 3.9.49	Vá para o "o que há de novo na página do conector BlueXP" e consulte as alterações incluídas nas versões 3.9.50 e 3.9.49.
Backup e recuperação	17 de março de 2025	Vá para o "o que há de novo na página de BlueXP backup and recovery" e consulte as alterações incluídas no comunicado de março de 2024.

Componente ou serviço	Versão incluída nesta versão	Mudanças desde o lançamento anterior do modo privado
Classificação	10 de março de 2025 (versão 1.41)	Vá para o "o que há de novo na página de BlueXP classification" e consulte as alterações incluídas nas versões 1.38 a 1.371.41.

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

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

10 de março de 2025

Conector 3.9.50

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

- O gerenciamento de sistemas Cloud Volumes ONTAP agora é suportado por conectores que têm o SELinux habilitado no sistema operacional.

  "Saiba mais sobre o SELinux"

No momento, a versão 3.9.50 está disponível para modo padrão e modo restrito.

NetApp Keystone beta disponível no BlueXP

O NetApp Keystone estará disponível em breve na BlueXP e agora está em versão beta. Você pode acessar a página de inscrição para o NetApp Keystone beta na barra de navegação esquerda do BlueXP.

6 de março de 2025

Atualização do conector 3.9.49

Acesso ao ONTAP System Manager quando o BlueXP usa um conector

Um administrador do BlueXP (usuários com a função de administrador da organização) pode configurar o BlueXP para solicitar que os usuários insiram suas credenciais do ONTAP para acessar o gerenciador do sistema ONTAP . Quando essa configuração está habilitada, os usuários precisam inserir suas credenciais do ONTAP sempre que elas não são armazenadas no BlueXP.

Este recurso está disponível no Connector versão 3.9.49 e superiores. "Aprenda a configurar as definições de credenciais." .

Atualização do conector 3.9.48

Capacidade de desabilitar a configuração de atualização automática do Conector

Você pode desativar o recurso de atualização automática do Connector.

Quando você usa o BlueXP no modo padrão ou restrito, o BlueXP atualiza automaticamente seu Connector

para a versão mais recente, desde que o Connector tenha acesso de saída à Internet para obter a atualização do software. Se você precisar gerenciar manualmente quando o conector será atualizado, agora você pode desabilitar as atualizações automáticas para o modo padrão ou restrito.

Essa alteração não afeta o modo privado do BlueXP , onde você sempre deve atualizar o conector.

Este recurso está disponível no Connector versão 3.9.48 e superiores.

"Saiba como desabilitar a atualização automática do Connector."

18 de fevereiro de 2025

Lançamento do modo privado (3.9.48)

Uma nova versão do modo privado já está disponível para download no "Site de suporte da NetApp"

A versão 3.9.48 inclui atualizações para os seguintes componentes e serviços do BlueXP .

Componente ou serviço	Versão incluída nesta versão	Mudanças desde o lançamento anterior do modo privado
Conector	3.9.48	Vá para o "o que há de novo na página do conector BlueXP" e consulte as alterações incluídas nas versões 3.9.48.
Backup e recuperação	21 de fevereiro de 2025	Vá para o "o que há de novo na página de BlueXP backup and recovery" e consulte as alterações incluídas no comunicado de fevereiro de 2025.
Classificação	22 de janeiro de 2025 (versão 1.39)	Vá para o "o que há de novo na página de BlueXP classification" e consulte as alterações incluídas na versão 1.39.

10 de fevereiro de 2025

Conector 3.9.49

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

No momento, a versão 3.9.49 está disponível para modo padrão e modo restrito.

Gerenciamento de identidade e acesso (IAM) BlueXP

- Suporte para atribuição de múltiplas funções a um usuário BlueXP .
- Suporte para atribuição de uma função em vários recursos da organização BlueXP (Org/pasta/projeto)
- As funções agora estão associadas a uma de duas categorias: plataforma e serviço de dados.

O modo restrito agora usa BlueXP IAM

O gerenciamento de identidade e acesso (IAM) do BlueXP agora é usado no modo restrito.

O gerenciamento de identidade e acesso (IAM) do BlueXP é um modelo de gerenciamento de recursos e acesso que substitui e aprimora a funcionalidade anterior fornecida pelas contas do BlueXP ao usar o BlueXP no modo padrão e restrito.

Informações relacionadas

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

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

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

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

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

Essas melhorias oferecem melhor controle sobre as ações que os usuários podem executar e os recursos que eles podem acessar.

Como o BlueXP IAM afeta sua conta existente no modo restrito

Ao efetuar login no BlueXP, você notará estas alterações:

- Sua *conta* agora é chamada de *organização*
- Seus *espaços de trabalho* agora são chamados de *projetos*
- Os nomes das funções do usuário foram alterados:
  - *Administrador da conta* agora é *Administrador da organização*
  - *Administrador do espaço de trabalho* agora é *Administrador de pasta ou projeto*
  - *Visualizador de conformidade* agora é *Visualizador de classificação*
- Em Configurações, você pode acessar o gerenciamento de identidade e acesso do BlueXP para aproveitar essas melhorias

Observe o seguinte:

- Não há alterações em seus usuários ou ambientes de trabalho existentes.
- Embora os nomes das funções tenham mudado, não há diferenças da perspectiva de permissões. Os usuários continuarão tendo acesso aos mesmos ambientes de trabalho de antes.
- Não há alterações na forma como você faz login no BlueXP. O BlueXP IAM funciona com logins de nuvem da NetApp , credenciais do site de suporte da NetApp e conexões federadas, assim como as contas BlueXP .
- Se você tinha várias contas BlueXP , agora você tem várias organizações BlueXP .

API para BlueXP IAM

Essa alteração introduz uma nova API para o BlueXP IAM, mas ela é compatível com versões anteriores da API de locação anterior. "Saiba mais sobre a API para BlueXP IAM"

Modos de implantação suportados

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

Lançamento do modo privado (3.9.48)

Uma nova versão do modo privado já está disponível para download no "Site de suporte da NetApp"

A versão 3.9.48 inclui atualizações para os seguintes componentes e serviços do BlueXP .

Componente ou serviço	Versão incluída nesta versão	Mudanças desde o lançamento anterior do modo privado
Conector	3.9.48	Vá para o "o que há de novo na página do conector BlueXP" e consulte as alterações incluídas nas versões 3.9.48.
Backup e recuperação	21 de fevereiro de 2025	Vá para o "o que há de novo na página de BlueXP backup and recovery" e consulte as alterações incluídas no comunicado de fevereiro de 2025.
Classificação	22 de janeiro de 2025 (versão 1.39)	Vá para o "o que há de novo na página de BlueXP classification" e consulte as alterações incluídas na versão 1.39.

13 de janeiro de 2025

Conector 3.9.48

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

No momento, a versão 3.9.48 está disponível para modo padrão e modo restrito.

Gerenciamento de identidade e acesso BlueXP

- A página Recursos agora exibe recursos não descobertos. Recursos não descobertos são recursos de armazenamento que o BlueXP conhece, mas para os quais você não criou ambientes de trabalho. Por exemplo, recursos exibidos no consultor digital que ainda não têm ambientes de trabalho são exibidos na página Recursos como recursos não descobertos.
- Os recursos do Amazon FSx for NetApp ONTAP não são exibidos na página de recursos do IAM, pois você não pode associá-los a uma função do IAM. Você pode visualizar esses recursos em suas respectivas telas ou em cargas de trabalho.

Crie um caso de suporte para serviços BlueXP adicionais

Depois de registrar o BlueXP para suporte, você pode criar um caso de suporte diretamente do console web

do BlueXP . Ao criar o caso, você precisa selecionar o serviço ao qual o problema está associado.

A partir desta versão, agora você pode criar um caso de suporte e associá-lo a serviços BlueXP adicionais:

- BlueXP disaster recovery
- BlueXP ransomware protection

"Saiba mais sobre como criar um caso de suporte" .

16 de dezembro de 2024

Novos endpoints seguros para obter imagens do conector

Quando você instala o Connector, ou quando ocorre uma atualização automática, o Connector entra em contato com repositórios para baixar imagens para a instalação ou atualização. Por padrão, o Conector sempre contatou os seguintes endpoints:

- https://*.blob.core.windows.net
- \ https://cloudmanagerinfraprod.azurecr.io

O primeiro ponto final inclui um curinga porque não podemos fornecer uma localização definitiva. O balanceamento de carga do repositório é gerenciado pelo provedor de serviços, o que significa que os downloads podem ocorrer de diferentes endpoints.

Para maior segurança, o Connector agora pode baixar imagens de instalação e atualizações de endpoints dedicados:

- \ https://bluexpinfraprod.eastus2.data.azurecr.io
- \ https://bluexpinfraprod.azurecr.io

Recomendamos que você comece a usar esses novos endpoints removendo os endpoints existentes das suas regras de firewall e permitindo os novos endpoints.

Esses novos endpoints são suportados a partir da versão 3.9.47 do Connector. Não há compatibilidade com versões anteriores do Connector.

Observe o seguinte:

- Os endpoints existentes ainda são suportados. Se você não quiser usar os novos endpoints, nenhuma alteração será necessária.
- O conector entra em contato primeiro com os pontos de extremidade existentes. Se esses pontos de extremidade não estiverem acessíveis, o Conector entrará em contato automaticamente com os novos pontos de extremidade.
- Os novos pontos de extremidade não são suportados nos seguintes cenários:
  - Se o conector estiver instalado em uma região governamental.
  - Se você usar o Conector com BlueXP backup and recovery ou BlueXP ransomware protection.

  Para ambos os cenários, você pode continuar a usar os pontos de extremidade existentes.

9 de dezembro de 2024

Conector 3.9.47

Esta versão do BlueXP Connector inclui correções de bugs e uma alteração nos endpoints contatados durante a instalação do Connector.

No momento, a versão 3.9.47 está disponível para modo padrão e modo restrito.

Ponto de extremidade para entrar em contato com o suporte da NetApp durante a instalação

Quando você instala manualmente o Connector, o instalador não contata mais \ https://support.netapp.com.

O instalador ainda entra em contato com \ https://mysupport.netapp.com.

Gerenciamento de identidade e acesso BlueXP

A página Conectores lista apenas os Conectores disponíveis no momento. Ele não exibe mais os conectores que você removeu.

26 de novembro de 2024

Lançamento do modo privado (3.9.46)

Uma nova versão do modo privado já está disponível para download no "Site de suporte da NetApp"

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

Componente ou serviço	Versão incluída nesta versão	Mudanças desde o lançamento anterior do modo privado
Conector	3.9.46	Pequenas melhorias de segurança e correções de bugs
Backup e recuperação	22 de novembro de 2024	Vá para o "o que há de novo na página de BlueXP backup and recovery" e consulte as alterações incluídas na versão de novembro de 2024
Classificação	4 de novembro de 2024 (versão 1.37)	Vá para o "o que há de novo na página de BlueXP classification" e consulte as alterações incluídas nas versões 1.32 a 1.37
Gerenciamento Cloud Volumes ONTAP	11 de novembro de 2024	Vá para o "o que há de novo na página de gerenciamento do Cloud Volumes ONTAP" e consulte as alterações incluídas nos lançamentos de outubro de 2024 e novembro de 2024
Gerenciamento de cluster ONTAP local	26 de novembro de 2024	Vá para o "o que há de novo na página de gerenciamento de cluster ONTAP local" e consulte as alterações incluídas na versão de novembro de 2024

Embora a BlueXP digital wallet e a BlueXP replication também estejam incluídas no modo privado, não há alterações em relação à versão anterior do modo privado.

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

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

11 de novembro de 2024

Conector 3.9.46

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

No momento, a versão 3.9.46 está disponível para modo padrão e modo restrito.

ID para projetos IAM

Agora você pode visualizar o ID de um projeto no gerenciamento de identidade e acesso do BlueXP . Pode ser necessário usar o ID ao fazer uma chamada de API.

"Aprenda como obter o ID de um projeto" .

10 de outubro de 2024

Patch do conector 3.9.45

Este patch inclui correções de bugs.

7 de outubro de 2024

Gerenciamento de identidade e acesso BlueXP

O gerenciamento de identidade e acesso (IAM) do BlueXP é um novo modelo de gerenciamento de recursos e acesso que substitui e aprimora a funcionalidade anterior fornecida pelas contas do BlueXP ao usar o BlueXP no modo padrão.

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

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

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

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

Essas melhorias oferecem melhor controle sobre as ações que os usuários podem executar e os recursos que eles podem acessar.

Como o BlueXP IAM afeta sua conta existente

Ao efetuar login no BlueXP, você notará estas alterações:

- Sua *conta* agora é chamada de *organização*
- Seus *espaços de trabalho* agora são chamados de *projetos*
- Os nomes das funções do usuário foram alterados:
  - *Administrador da conta* agora é *Administrador da organização*
  - *Administrador do espaço de trabalho* agora é *Administrador de pasta ou projeto*
  - *Visualizador de conformidade* agora é *Visualizador de classificação*
- Em Configurações, você pode acessar o gerenciamento de identidade e acesso do BlueXP para aproveitar essas melhorias

Observe o seguinte:

- Não há alterações em seus usuários ou ambientes de trabalho existentes.
- Embora os nomes das funções tenham mudado, não há diferenças da perspectiva de permissões. Os usuários continuarão tendo acesso aos mesmos ambientes de trabalho de antes.
- Não há alterações na forma como você faz login no BlueXP. O BlueXP IAM funciona com logins de nuvem da NetApp , credenciais do site de suporte da NetApp e conexões federadas, assim como as contas BlueXP .
- Se você tinha várias contas BlueXP , agora você tem várias organizações BlueXP .

API para BlueXP IAM

Essa alteração introduz uma nova API para o BlueXP IAM, mas ela é compatível com versões anteriores da API de locação anterior. "Saiba mais sobre a API para BlueXP IAM"

Modos de implantação suportados

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

Para onde ir a seguir

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

Conector 3.9.45

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

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

Suporte para Ubuntu 24.04 LTS

A partir da versão 3.9.45, o BlueXP agora oferece suporte a novas instalações do Connector em hosts Ubuntu 24.04 LTS ao usar o BlueXP no modo padrão ou restrito.

"Exibir requisitos do host do conector" .

Suporte para SELinux com hosts RHEL

O BlueXP agora oferece suporte ao Connector com hosts Red Hat Enterprise Linux que tenham o SELinux habilitado no modo de imposição ou no modo permissivo.

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

Observe as seguintes limitações:

- O BlueXP não oferece suporte ao SELinux com hosts Ubuntu.
- O gerenciamento de sistemas Cloud Volumes ONTAP não é suportado por Conectores que tenham o SELinux habilitado no sistema operacional.

"Saiba mais sobre o SELinux"

30 de setembro de 2024

Lançamento do modo privado (3.9.44)

Uma nova versão do modo privado já está disponível para download no site de suporte da NetApp .

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

Serviço	Versão incluída
Conector	3.9.44
Backup e recuperação	27 de setembro de 2024
Classificação	15 de maio de 2024 (versão 1.31)
Gerenciamento Cloud Volumes ONTAP	9 de setembro de 2024
carteira digital	30 Julho 2023
Gerenciamento de cluster ONTAP local	22 de abril de 2024
Replicação	18 de setembro de 2022

Para o Connector, a versão 3.9.44 do modo privado inclui as atualizações introduzidas nas versões de agosto de 2024 e setembro de 2024. Mais notavelmente, suporte ao Red Hat Enterprise Linux 9.4.

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

- "Novidades na versão de setembro de 2024 do Connector"
- "Novidades na versão de agosto de 2024 do Connector"
- "Novidades no BlueXP backup and recovery"
- "O que há de novo na BlueXP classification"
- "Novidades no gerenciamento do Cloud Volumes ONTAP no BlueXP"

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

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

9 de setembro de 2024

Conector 3.9.44

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

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

Suporte para Docker Engine 26 com novas instalações

A partir da versão 3.9.44 do Connector, o Docker Engine 26 agora é compatível com *novas* instalações do Connector em hosts Ubuntu.

Se você tiver um Connector criado antes da versão 3.9.44, o Docker Engine 25.0.5 ainda será a versão máxima suportada em hosts Ubuntu.

"Saiba mais sobre os requisitos do Docker Engine" .

Certificado SSL atualizado para acesso à interface de usuário local

Quando você usa o BlueXP no modo restrito ou privado, a interface do usuário pode ser acessada na máquina virtual do Connector implantada na sua região de nuvem ou no local. Por padrão, o BlueXP usa um certificado SSL autoassinado para fornecer acesso HTTPS seguro ao console baseado na web em execução no Connector.

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

- O nome comum do certificado agora corresponde ao nome curto do host
- O Nome Alternativo do Assunto do Certificado é o Nome de Domínio Totalmente Qualificado (FQDN) da máquina host

Suporte para RHEL 9.4

O BlueXP agora oferece suporte à instalação do Connector em um host Red Hat Enterprise Linux 9.4 ao usar o BlueXP no modo padrão ou restrito.

O suporte para RHEL 9.4 começa com a versão 3.9.40 do Connector.

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

- 8,6 a 8,10
- 9.1 a 9.4

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

Suporte para Podman 4.9.4 com todas as versões do RHEL

O Podman 4.9.4 agora é compatível com todas as versões suportadas do Red Hat Enterprise Linux. A versão

4.9.4 era suportada anteriormente apenas com o RHEL 8.10.

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

O Podman é necessário para hosts RHEL a partir da versão 3.9.40 do Connector.

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

Permissões atualizadas da AWS e do Azure

Atualizamos as políticas da AWS e do Azure para o Conector para remover permissões que não são mais necessárias. As permissões estavam relacionadas ao cache de borda do BlueXP e à descoberta e gerenciamento de clusters do Kubernetes, que não são mais suportados desde agosto de 2024.

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

22 de agosto de 2024

Patch do conector 3.9.43

Atualizamos o Connector para oferecer suporte à versão 9.15.1 do Cloud Volumes ONTAP .

O suporte para esta versão inclui uma atualização da política do Conector para o Azure. A política agora inclui as seguintes permissões:

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

Essas permissões são necessárias para o suporte do Cloud Volumes ONTAP aos conjuntos de dimensionamento de máquinas virtuais. Se você tiver Conectores existentes e quiser usar esse novo recurso, precisará adicionar essas permissões às funções personalizadas associadas às suas credenciais do Azure.

- "Saiba mais sobre a versão 9.15.1 do Cloud Volumes ONTAP"
- "Exibir permissões do Azure para o Conector" .

8 de agosto de 2024

Conector 3.9.43

Esta versão inclui pequenas melhorias e correções de bugs.

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

Requisitos de CPU e RAM atualizados

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

- CPU: 8 núcleos ou 8 vCPUs (o requisito anterior era 4)

- RAM: 32 GB (o requisito anterior era 14 GB)

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

- AWS: t3.2xgrande
- Azure: Padrão_D8s_v3
- Google Cloud: n2-padrão-8

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

Suporte para Podman 4.9.4 com RHEL 8.10

O Podman versão 4.9.4 agora é compatível ao instalar o Connector em um host Red Hat Enterprise Linux 8.10.

Validação de usuário para federação de identidade

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

31 de julho de 2024

Lançamento do modo privado (3.9.42)

Uma nova versão do modo privado já está disponível para download no site de suporte da NetApp .

Suporte para RHEL 8 e 9

Esta versão inclui suporte para instalação do Connector em um host Red Hat Enterprise Linux 8 ou 9 ao usar o BlueXP no modo privado. As seguintes versões do RHEL são suportadas:

- 8,6 a 8,10
- 9.1 a 9.3

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

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

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

Versões incluídas nesta versão

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

Serviço	Versão incluída
Conector	3.9.42
Backup e recuperação	18 de julho de 2024
Classificação	1 de julho de 2024 (versão 1.33)
Gerenciamento Cloud Volumes ONTAP	10 de junho de 2024

Serviço	Versão incluída
carteira digital	30 Julho 2023
Gerenciamento de cluster ONTAP local	30 Julho 2023
Replicação	18 de setembro de 2022

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

- "Saiba mais sobre o modo privado"
- "Aprenda como começar a usar o BlueXP no modo privado"
- "Aprenda como atualizar o Conector ao usar o modo privado"
- "Saiba o que há de novo no BlueXP backup and recovery"
- "Saiba o que há de novo na BlueXP classification"
- "Saiba o que há de novo no gerenciamento do Cloud Volumes ONTAP no BlueXP"

15 de julho de 2024

Suporte para RHEL 8.10

O BlueXP agora oferece suporte à instalação do Connector em um host Red Hat Enterprise Linux 8.10 ao usar o modo padrão ou o modo restrito.

O suporte para RHEL 8.10 começa com a versão 3.9.40 do Connector.

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

8 de julho de 2024

Conector 3.9.42

Esta versão inclui pequenas melhorias, correções de bugs e suporte para o conector na região AWS Canadá Oeste (Calgary).

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

Requisitos atualizados do Docker Engine

Quando o Connector é instalado em um host Ubuntu, a versão mínima suportada do Docker Engine agora é 23.0.6. Anteriormente era 19.3.1.

A versão máxima suportada ainda é 25.0.5.

"Exibir requisitos do host do conector" .

A verificação de e-mail agora é necessária

Novos usuários que se inscreverem no BlueXP agora precisam verificar seu endereço de e-mail antes de poderem efetuar login.

12 de junho de 2024

Conector 3.9.41

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

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

4 de junho de 2024

Lançamento do modo privado (3.9.40)

Uma nova versão do modo privado já está disponível para download no site de suporte da NetApp . Esta versão inclui as seguintes versões dos serviços BlueXP que são compatíveis com o modo privado.

Observe que esta versão em modo privado *não* inclui suporte para o Connector com Red Hat Enterprise Linux 8 e 9.

Serviço	Versão incluída
Conector	3.9.40
Backup e recuperação	17 de maio de 2024
Classificação	15 de maio de 2024 (versão 1.31)
Gerenciamento Cloud Volumes ONTAP	17 de maio de 2024
carteira digital	30 Julho 2023
Gerenciamento de cluster ONTAP local	30 Julho 2023
Replicação	18 de setembro de 2022

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

- "Saiba mais sobre o modo privado"
- "Aprenda como começar a usar o BlueXP no modo privado"
- "Aprenda como atualizar o Conector ao usar o modo privado"
- "Saiba o que há de novo no BlueXP backup and recovery"
- "Saiba o que há de novo na BlueXP classification"
- "Saiba o que há de novo no gerenciamento do Cloud Volumes ONTAP no BlueXP"

17 de maio de 2024

Conector 3.9.40

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

No momento, a versão 3.9.40 está disponível para modo padrão e modo restrito.

Suporte para RHEL 8 e 9

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

- 8,6 a 8,9
- 9.1 a 9.3

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

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

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

Fim do suporte para RHEL 7 e CentOS 7

Em 30 de junho de 2024, o RHEL 7 atingirá o fim da manutenção (EOM), enquanto o CentOS 7 atingirá o fim da vida útil (EOL). A NetApp continuará a oferecer suporte ao Connector nessas distribuições Linux até 30 de junho de 2024.

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

Atualização de permissões da AWS

Na versão 3.9.38, atualizamos a política do Connector para AWS para incluir a permissão "ec2:DescribeAvailabilityZones". Essa permissão agora é necessária para dar suporte ao AWS Local Zones com o Cloud Volumes ONTAP.

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

Limitações conhecidas do NetApp Console

Limitações conhecidas identificam plataformas, dispositivos ou funções que não são suportados por esta versão do produto ou que não interoperam corretamente com ele. Revise essas limitações cuidadosamente.

Essas limitações são específicas para a configuração do NEtApp Console e administração: o agente, a plataforma de software como serviço (SaaS) e muito mais.

Limitações do agente do console

Possível conflito com endereços IP no intervalo 172

O NetApp Console implanta um agente com duas interfaces que têm endereços IP nos intervalos 172.17.0.0/16 e 172.18.0.0/16.

Se sua rede tiver uma sub-rede configurada com qualquer um desses intervalos, você poderá enfrentar falhas de conectividade no Console. Por exemplo, a descoberta de clusters ONTAP locais no Console pode falhar.

Veja o artigo da Base de Conhecimento"Conflito de IP do agente com a rede existente" para obter instruções sobre como alterar o endereço IP das interfaces do agente.

A descriptografia SSL não é suportada

O Console não oferece suporte a configurações de firewall que tenham a descriptografia SSL habilitada. Se a descriptografia SSL estiver habilitada, mensagens de erro aparecerão no Console e a instância do agente será exibida como inativa.

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

Página em branco ao carregar a interface do usuário local

Se você carregar o console baseado na web que está sendo executado em um agente, a interface poderá falhar ao ser exibida algumas vezes, e você verá apenas uma página em branco.

Esse problema está relacionado a um problema de cache. A solução alternativa é usar uma sessão anônima ou privada do navegador.

Hosts Linux compartilhados não são suportados

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

Agentes e extensões de terceiros

Agentes de terceiros ou extensões de VM não são suportados na VM do agente.

Alterações nos sistemas operacionais Linux suportados

Às vezes, a NetApp adiciona e remove suporte para o agente do Console em sistemas operacionais Linux específicos. Saiba como esse suporte afeta seus agentes do Console existentes.

Sistemas operacionais suportados

A NetApp oferece suporte ao agente com os seguintes sistemas operacionais Linux.

Modo padrão

Instalação manual

- Ubuntu 24.04 LTS
- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8,6 a 8,10
  - 9.1 a 9.4

Implantação do NetApp Console

Ubuntu 22.04 LTS

Implantação do AWS Marketplace

Ubuntu 22.04 LTS

Implantação do Azure Marketplace

Ubuntu 22.04 LTS

Modo restrito

Instalação manual

- Ubuntu 24.04 LTS
- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8,6 a 8,10
  - 9.1 a 9.4

Implantação do AWS Marketplace

Ubuntu 22.04 LTS

Implantação do Azure Marketplace

Ubuntu 22.04 LTS

Modo privado

Instalação manual

- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8,6 a 8,10
  - 9.1 a 9.4

Suporte para RHEL 8 e 9

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

Limitações

A Classificação de Dados NetApp será suportada se você instalar o agente em um host RHEL 8 ou 9 que resida no local. Não há suporte se o host RHEL 8 ou 9 residir na AWS, Azure ou Google Cloud.

Ferramenta de orquestração de contêineres

Você deve usar a ferramenta Podman como ferramenta de orquestração de contêineres ao instalar o agente do Console em um host RHEL 8 ou 9. O Docker Engine não é compatível com RHEL 8 e 9.

Modo de implantação

RHEL 8 e 9 são suportados ao usar o Console no modo padrão e no modo restrito.

Versões do agente do console suportadas

A NetApp oferece suporte ao RHEL 8 e 9 a partir das seguintes versões do agente do Console:

- 3.9.40 ao usar o Console no modo padrão ou no modo restrito

Somente novas instalações manuais

O RHEL 8 e 9 são suportados com *novas* instalações de agentes ao instalar agentes manualmente em hosts executados em suas instalações ou na nuvem.

Atualizações do RHEL

Se você tiver um agente existente em execução em um host RHEL 7, a NetApp não oferece suporte à atualização do sistema operacional RHEL 7 para RHEL 8 ou 9. Saiba mais sobre os agentes de console existentes no RHEL 7 ou CentOS 7 .

Fim do suporte para RHEL 7 e CentOS 7

Em 30 de junho de 2024, o RHEL 7 atingiu o fim da manutenção (EOM), enquanto o CentOS 7 atingiu o fim da vida útil (EOL). A NetApp descontinuou o suporte para agentes nessas distribuições Linux em 30 de junho de 2024.

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

Agentes de console existentes no RHEL 7 ou CentOS 7

Se você tiver um agente existente em execução no RHEL 7 ou CentOS 7, a NetApp não oferece suporte à atualização ou conversão do sistema operacional para RHEL 8 ou 9. Você precisa criar um novo agente em um sistema operacional compatível.

1. Configure um host RHEL 8 ou 9.
2. Instale o Podman.
3. Instalar um *novo* agente.
4. Configure o agente para descobrir os sistemas que o agente anterior estava gerenciando.

Informações relacionadas

Como começar a usar o RHEL 8 e 9

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

Modo padrão

- "Instalar e configurar um agente de console no local"
- "Instalar manualmente o agente do Console na AWS"
- "Instalar manualmente o agente do Console no Azure"
- "Instalar manualmente o agente do Console no Google Cloud"

Modo restrito

"Preparar para implantação no modo restrito"

Como redescobrir seus sistemas

Consulte as páginas a seguir para redescobrir seus sistemas depois de implantar um novo agente do Console.

- "Adicionar sistemas Cloud Volumes ONTAP existentes"
- "Descubra clusters ONTAP locais"
- "Crie ou descubra um sistema FSx para ONTAP"
- "Criar um sistema de Azure NetApp Files"
- "Descubra os sistemas da Série E"
- "Descubra os sistemas StorageGRID"

Começar

Aprenda o básico

Saiba mais sobre o NetApp Console

O NetApp Console fornece gerenciamento centralizado do armazenamento NetApp e do NetApp Data Services em ambientes locais e na nuvem em nível empresarial, fornecendo insights em tempo real, fluxos de trabalho mais rápidos e administração simplificada, de forma altamente segura e compatível.

Está disponível como uma plataforma de serviço (SaaS) que fornece gerenciamento de armazenamento, mobilidade de dados, proteção de dados e análise e controle de dados. Os recursos de gerenciamento são fornecidos por meio de um console baseado na web e APIs.

Características

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

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

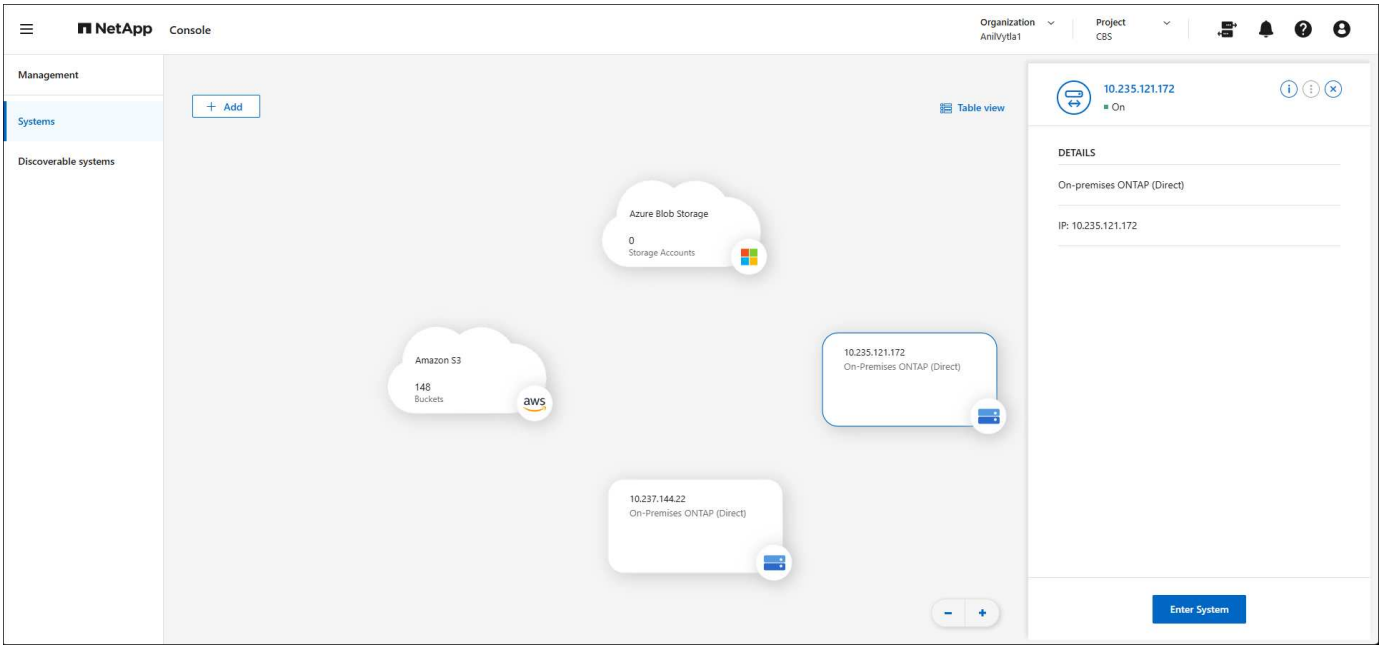
Armazenamento de objetos em nuvem

- 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 .

Backup e recuperação da NetApp

Faça backup e restaure dados na nuvem e no local.

Classificação de dados da NetApp

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

Cópia e sincronização da NetApp

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.

Licenças e assinaturas

Gerencie e monitore suas licenças e assinaturas.

Recuperação de desastres da NetApp

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.

Resiliência do NetApp Ransomware

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

Replicação NetApp

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.

Camadas de nuvem da NetApp

Amplie seu armazenamento ONTAP local para a nuvem.

Cache de volume da NetApp

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" .

Modos de implantação

A NetApp oferece dois modos de implantação para o NetApp Console: o *modo padrão* usa uma camada de software como serviço (SaaS) para funcionalidade completa, enquanto o *modo restrito* limita a conectividade de saída.

A NetApp continua oferecendo o BlueXP para sites que não precisam de conectividade de saída. O BlueXP está disponível somente no modo privado."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 agentes do NetApp Console

Um *agente de console* é executado na sua rede em nuvem ou na rede local. Use um agente do Console para conectar os serviços do NetApp Console aos seus ambientes de armazenamento.

O que você pode fazer sem um agente de console

Alguns recursos e serviços do Console estarão disponíveis se você não implantar um agente do Console:

- Amazon FSx for NetApp ONTAP

  Algumas ações exigem um agente do Console ou um link do NetApp Workloads. "Saiba quais ações exigem um agente ou link do Console"

- Centro de automação
- Azure NetApp Files

  Você não precisa de um agente de console para gerenciar o Azure NetApp Files, mas é necessário um para usar a Classificação de Dados do NetApp para verificar o Azure NetApp Files.

- Google Cloud NetApp Volumes
- Cópia e sincronização da NetApp
- Consultor digital
- Monitorar o uso da licença, o monitoramento da assinatura requer um agente do Console

  Normalmente, você pode adicionar uma licença ao NetApp Console sem um agente do Console.

  É necessário um agente para adicionar licenças baseadas em nós do Cloud Volumes ONTAP porque os dados vêm das licenças instaladas nos sistemas Cloud Volumes ONTAP .

- Descoberta direta de clusters ONTAP locais

  Você não precisa de um agente do Console para adicionar um cluster ONTAP local ao Console, mas um é necessário para recursos adicionais do Console e serviços de dados.

  "Saiba mais sobre opções de descoberta e gerenciamento para clusters ONTAP locais"

- Atualizações de software
- Sustentabilidade
- Cargas de trabalho da NetApp

Quando um agente de console é necessário

No modo padrão, o Console requer um agente de Console para:

- Alertas
- Recursos de gerenciamento do Amazon FSx para ONTAP
- Armazenamento Amazon S3
- Armazenamento de Blobs do Azure
- Backup e recuperação da NetApp
- Classificação de Dados
- Cloud Volumes ONTAP
- Recuperação de desastres da NetApp
- Sistemas da série E
- Eficiência econômica [1]
- Baldes do Google Cloud Storage
- Integração de cluster ONTAP local com serviços de dados NetApp
- Resiliência do NetApp Ransomware
- Sistemas StorageGRID

- Camadas de nuvem da NetApp
- Cache de volume da NetApp

[1] Você pode acessar esses serviços sem um agente do Console, mas um agente do Console é necessário para iniciar ações.

Você sempre precisa de um agente do Console para usar o Console no modo restrito.

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. A maneira como você começa depende se você está usando o Console no modo padrão ou no modo restrito.

- "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 de nuvem

Você precisa de permissões específicas para criar o agente do Console diretamente do NetApp Console e outro conjunto de permissões para a própria instância do 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.

No modo padrão ou restrito, o agente do Console é atualizado automaticamente se tiver 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 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"

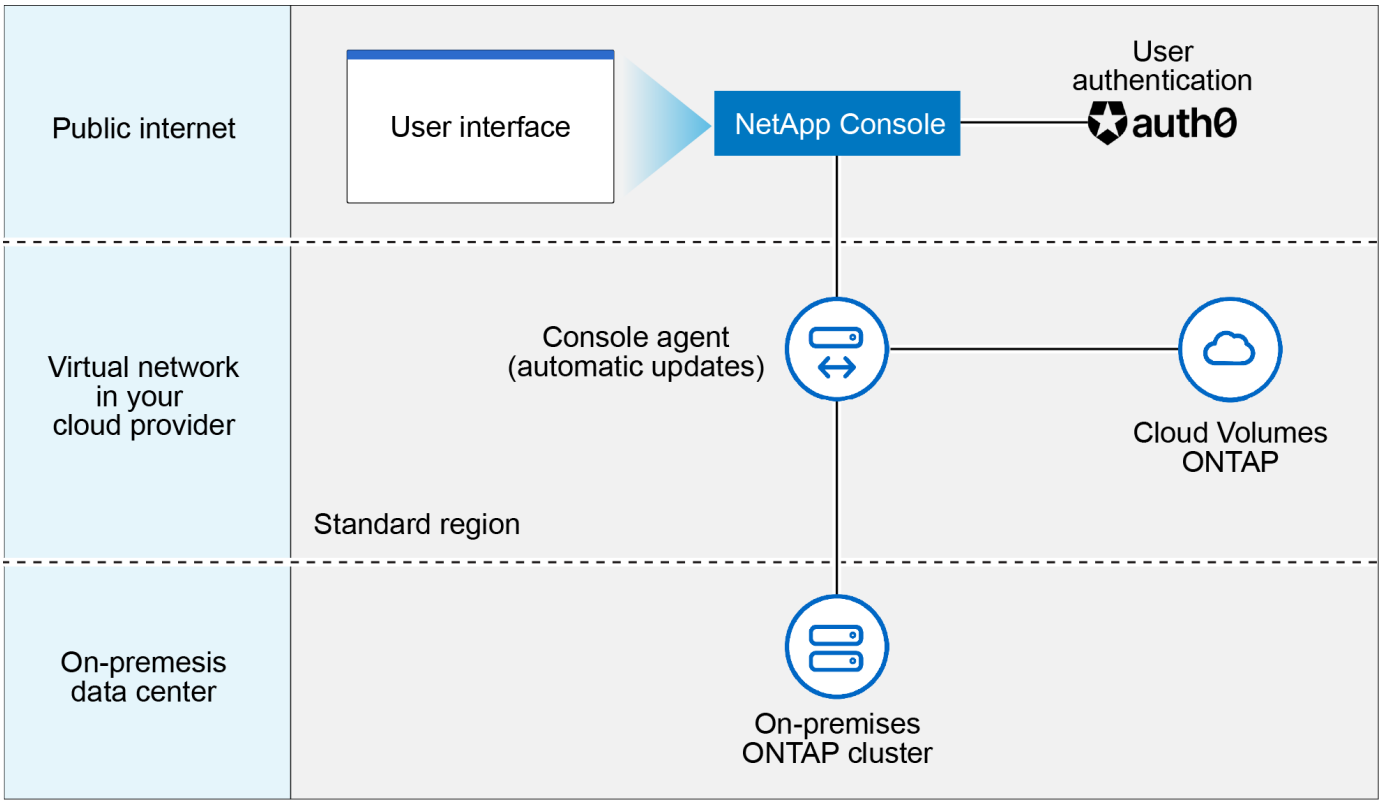
A tabela a seguir fornece uma comparação do console NetApp .

	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
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 seu agente automaticamente 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.

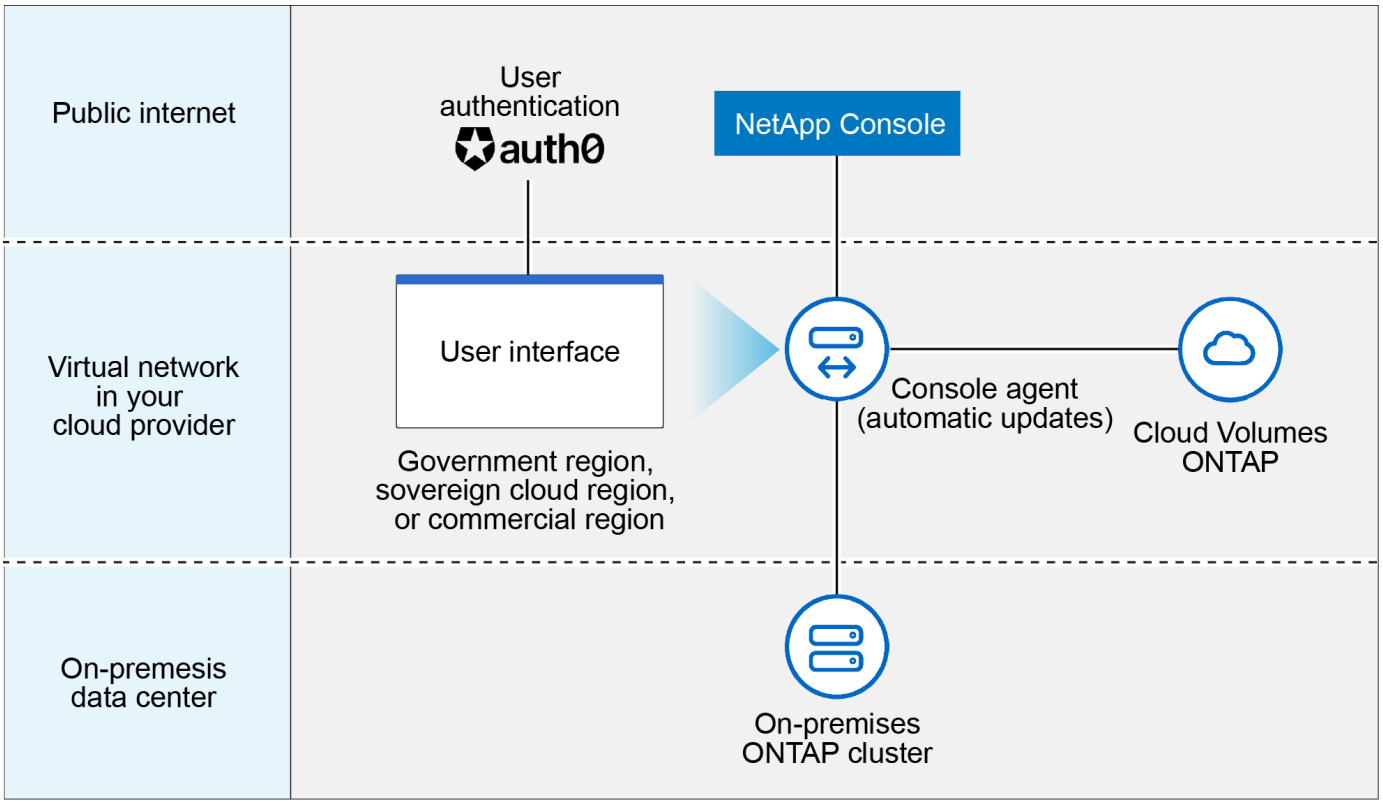
Como começar com o modo padrão

Vá para o "Console NetApp" 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 os 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.
Classificação de dados da NetApp	Suportado em regiões governamentais com modo restrito. Não suportado em regiões comerciais ou em regiões soberanas com modo restrito.
Cloud Volumes ONTAP	Suporte total

Serviços suportados	Notas
Licenças e assinaturas	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
Serviços de Dados	Backup e recuperação da NetApp	Simhttps://docs.netapp.com/us-en/bluexp-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"^]
	Classificação de dados da NetApp	Sim
	Cópia e sincronização da NetApp	Não
	Recuperação de desastres da NetApp	Não
	Resiliência do NetApp Ransomware	Não
	Replicação NetApp	Sim
	Camadas de nuvem da NetApp	Não
	Cache de volume do NetApp	Não
	Fábrica de carga de trabalho da NetApp	Não

Área de produtos	Serviço ou recurso de dados NetApp	Modo restrito
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

Comece a usar o assistente NetApp

Comece a usar o NetApp Console Assistant

Se você for um usuário iniciante do NetApp Console com 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 dos 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.

Quando o Assistente do Console aparece?

O Console Assistant fica disponível na página inicial do NetApp Console até que as tarefas de configuração obrigatórias sejam concluídas.

Use o Assistente para concluir estas tarefas, algumas das quais são obrigatórias:

- Adicione uma conta do NetApp Support Site (NSS).
- Conecte-se ao seu estado de armazenamento implantando um agente do Console (etapa obrigatória).
- Gerencie seu sistema adicionando ou descobrindo um cluster (etapa obrigatória).

- Adicione uma assinatura de mercado ou uma licença PAYGO.
- Links de serviços de dados abertos.

Habilitar o Assistente do Console

Por padrão, o NetApp Console exibe o Assistente do Console na página inicial para novos usuários que têm a função de administrador da organização.

Você pode dispensar o Assistente somente depois que você ou outra pessoa concluir os itens obrigatórios. Após concluir os itens obrigatórios, o Assistente será dispensado para todos os usuários da sua organização e não aparecerá novamente.

Use o Assistente do Console para começar

O Console Assistant orienta você na configuração do seu ambiente NetApp Console com estas tarefas:

- Adicione uma conta do NetApp Support Site (NSS).
- Conecte-se ao seu estado de armazenamento implantando um agente do Console, no local ou na nuvem. Você pode implantá-lo manualmente ou baixando um OVA. Esta etapa é obrigatória.
- Gerencie seu sistema adicionando ou descobrindo um cluster. Esta etapa é obrigatória.
- Adicione uma assinatura de mercado ou uma licença PAYGO.
- Saiba mais sobre os serviços de dados da NetApp .

Comece com o modo padrão

Fluxo de trabalho de introdução (modo padrão)

Comece a usar o NetApp Console no modo padrão preparando a rede para o Console, inscrevendo-se e criando uma conta e, opcionalmente, criando um agente do Console.

No modo padrão, você acessa um console baseado na Web hospedado como um produto de software como serviço (SaaS) da NetApp. Antes de começar, certifique-se de entender"modos de implantação" e"Agentes de console" .

1 **"Preparar a rede para usar o console NetApp"**

Os computadores que acessam o console do NetApp devem ter conexões com endpoints específicos. Se sua rede restringir o acesso de saída, você deve garantir que esses endpoints sejam permitidos.

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

Vá para o "Console NetApp" e inscreva-se. Você terá a opção de criar uma organização, mas deverá pular essa etapa se sua empresa já tiver uma organização existente.

Neste ponto, você está conectado e pode começar a gerenciar o armazenamento e usar serviços como Digital Advisor, Amazon FSx for ONTAP, Azure NetApp Files e muito mais. "Aprenda o que você pode fazer sem um agente de console" .

3 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"

Para usar o NetApp Intelligent Data Services para gerenciar armazenamento e dados no Google Cloud, certifique-se de que o agente do Console seja executado no Google Cloud.

4 "Assine o NetApp Intelligent Services (opcional)"

Inscreva-se no NetApp Intelligent Services por meio do seu provedor de nuvem para pagar por hora (PAYGO) ou por meio de um contrato anual. Os serviços inteligentes da NetApp incluem backup e recuperação da NetApp , Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience e NetApp Disaster Recovery. A classificação de dados da NetApp está incluída na sua assinatura sem custo adicional.

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)
- Locais de rede onde você implanta agentes do Console que você instala no local ou na nuvem.
- Pontos de extremidade adicionais para determinados serviços de dados da NetApp , incluindo Cloud Volumes ONTAP.

> ⓘ 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

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

O sistema contata esses terminais em dois cenários:

- A partir de um computador acessando o "Console NetApp" como software como serviço (SaaS).
- De um computador acessando diretamente um host do agente do Console, para efetuar login e configurá-lo ou acessar o Console a partir do host do agente.

Pontos finais	Propósito
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://support.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://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.

Preparar a rede para o agente do Console

Você instala o agente do Console no local ou na nuvem, e ele entra em contato com os endpoints para concluir as ações iniciadas pelo Console.

Os agentes do console devem ter acesso aos mesmos endpoints que o NetApp Console, além de endpoints adicionais, dependendo de onde você instalar o agente.

Configure o acesso ao ponto de extremidade da rede 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"
- "Configurar acesso à rede local para um agente do Console"

Preparar a rede para o Cloud Volumes ONTAP

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"

"Consulte a documentação dos respectivos serviços de dados da NetApp ."

Inscreva-se ou faça login no NetApp Console

O NetApp Console pode ser acessado por meio de um console baseado na Web. Para começar a usar o Console, o primeiro passo é se inscrever ou fazer login usando suas credenciais do site de suporte da NetApp ou criando um login no Console da NetApp .

Sobre esta tarefa

Ao acessar o Console pela primeira vez, você pode se inscrever ou fazer login usando uma das seguintes opções:

Login do console NetApp

Você pode se inscrever criando um login. Este método de autenticação exige que você especifique seu endereço de e-mail e uma senha. Depois de verificar seu endereço de e-mail, você pode fazer login e criar uma organização, caso ainda não pertença a uma.

Credenciais do NetApp Support Site (NSS)

Se você já tiver credenciais do Site de Suporte da NetApp , não precisará se inscrever no Console. Você faz login usando suas credenciais do NSS e então o Console solicita que você crie uma organização, caso ainda não pertença a uma.

Você receberá uma senha de uso único (OTP) para o endereço de e-mail registrado. Um novo OTP é gerado a cada tentativa de login.

Conexão federada

Se sua empresa já tiver uma instância do NetApp Console, o administrador do Console poderá ter configurado o logon único para efetuar login usando credenciais do seu diretório corporativo (identidade federada).

"Aprenda a usar a federação de identidades com o NetApp Console" .

Passos

1. Abra um navegador da web e vá para o "Console NetApp"
2. Se você tiver uma conta no site de suporte da NetApp ou se já tiver configurado a federação de identidade, insira o endereço de e-mail associado à sua conta diretamente na página **Fazer 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**.

      Observe que 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.

      Esta etapa é necessária antes que você possa efetuar login no Console.

4. Após efetuar login, revise o Contrato de Licença do Usuário Final e aceite os termos.

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

5. Na página **Boas-vindas**, insira um nome para sua organização do Console.

   O Console define uma organização como o elemento de nível superior no gerenciamento de identidade e acesso (IAM) do Console. "Saiba mais sobre o IAM" .

   Se sua empresa já tiver uma organização e você quiser ingressar nela, feche o Console e peça ao administrador da organização para associá-lo à organização. Depois de ser adicionado, você poderá efetuar login e terá acesso à organização do Console. "Aprenda como adicionar membros a uma organização existente" .

6. Selecione **Vamos começar**.

Criar um agente de console

AWS

Opções de instalação do agente de console na AWS

Existem algumas maneiras diferentes de criar um agente de console na AWS. Diretamente do NetApp Console é a maneira mais comum.

As seguintes opções de instalação estão disponíveis:

- "Crie o agente do Console diretamente do Console"(esta é a opção padrão)

  Esta ação inicia uma instância do EC2 executando o Linux e o software do agente do Console em uma VPC de sua escolha.

- "Crie um agente de console no AWS Marketplace"

  Esta ação também inicia uma instância do EC2 executando o Linux e o software do agente do Console, mas a implantação é iniciada diretamente do AWS Marketplace, e não do Console.

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

A opção de instalação escolhida afeta a maneira como você se prepara para a instalação. Isso inclui como você fornece ao Console as permissões necessárias para autenticar e gerenciar recursos na AWS.

Crie um agente de console na AWS a partir do NetApp Console

Você pode criar um agente de console na AWS diretamente do NetApp Console. Antes de criar um agente do Console na AWS a partir do Console, você precisa configurar sua rede e preparar as permissões da AWS.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Você deve revisar"Limitações do agente do console" .

Etapa 1: configurar a rede para implantar um agente de console na AWS

Certifique-se de que o local de rede onde você planeja instalar o agente do Console suporte os seguintes requisitos. Esses requisitos permitem que o agente do Console gerencie recursos e processos na sua nuvem híbrida.

VPC e sub-rede

Ao criar o agente do Console, você precisa especificar a VPC e a sub-rede onde ele deve residir.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
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)	Para gerenciar recursos da AWS. O ponto de extremidade depende da sua região da AWS. "Consulte a documentação da AWS para obter detalhes"

Pontos finais	Propósito
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://support.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://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.

Endpoints contatados do console NetApp

À medida que você usa o NetApp Console baseado na Web fornecido pela camada SaaS, ele entra em contato com vários endpoints para concluir tarefas de gerenciamento de dados. Isso inclui endpoints que são contatados para implantar o agente do Console a partir do Console.

"Exibir a lista de endpoints contatados pelo console do NetApp" .

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 estiver planejando usar o NetApp Data Classification para verificar suas fontes de dados corporativos, deverá habilitar 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"

Você precisará implementar esse requisito de rede depois de criar o agente do Console.

Etapa 2: configurar permissões da AWS para o agente do Console

O Console precisa ser autenticado com a AWS antes de poder implantar a instância do agente do Console na sua VPC. Você pode escolher um destes métodos de autenticação:

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

Com qualquer uma das opções, o primeiro passo é criar uma política de IAM. Esta política contém apenas as permissões necessárias para iniciar a instância do agente do Console na AWS a partir do Console.

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

Passos

1. Acesse o console do AWS IAM.
2. Selecione **Políticas > Criar política**.
3. Selecione **JSON**.
4. Copie e cole a seguinte política:

   Esta política contém apenas as permissões necessárias para iniciar a instância do agente do Console na AWS a partir do Console. Quando o Console cria o agente do Console, ele aplica um novo conjunto de permissões à instância do agente do Console que permite que o agente do Console gerencie recursos da AWS. "Exibir permissões necessárias para a própria instância do agente do Console" .

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

```
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
```

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

5. Selecione **Avançar** e adicione tags, se necessário.
6. Selecione **Avançar** e insira um nome e uma descrição.
7. Selecione **Criar política**.
8. Anexe a política a uma função do IAM que o Console pode assumir ou a um usuário do IAM para que você possa fornecer chaves de acesso ao Console:
   - (Opção 1) Configure uma função do IAM que o Console pode assumir:
     i. Acesse o console do AWS IAM na conta de destino.
     ii. Em Gerenciamento de acesso, selecione **Funções > Criar função** e siga as etapas para criar a função.
     iii. Em **Tipo de entidade confiável**, selecione **Conta AWS**.
     iv. Selecione **Outra conta AWS** e insira o ID da conta SaaS do Console: 952013314444
     v. Selecione a política que você criou na seção anterior.
     vi. Depois de criar a função, copie o ARN da função para poder colá-lo no Console ao criar o agente do Console.
   - (Opção 2) Configure permissões para um usuário do IAM para que você possa fornecer chaves de acesso ao Console:
     i. No console do AWS IAM, selecione **Usuários** e, em seguida, selecione o nome do usuário.
     ii. Selecione **Adicionar permissões > Anexar políticas existentes diretamente**.
     iii. Selecione a política que você criou.
     iv. Selecione **Avançar** e depois selecione **Adicionar permissões**.

v. Certifique-se de ter a chave de acesso e a chave secreta para o usuário do IAM.

Resultado

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

Etapa 3: Criar o agente do Console

Crie o agente do Console diretamente do console baseado na Web.

Sobre esta tarefa

- A criação do agente do Console a partir do Console implanta uma instância do EC2 na AWS usando uma configuração padrão. Não mude para uma instância EC2 menor com menos CPUs ou menos RAM depois de criar o agente do Console. "Saiba mais sobre a configuração padrão do agente do Console" .
- Quando o Console cria o agente do Console, ele cria uma função do IAM e um perfil de instância para a instância. Esta função inclui permissões que permitem ao agente do Console gerenciar recursos da AWS. Garanta que a função seja atualizada conforme novas permissões forem adicionadas em versões futuras. "Saiba mais sobre a política do IAM para o agente do Console" .

Antes de começar

Você deve ter o seguinte:

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

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione **Implantar agente > AWS**
3. Siga as etapas do assistente para criar o agente do Console:
4. Na página **Introdução** é fornecida uma visão geral do processo
5. Na página **Credenciais da AWS**, especifique sua região da AWS e escolha um método de autenticação, que pode ser uma função do IAM que o Console pode assumir ou uma chave de acesso e uma chave secreta da AWS.

   Se você escolher **Assumir função**, poderá criar o primeiro conjunto de credenciais no assistente de implantação do agente do Console. Qualquer conjunto adicional de credenciais deve ser criado na página Credenciais. Eles estarão disponíveis no assistente em uma lista suspensa. "Aprenda como adicionar credenciais adicionais" .

6. Na página **Detalhes**, forneça detalhes sobre o agente do Console.
   - Digite um nome para a instância.

- Adicione tags personalizadas (metadados) à instância.
- Escolha se deseja que o Console crie uma nova função que tenha as permissões necessárias ou se deseja selecionar uma função existente que você configurou com"as permissões necessárias" .
- Escolha se deseja criptografar os discos EBS do agente do Console. Você tem a opção de usar a chave de criptografia padrão ou usar uma chave personalizada.

7. Na página **Rede**, especifique uma VPC, uma sub-rede e um par de chaves para a instância, escolha se deseja habilitar um endereço IP público e, opcionalmente, especifique uma configuração de proxy.

   Certifique-se de ter o par de chaves correto para acessar a máquina virtual do agente do Console. Sem um par de chaves, você não pode acessá-lo.

8. Na página **Grupo de segurança**, escolha se deseja criar um novo grupo de segurança ou se deseja selecionar um grupo de segurança existente que permita as regras de entrada e saída necessárias.

   "Exibir regras de grupo de segurança para AWS" .

9. Revise suas seleções para verificar se sua configuração está correta.

   a. A caixa de seleção **Validar configuração do agente** é marcada por padrão para que o Console valide os requisitos de conectividade de rede quando você implantar. Se o Console não conseguir implantar o agente, ele fornecerá um relatório para ajudar você a solucionar o problema. Se a implantação for bem-sucedida, nenhum relatório será fornecido.

   Se você ainda estiver usando o"pontos finais anteriores" usado para atualizações de agentes, a validação falha com um erro. Para evitar isso, desmarque a caixa de seleção para pular a verificação de validação.

10. Selecione **Adicionar**.

    O Console prepara a instância em cerca de 10 minutos. Permaneça na página até que o processo seja concluído.

Resultado

Após a conclusão do processo, o agente do Console estará disponível para uso no Console.

Se a implantação falhar, você poderá baixar um relatório e logs do Console para ajudar a corrigir os problemas."Aprenda a solucionar problemas de instalação."

Se você tiver buckets do Amazon S3 na mesma conta da AWS onde criou o agente do Console, verá um ambiente de trabalho do Amazon S3 aparecer automaticamente na página **Sistemas**. "Aprenda a gerenciar buckets do S3 no NetApp Console"

Crie um agente de console no AWS Marketplace

Você cria um agente de console na AWS diretamente do AWS Marketplace. Para criar um agente do Console no AWS Marketplace, você precisa configurar sua rede, preparar as permissões da AWS, revisar os requisitos da instância e, em seguida, criar o agente do Console.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Você deve revisar"Limitações do agente do console" .

Etapa 1: configurar a rede

Certifique-se de que o local de rede do agente do Console atenda aos seguintes requisitos para gerenciar recursos de nuvem híbrida.

VPC e sub-rede

Ao criar o agente do Console, você precisa especificar a VPC e a sub-rede onde ele deve residir.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
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)	Para gerenciar recursos da AWS. O ponto de extremidade depende da sua região da AWS. "Consulte a documentação da AWS para obter detalhes"
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://support.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .

Pontos finais	Propósito
\ https://signin.b2c.netapp.com	Para atualizar as credenciais do NetApp Support Site (NSS) ou adicionar novas credenciais do NSS ao NetApp Console.
\ 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.

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 estiver planejando usar o NetApp Data Classification para verificar suas fontes de dados corporativos, deverá habilitar 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"

Implemente esse acesso à rede depois de criar o agente do Console.

Etapa 2: configurar permissões da AWS

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

Passos

1. Faça login no console da AWS e navegue até o serviço 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.

      Talvez seja necessário criar uma segunda política com base nos serviços de dados da NetApp que você planeja usar. 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. 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 que pode ser associada à instância do EC2 durante a implantação no AWS Marketplace.

Etapa 3: Revisar os requisitos da instância

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

CPU

8 núcleos ou 8 vCPUs

BATER

32 GB

Tipo de instância AWS EC2

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

Etapa 4: criar o agente do console

Crie o agente do Console diretamente do AWS Marketplace.

Sobre esta tarefa

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

Antes de começar

Você deve ter o seguinte:

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

Passos

1. Vá para 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**.

     A AWS inicia o agente do Console com as configurações especificadas, e o agente do Console é executado em cerca de dez minutos.

     Se a instalação falhar, você poderá visualizar logs e um relatório para ajudar a solucionar problemas."Aprenda a solucionar problemas de instalação."
8. Abra um navegador da Web em um host que tenha uma conexão com a máquina virtual do agente do Console e a URL do agente do Console.
9. Após efetuar login, configure o agente do Console:
   a. Especifique a organização do Console a ser associada ao agente do Console.
   b. Digite um nome para o sistema.
   c. Em **Você está executando em um ambiente seguro?** mantenha o modo restrito desabilitado.

      Mantenha o modo restrito desabilitado para usar o Console no modo padrão. Você deve habilitar o modo restrito somente se tiver um ambiente seguro e quiser desconectar esta conta dos serviços de backend do Console. Se for esse o caso,"siga as etapas para começar a usar o NetApp Console no modo restrito" .
   d. Selecione **Vamos começar**.

Resultado

O agente do Console agora está instalado e configurado com sua organização do Console.

Abra um navegador da web e vá para o "Console NetApp" para começar a usar o agente do Console com o Console.

Se você tiver buckets do Amazon S3 na mesma conta da AWS onde criou o agente do Console, verá um ambiente de trabalho do Amazon S3 aparecer automaticamente na página **Sistemas**. "Aprenda a gerenciar buckets do S3 no NetApp Console"

Instalar manualmente o agente do Console na AWS

Você pode instalar manualmente um agente do Console em um host Linux em execução na AWS. Para instalar manualmente o agente do Console no seu próprio host Linux, você precisa revisar os requisitos do host, configurar sua rede, preparar as permissões da AWS, instalar o agente do Console e, em seguida, fornecer as permissões que você preparou.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Você deve revisar"Limitações do agente do console" .

Etapa 1: Revise os requisitos do host

O software do agente do Console deve ser executado em um host que atenda aos requisitos específicos do sistema operacional, requisitos de RAM, requisitos de porta e assim por diante.

> O agente do Console reserva o intervalo de UID e GID de 19000 a 19200. Este intervalo é fixo e não pode ser modificado. Se algum software de terceiros no seu host estiver usando UIDs ou GIDs dentro desse intervalo, a instalação do agente falhará. A NetApp recomenda usar um host livre de software de terceiros para evitar conflitos.

Host dedicado

O agente do Console não é suportado em um host compartilhado com outros aplicativos. O host deve ser um host dedicado. O host pode ter qualquer arquitetura que atenda aos seguintes 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 Docker ou o Podman são arquitetados para criar os contêineres dentro deste diretório. Especificamente, eles criarão contêineres no `/var/lib/containers/storage` diretório. Montagens externas ou links simbólicos não funcionam neste espaço.

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 a
Red Hat Enterprise Linux	9.1 a 9.4 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 Ver requisitos de configuração do Podman .	Suportado no modo de imposição ou no modo permissivo • O gerenciamento de sistemas Cloud Volumes ONTAP NÃO é suportado por agentes que tenham o SELinux habilitado no sistema operacional.
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

Tipo de instância AWS EC2

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

Par de chaves

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

Limite de salto de resposta PUT ao usar IMDSv2

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

- "Exigir o uso do IMDSv2 em instâncias do Amazon EC2"

- "Documentação da AWS: Alterar o limite de salto de resposta PUT"

Espaço em disco em /opt

100 GiB de espaço devem estar disponíveis

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

Espaço em disco em /var

20 GiB de espaço devem estar disponíveis

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

Etapa 2: instalar 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 8, verifique se sua versão do Podman está usando o DNS 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.

   Para Red Hat Enterprise Linux 9:

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

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

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<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.
6. Se estiver usando o Red Hat Enterprise:

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

   Para Red Hat Enterprise Linux 9:

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

   Para Red Hat Enterprise Linux 8:

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

7. 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.

8. 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.

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

      ```
      podman info | grep networkBackend
      ```

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

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

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

   d. 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 .

9. Reinicie o podman.

```
systemctl restart podman
```

10. 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 3: configurar a rede

Certifique-se de que o local de rede onde você planeja instalar o agente do Console suporte os seguintes requisitos. Atender a esses requisitos permite que o agente do Console gerencie recursos e processos dentro do seu ambiente de nuvem híbrida.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados de computadores ao usar o NetApp Console baseado na Web

Os computadores que acessam o Console a partir de um navegador da web devem ter a capacidade de contatar vários terminais. Você precisará usar o Console para configurar o agente do Console e para o uso diário do Console.

"Preparar a rede para o console NetApp" .

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
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)	Para gerenciar recursos da AWS. O ponto de extremidade depende da sua região da AWS. "Consulte a documentação da AWS para obter detalhes"
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://support.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://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.

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 estiver planejando usar o NetApp Data Classification para verificar suas fontes de dados corporativos, deverá habilitar 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"

Etapa 4: configurar permissões da AWS para o console

Você precisa fornecer permissões da AWS para o NetApp Console usando uma das seguintes opções:

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

Siga as etapas para preparar permissões para o Console.

Função IAM

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. 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 que pode ser associada à instância do EC2 após instalar o agente do Console.

Chave de acesso AWS

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.

Resultado

Agora você tem um usuário do IAM que tem as permissões necessárias e uma chave de acesso que você pode fornecer ao Console.

Etapa 5: instalar o agente do console

Após a conclusão dos pré-requisitos, você pode instalar manualmente o software no seu próprio host Linux.

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" .

Sobre esta tarefa

O instalador disponível no site de suporte da NetApp pode ser uma versão anterior. 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 em "Site de suporte da NetApp" e, em seguida, copie-o para o host Linux.

   Você deve baixar o instalador do agente "online" destinado ao uso em sua rede ou na nuvem.

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 transparente ou explícito. Os parâmetros --proxy e --cacert são opcionais e você não será solicitado a adicioná-los. Se você tiver um servidor proxy, precisará inserir os parâmetros conforme mostrado.

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-de-usuário:senha@endereço:porta
- http://nome-de-domínio%92nome-de-usuário:senha@endereço:porta
- https://endereço:porta
- https://nome-de-usuário:senha@endereço:porta
- https://nome-de-domínio%92nome-de-usuário:senha@endereço:porta

  Observe o seguinte:

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

    Por exemplo:

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

`--cacert`especifica um certificado assinado pela CA a ser usado para acesso HTTPS entre o agente do Console e o servidor proxy. Este parâmetro é necessário para servidores proxy HTTPS, servidores proxy de interceptação e servidores proxy transparentes.

+ Aqui está um exemplo de configuração de um servidor proxy transparente. Ao configurar um proxy

transparente, você não precisa definir o servidor proxy. Você só adiciona um certificado assinado pela CA ao host do agente do Console:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

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
      ...
      # 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
      ...
      Esc:wq
      ```

   c. Reinicie a máquina virtual do agente do Console.
2. Aguarde a conclusão da instalação.

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

   Se a instalação falhar, você pode visualizar o relatório e os logs da instalação para ajudar a corrigir os problemas."Aprenda a solucionar problemas de instalação."

1. Abra um navegador da Web em um host que tenha uma conexão com a máquina virtual do agente do Console e insira o seguinte URL:

   https://ipaddress

2. Após efetuar login, configure o agente do Console:
   a. Especifique a organização a ser associada ao agente do Console.
   b. Digite um nome para o sistema.
   c. Em **Você está executando em um ambiente seguro?** mantenha o modo restrito desabilitado.

      Você deve manter o modo restrito desabilitado porque estas etapas descrevem como usar o Console no modo padrão. Você deve habilitar o modo restrito somente se tiver um ambiente seguro e quiser

desconectar esta conta dos serviços de backend. Se for esse o caso,"siga as etapas para começar a usar o NetApp Console no modo restrito" .

d. Selecione **Vamos começar**.

Se você tiver buckets do Amazon S3 na mesma conta da AWS onde criou o agente do Console, verá um sistema de armazenamento do Amazon S3 aparecer na página **Sistemas** automaticamente. "Aprenda a gerenciar buckets S3 no NetApp ConsoleP"

Etapa 6: fornecer permissões ao NetApp Console

Agora que você instalou o agente do Console, precisa fornecer ao Console as permissões da AWS que você configurou anteriormente. Fornecer as permissões permite que o agente do Console gerencie seus dados e infraestrutura de armazenamento na AWS.

Função IAM

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

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**.

Vá para o "Console NetApp" para começar a usar o agente do Console.

Chave de acesso AWS

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

Passos

1. Certifique-se de que o agente correto do Console esteja selecionado no Console.
2. Selecione **Administração > Credenciais**.
3. Selecione **Credenciais da organização**.
4. 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**.

Vá para o "Console NetApp" para começar a usar o agente do Console.

Azul

Opções de instalação do agente de console no Azure

Existem algumas maneiras diferentes de criar um agente de console no Azure. Diretamente do NetApp Console é a maneira mais comum.

As seguintes opções de instalação estão disponíveis:

- "Crie um agente de console diretamente do NetApp Console"(esta é a opção padrão)

  Esta ação inicia uma VM executando Linux e o software do agente do Console em uma VNet de sua escolha.

- "Crie um agente de console no Azure Marketplace"

  Esta ação também inicia uma VM executando Linux e o software do agente do Console, mas a implantação é iniciada diretamente do Azure Marketplace, e não do Console.

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

A opção de instalação escolhida afeta a maneira como você se prepara para a instalação. Isso inclui como você fornece ao agente do Console as permissões necessárias para autenticar e gerenciar recursos no Azure.

Criar um agente de console no Azure a partir do NetApp Console

Para criar um agente do Console no Azure a partir do NetApp Console, você precisa configurar sua rede, preparar as permissões do Azure e, em seguida, criar o agente do Console.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Você deve revisar"Limitações do agente do console" .

Etapa 1: configurar a rede

Certifique-se de que o local de rede onde você planeja instalar o agente do Console suporte os seguintes requisitos. Esses requisitos permitem que o agente do Console gerencie recursos de nuvem híbrida.

Região Azure

Se você usar o Cloud Volumes ONTAP, o agente do Console deverá ser implantado na mesma região do Azure que os sistemas Cloud Volumes ONTAP que ele gerencia ou no "Par de regiões do Azure" para os sistemas Cloud Volumes ONTAP . Esse requisito 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"

VNet e sub-rede

Ao criar o agente do Console, você precisa especificar a VNet e a sub-rede onde ele deve residir.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Para gerenciar recursos em regiões públicas do Azure.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Para gerenciar recursos nas regiões do Azure China.
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://support.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://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.

Endpoints contatados do console NetApp

À medida que você usa o NetApp Console baseado na Web fornecido pela camada SaaS, ele entra em contato com vários endpoints para concluir tarefas de gerenciamento de dados. Isso inclui endpoints que são contatados para implantar o agente do Console a partir do Console.

"Exibir a lista de endpoints contatados pelo console do NetApp" .

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 estiver planejando usar o NetApp Data Classification para verificar suas fontes de dados corporativos, deverá habilitar 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"

Você precisa implementar esse requisito de rede depois de criar o agente do Console.

Etapa 2: criar uma política de implantação do agente do console (função personalizada)

Você precisa criar uma função personalizada que tenha permissões para implantar o agente do Console no Azure.

Crie uma função personalizada do Azure que você pode atribuir à sua conta do Azure ou a uma entidade de serviço do Microsoft Entra. O Console é autenticado com o Azure e usa essas permissões para criar a instância do agente do Console em seu nome.

O Console implanta a VM do agente do Console no Azure, habilita um "identidade gerenciada atribuída pelo sistema" , cria a função necessária e a atribui à VM. "Revise como o Console usa as permissões" .

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

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

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

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

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

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

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
d",
        "Microsoft.Network/networkInterfaces/ipConfigurations/read",
        "Microsoft.Resources/deployments/operations/read",
        "Microsoft.Resources/deployments/read",
        "Microsoft.Resources/deployments/delete",
        "Microsoft.Resources/deployments/cancel/action",
        "Microsoft.Resources/deployments/validate/action",
        "Microsoft.Resources/resources/read",
        "Microsoft.Resources/subscriptions/operationresults/read",
        "Microsoft.Resources/subscriptions/resourceGroups/delete",
```

```
        "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
        "Microsoft.Resources/subscriptions/resourceGroups/write",
        "Microsoft.Authorization/roleDefinitions/write",
        "Microsoft.Authorization/roleAssignments/write",

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

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

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

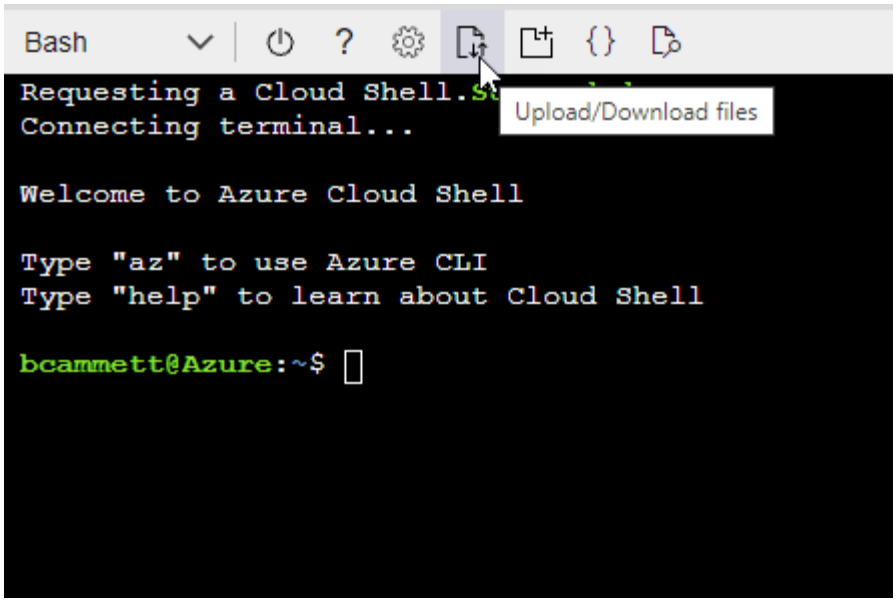
   Exemplo

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

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

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

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



c. Digite o seguinte comando da CLI do Azure:

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

Agora você tem uma função personalizada chamada *Azure SetupAsService*. Você pode aplicar essa função personalizada à sua conta de usuário ou a uma entidade de serviço.

Etapa 3: Configurar autenticação

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

1. Sign in com sua conta do Azure quando solicitado. Esta conta deve ter permissões específicas do Azure. Esta é a opção padrão.
2. Forneça detalhes sobre uma entidade de serviço do Microsoft Entra. Este principal de serviço também requer permissões específicas.

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

Conta do Azure

Atribua a função personalizada ao usuário que implantará o agente do Console a partir do Console.

Passos

1. No portal do Azure, abra o serviço **Assinaturas** e selecione a assinatura do usuário.
2. Clique em **Controle de acesso (IAM)**.
3. Clique em **Adicionar** > **Adicionar atribuição de função** e adicione as permissões:
   a. Selecione a função **Azure SetupAsService** e clique em **Avançar**.

      Azure SetupAsService é o nome padrão fornecido na política de implantação do agente do Console para o Azure. Se você escolheu um nome diferente para a função, selecione esse nome.

   b. Mantenha **Usuário, grupo ou entidade de serviço** selecionado.
   c. Clique em **Selecionar membros**, escolha sua conta de usuário e clique em **Selecionar**.
   d. Clique em **Avançar**.
   e. Clique em **Revisar + atribuir**.

Diretor de serviço

Em vez de fazer login com sua conta do Azure, você pode fornecer ao Console as credenciais de uma entidade de serviço do Azure que tenha as permissões necessárias.

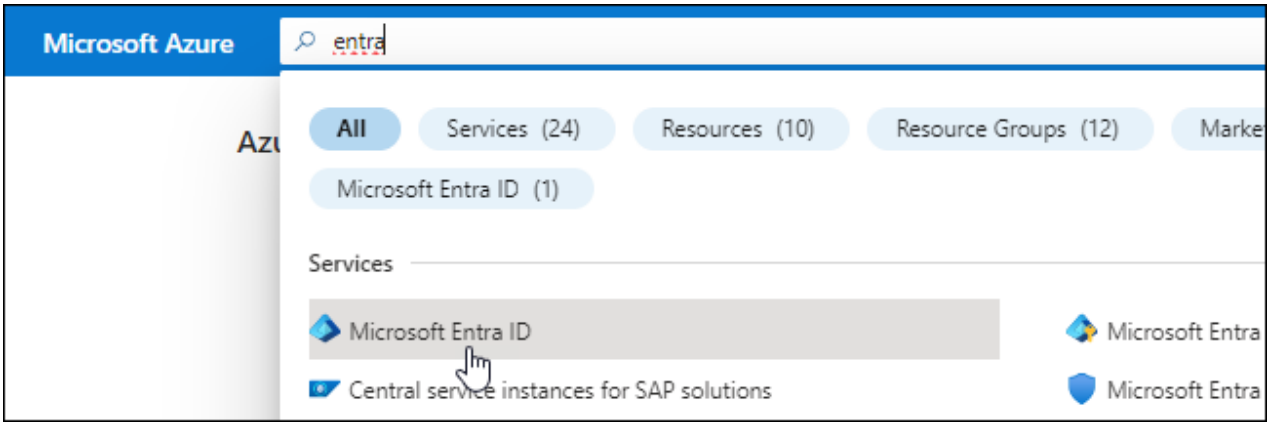
Crie e configure uma entidade de serviço no Microsoft Entra ID e obtenha as credenciais do Azure necessárias para o Console.

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**.

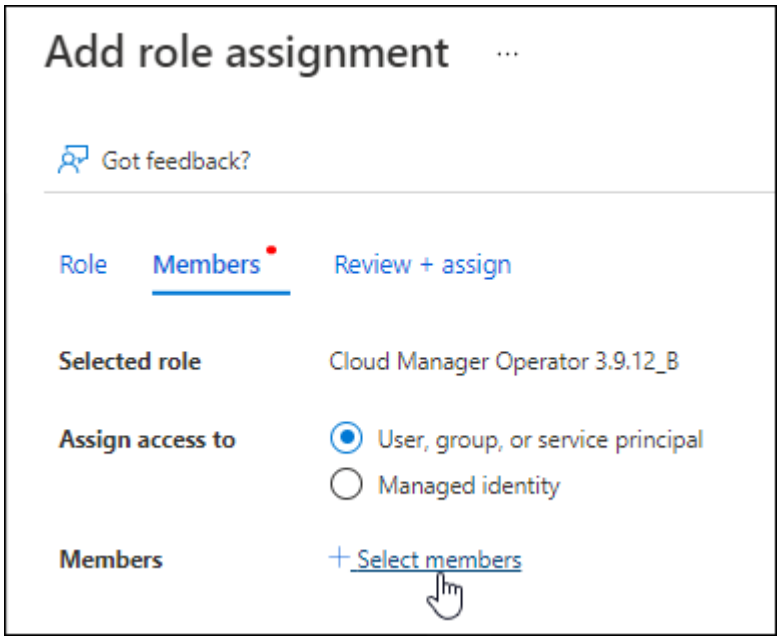
   Você criou o aplicativo AD e a entidade de serviço.

Atribuir a função personalizada ao aplicativo

1. No portal do Azure, abra o serviço **Assinaturas**.
2. Selecione a assinatura.
3. Clique em **Controle de acesso (IAM) > Adicionar > Adicionar atribuição de função**.
4. Na guia **Função**, selecione a função **Operador de console** e clique em **Avançar**.
5. Na aba **Membros**, complete os seguintes passos:

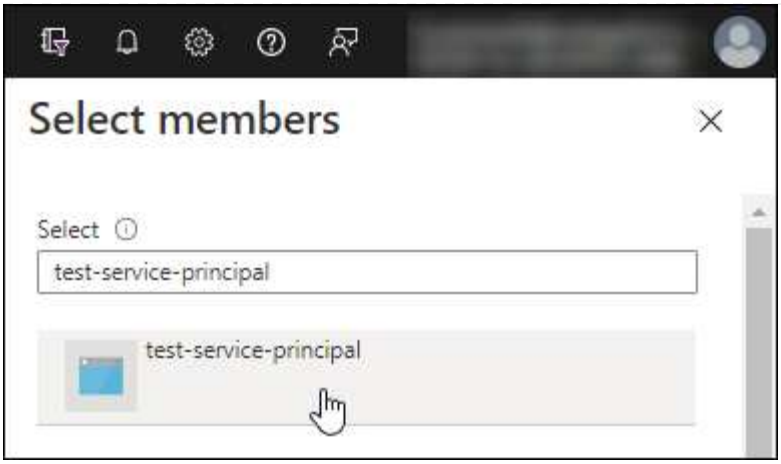
   a. Mantenha **Usuário, grupo ou entidade de serviço** selecionado.

   b. Clique em **Selecionar membros**.



   c. Pesquise o nome do aplicativo.

   Aqui está um exemplo:



a. Selecione o aplicativo e clique em **Selecionar**.

b. Clique em **Avançar**.

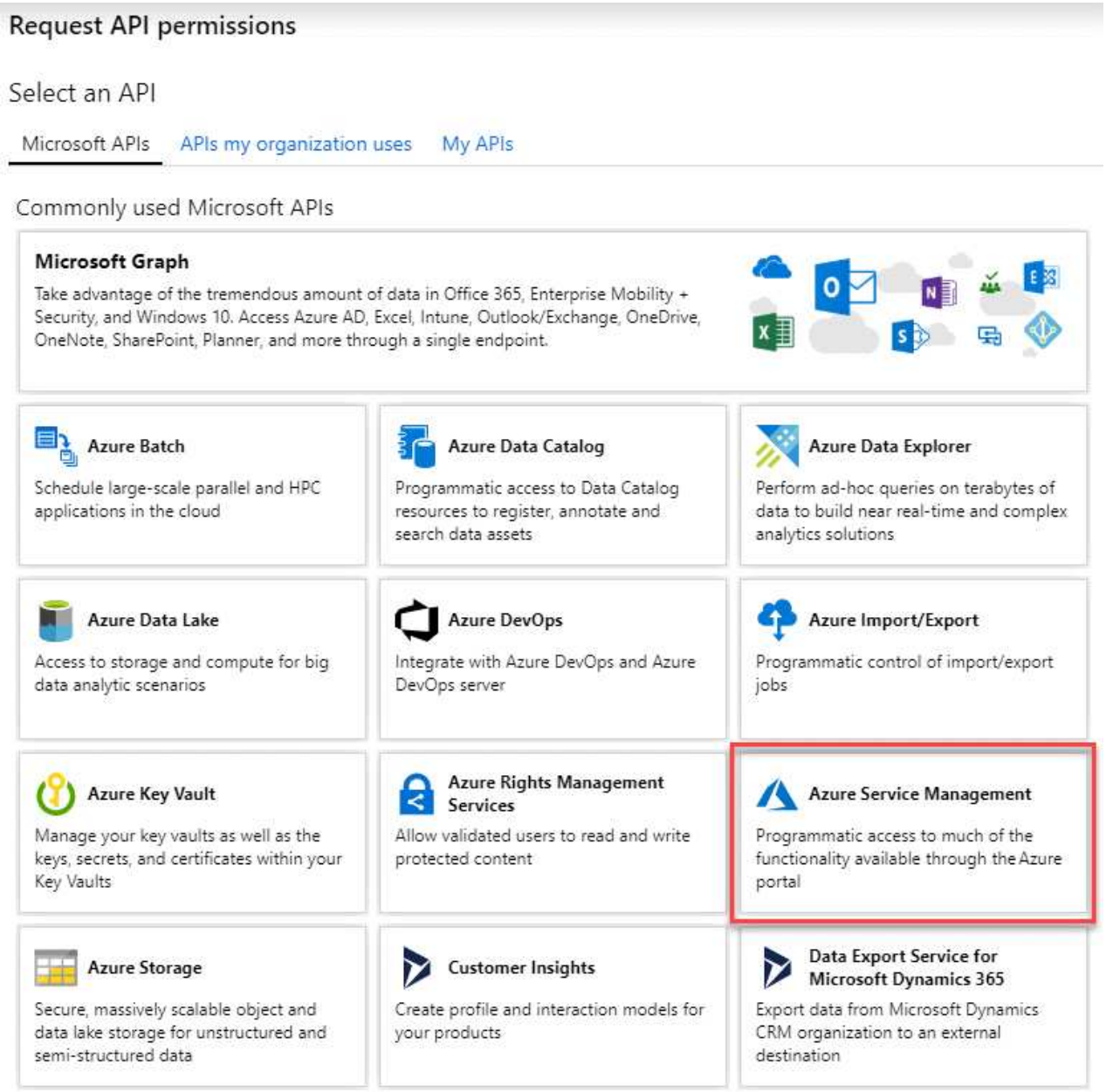
6. Clique em **Revisar + atribuir**.

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

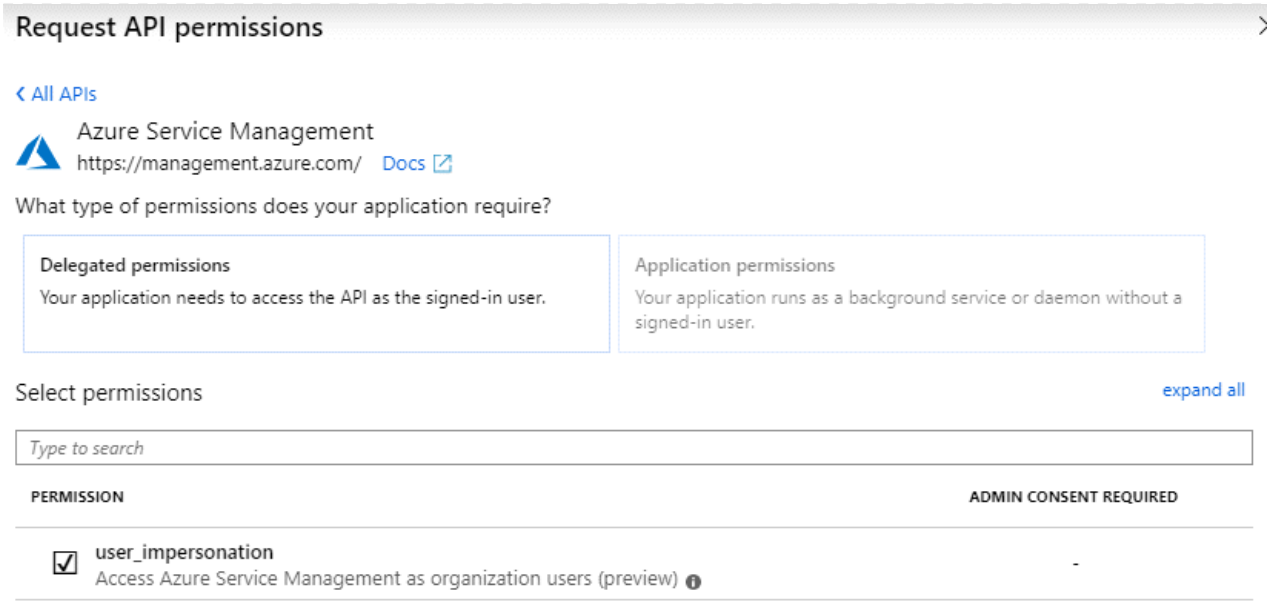
   Se você quiser gerenciar recursos em várias assinaturas do Azure, deverá vincular a entidade de serviço a cada uma dessas assinaturas. Por exemplo, o Console permite que você selecione a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

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**.

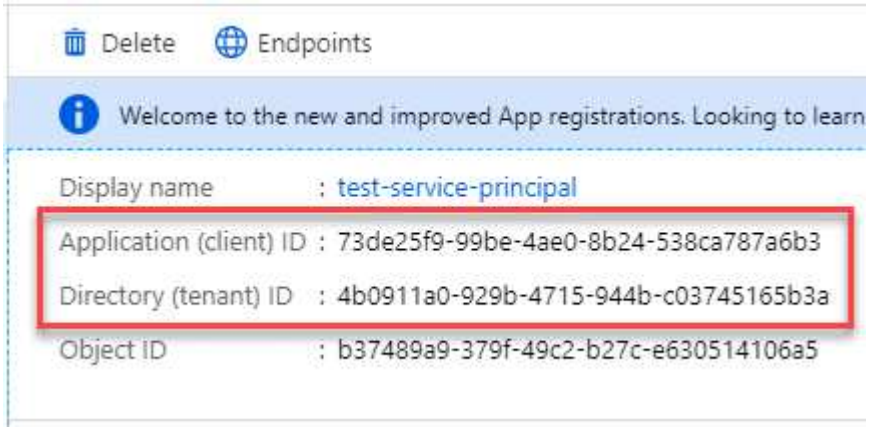


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



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 criar o agente do Console.

Etapa 4: criar o agente do console

Crie o agente do Console diretamente do NetApp Console.

Sobre esta tarefa

- A criação do agente do Console a partir do Console implanta uma máquina virtual no Azure usando uma configuração padrão. Não mude para uma instância de VM menor com menos CPUs ou menos RAM depois de criar o agente do Console. "Saiba mais sobre a configuração padrão do agente do Console" .
- Quando o Console implanta o agente do Console, ele cria uma função personalizada e a atribui à VM do agente do Console. Esta função inclui permissões que permitem ao agente do Console gerenciar recursos do Azure. Você precisa garantir que a função seja mantida atualizada à medida que novas permissões forem adicionadas em versões subsequentes. "Saiba mais sobre a função personalizada do agente do Console" .

Antes de começar

Você deve ter o seguinte:

- Uma assinatura do Azure.
- Uma VNet e uma sub-rede na região do Azure de sua escolha.
- Detalhes sobre um servidor proxy, caso sua organização exija um proxy para todo o tráfego de saída da Internet:
  - Endereço IP
  - Credenciais
  - Certificado HTTPS
- Uma chave pública SSH, se você quiser usar esse método de autenticação para a máquina virtual do agente do Console. A outra opção para o método de autenticação é usar uma senha.

  "Saiba mais sobre como se conectar a uma VM Linux no Azure"

- Se você não quiser que o Console crie automaticamente uma função do Azure para o agente do Console, será necessário criar sua própria"usando a política nesta página" .

  Essas permissões são para a própria instância do agente do Console. É um conjunto diferente de permissões do que você configurou anteriormente para implantar a VM do agente do Console.

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione **Implantar agente > Azure**
3. Na página **Revisão**, revise os requisitos para implantar um agente. Esses requisitos também estão detalhados acima nesta página.
4. Na página **Autenticação de Máquina Virtual**, selecione a opção de autenticação que corresponde à forma como você configura as permissões do Azure:

   - Selecione **Fazer login** para fazer login na sua conta da Microsoft, que deve ter as permissões necessárias.

     O formulário é de propriedade e hospedado pela Microsoft. Suas credenciais não são fornecidas à NetApp.

     Se você já estiver conectado a uma conta do Azure, o Console usará essa conta automaticamente. Se você tiver várias contas, talvez seja necessário sair primeiro para garantir que está usando a conta correta.

   - Selecione **Principal do serviço do Active Directory** para inserir informações sobre o principal do serviço do Microsoft Entra que concede as permissões necessárias:
     - ID do aplicativo (cliente)
     - ID do diretório (inquilino)
     - Segredo do cliente

   Aprenda como obter esses valores para um principal de serviço .

5. Na página **Autenticação de Máquina Virtual**, escolha uma assinatura do Azure, um local, um novo grupo de recursos ou um grupo de recursos existente e, em seguida, escolha um método de autenticação para a máquina virtual do agente do Console que você está criando.

   O método de autenticação para a máquina virtual pode ser uma senha ou uma chave pública SSH.

   "Saiba mais sobre como se conectar a uma VM Linux no Azure"

6. Na página **Detalhes**, insira um nome para a instância, especifique as tags e escolha se deseja que o Console crie uma nova função que tenha as permissões necessárias ou se deseja selecionar uma função existente que você configurou com"as permissões necessárias" .

   Observe que você pode escolher as assinaturas do Azure associadas a essa função. Cada assinatura escolhida fornece ao agente do Console permissões para gerenciar recursos nessa assinatura (por exemplo, Cloud Volumes ONTAP).

7. Na página **Rede**, escolha uma VNet e uma sub-rede, se deseja habilitar um endereço IP público e, opcionalmente, especifique uma configuração de proxy.

   - Na página **Grupo de segurança**, escolha se deseja criar um novo grupo de segurança ou se deseja selecionar um grupo de segurança existente que permita as regras de entrada e saída necessárias.

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

8. Revise suas seleções para verificar se sua configuração está correta.

   a. A caixa de seleção **Validar configuração do agente** é marcada por padrão para que o Console valide

os requisitos de conectividade de rede quando você implantar. Se o Console não conseguir implantar o agente, ele fornecerá um relatório para ajudar você a solucionar o problema. Se a implantação for bem-sucedida, nenhum relatório será fornecido.

Se você ainda estiver usando o"pontos finais anteriores" usado para atualizações de agentes, a validação falha com um erro. Para evitar isso, desmarque a caixa de seleção para pular a verificação de validação.

9. Selecione **Adicionar**.

   O Console prepara a instância em cerca de 10 minutos. Permaneça na página até que o processo seja concluído.

Resultado

Após a conclusão do processo, o agente do Console estará disponível para uso no Console.

Se a implantação falhar, você poderá baixar um relatório e logs do Console para ajudar a corrigir os problemas."Aprenda a solucionar problemas de instalação."

Se você tiver armazenamento de Blobs do Azure na mesma assinatura do Azure em que criou o agente do Console, verá um sistema de armazenamento de Blobs do Azure aparecer na página **Sistemas** automaticamente. "Aprenda a gerenciar o armazenamento de Blobs do Azure no NetApp Console"

Crie um agente de console no Azure Marketplace

Você pode criar um agente de console no Azure diretamente do Azure Marketplace. Para criar um agente do Console no Azure Marketplace, você precisa configurar sua rede, preparar as permissões do Azure, revisar os requisitos da instância e, em seguida, criar o agente do Console.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Análise"Limitações do agente do console" .

Etapa 1: configurar a rede

Certifique-se de que o local de rede onde você planeja instalar o agente do Console atenda aos seguintes requisitos. Esses requisitos permitem que o agente do Console gerencie recursos na sua nuvem híbrida.

Região Azure

Se você usar o Cloud Volumes ONTAP, o agente do Console deverá ser implantado na mesma região do Azure que os sistemas Cloud Volumes ONTAP que ele gerencia ou no "Par de regiões do Azure" para os sistemas Cloud Volumes ONTAP . Esse requisito 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"

VNet e sub-rede

Ao criar o agente do Console, você precisa especificar a VNet e a sub-rede onde ele deve residir.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Para gerenciar recursos em regiões públicas do Azure.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Para gerenciar recursos nas regiões do Azure China.
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://support.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://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.

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 estiver planejando usar o NetApp Data Classification para verificar suas fontes de dados corporativos, deverá habilitar 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"

Implemente os requisitos de rede após criar o agente do Console.

Etapa 2: Revisar os requisitos da VM

Ao criar o agente do Console, escolha um tipo de máquina virtual que atenda aos seguintes requisitos.

CPU

8 núcleos ou 8 vCPUs

BATER

32 GB

Tamanho da VM do Azure

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos Standard_D8s_v3.

Etapa 3: Configurar permissões

Você pode fornecer permissões das seguintes maneiras:

- Opção 1: atribuir uma função personalizada à VM do Azure usando uma identidade gerenciada atribuída pelo sistema.
- Opção 2: forneça ao Console as credenciais para uma entidade de serviço do Azure que tenha as permissões necessárias.

Siga estas etapas para configurar permissões para o Console.

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"

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.

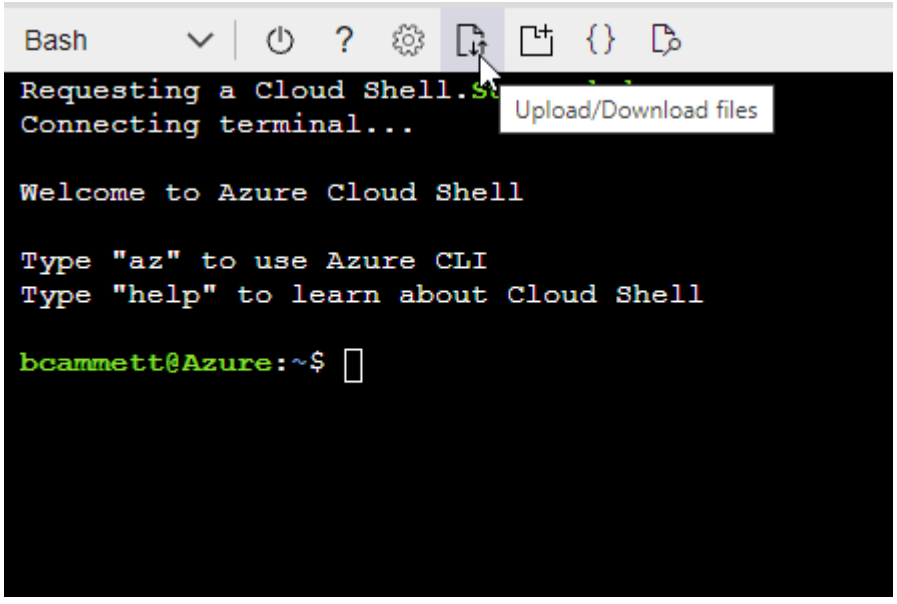
   Exemplo

   ```
   "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 Connector_Policy.json
```

Diretor de serviço

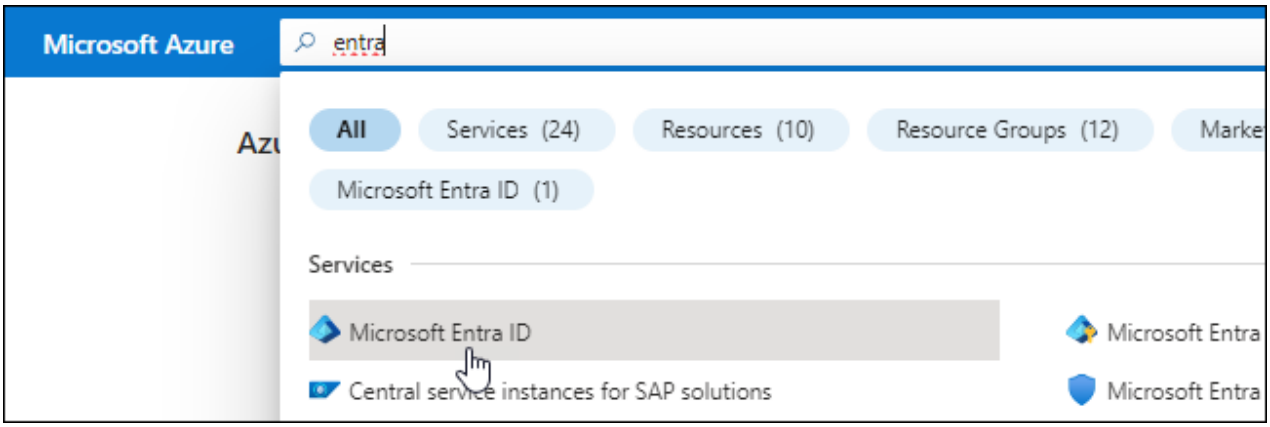
Crie e configure uma entidade de serviço no Microsoft Entra ID e obtenha as credenciais do Azure necessárias para o Console.

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 .

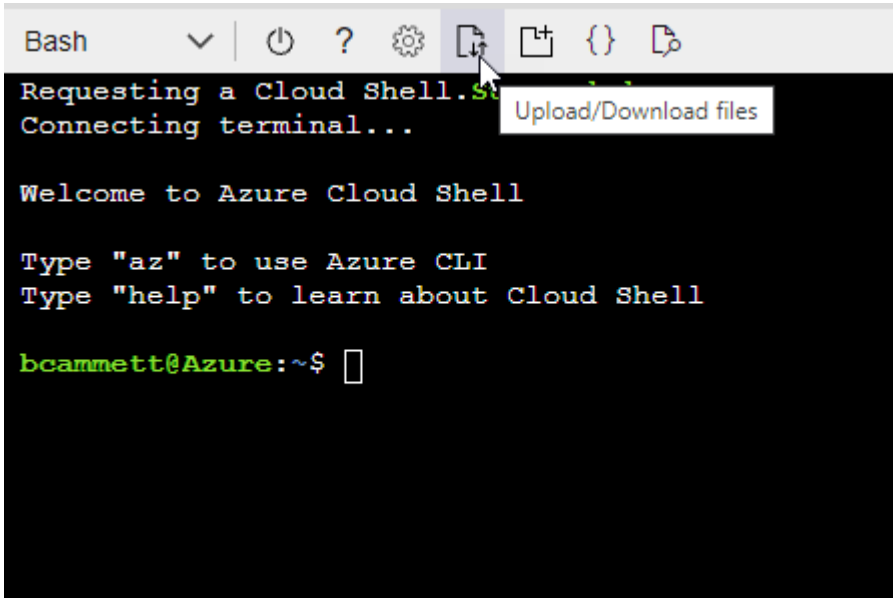
Exemplo

```
"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
Connector_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**.

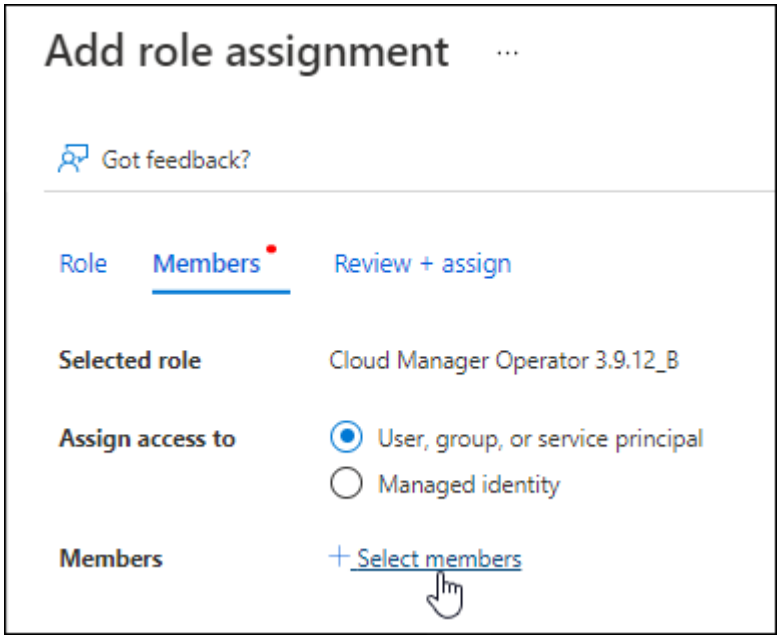
b. Selecione a assinatura.

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

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

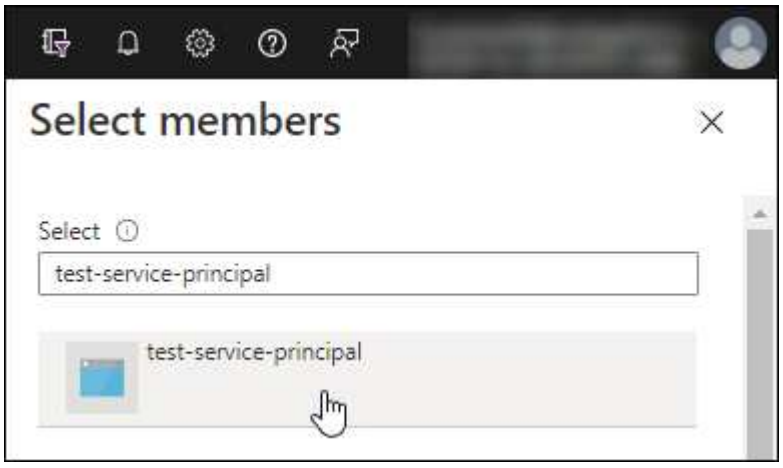
e. Na aba **Membros**, complete os seguintes passos:

- 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**.

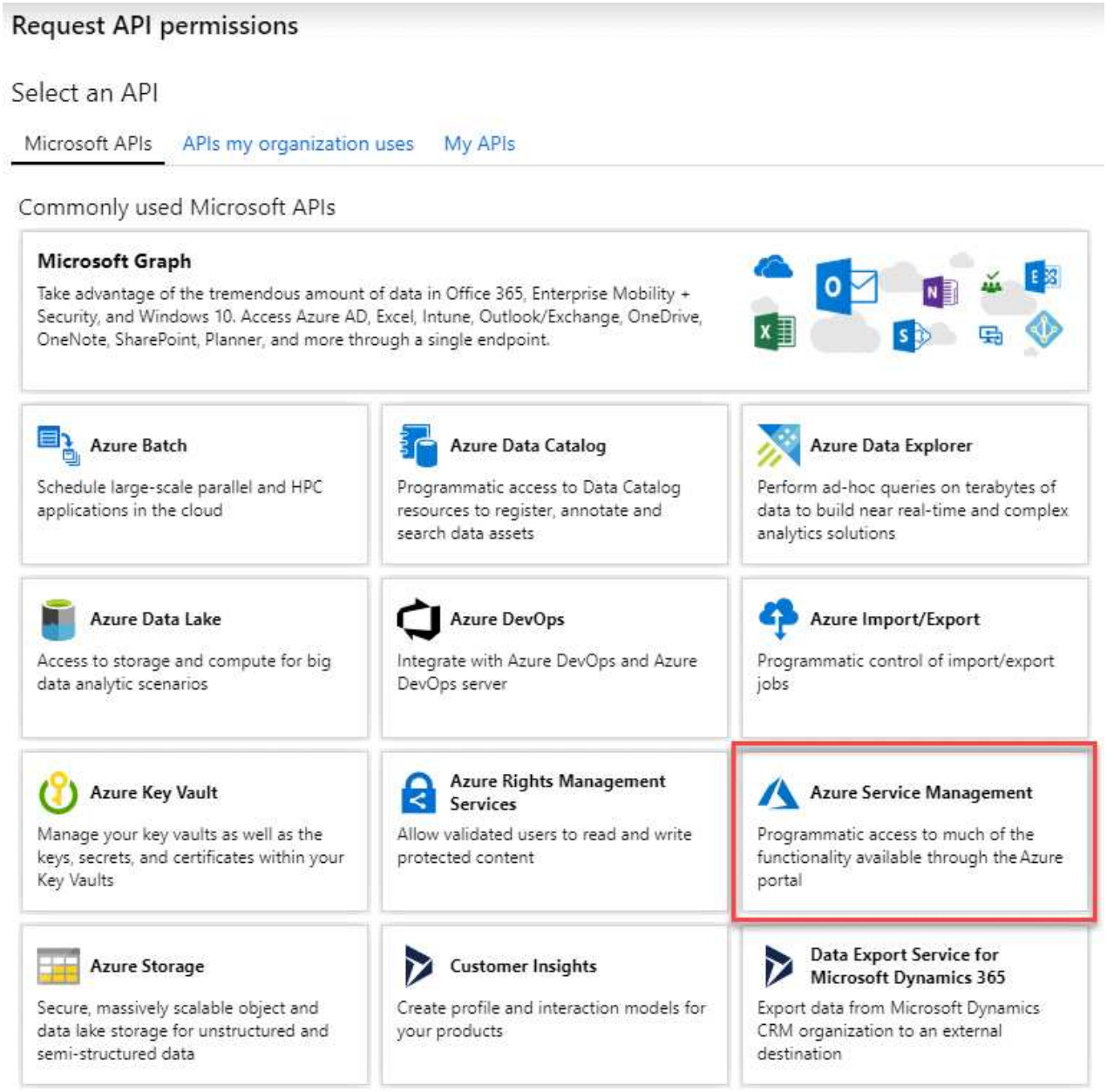
O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

Se você quiser implantar o Cloud Volumes ONTAP de várias assinaturas do Azure, será necessário

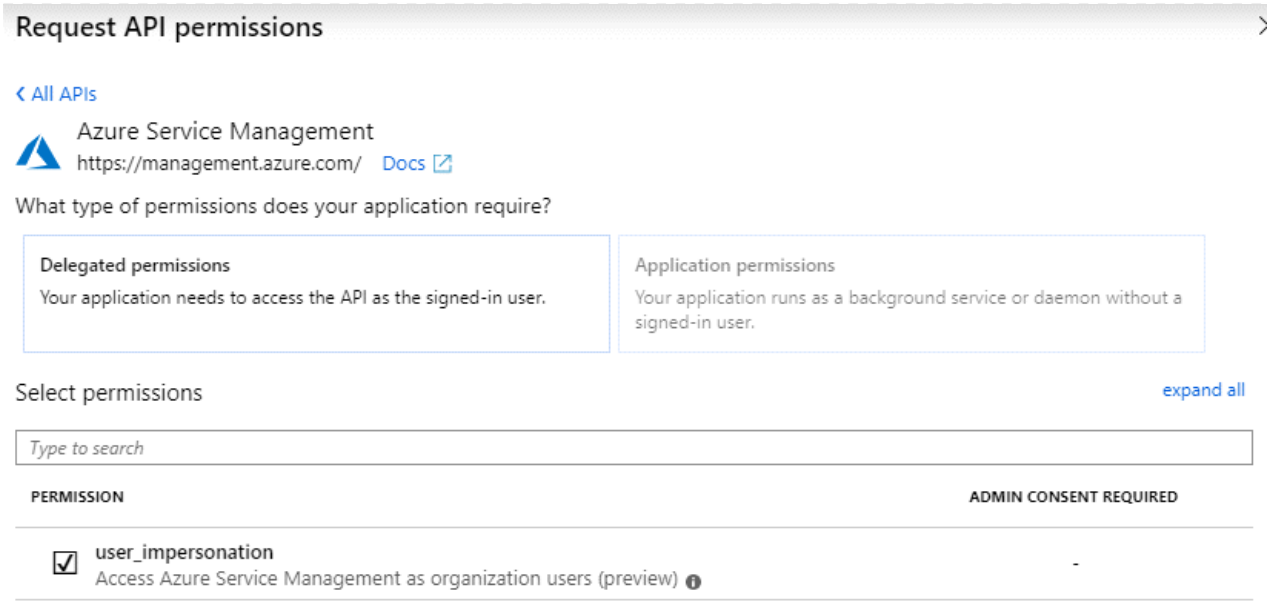
vincular a entidade de serviço a cada uma dessas assinaturas. No NetApp Console, você pode selecionar a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

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**.

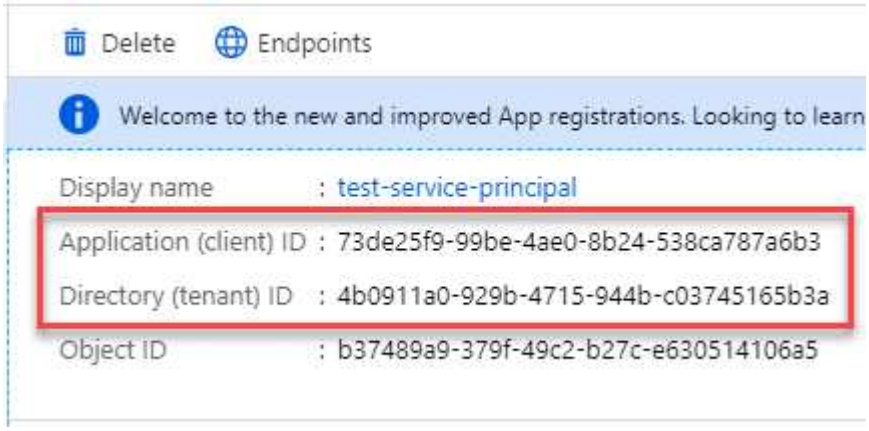


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



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

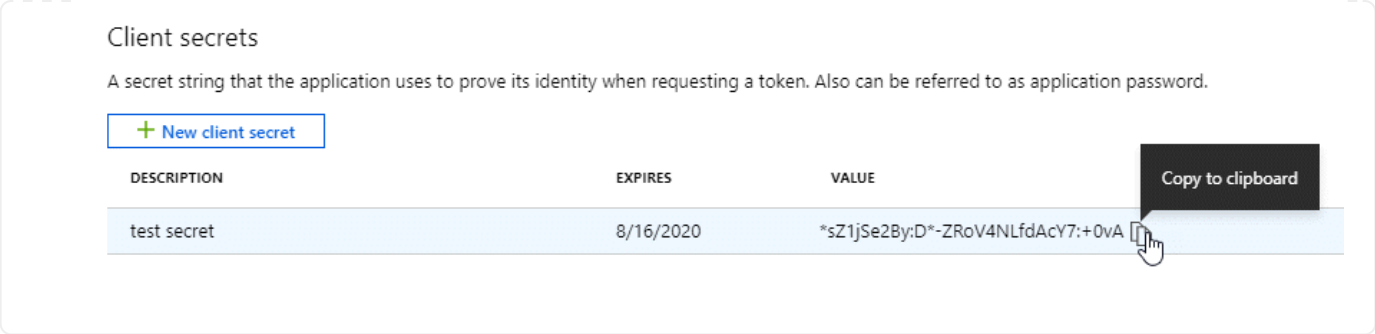
1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



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.



Etapa 4: criar o agente do console

Inicie o agente do Console diretamente do Azure Marketplace.

Sobre esta tarefa

A criação do agente do Console no Azure Marketplace configura uma máquina virtual com uma configuração padrão. "Saiba mais sobre a configuração padrão do agente do Console" .

Antes de começar

Você deve ter o seguinte:

- Uma assinatura do Azure.
- Uma VNet e uma sub-rede na região do Azure de sua escolha.
- Detalhes sobre um servidor proxy, caso sua organização exija um proxy para todo o tráfego de saída da Internet:
  - Endereço IP
  - Credenciais
  - Certificado HTTPS
- Uma chave pública SSH, se você quiser usar esse método de autenticação para a máquina virtual do agente do Console. A outra opção para o método de autenticação é usar uma senha.

  "Saiba mais sobre como se conectar a uma VM Linux no Azure"

- Se você não quiser que o Console crie automaticamente uma função do Azure para o agente do Console, será necessário criar sua própria"usando a política nesta página" .

  Essas permissões são para a própria instância do agente do Console. É um conjunto diferente de permissões do que você configurou anteriormente para implantar a VM do agente do Console.

Passos

1. Acesse a página da VM do agente do NetApp Console no Azure Marketplace.

   "Página do Azure Marketplace para regiões comerciais"

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.
- **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**.

  Essa configuração é importante porque uma identidade gerenciada permite que a máquina virtual do agente do Console se identifique no Microsoft Entra ID sem fornecer nenhuma credencial. "Saiba mais sobre identidades gerenciadas para recursos do Azure" .

4. Na página **Revisar + criar**, revise suas seleções e selecione **Criar** para iniciar a implantação.

   O Azure implanta a máquina virtual com as configurações especificadas. Você deverá ver a máquina virtual e o software do agente do console em execução em cerca de dez minutos.

   Se a instalação falhar, você poderá visualizar logs e um relatório para ajudar a solucionar problemas."Aprenda a solucionar problemas de instalação."

5. Abra um navegador da Web em um host que tenha uma conexão com a máquina virtual do agente do Console e insira o seguinte URL:

   https://ipaddress

6. Após efetuar login, configure o agente do Console:
   a. Especifique a organização do Console a ser associada ao agente do Console.
   b. Digite um nome para o sistema.
   c. Em **Você está executando em um ambiente seguro?** mantenha o modo restrito desabilitado.

      Mantenha o modo restrito desabilitado para usar o Console no modo padrão. Você deve habilitar o modo restrito somente se tiver um ambiente seguro e quiser desconectar esta conta dos serviços de backend do Console. Se for esse o caso,"siga os passos para começar a usar o Console no modo restrito" .

   d. Selecione **Vamos começar**.

Resultado

Agora você instalou o agente do Console e o configurou com sua organização do Console.

Se você tiver armazenamento de Blobs do Azure na mesma assinatura do Azure em que criou o agente do Console, verá um sistema de armazenamento de Blobs do Azure aparecer na página **Sistemas** automaticamente. "Aprenda a gerenciar o armazenamento de Blobs do Azure no Console"

Etapa 5: fornecer permissões ao agente do Console

Agora que você criou o agente do Console, precisa fornecer a ele as permissões que configurou anteriormente. Fornecer as permissões permite que o agente do Console gerencie seus dados e infraestrutura de armazenamento no Azure.

Função personalizada

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.

O que vem a seguir?

Vá para o "Console NetApp" para começar a usar o agente do Console.

Diretor de serviço

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 Console agora tem as permissões necessárias para executar ações no Azure em seu nome.

Instalar manualmente o agente do Console no Azure

Para instalar manualmente o agente do Console no seu próprio host Linux, você precisa revisar os requisitos do host, configurar sua rede, preparar as permissões do Azure, instalar o agente do Console e, em seguida, fornecer as permissões que você preparou.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Você deve revisar"Limitações do agente do console" .

Etapa 1: Revise os requisitos do host

O software do agente do Console deve ser executado em um host que atenda aos requisitos específicos do sistema operacional, requisitos de RAM, requisitos de porta e assim por diante.

O agente do Console reserva o intervalo de UID e GID de 19000 a 19200. Este intervalo é fixo e não pode ser modificado. Se algum software de terceiros no seu host estiver usando UIDs ou GIDs dentro desse intervalo, a instalação do agente falhará. A NetApp recomenda usar um host livre de software de terceiros para evitar conflitos.

Host dedicado

O agente do Console não é suportado em um host compartilhado com outros aplicativos. O host deve ser um host dedicado. O host pode ter qualquer arquitetura que atenda aos seguintes 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 Docker ou o Podman são arquitetados para criar os contêineres dentro deste diretório. Especificamente, eles criarão contêineres no `/var/lib/containers/storage` diretório. Montagens externas ou links simbólicos não funcionam neste espaço.

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 a
Red Hat Enterprise Linux	9.1 a 9.4 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 Ver requisitos de configuração do Podman .	Suportado no modo de imposição ou no modo permissivo • O gerenciamento de sistemas Cloud Volumes ONTAP NÃO é suportado por agentes que tenham o SELinux habilitado no sistema operacional.
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

Tamanho da VM do Azure

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos Standard_D8s_v3.

Espaço em disco em /opt

100 GiB de espaço devem estar disponíveis

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

Espaço em disco em /var

20 GiB de espaço devem estar disponíveis

O agente do Console requer este espaço em `/var` porque o Docker ou o Podman são arquitetados para criar os contêineres dentro deste diretório. Especificamente, eles criarão contêineres no

`/var/lib/containers/storage` diretório. Montagens externas ou links simbólicos não funcionam neste espaço.

Etapa 2: instalar 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 2. 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 8, verifique se sua versão do Podman está usando o DNS 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.

   Para Red Hat Enterprise Linux 9:

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

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

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<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.
6. Se estiver usando o Red Hat Enterprise:

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

   Para Red Hat Enterprise Linux 9:

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

   Para Red Hat Enterprise Linux 8:

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

7. 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.

8. 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.

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

      ```
      podman info | grep networkBackend
      ```

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

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

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

   d. 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 .

9. Reinicie o podman.

```
systemctl restart podman
```

10. 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 3: configurar a rede

Certifique-se de que o local de rede onde você planeja instalar o agente do Console suporte os seguintes requisitos. Atender a esses requisitos permite que o agente do Console gerencie recursos e processos dentro do seu ambiente de nuvem híbrida.

Região Azure

Se você usar o Cloud Volumes ONTAP, o agente do Console deverá ser implantado na mesma região do Azure que os sistemas Cloud Volumes ONTAP que ele gerencia ou no "Par de regiões do Azure" para os sistemas Cloud Volumes ONTAP . Esse requisito 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"

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados de computadores ao usar o NetApp Console baseado na Web

Os computadores que acessam o Console a partir de um navegador da web devem ter a capacidade de contatar vários terminais. Você precisará usar o Console para configurar o agente do Console e para o uso diário do Console.

"Preparar a rede para o console NetApp" .

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Para gerenciar recursos em regiões públicas do Azure.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Para gerenciar recursos nas regiões do Azure China.
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://support.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://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.

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 estiver planejando usar o NetApp Data Classification para verificar suas fontes de dados corporativos, deverá habilitar 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"

Etapa 4: configurar permissões de implantação do agente do console

Você precisa fornecer permissões do Azure ao agente do Console usando uma das seguintes opções:

- Opção 1: atribuir uma função personalizada à VM do Azure usando uma identidade gerenciada atribuída pelo sistema.
- Opção 2: forneça ao agente do Console as credenciais para uma entidade de serviço do Azure que tenha as permissões necessárias.

Siga as etapas para preparar permissões para o agente do Console.

Criar uma função personalizada para implantação 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.

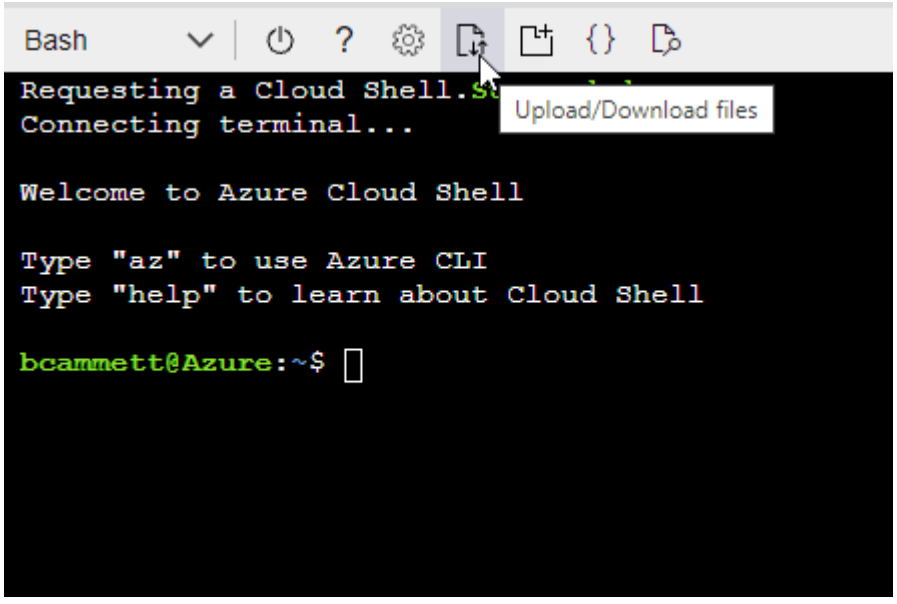
   Exemplo

   ```
   "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 Connector_Policy.json
```

Diretor de serviço

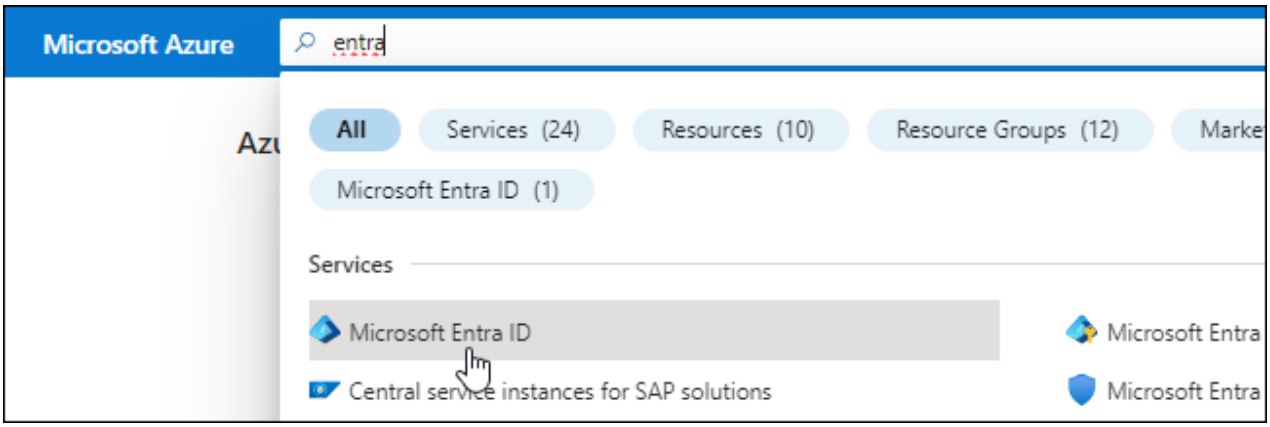
Crie e configure uma entidade de serviço no Microsoft Entra ID e obtenha as credenciais do Azure necessárias para o agente do Console.

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 .

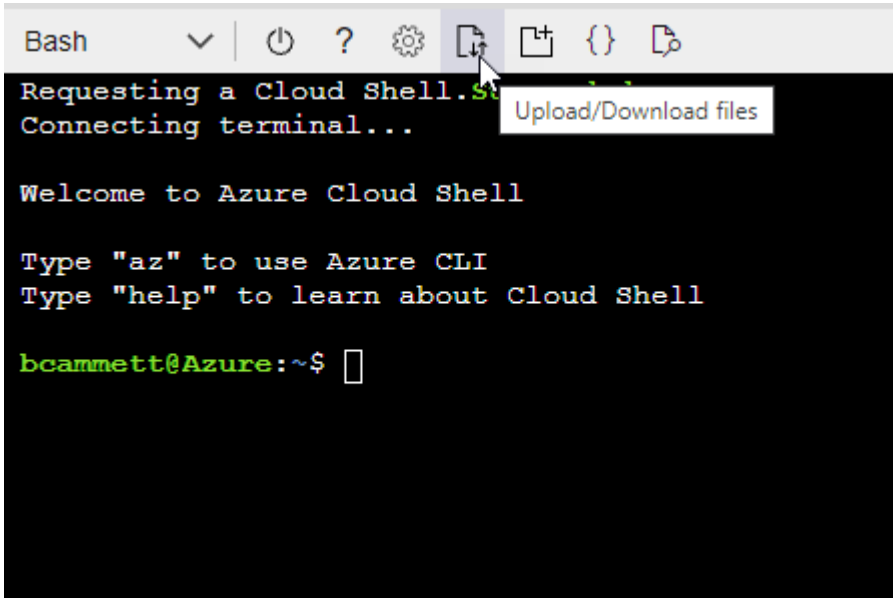
Exemplo

```
"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
Connector_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**.

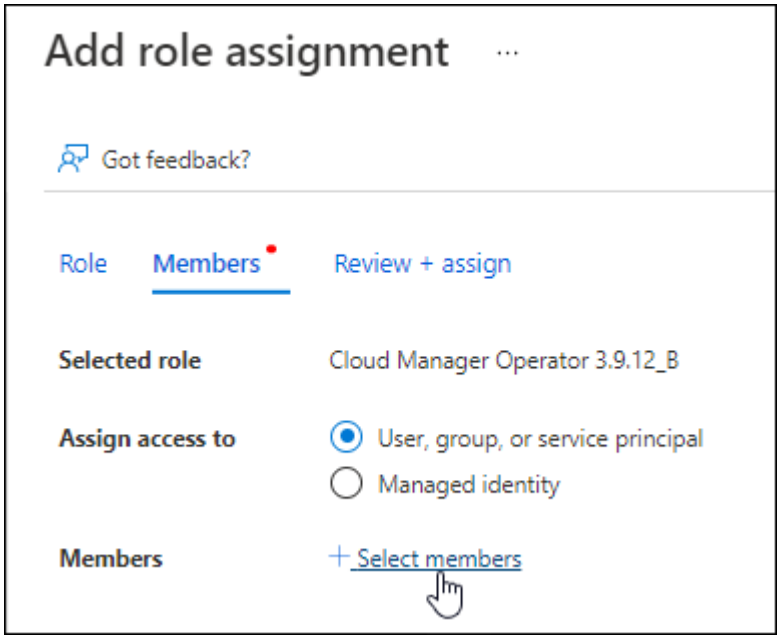
b. Selecione a assinatura.

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

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

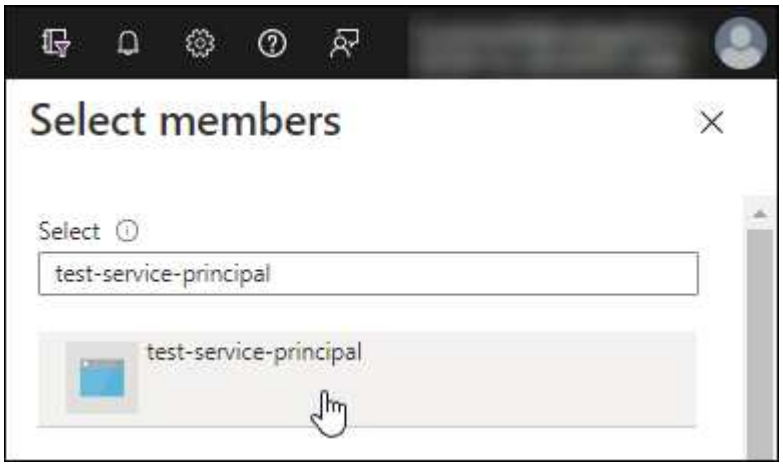
e. Na aba **Membros**, complete os seguintes passos:

- 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**.

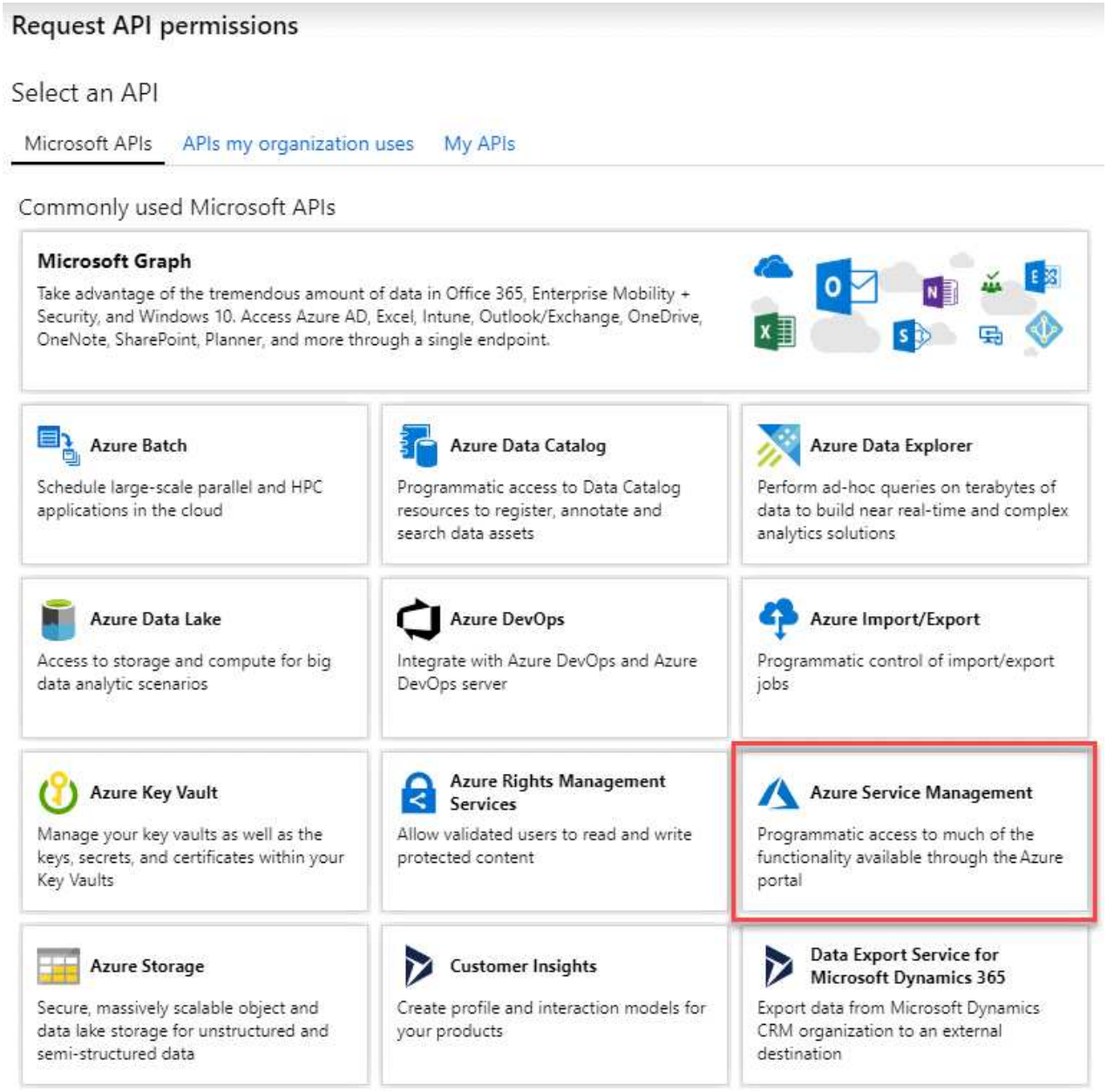
O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

Se você quiser implantar o Cloud Volumes ONTAP de várias assinaturas do Azure, será necessário

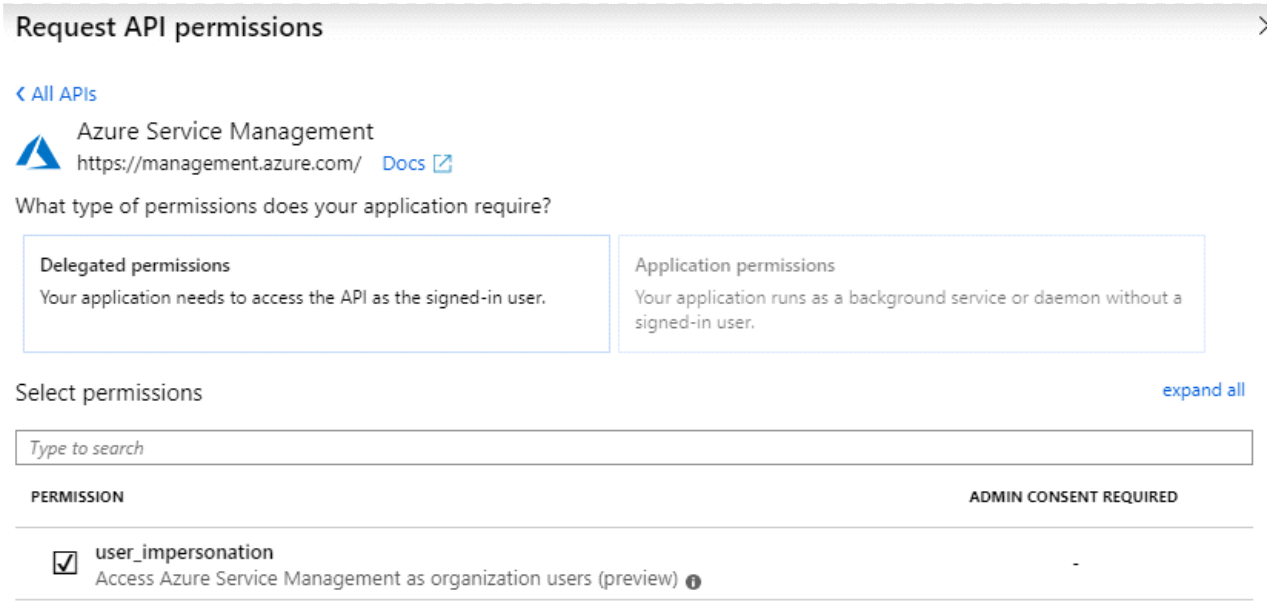
vincular a entidade de serviço a cada uma dessas assinaturas. No NetApp Console, você pode selecionar a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

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**.

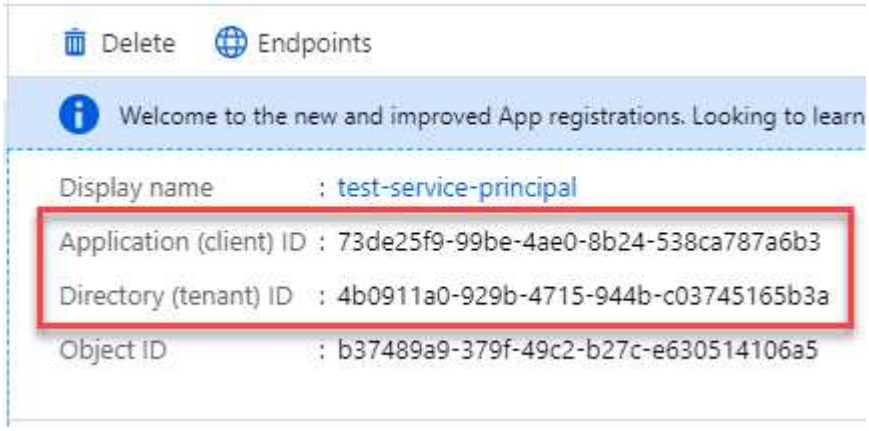


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



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.

Etapa 5: instalar o agente do console

Após a conclusão dos pré-requisitos, você pode instalar manualmente o software no seu próprio host Linux.

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" .

- Uma identidade gerenciada habilitada na VM no Azure para que você possa fornecer as permissões necessárias do Azure por meio de uma função personalizada.

  "Documentação do Microsoft Azure: Configurar identidades gerenciadas para recursos do Azure em uma VM usando o portal do Azure"

Sobre esta tarefa

O instalador disponível no site de suporte da NetApp pode ser uma versão anterior. Após a instalação, o 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 em "Site de suporte da NetApp" e, em seguida, copie-o para o host Linux.

   Você deve baixar o instalador do agente "online" destinado ao uso em sua rede ou na nuvem.

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 transparente ou explícito. Os parâmetros --proxy e --cacert são opcionais e você não será solicitado a adicioná-los. Se você tiver um servidor proxy, precisará inserir os parâmetros conforme mostrado.

   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-de-usuário:senha@endereço:porta
   - http://nome-de-domínio%92nome-de-usuário:senha@endereço:porta
   - https://endereço:porta
   - https://nome-de-usuário:senha@endereço:porta
   - https://nome-de-domínio%92nome-de-usuário:senha@endereço:porta

Observe o seguinte:

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

  Por exemplo:

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

`--cacert`especifica um certificado assinado pela CA a ser usado para acesso HTTPS entre o agente do Console e o servidor proxy. Este parâmetro é necessário para servidores proxy HTTPS, servidores proxy de interceptação e servidores proxy transparentes.

+ Aqui está um exemplo de configuração de um servidor proxy transparente. Ao configurar um proxy transparente, você não precisa definir o servidor proxy. Você só adiciona um certificado assinado pela CA ao host do agente do Console:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

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
      ...
      # 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
      ...
      Esc:wq
      ```

   c. Reinicie a máquina virtual do agente do Console.
2. Aguarde a conclusão da instalação.

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

Se a instalação falhar, você pode visualizar o relatório e os logs da instalação para ajudar a corrigir os problemas."Aprenda a solucionar problemas de instalação."

1. Abra um navegador da Web em um host que tenha uma conexão com a máquina virtual do agente do Console e insira o seguinte URL:

   https://ipaddress

2. Após efetuar login, configure o agente do Console:
   a. Especifique a organização a ser associada ao agente do Console.
   b. Digite um nome para o sistema.
   c. Em **Você está executando em um ambiente seguro?** mantenha o modo restrito desabilitado.

      Você deve manter o modo restrito desabilitado porque estas etapas descrevem como usar o Console no modo padrão. Você deve habilitar o modo restrito somente se tiver um ambiente seguro e quiser desconectar esta conta dos serviços de backend. Se for esse o caso,"siga as etapas para começar a usar o NetApp Console no modo restrito" .

   d. Selecione **Vamos começar**.

Se você tiver armazenamento de Blobs do Azure na mesma assinatura do Azure em que criou o agente do Console, verá um sistema de armazenamento de Blobs do Azure aparecer na página **Sistemas** automaticamente. "Aprenda a gerenciar o armazenamento de Blobs do Azure no NetApp Console"

Etapa 6: fornecer permissões ao NetApp Console

Agora que você instalou o agente do Console, precisa fornecer a ele as permissões do Azure que você configurou anteriormente. Fornecer as permissões permite que o Console gerencie seus dados e infraestrutura de armazenamento no Azure.

Função personalizada

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.

O que vem a seguir?

Vá para o "Console NetApp" para começar a usar o agente do Console.

Diretor de serviço

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 agente do Console agora tem as permissões necessárias para executar ações no Azure em seu nome.

Google Cloud

Opções de instalação do agente de console no Google Cloud

Existem algumas maneiras diferentes de criar um agente do Console no Google Cloud. Diretamente do NetApp Console é a maneira mais comum. ---

As seguintes opções de instalação estão disponíveis:

- "Crie o agente do Console diretamente do Console"(esta é a opção padrão)

  Esta ação inicia uma instância de VM executando Linux e o software do agente do Console em uma VPC de sua escolha.

- "Crie o agente do Console usando a plataforma Google"

  Esta ação também inicia uma instância de VM executando o Linux e o software do agente do Console, mas a implantação é iniciada diretamente do Google Cloud, e não do Console.

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

A opção de instalação escolhida afeta a maneira como você se prepara para a instalação. Isso inclui como você fornece ao Console as permissões necessárias para autenticar e gerenciar recursos no Google Cloud.

Crie um agente de console no Google Cloud a partir do NetApp Console

Você pode criar um agente do Console no Google Cloud a partir do Console. Você precisa configurar sua rede, preparar as permissões do Google Cloud, habilitar as APIs do Google Cloud e, em seguida, criar o agente do Console.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Você deve revisar"Limitações do agente do console" .

Etapa 1: configurar a rede

Configure a rede para garantir que o agente do Console possa gerenciar recursos, com conexões a redes de destino e acesso de saída à Internet.

VPC e sub-rede

Ao criar o agente do Console, você precisa especificar a VPC e a sub-rede onde ele deve residir.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://www.googleapis.com/deploymentmanager/v2/projects	Para gerenciar recursos no Google Cloud.
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://support.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://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.

Endpoints contatados do console NetApp

À medida que você usa o NetApp Console baseado na Web fornecido pela camada SaaS, ele entra em contato com vários endpoints para concluir tarefas de gerenciamento de dados. Isso inclui endpoints que são contatados para implantar o agente do Console a partir do Console.

"Exibir a lista de endpoints contatados pelo console do NetApp" .

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 estiver planejando usar o NetApp Data Classification para verificar suas fontes de dados corporativos, deverá habilitar 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"

Implemente este requisito de rede após criar o agente do Console.

Etapa 2: configurar permissões para criar o agente do Console

Antes de poder implantar um agente do Console a partir do Console, você precisa configurar permissões para o usuário da Plataforma Google que implanta a VM do agente do Console.

Passos

1. Crie uma função personalizada na plataforma Google:

   a. Crie um arquivo YAML que inclua as seguintes permissões:

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
```

```
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list
```

b. No Google Cloud, ative o Cloud Shell.

c. Faça upload do arquivo YAML que inclui as permissões necessárias.

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

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

gcloud iam roles criar connectorDeployment --project=myproject --file=connector-deployment.yaml

"Documentação do Google Cloud: Criação e gerenciamento de funções personalizadas"

2. Atribua esta função personalizada ao usuário que implantará o agente do Console a partir do Console ou usando o gcloud.

"Documentação do Google Cloud: Conceder uma única função"

Etapa 3: Configurar permissões para as operações do agente do Console

Uma conta de serviço do Google Cloud é necessária para fornecer ao agente do Console as permissões necessárias para que o Console gerencie recursos no Google Cloud. Ao criar o agente do Console, você precisará associar essa conta de serviço à VM do agente do Console.

É sua responsabilidade atualizar a função personalizada à medida que novas permissões são adicionadas em versões subsequentes. Se novas permissões forem necessárias, elas serão listadas nas notas de versão.

Passos

1. Crie uma função personalizada no Google Cloud:

   a. Crie um arquivo YAML que inclua o conteúdo do"permissões de conta de serviço para o agente do Console" .

   b. No Google Cloud, ative o Cloud Shell.

   c. Faça upload do arquivo YAML que inclui as permissões necessárias.

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

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

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

   "Documentação do Google Cloud: Criação e gerenciamento de funções personalizadas"

2. Crie uma conta de serviço no Google Cloud e atribua a função à conta de serviço:

   a. No serviço IAM e Admin, selecione **Contas de serviço > Criar conta de serviço**.

   b. Insira os detalhes da conta de serviço e selecione **Criar e continuar**.

   c. Selecione a função que você acabou de criar.

   d. Conclua as etapas restantes para criar a função.

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

3. Se você planeja implantar sistemas Cloud Volumes ONTAP em projetos diferentes daquele em que o agente do Console reside, será necessário fornecer à conta de serviço do agente do Console acesso a esses projetos.

   Por exemplo, digamos que o agente do Console esteja no projeto 1 e você queira criar sistemas Cloud Volumes ONTAP no projeto 2. Você precisará conceder acesso à conta de serviço no projeto 2.

   a. No serviço IAM e Admin, selecione o projeto do Google Cloud onde você deseja criar sistemas Cloud

Volumes ONTAP .

b. Na página **IAM**, selecione **Conceder acesso** e forneça os detalhes necessários.
   - Digite o e-mail da conta de serviço do agente do Console.
   - Selecione a função personalizada do agente do Console.
   - Selecione **Salvar**.

Para mais detalhes, consulte "Documentação do Google Cloud"

Etapa 4: configurar permissões de VPC compartilhadas

Se você estiver usando uma VPC compartilhada para implantar recursos em um projeto de serviço, precisará preparar suas permissões.

Esta tabela é para referência e seu ambiente deve refletir a tabela de permissões quando a configuração do IAM estiver concluída.

Exibir permissões de VPC compartilhadas

Identidade	Criador	Hospedado em	Permissões do projeto de serviço	Permissões do projeto host	Propósito
Conta do Google para implantar o agente	Personalizado	Projeto de Serviço	"Política de implantação do agente"	compute.networkUser	Implantando o agente no projeto de serviço
conta de serviço do agente	Personalizado	Projeto de serviço	"Política de conta de serviço do agente"	compute.networkUser gerenciador de implantação.editor	Implantando e mantendo o Cloud Volumes ONTAP e serviços no projeto de serviço
Conta de serviço Cloud Volumes ONTAP	Personalizado	Projeto de serviço	membro storage.admin: conta de serviço do NetApp Console como serviceAccount.user	N / D	(Opcional) Para NetApp Cloud Tiering e NetApp Backup and Recovery
Agente de serviço de APIs do Google	Google Cloud	Projeto de serviço	(Padrão) Editor	compute.networkUser	Interage com as APIs do Google Cloud em nome da implantação. Permite que o Console use a rede compartilhada.
Conta de serviço padrão do Google Compute Engine	Google Cloud	Projeto de serviço	(Padrão) Editor	compute.networkUser	Implanta instâncias do Google Cloud e infraestrutura de computação em nome da implantação. Permite que o Console use a rede compartilhada.

Observações:

1. deploymentmanager.editor só é necessário no projeto host se você não estiver passando regras de firewall para a implantação e optar por deixar que o Console as crie para você. O NetApp Console cria uma implantação no projeto host que contém a regra de firewall VPC0 se nenhuma regra for especificada.
2. firewall.create e firewall.delete só são necessários se você não estiver passando regras de firewall para a implantação e optar por deixar que o Console as crie para você. Essas permissões residem no arquivo .yaml da conta do Console. Se você estiver implantando um par de HA usando uma VPC compartilhada, essas permissões serão usadas para criar as regras de firewall para VPC1, 2 e 3. Para todas as outras implantações, essas permissões também serão usadas para criar regras para VPC0.
3. Para Cloud Tiering, a conta de serviço de hierarquização deve ter a função serviceAccount.user na conta de serviço, não apenas no nível do projeto. Atualmente, se você atribuir serviceAccount.user

no nível do projeto, as permissões não serão exibidas quando você consultar a conta de serviço com getIAMPolicy.

Etapa 5: habilitar as APIs do Google Cloud

Você deve habilitar várias APIs do Google Cloud antes de implantar o agente do Console e o Cloud Volumes ONTAP.

Etapa

1. Ative as seguintes APIs do Google Cloud no seu projeto:
   - 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))

"Documentação do Google Cloud: Habilitando APIs"

Etapa 6: Criar o agente do Console

Crie um agente do Console diretamente do Console.

Sobre esta tarefa

A criação do agente do Console implanta uma instância de máquina virtual no Google Cloud usando uma configuração padrão. Não mude para uma instância de VM menor com menos CPUs ou menos RAM depois de criar o agente do Console. "Saiba mais sobre a configuração padrão do agente do Console" .

Antes de começar

Você deve ter o seguinte:

- As permissões necessárias do Google Cloud para criar o agente do Console e uma conta de serviço para a VM do agente do Console.
- Uma VPC e uma sub-rede que atendem aos requisitos de rede.
- Detalhes sobre um servidor proxy, caso um proxy seja necessário para acesso à Internet a partir do agente do Console.

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione **Implantar agente > Google Cloud**
3. Na página **Implantando um agente**, revise os detalhes sobre o que você precisará. Você tem duas opções:
   a. Selecione **Continuar** para se preparar para a implantação usando o guia do produto. Cada etapa do guia do produto inclui as informações contidas nesta página da documentação.

b. Selecione **Ir para a implantação** se você já se preparou seguindo as etapas desta página.

4. Siga as etapas do assistente para criar o agente do Console:
   - Se solicitado, faça login na sua conta do Google, que deve ter as permissões necessárias para criar a instância da máquina virtual.

     O formulário é de propriedade e hospedado pelo Google. Suas credenciais não são fornecidas à NetApp.

   - **Detalhes**: Insira um nome para a instância da máquina virtual, especifique tags, selecione um projeto e, em seguida, selecione a conta de serviço que tem as permissões necessárias (consulte a seção acima para obter detalhes).
   - **Localização**: especifique uma região, zona, VPC e sub-rede para a instância.
   - **Rede**: Escolha se deseja habilitar um endereço IP público e, opcionalmente, especifique uma configuração de proxy.
   - **Tags de rede**: adicione uma tag de rede à instância do agente do Console se estiver usando um proxy transparente. As tags de rede devem começar com uma letra minúscula e podem conter letras minúsculas, números e hifens. As tags devem terminar com uma letra minúscula ou um número. Por exemplo, você pode usar a tag "console-agent-proxy".
   - **Política de firewall**: escolha se deseja criar uma nova política de firewall ou selecionar uma política de firewall existente que permita as regras de entrada e saída necessárias.

     "Regras de firewall no Google Cloud"

5. Revise suas seleções para verificar se sua configuração está correta.

   a. A caixa de seleção **Validar configuração do agente** é marcada por padrão para que o Console valide os requisitos de conectividade de rede quando você implantar. Se o Console não conseguir implantar o agente, ele fornecerá um relatório para ajudar você a solucionar o problema. Se a implantação for bem-sucedida, nenhum relatório será fornecido.

   Se você ainda estiver usando o"pontos finais anteriores" usado para atualizações de agentes, a validação falha com um erro. Para evitar isso, desmarque a caixa de seleção para pular a verificação de validação.

6. Selecione **Adicionar**.

   A instância estará pronta em aproximadamente 10 minutos; permaneça na página até que o processo seja concluído.

Resultado

Após a conclusão do processo, o agente do Console estará disponível para uso.

Se a implantação falhar, você poderá baixar um relatório e logs do Console para ajudar a corrigir os problemas."Aprenda a solucionar problemas de instalação."

Se você tiver buckets do Google Cloud Storage na mesma conta do Google Cloud onde criou o agente do Console, verá um sistema do Google Cloud Storage aparecer na página **Sistemas** automaticamente. "Aprenda a gerenciar o Google Cloud Storage pelo Console"

Para criar um agente do Console no Google Cloud usando o Google Cloud, você precisa configurar sua rede, preparar as permissões do Google Cloud, habilitar as APIs do Google Cloud e, em seguida, criar o agente do Console.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Você deve revisar"Limitações do agente do console" .

Etapa 1: configurar a rede

Configure a rede para permitir que o agente do Console gerencie recursos e se conecte às redes de destino e à Internet.

VPC e sub-rede

Ao criar o agente do Console, você precisa especificar a VPC e a sub-rede onde ele deve residir.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://www.googleapis.com/deploymentmanager/v2/projects	Para gerenciar recursos no Google Cloud.
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .

Pontos finais	Propósito
\ https://support.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://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.

Endpoints contatados do console NetApp

À medida que você usa o NetApp Console baseado na Web fornecido pela camada SaaS, ele entra em contato com vários endpoints para concluir tarefas de gerenciamento de dados. Isso inclui endpoints que

são contatados para implantar o agente do Console a partir do Console.

"Exibir a lista de endpoints contatados pelo console do NetApp" .

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 estiver planejando usar o NetApp Data Classification para verificar suas fontes de dados corporativos, deverá habilitar 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"

Implemente este requisito de rede após criar o agente do Console.

Etapa 2: configurar permissões para criar o agente do Console

Configure permissões para o usuário do Google Cloud implantar a VM do agente do Console do Google Cloud.

Passos

1. Crie uma função personalizada na plataforma Google:

   a. Crie um arquivo YAML que inclua as seguintes permissões:

```
title: Console agent deployment policy
description: Permissions for the user who deploys the NetApp Console
agent
```

```
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
```

```
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list
```

b. No Google Cloud, ative o Cloud Shell.

c. Faça upload do arquivo YAML que inclui as permissões necessárias.

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

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

gcloud iam roles criar connectorDeployment --project=myproject --file=connector-deployment.yaml

"Documentação do Google Cloud: Criação e gerenciamento de funções personalizadas"

2. Atribua esta função personalizada ao usuário que implanta o agente do Console do Google Cloud.

"Documentação do Google Cloud: Conceder uma única função"

Etapa 3: Configurar permissões para as operações do agente do Console

Uma conta de serviço do Google Cloud é necessária para fornecer ao agente do Console as permissões necessárias para que o Console gerencie recursos no Google Cloud. Ao criar o agente do Console, você precisará associar essa conta de serviço à VM do agente do Console.

É sua responsabilidade atualizar a função personalizada à medida que novas permissões são adicionadas em versões subsequentes. Se novas permissões forem necessárias, elas serão listadas nas notas de versão.

Passos

1. Crie uma função personalizada no Google Cloud:

a. Crie um arquivo YAML que inclua o conteúdo do"permissões de conta de serviço para o agente do Console" .

b. No Google Cloud, ative o Cloud Shell.

c. Faça upload do arquivo YAML que inclui as permissões necessárias.

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

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

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

"Documentação do Google Cloud: Criação e gerenciamento de funções personalizadas"

2. Crie uma conta de serviço no Google Cloud e atribua a função à conta de serviço:
   a. No serviço IAM e Admin, selecione **Contas de serviço > Criar conta de serviço**.
   b. Insira os detalhes da conta de serviço e selecione **Criar e continuar**.
   c. Selecione a função que você acabou de criar.
   d. Conclua as etapas restantes para criar a função.

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

3. Se você planeja implantar sistemas Cloud Volumes ONTAP em projetos diferentes daquele em que o agente do Console reside, será necessário fornecer à conta de serviço do agente do Console acesso a esses projetos.

   Por exemplo, digamos que o agente do Console esteja no projeto 1 e você queira criar sistemas Cloud Volumes ONTAP no projeto 2. Você precisará conceder acesso à conta de serviço no projeto 2.

   a. No serviço IAM e Admin, selecione o projeto do Google Cloud onde você deseja criar sistemas Cloud Volumes ONTAP .
   b. Na página **IAM**, selecione **Conceder acesso** e forneça os detalhes necessários.
      - Digite o e-mail da conta de serviço do agente do Console.
      - Selecione a função personalizada do agente do Console.
      - Selecione **Salvar**.

   Para mais detalhes, consulte "Documentação do Google Cloud"

Etapa 4: configurar permissões de VPC compartilhadas

Se você estiver usando uma VPC compartilhada para implantar recursos em um projeto de serviço, precisará preparar suas permissões.

Esta tabela é para referência e seu ambiente deve refletir a tabela de permissões quando a configuração do IAM estiver concluída.

Exibir permissões de VPC compartilhadas

Identidade	Criador	Hospedado em	Permissões do projeto de serviço	Permissões do projeto host	Propósito
Conta do Google para implantar o agente	Personalizado	Projeto de Serviço	"Política de implantação do agente"	compute.networkUser	Implantando o agente no projeto de serviço
conta de serviço do agente	Personalizado	Projeto de serviço	"Política de conta de serviço do agente"	compute.networkUser gerenciador de implantação.editor	Implantando e mantendo o Cloud Volumes ONTAP e serviços no projeto de serviço
Conta de serviço Cloud Volumes ONTAP	Personalizado	Projeto de serviço	membro storage.admin: conta de serviço do NetApp Console como serviceAccount.user	N / D	(Opcional) Para NetApp Cloud Tiering e NetApp Backup and Recovery
Agente de serviço de APIs do Google	Google Cloud	Projeto de serviço	(Padrão) Editor	compute.networkUser	Interage com as APIs do Google Cloud em nome da implantação. Permite que o Console use a rede compartilhada.
Conta de serviço padrão do Google Compute Engine	Google Cloud	Projeto de serviço	(Padrão) Editor	compute.networkUser	Implanta instâncias do Google Cloud e infraestrutura de computação em nome da implantação. Permite que o Console use a rede compartilhada.

Observações:

1. deploymentmanager.editor só é necessário no projeto host se você não estiver passando regras de firewall para a implantação e optar por deixar que o Console as crie para você. O NetApp Console cria uma implantação no projeto host que contém a regra de firewall VPC0 se nenhuma regra for especificada.
2. firewall.create e firewall.delete só são necessários se você não estiver passando regras de firewall para a implantação e optar por deixar que o Console as crie para você. Essas permissões residem no arquivo .yaml da conta do Console. Se você estiver implantando um par de HA usando uma VPC compartilhada, essas permissões serão usadas para criar as regras de firewall para VPC1, 2 e 3. Para todas as outras implantações, essas permissões também serão usadas para criar regras para VPC0.
3. Para Cloud Tiering, a conta de serviço de hierarquização deve ter a função serviceAccount.user na conta de serviço, não apenas no nível do projeto. Atualmente, se você atribuir serviceAccount.user

no nível do projeto, as permissões não serão exibidas quando você consultar a conta de serviço com getIAMPolicy.

Etapa 5: habilitar as APIs do Google Cloud

Habilite várias APIs do Google Cloud antes de implantar o agente do Console e o Cloud Volumes ONTAP.

Etapa

1. Ative as seguintes APIs do Google Cloud no seu projeto:
   - 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))

"Documentação do Google Cloud: Habilitando APIs"

Etapa 6: Criar o agente do Console

Crie um agente do Console usando o Google Cloud.

A criação do agente do Console implanta uma instância de VM no Google Cloud com a configuração padrão. Não mude para uma instância de VM menor com menos CPUs ou menos RAM depois de criar o agente do Console. "Saiba mais sobre a configuração padrão do agente do Console" .

Antes de começar

Você deve ter o seguinte:

- As permissões necessárias do Google Cloud para criar o agente do Console e uma conta de serviço para a VM do agente do Console.
- Uma VPC e uma sub-rede que atendem aos requisitos de rede.
- Uma compreensão dos requisitos da instância de VM.
  - **CPU**: 8 núcleos ou 8 vCPUs
  - **RAM**: 32 GB
  - **Tipo de máquina**: Recomendamos n2-standard-8.

    O agente do Console é compatível com o Google Cloud em uma instância de VM com um sistema operacional compatível com recursos de VM protegida.

Passos

1. Faça login no Google Cloud SDK usando seu método preferido.

   Este exemplo usa um shell local com o gcloud SDK instalado, mas você também pode usar o Google

Cloud Shell.

Para obter mais informações sobre o Google Cloud SDK, visite o"Página de documentação do Google Cloud SDK" .

2. Verifique se você está conectado como um usuário que possui as permissões necessárias definidas na seção acima:

```
gcloud auth list
```

A saída deve mostrar o seguinte, onde * a conta de usuário é a conta de usuário desejada para efetuar login:

```
Credentialed Accounts
ACTIVE  ACCOUNT
     some_user_account@domain.com
*    desired_user_account@domain.com
To set the active account, run:
 $ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install them,
please run:
$ gcloud components update
```

3. Execute o `gcloud compute instances create` comando:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-8
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

nome da instância
: O nome da instância desejada para a instância da VM.

projeto
: (Opcional) O projeto onde você deseja implantar a VM.

conta de serviço

A conta de serviço especificada na saída da etapa 2.

zona

A zona onde você deseja implantar a VM

sem endereço

(Opcional) Nenhum endereço IP externo é usado (você precisa de um NAT ou proxy na nuvem para rotear o tráfego para a Internet pública)

tag de rede

(Opcional) Adicione marcação de rede para vincular uma regra de firewall usando tags à instância do agente do Console

caminho de rede

(Opcional) Adicione o nome da rede na qual implantar o agente do Console (para uma VPC compartilhada, você precisa do caminho completo)

caminho de sub-rede

(Opcional) Adicione o nome da sub-rede para implantar o agente do Console (para uma VPC compartilhada, você precisa do caminho completo)

kms-chave-caminho

(Opcional) Adicione uma chave KMS para criptografar os discos do agente do Console (as permissões do IAM também precisam ser aplicadas)

Para mais informações sobre essas bandeiras, visite o"Documentação do SDK de computação do Google Cloud" .

Executar o comando implanta o agente do Console. A instância do agente do Console e o software devem estar em execução em aproximadamente cinco minutos.

4. Abra um navegador da Web e insira o URL do host do agente do Console:

   O URL do host do console pode ser um host local, um endereço IP privado ou um endereço IP público, dependendo da configuração do host. Por exemplo, se o agente do Console estiver na nuvem pública sem um endereço IP público, você deverá inserir um endereço IP privado de um host que tenha uma conexão com o host do agente do Console.

5. Após efetuar login, configure o agente do Console:
   a. Especifique a organização do Console a ser associada ao agente do Console.

      "Aprenda sobre gerenciamento de identidade e acesso" .

   b. Digite um nome para o sistema.

Resultado

O agente do Console agora está instalado e configurado com sua organização do Console.

Abra um navegador da web e vá para o "Console NetApp" para começar a usar o agente do Console.

Instalar manualmente o agente do Console no Google Cloud

Para instalar manualmente o agente do Console no seu próprio host Linux, você precisa revisar os requisitos do host, configurar sua rede, preparar as permissões do Google Cloud, habilitar as APIs do Google Cloud, instalar o Console e, em seguida, fornecer as permissões que você preparou.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Você deve revisar"Limitações do agente do console" .

Etapa 1: Revise os requisitos do host

O software do agente do Console deve ser executado em um host que atenda aos requisitos específicos do sistema operacional, requisitos de RAM, requisitos de porta e assim por diante.

> O agente do Console reserva o intervalo de UID e GID de 19000 a 19200. Este intervalo é fixo e não pode ser modificado. Se algum software de terceiros no seu host estiver usando UIDs ou GIDs dentro desse intervalo, a instalação do agente falhará. A NetApp recomenda usar um host livre de software de terceiros para evitar conflitos.

Host dedicado

O agente do Console não é suportado em um host compartilhado com outros aplicativos. O host deve ser um host dedicado. O host pode ter qualquer arquitetura que atenda aos seguintes 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 Docker ou o Podman são arquitetados para criar os contêineres dentro deste diretório. Especificamente, eles criarão contêineres no `/var/lib/containers/storage` diretório. Montagens externas ou links simbólicos não funcionam neste espaço.

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 a
Red Hat Enterprise Linux	9.1 a 9.4 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 Ver requisitos de configuração do Podman .	Suportado no modo de imposição ou no modo permissivo • O gerenciamento de sistemas Cloud Volumes ONTAP NÃO é suportado por agentes que tenham o SELinux habilitado no sistema operacional.
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

Tipo de máquina do Google Cloud

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos 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"

Espaço em disco em /opt

100 GiB de espaço devem estar disponíveis

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

Espaço em disco em /var

20 GiB de espaço devem estar disponíveis

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

Etapa 2: instalar 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 3. 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 8, verifique se sua versão do Podman está usando o DNS 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.

   Para Red Hat Enterprise Linux 9:

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

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

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<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.
6. Se estiver usando o Red Hat Enterprise:

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

   Para Red Hat Enterprise Linux 9:

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

   Para Red Hat Enterprise Linux 8:

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

7. 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.

8. 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.

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

      ```
      podman info | grep networkBackend
      ```

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

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

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

   d. 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 .

9. Reinicie o podman.

```
systemctl restart podman
```

10. 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 3: configurar a rede

Configure sua rede para que o agente do Console possa gerenciar recursos e processos dentro do seu ambiente de nuvem híbrida. Por exemplo, você precisa garantir que as conexões estejam disponíveis para as redes de destino e que o acesso de saída à Internet esteja disponível.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados de computadores ao usar o NetApp Console baseado na Web

Os computadores que acessam o Console a partir de um navegador da web devem ter a capacidade de contatar vários terminais. Você precisará usar o Console para configurar o agente do Console e para o uso diário do Console.

"Preparar a rede para o console NetApp" .

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://www.googleapis.com/deploymentmanager/v2/projects	Para gerenciar recursos no Google Cloud.
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://support.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://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.

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 estiver planejando usar o NetApp Data Classification para verificar suas fontes de dados corporativos, deverá habilitar 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"

Etapa 4: configurar permissões para o agente do Console

Uma conta de serviço do Google Cloud é necessária para fornecer ao agente do Console as permissões necessárias para que o Console gerencie recursos no Google Cloud. Ao criar o agente do Console, você precisará associar essa conta de serviço à VM do agente do Console.

É sua responsabilidade atualizar a função personalizada à medida que novas permissões são adicionadas em versões subsequentes. Se novas permissões forem necessárias, elas serão listadas nas notas de versão.

Passos

1. Crie uma função personalizada no Google Cloud:

   a. Crie um arquivo YAML que inclua o conteúdo do"permissões de conta de serviço para o agente do Console" .

   b. No Google Cloud, ative o Cloud Shell.

   c. Faça upload do arquivo YAML que inclui as permissões necessárias.

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

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

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

   "Documentação do Google Cloud: Criação e gerenciamento de funções personalizadas"

2. Crie uma conta de serviço no Google Cloud e atribua a função à conta de serviço:

   a. No serviço IAM e Admin, selecione **Contas de serviço > Criar conta de serviço**.

   b. Insira os detalhes da conta de serviço e selecione **Criar e continuar**.

   c. Selecione a função que você acabou de criar.

   d. Conclua as etapas restantes para criar a função.

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

3. Se você planeja implantar sistemas Cloud Volumes ONTAP em projetos diferentes daquele em que o agente do Console reside, será necessário fornecer à conta de serviço do agente do Console acesso a esses projetos.

   Por exemplo, digamos que o agente do Console esteja no projeto 1 e você queira criar sistemas Cloud Volumes ONTAP no projeto 2. Você precisará conceder acesso à conta de serviço no projeto 2.

a. No serviço IAM e Admin, selecione o projeto do Google Cloud onde você deseja criar sistemas Cloud Volumes ONTAP .

b. Na página **IAM**, selecione **Conceder acesso** e forneça os detalhes necessários.

   - Digite o e-mail da conta de serviço do agente do Console.
   - Selecione a função personalizada do agente do Console.
   - Selecione **Salvar**.

Para mais detalhes, consulte "Documentação do Google Cloud"

Etapa 5: configurar permissões de VPC compartilhadas

Se você estiver usando uma VPC compartilhada para implantar recursos em um projeto de serviço, precisará preparar suas permissões.

Esta tabela é para referência e seu ambiente deve refletir a tabela de permissões quando a configuração do IAM estiver concluída.

Exibir permissões de VPC compartilhadas

Identidade	Criador	Hospedado em	Permissões do projeto de serviço	Permissões do projeto host	Propósito
Conta do Google para implantar o agente	Personalizado	Projeto de Serviço	"Política de implantação do agente"	compute.networkUser	Implantando o agente no projeto de serviço
conta de serviço do agente	Personalizado	Projeto de serviço	"Política de conta de serviço do agente"	compute.networkUser gerenciador de implantação.editor	Implantando e mantendo o Cloud Volumes ONTAP e serviços no projeto de serviço
Conta de serviço Cloud Volumes ONTAP	Personalizado	Projeto de serviço	membro storage.admin: conta de serviço do NetApp Console como serviceAccount.user	N / D	(Opcional) Para NetApp Cloud Tiering e NetApp Backup and Recovery
Agente de serviço de APIs do Google	Google Cloud	Projeto de serviço	(Padrão) Editor	compute.networkUser	Interage com as APIs do Google Cloud em nome da implantação. Permite que o Console use a rede compartilhada.
Conta de serviço padrão do Google Compute Engine	Google Cloud	Projeto de serviço	(Padrão) Editor	compute.networkUser	Implanta instâncias do Google Cloud e infraestrutura de computação em nome da implantação. Permite que o Console use a rede compartilhada.

Observações:

1. deploymentmanager.editor só é necessário no projeto host se você não estiver passando regras de firewall para a implantação e optar por deixar que o Console as crie para você. O NetApp Console cria uma implantação no projeto host que contém a regra de firewall VPC0 se nenhuma regra for especificada.
2. firewall.create e firewall.delete só são necessários se você não estiver passando regras de firewall para a implantação e optar por deixar que o Console as crie para você. Essas permissões residem no arquivo .yaml da conta do Console. Se você estiver implantando um par de HA usando uma VPC compartilhada, essas permissões serão usadas para criar as regras de firewall para VPC1, 2 e 3. Para todas as outras implantações, essas permissões também serão usadas para criar regras para VPC0.
3. Para Cloud Tiering, a conta de serviço de hierarquização deve ter a função serviceAccount.user na conta de serviço, não apenas no nível do projeto. Atualmente, se você atribuir serviceAccount.user

no nível do projeto, as permissões não serão exibidas quando você consultar a conta de serviço com getIAMPolicy.

Etapa 6: habilitar as APIs do Google Cloud

Várias APIs do Google Cloud devem ser ativadas antes que você possa implantar sistemas Cloud Volumes ONTAP no Google Cloud.

Etapa

1. Ative as seguintes APIs do Google Cloud no seu projeto:
   - 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))

"Documentação do Google Cloud: Habilitando APIs"

Etapa 7: instalar o agente do console

Após a conclusão dos pré-requisitos, você pode instalar manualmente o software no seu próprio host Linux.

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" .

Sobre esta tarefa

O instalador disponível no site de suporte da NetApp pode ser uma versão anterior. 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 em "Site de suporte da NetApp" e, em seguida, copie-o para o host Linux.

   Você deve baixar o instalador do agente "online" destinado ao uso em sua rede ou na nuvem.

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 transparente ou explícito. Os parâmetros --proxy e --cacert são opcionais e você não será solicitado a adicioná-los. Se você tiver um servidor proxy, precisará inserir os parâmetros conforme mostrado.

   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-de-usuário:senha@endereço:porta
   - http://nome-de-domínio%92nome-de-usuário:senha@endereço:porta
   - https://endereço:porta

- https://nome-de-usuário:senha@endereço:porta
- https://nome-de-domínio%92nome-de-usuário:senha@endereço:porta

  Observe o seguinte:

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

    Por exemplo:

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

`--cacert`especifica um certificado assinado pela CA a ser usado para acesso HTTPS entre o agente do Console e o servidor proxy. Este parâmetro é necessário para servidores proxy HTTPS, servidores proxy de interceptação e servidores proxy transparentes.

+ Aqui está um exemplo de configuração de um servidor proxy transparente. Ao configurar um proxy transparente, você não precisa definir o servidor proxy. Você só adiciona um certificado assinado pela CA ao host do agente do Console:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

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
      ...
      # 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
      ...
      Esc:wq
      ```

c. Reinicie a máquina virtual do agente do Console.

2. Aguarde a conclusão da instalação.

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

   Se a instalação falhar, você pode visualizar o relatório e os logs da instalação para ajudar a corrigir os problemas."Aprenda a solucionar problemas de instalação."

1. Abra um navegador da Web em um host que tenha uma conexão com a máquina virtual do agente do Console e insira o seguinte URL:

   https://ipaddress

2. Após efetuar login, configure o agente do Console:

   a. Especifique a organização a ser associada ao agente do Console.

   b. Digite um nome para o sistema.

   c. Em **Você está executando em um ambiente seguro?** mantenha o modo restrito desabilitado.

      Você deve manter o modo restrito desabilitado porque estas etapas descrevem como usar o Console no modo padrão. Você deve habilitar o modo restrito somente se tiver um ambiente seguro e quiser desconectar esta conta dos serviços de backend. Se for esse o caso,"siga as etapas para começar a usar o NetApp Console no modo restrito" .

   d. Selecione **Vamos começar**.

   Se a instalação falhar, você poderá visualizar logs e um relatório para ajudar a solucionar problemas."Aprenda a solucionar problemas de instalação."

Se você tiver buckets do Google Cloud Storage na mesma conta do Google Cloud onde criou o agente do Console, verá um sistema do Google Cloud Storage aparecer na página **Sistemas** automaticamente. "Aprenda a gerenciar o Google Cloud Storage no NetApp Console"

Etapa 8: fornecer permissões ao agente do console

Você precisa fornecer ao agente do Console as permissões do Google Cloud que você configurou anteriormente. Fornecer as permissões permite que o agente do Console gerencie seus dados e infraestrutura de armazenamento no Google Cloud.

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 do Google Cloud, 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.

Instalar um agente no local

Instalar manualmente um agente do Console no local

Instale um agente do Console no local, faça login e configure-o para funcionar com sua organização do Console.

Se você for um usuário do VMWare, poderá usar um OVA para instalar um agente de console no seu VCenter."Saiba mais sobre como instalar um agente em um VCenter."

Antes de instalar, você precisará garantir que seu host (VM ou host Linux) atenda aos requisitos e que o agente do Console terá acesso de saída à Internet, bem como às redes de destino. Se você planeja usar serviços de dados NetApp ou opções de armazenamento em nuvem, como o Cloud Volumes ONTAP, será necessário criar credenciais no seu provedor de nuvem para adicionar ao Console, para que o agente do Console possa executar ações na nuvem em seu nome.

Preparar para instalar o agente do Console

Antes de instalar um agente do Console, você deve garantir que tenha uma máquina host que atenda aos requisitos de instalação. Você também precisará trabalhar com seu administrador de rede para garantir que o agente do Console tenha acesso de saída aos endpoints necessários e conexões às redes de destino.

Revisar os requisitos do host do agente do console

Execute o agente do Console em um host x86 que atenda aos requisitos de sistema operacional, RAM e porta. Certifique-se de que seu host atenda a esses requisitos antes de instalar o agente do Console.

O agente do Console reserva o intervalo de UID e GID de 19000 a 19200. Este intervalo é fixo e não pode ser modificado. Se algum software de terceiros no seu host estiver usando UIDs ou GIDs dentro desse intervalo, a instalação do agente falhará. A NetApp recomenda usar um host livre de software de terceiros para evitar conflitos.

Host dedicado

O agente do Console não é suportado em um host compartilhado com outros aplicativos. O host deve ser um host dedicado. O host pode ter qualquer arquitetura que atenda aos seguintes 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 Docker ou o Podman são arquitetados para criar os contêineres dentro deste diretório. Especificamente, eles criarão contêineres no `/var/lib/containers/storage` diretório. Montagens externas ou links simbólicos não funcionam neste espaço.

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 a
Red Hat Enterprise Linux	9.1 a 9.4 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 Ver requisitos de configuração do Podman .	Suportado no modo de imposição ou no modo permissivo • O gerenciamento de sistemas Cloud Volumes ONTAP NÃO é suportado por agentes que tenham o SELinux habilitado no sistema operacional.
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

Configurar acesso à rede para o agente do Console

Configure o acesso à rede para garantir que o agente do Console possa gerenciar recursos. Ele precisa de conexões para redes de destino e acesso de saída à Internet para endpoints específicos.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados de computadores ao usar o NetApp Console baseado na Web

Os computadores que acessam o Console a partir de um navegador da web devem ter a capacidade de contatar vários terminais. Você precisará usar o Console para configurar o agente do Console e para o uso diário do Console.

"Preparar a rede para o console NetApp" .

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Um agente do Console instalado em suas instalações não pode gerenciar recursos no Google Cloud. Se você quiser gerenciar recursos do Google Cloud, precisará instalar um agente no Google Cloud.

AWS

Quando o agente do Console é instalado no local, ele precisa de acesso à rede para os seguintes endpoints da AWS para gerenciar sistemas NetApp (como o Cloud Volumes ONTAP) implantados na AWS.

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
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)	Para gerenciar recursos da AWS. O ponto de extremidade depende da sua região da AWS. "Consulte a documentação da AWS para obter detalhes"
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://support.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://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.

Azul

Quando o agente do Console é instalado no local, ele precisa de acesso à rede para os seguintes pontos de extremidade do Azure para gerenciar sistemas NetApp (como o Cloud Volumes ONTAP) implantados no Azure.

Pontos finais	Propósito
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Para gerenciar recursos em regiões públicas do Azure.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Para gerenciar recursos nas regiões do Azure China.
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .

Pontos finais	Propósito
\ https://support.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://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.

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 estiver planejando usar o NetApp Data Classification para verificar suas fontes de dados corporativos, deverá habilitar 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"

Criar permissões de nuvem do agente do Console para AWS ou Azure

Se você quiser usar os serviços de dados da NetApp na AWS ou no Azure com um agente do Console local, será necessário configurar permissões no seu provedor de nuvem e adicionar as credenciais ao agente do Console após instalá-lo.

Você deve instalar o agente do Console no Google Cloud para gerenciar quaisquer recursos que residam lá.

AWS

Quando o agente do Console é instalado no local, você precisa fornecer ao Console permissões da AWS adicionando chaves de acesso para um usuário do IAM que tenha as permissões necessárias.

Você deve usar este método de autenticação se o agente do Console estiver instalado no local. Você não pode usar uma função do IAM.

Passos

1. Faça login no console da AWS e navegue até o serviço 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.

Resultado

Agora você deve ter chaves de acesso para um usuário do IAM que tenha as permissões necessárias. Depois de instalar o agente do Console, associe essas credenciais ao agente do Console do Console.

Azul

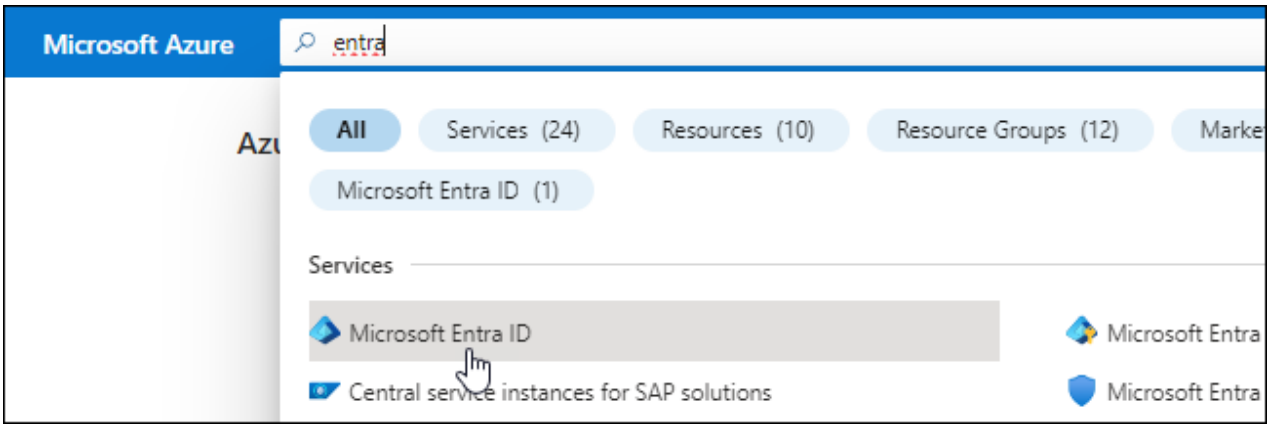
Quando o agente do Console é instalado no local, você precisa fornecer ao agente do Console permissões do Azure configurando uma entidade de serviço no Microsoft Entra ID e obtendo as credenciais do Azure necessárias para o agente do Console.

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 .

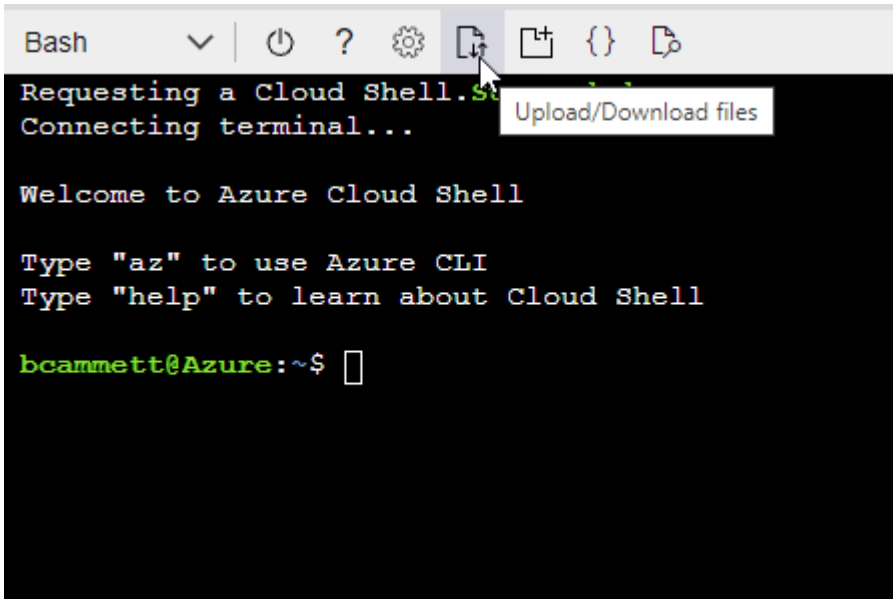
      Exemplo

```
"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
Connector_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**.

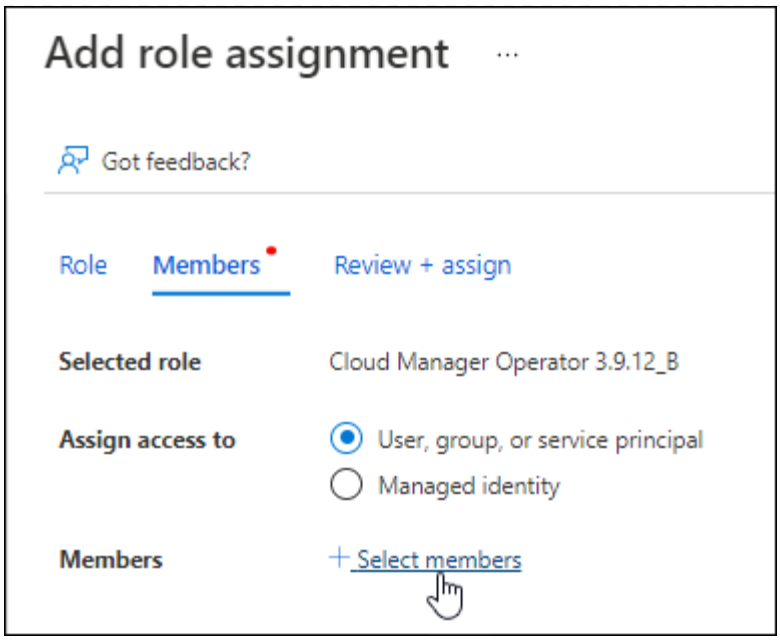
   b. Selecione a assinatura.

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

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

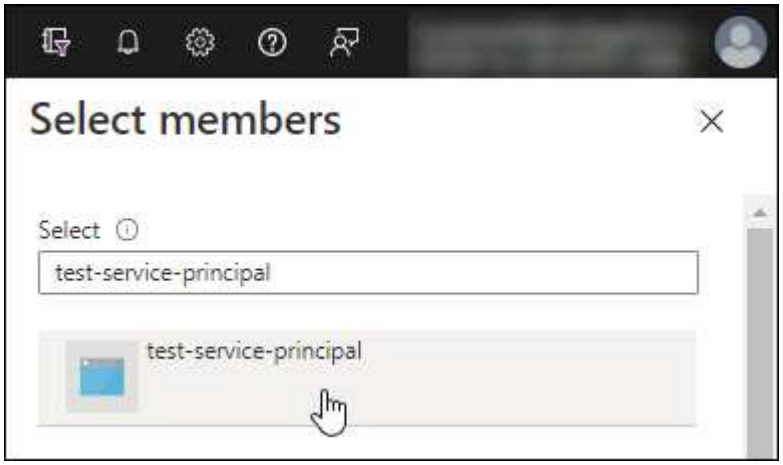
   e. Na aba **Membros**, complete os seguintes passos:

      - 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**.

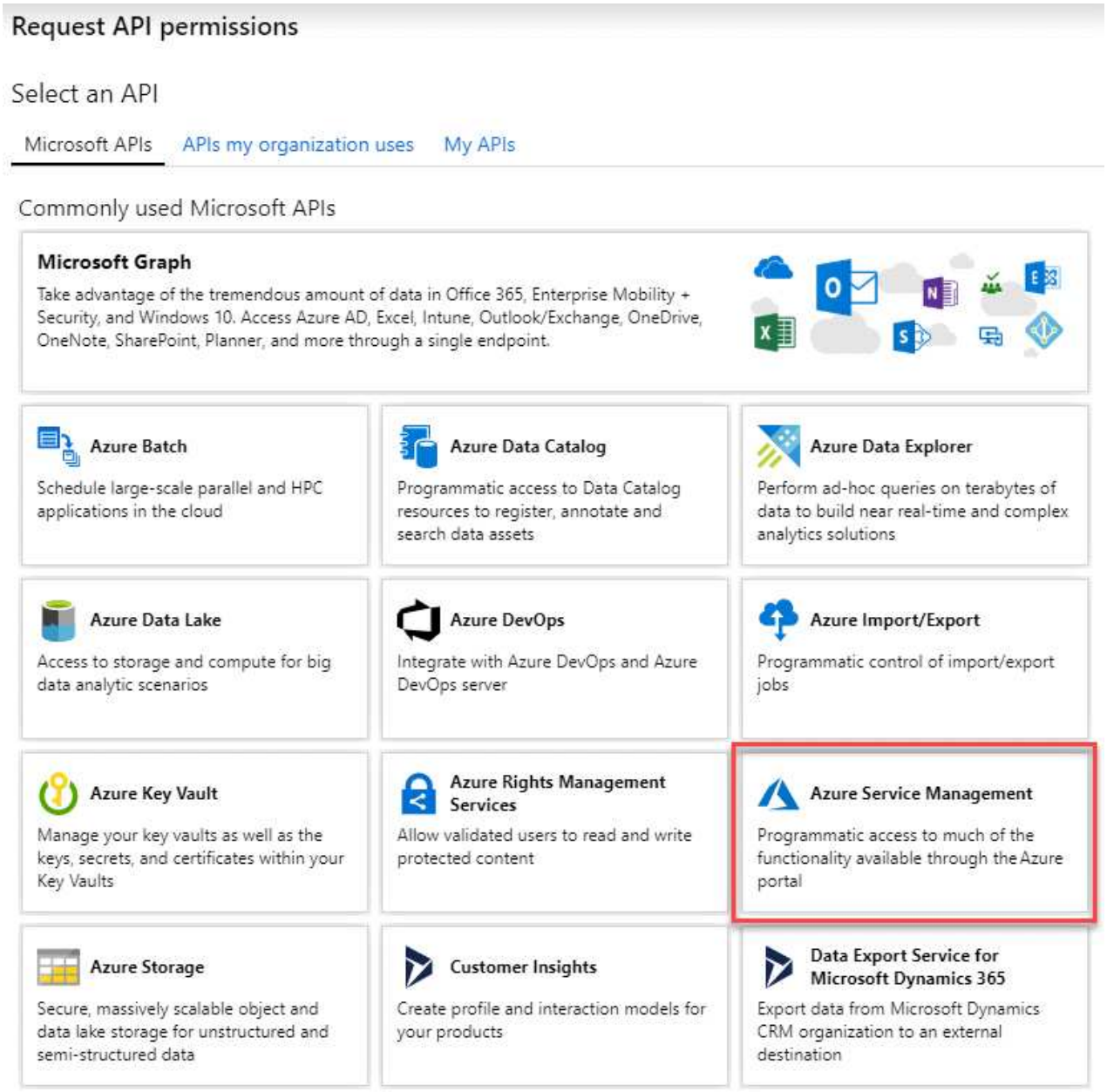
O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

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.

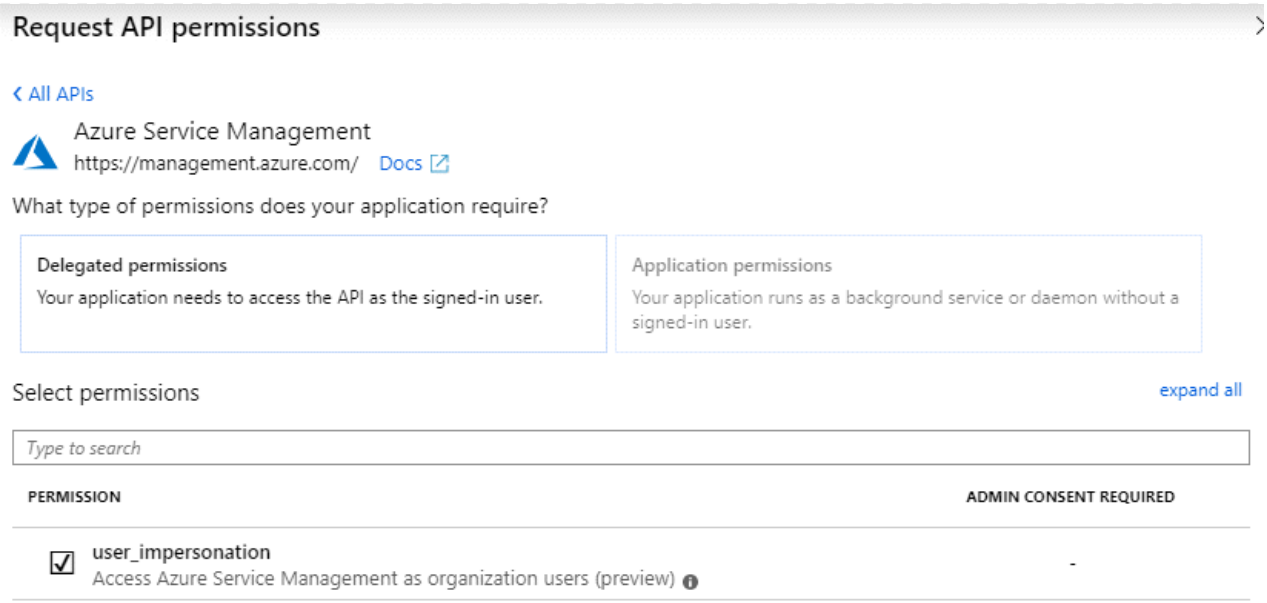
Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

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**.

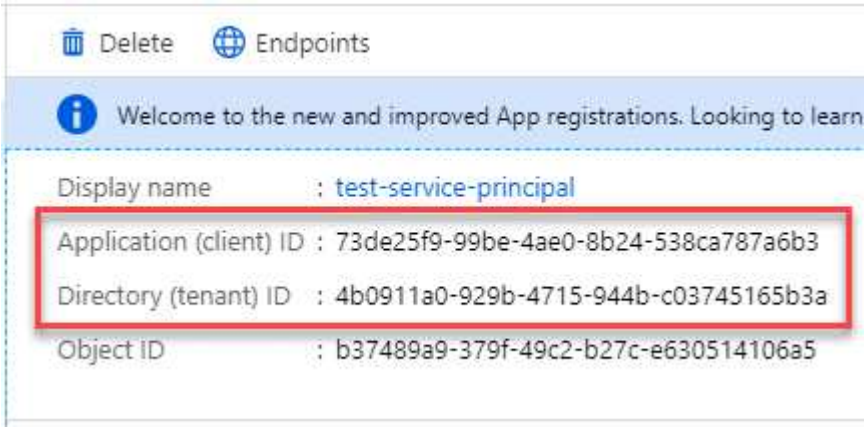


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



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

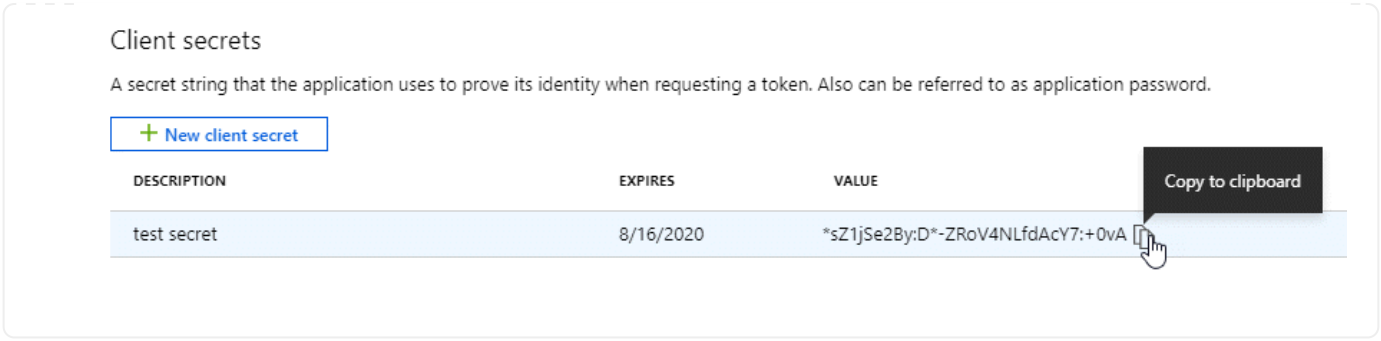
1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



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.



Instalar manualmente um agente do Console

Ao instalar manualmente um agente do Console, você precisa preparar o ambiente da sua máquina para que ele atenda aos requisitos. Você precisará de uma máquina Linux e instalar o Podman ou o Docker, dependendo do seu sistema operacional Linux.

Instalar Podman ou 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 4. 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 8, verifique se sua versão do Podman está usando o DNS 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.

   Para Red Hat Enterprise Linux 9:

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

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

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<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.
6. Se estiver usando o Red Hat Enterprise:

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

   Para Red Hat Enterprise Linux 9:

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

   Para Red Hat Enterprise Linux 8:

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

7. 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.

8. 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.

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

      ```
      podman info | grep networkBackend
      ```

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

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

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

   d. 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 .
```

9. Reinicie o podman.

```
systemctl restart podman
```

10. 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
```

Instalar o agente do Console manualmente

Baixe e instale o software do agente do Console em um host Linux existente no local.

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" .

Sobre esta tarefa

O instalador disponível no site de suporte da NetApp pode ser uma versão anterior. 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 em "Site de suporte da NetApp" e, em seguida, copie-o para o host Linux.

   Você deve baixar o instalador do agente "online" destinado ao uso em sua rede ou na nuvem.

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 transparente ou explícito. Os parâmetros --proxy e --cacert são opcionais e você não será solicitado a adicioná-los. Se você tiver um servidor proxy, precisará inserir os parâmetros conforme mostrado.

   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-de-usuário:senha@endereço:porta

- http://nome-de-domínio%92nome-de-usuário:senha@endereço:porta
- https://endereço:porta
- https://nome-de-usuário:senha@endereço:porta
- https://nome-de-domínio%92nome-de-usuário:senha@endereço:porta

  Observe o seguinte:

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

    Por exemplo:

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

`--cacert`especifica um certificado assinado pela CA a ser usado para acesso HTTPS entre o agente do Console e o servidor proxy. Este parâmetro é necessário para servidores proxy HTTPS, servidores proxy de interceptação e servidores proxy transparentes.

+ Aqui está um exemplo de configuração de um servidor proxy transparente. Ao configurar um proxy transparente, você não precisa definir o servidor proxy. Você só adiciona um certificado assinado pela CA ao host do agente do Console:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

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
...
# 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
...
Esc:wq
```

c. Reinicie a máquina virtual do agente do Console.

O que vem a seguir?

Você precisará registrar o agente do Console no NetApp Console.

Registre o agente do Console com o NetApp Console

Efetue login no Console e associe o agente do Console à sua organização. A forma como você efetua login depende do modo em que você está usando o Console. Se você estiver usando o Console no modo padrão, faça login pelo site do SaaS. Se estiver usando o Console no modo restrito, faça login localmente no host do agente do Console.

Passos

1. Abra um navegador da Web e insira o URL do host do agente do Console:

   O URL do host do console pode ser um host local, um endereço IP privado ou um endereço IP público, dependendo da configuração do host. Por exemplo, se o agente do Console estiver na nuvem pública sem um endereço IP público, você deverá inserir um endereço IP privado de um host que tenha uma conexão com o host do agente do Console.

2. Cadastre-se ou faça login.
3. Após efetuar login, configure o Console:
   a. Especifique a organização do Console a ser associada ao agente do Console.
   b. Digite um nome para o sistema.
   c. Em **Você está executando em um ambiente seguro?** mantenha o modo restrito desabilitado.

      O modo restrito não é suportado quando o agente do Console é instalado no local.

   d. Selecione **Vamos começar**.

Forneça credenciais do provedor de nuvem ao NetApp Console

Depois de instalar e configurar o agente do Console, adicione suas credenciais de nuvem para que o agente do Console tenha as permissões necessárias para executar ações na AWS ou no Azure.

AWS

Antes de começar

Se você acabou de criar essas credenciais da AWS, elas podem levar alguns minutos para ficarem disponíveis. Aguarde alguns minutos antes de adicionar as credenciais ao Console.

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**.

Agora você pode ir para o "Console NetApp" para começar a usar o agente do Console.

Azul

Antes de começar

Se você acabou de criar essas credenciais do Azure, elas podem levar alguns minutos para ficarem disponíveis. Aguarde alguns minutos antes de adicionar as credenciais do agente do Console.

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 agente do Console agora tem as permissões necessárias para executar ações no Azure em seu nome. Agora você pode ir para o "Console NetApp" para começar a usar o agente do Console.

Instalar um agente de console no local usando o VCenter

Se você for um usuário do VMWare, poderá usar um OVA para instalar um agente de console no seu VCenter. O download ou URL do OVA está disponível no NetApp Console.

Ao instalar um agente do Console com suas ferramentas do VCenter, você pode usar o console da Web da VM para executar tarefas de manutenção."Saiba mais sobre o console da VM para o agente."

Preparar para instalar o agente do Console

Antes da instalação, certifique-se de que o host da VM atenda aos requisitos e que o agente do Console possa acessar a Internet e as redes de destino. Para usar os serviços de dados do NetApp ou o Cloud Volumes ONTAP, crie credenciais do provedor de nuvem para que o agente do Console execute ações em seu nome.

Revisar os requisitos do host do agente do console

Certifique-se de que sua máquina host atenda aos requisitos de instalação antes de instalar o agente do Console.

- CPU: 8 núcleos ou 8 vCPUs
- RAM: 32 GB
- Espaço em disco: 165 GB (provisionamento denso)
- vSphere 7.0 ou superior
- Host ESXi 7.03 ou superior

Instale o agente em um ambiente vCenter em vez de diretamente em um host ESXi.

Configurar acesso à rede para o agente do Console

Trabalhe com seu administrador de rede para garantir que o agente do Console tenha acesso de saída aos endpoints necessários e conexões com redes de destino.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados de computadores ao usar o NetApp Console baseado na Web

Os computadores que acessam o Console a partir de um navegador da web devem ter a capacidade de contatar vários terminais. Você precisará usar o Console para configurar o agente do Console e para o uso diário do Console.

"Preparar a rede para o console NetApp" .

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Não é possível gerenciar recursos no Google Cloud com um agente do Console instalado em suas instalações. Para gerenciar recursos do Google Cloud, instale um agente no Google Cloud.

AWS

Quando o agente do Console é instalado no local, ele precisa de acesso à rede para os seguintes endpoints da AWS para gerenciar sistemas NetApp (como o Cloud Volumes ONTAP) implantados na AWS.

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
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)	Para gerenciar recursos da AWS. O ponto de extremidade depende da sua região da AWS. "Consulte a documentação da AWS para obter detalhes"
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://support.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://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.

Azul

Quando o agente do Console é instalado no local, ele precisa de acesso à rede para os seguintes pontos de extremidade do Azure para gerenciar sistemas NetApp (como o Cloud Volumes ONTAP) implantados no Azure.

Pontos finais	Propósito
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Para gerenciar recursos em regiões públicas do Azure.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Para gerenciar recursos nas regiões do Azure China.
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .

Pontos finais	Propósito
\ https://support.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://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.

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 estiver planejando usar o NetApp Data Classification para verificar suas fontes de dados corporativos, deverá habilitar 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"

Criar permissões de nuvem do agente do Console para AWS ou Azure

Se você quiser usar os serviços de dados do NetApp na AWS ou no Azure com um agente do Console local, precisará configurar permissões no seu provedor de nuvem para poder adicionar as credenciais ao agente do Console após instalá-lo.

Não é possível gerenciar recursos no Google Cloud com um agente do Console instalado em suas instalações. Se você quiser gerenciar recursos do Google Cloud, precisará instalar um agente no Google Cloud.

AWS

Para agentes do Console locais, forneça permissões da AWS adicionando chaves de acesso de usuário do IAM.

Use chaves de acesso de usuário do IAM para agentes do Console locais; funções do IAM não são suportadas para agentes do Console locais.

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.

Resultado

Agora você deve ter chaves de acesso de usuário do IAM com as permissões necessárias. Depois de instalar o agente do Console, associe essas credenciais ao agente do Console no Console.

Azul

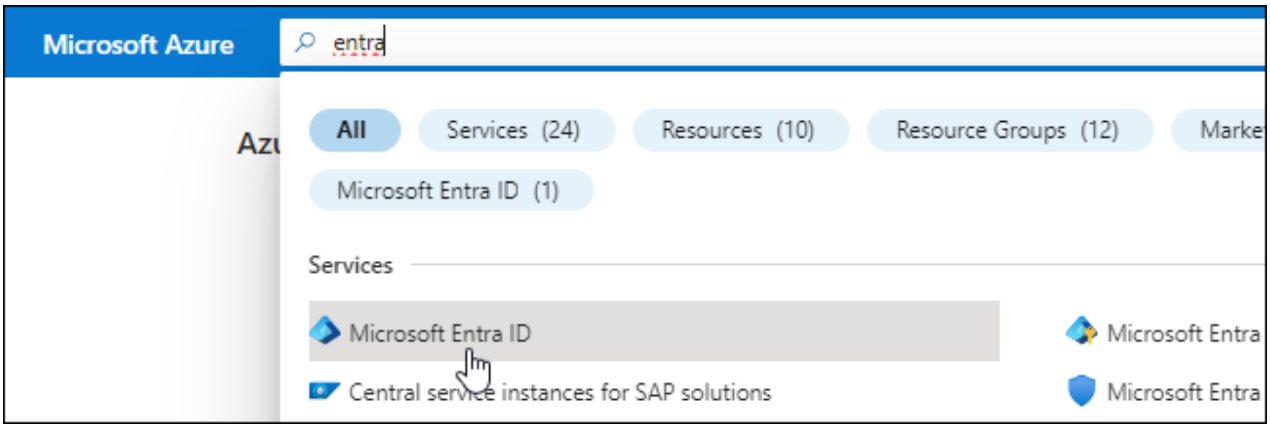
Quando o agente do Console estiver instalado no local, você precisará conceder permissões do Azure ao agente do Console configurando uma entidade de serviço no Microsoft Entra ID e obtendo as credenciais do Azure necessárias para o agente do Console.

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 .

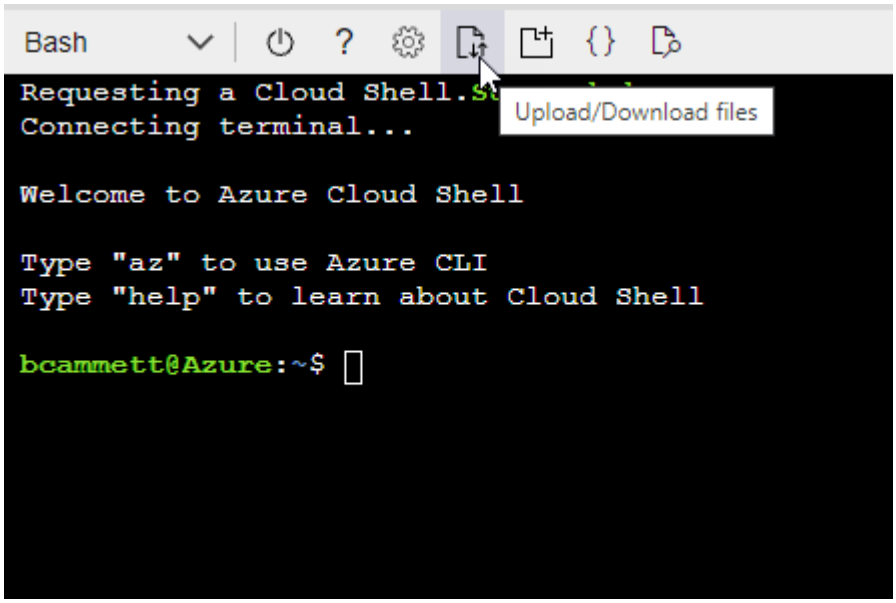
      Exemplo

```
"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
Connector_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**.

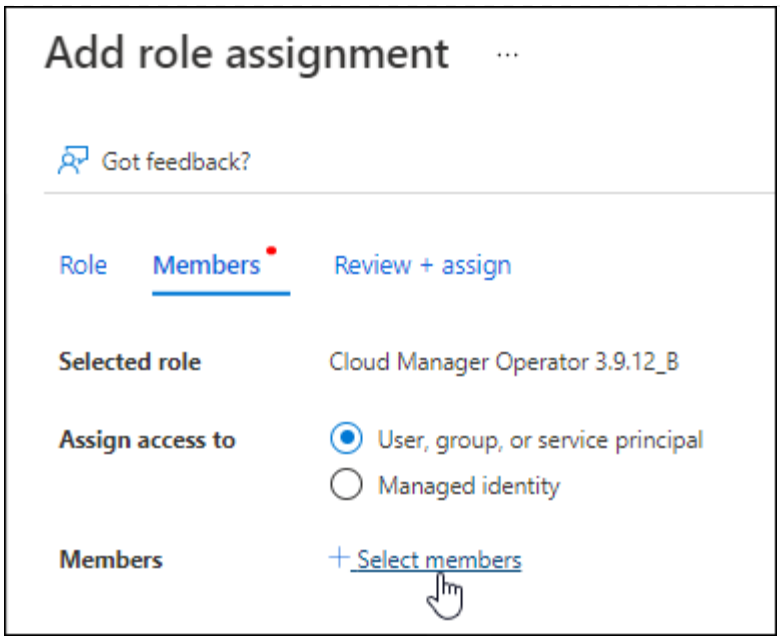
   b. Selecione a assinatura.

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

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

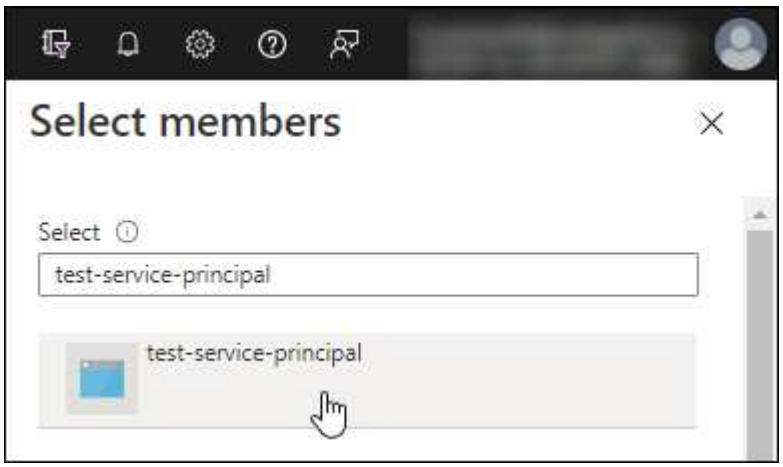
   e. Na aba **Membros**, complete os seguintes passos:

      - 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**.

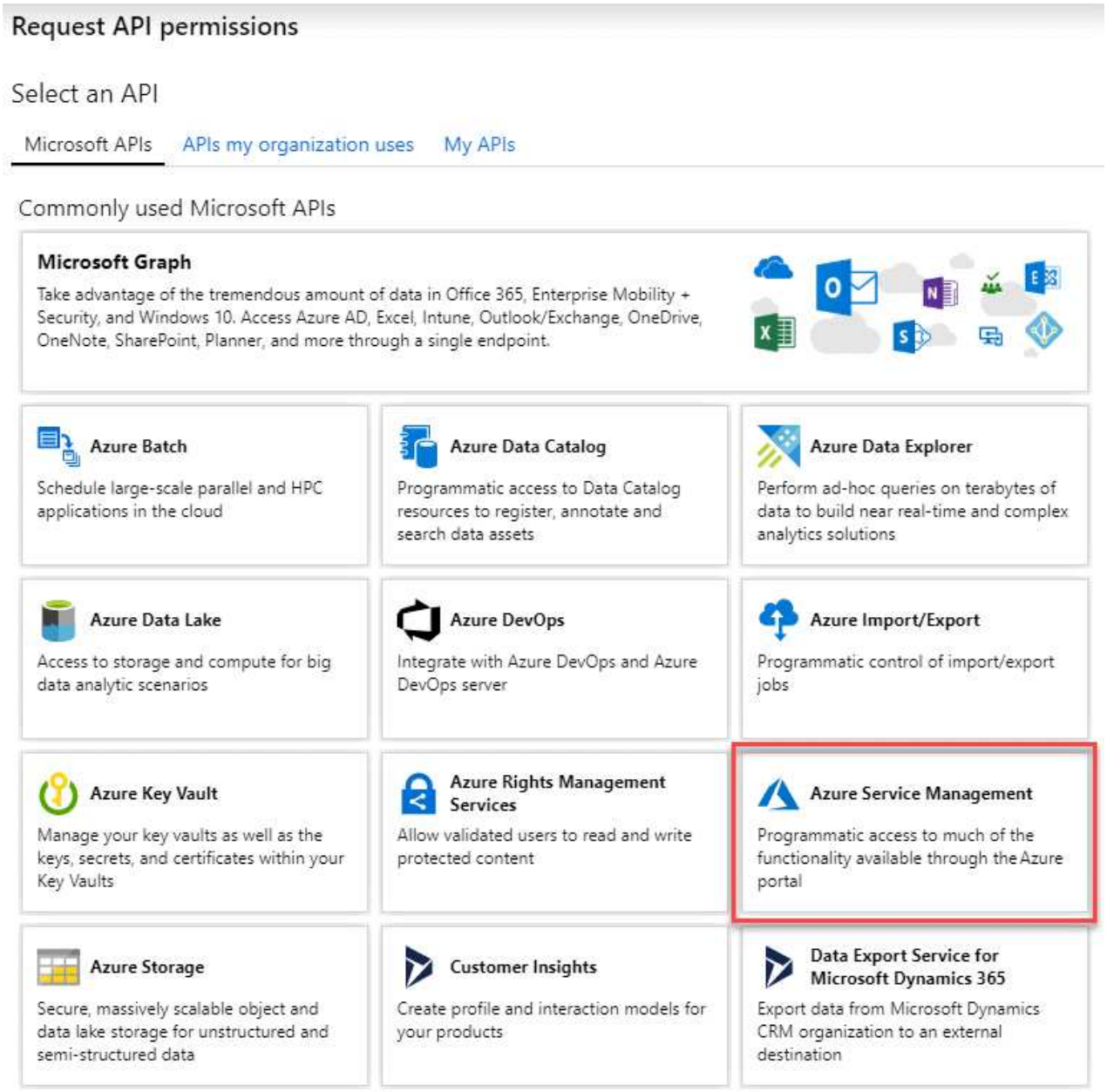
O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

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.

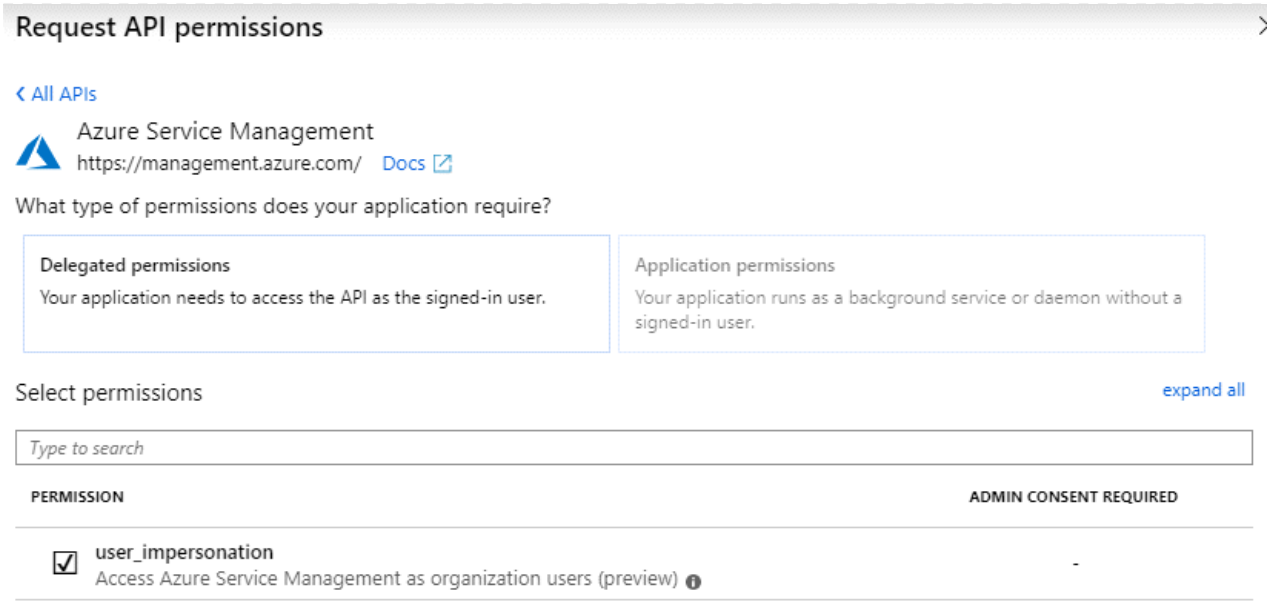
Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

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**.

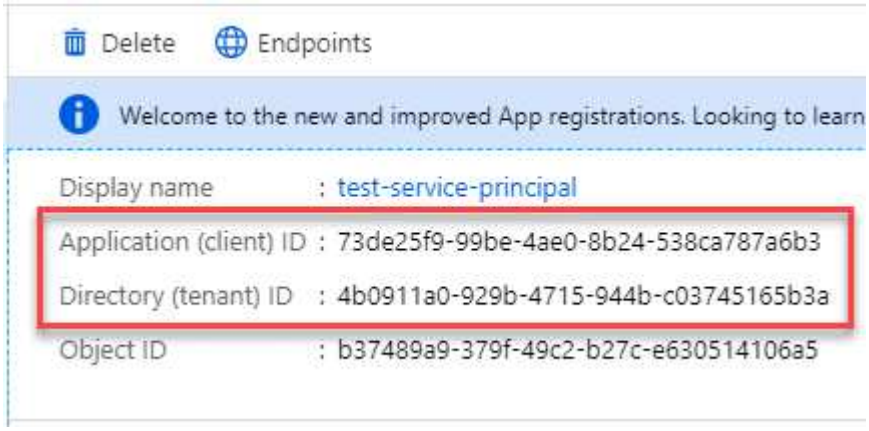


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



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

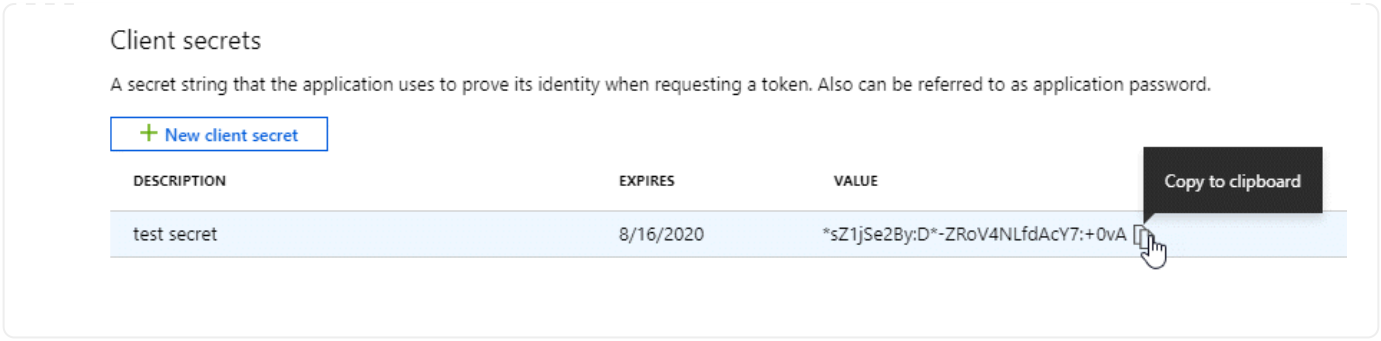
1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



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.



Instale um agente de console no seu ambiente VCenter

A NetApp oferece suporte à instalação do agente do Console no seu ambiente VCenter. O arquivo OVA inclui uma imagem de VM pré-configurada que você pode implantar no seu ambiente VMware. Um download de arquivo ou implantação de URL está disponível diretamente no NetApp Console. Inclui o software do agente do Console e um certificado autoassinado.

Baixe o OVA ou copie o URL

Baixe o OVA ou copie o URL do OVA diretamente do NetApp Console.

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione **Implantar agente > No local**.
3. Selecione **Com OVA**.
4. Escolha entre baixar o OVA ou copiar o URL para usar no VCenter.

Implante o agente no seu VCenter

Efetue login no seu ambiente VCenter para implantar o agente.

Passos

1. Carregue o certificado autoassinado nos seus certificados confiáveis se o seu ambiente exigir. Você substitui este certificado após a instalação."Aprenda como substituir o certificado autoassinado."
2. Implante o OVA da biblioteca de conteúdo ou do sistema local.

Do sistema local	Da biblioteca de conteúdo
a. Clique com o botão direito e selecione **Implantar modelo OVF…**. b. Escolha o arquivo OVA na URL ou navegue até seu local e selecione **Avançar**.	a. Acesse sua biblioteca de conteúdo e selecione o agente OVA do Console. b. Selecione **Ações** > **Nova VM deste modelo**

3. Conclua o assistente Implantar modelo OVF para implantar o agente do Console.
4. Selecione um nome e uma pasta para a VM e selecione **Avançar**.
5. Selecione um recurso de computação e, em seguida, selecione **Avançar**.
6. Revise os detalhes do modelo e selecione **Avançar**.
7. Aceite o contrato de licença e selecione **Avançar**.
8. Escolha o tipo de configuração de proxy que você deseja usar: proxy explícito, proxy transparente ou nenhum proxy.
9. Selecione o armazenamento de dados onde você deseja implantar a VM e selecione **Avançar**. Certifique-

se de que ele atenda aos requisitos do host.

10. Selecione a rede à qual você deseja conectar a VM e selecione **Avançar**. Certifique-se de que a rede seja IPv4 e tenha acesso de saída à Internet para os terminais necessários.
11. na janela **Personalizar modelo**, preencha os seguintes campos:
    - **Informações de proxy**
      - Se você selecionou proxy explícito, insira o nome do host ou endereço IP do servidor proxy e o número da porta, bem como o nome de usuário e a senha.
      - Se você selecionou proxy transparente, carregue o respectivo certificado.
    - **Configuração da Máquina Virtual**
      - **Ignorar verificação de configuração**: esta caixa de seleção fica desmarcada por padrão, o que significa que o agente executa uma verificação de configuração para validar o acesso à rede.
        - A NetApp recomenda deixar esta caixa desmarcada para que a instalação inclua uma verificação de configuração do agente. A verificação de configuração valida se o agente tem acesso de rede aos terminais necessários. Se a implantação falhar devido a problemas de conectividade, você poderá acessar o relatório de validação e os logs do host do agente. Em alguns casos, se você tiver certeza de que o agente tem acesso à rede, você pode optar por pular a verificação. Por exemplo, se você ainda estiver usando o"pontos finais anteriores" usado para atualizações de agentes, a validação falha com um erro. Para evitar isso, marque a caixa de seleção para instalar sem uma verificação de validação. "Aprenda como atualizar sua lista de endpoints" .
      - **Senha de manutenção**: Defina a senha para o `maint` usuário que permite acesso ao console de manutenção do agente.
      - **Servidores NTP**: especifique um ou mais servidores NTP para sincronização de horário.
      - **Nome do host**: define o nome do host para esta VM. Não deve incluir o domínio de pesquisa. Por exemplo, um FQDN de console10.searchdomain.company.com deve ser inserido como console10.
      - **DNS primário**: especifique o servidor DNS primário a ser usado para resolução de nomes.
      - **DNS secundário**: especifique o servidor DNS secundário a ser usado para resolução de nomes.
      - Domínios de pesquisa: especifique o nome do domínio de pesquisa a ser usado ao resolver o nome do host. Por exemplo, se o FQDN for console10.searchdomain.company.com, insira searchdomain.company.com.
      - **Endereço IPv4**: O endereço IP mapeado para o nome do host.
      - **Máscara de sub-rede IPv4**: A máscara de sub-rede para o endereço IPv4.
      - **Endereço de gateway IPv4**: O endereço de gateway para o endereço IPv4.
12. Selecione **Avançar**.
13. Revise os detalhes na janela **Pronto para concluir** e selecione **Concluir**.

    A barra de tarefas do vSphere mostra o progresso conforme o agente do Console é implantado.

14. Ligue a VM.

> Se a implantação falhar, você poderá acessar o relatório de validação e os logs do host do agente."Aprenda a solucionar problemas de instalação."

Registre o agente do Console com o NetApp Console

Efetue login no Console e associe o agente do Console à sua organização. A forma como você efetua login depende do modo em que você está usando o Console. Se você estiver usando o Console no modo padrão, faça login pelo site do SaaS. Se você estiver usando o Console no modo restrito ou privado, faça login localmente no host do agente do Console.

Passos

1. Abra um navegador da Web e insira o URL do host do agente do Console:

   O URL do host do console pode ser um host local, um endereço IP privado ou um endereço IP público, dependendo da configuração do host. Por exemplo, se o agente do Console estiver na nuvem pública sem um endereço IP público, você deverá inserir um endereço IP privado de um host que tenha uma conexão com o host do agente do Console.

2. Cadastre-se ou faça login.
3. Após efetuar login, configure o Console:
   a. Especifique a organização do Console a ser associada ao agente do Console.
   b. Digite um nome para o sistema.
   c. Em **Você está executando em um ambiente seguro?** mantenha o modo restrito desabilitado.

      O modo restrito não é suportado quando o agente do Console é instalado no local.

   d. Selecione **Vamos começar**.

Adicionar credenciais do provedor de nuvem ao Console

Depois de instalar e configurar o agente do Console, adicione suas credenciais de nuvem para que o agente do Console tenha as permissões necessárias para executar ações na AWS ou no Azure.

AWS

Antes de começar

Se você acabou de criar essas credenciais da AWS, elas podem levar alguns minutos para ficarem disponíveis. Aguarde alguns minutos antes de adicionar as credenciais ao Console.

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**.

Agora você pode ir para o "Console NetApp" para começar a usar o agente do Console.

Azul

Antes de começar

Se você acabou de criar essas credenciais do Azure, elas podem levar alguns minutos para ficarem disponíveis. Aguarde alguns minutos antes de adicionar as credenciais do agente do Console.

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 agente do Console agora tem as permissões necessárias para executar ações no Azure em seu nome. Agora você pode ir para o "Console NetApp" para começar a usar o agente do Console.

Assine o NetApp Intelligent Services (modo padrão)

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 da NetApp :

- Backup e recuperação da NetApp
- Cloud Volumes ONTAP
- Camadas de nuvem da NetApp
- Resiliência do NetApp Ransomware
- Recuperação de desastres da NetApp

A classificação de dados da NetApp 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

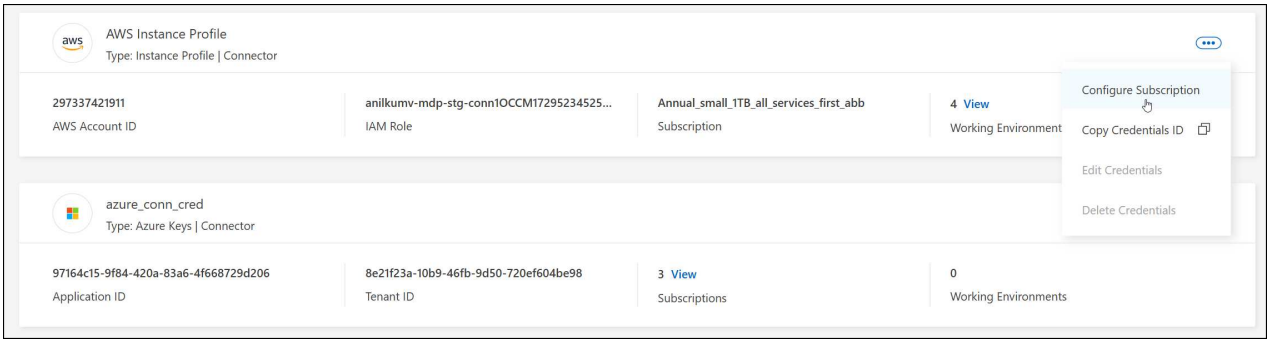
O vídeo a seguir mostra as etapas para assinar o NetApp Intelligent Services no AWS Marketplace:

Assine o NetApp Intelligent Services no AWS Marketplace

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**.

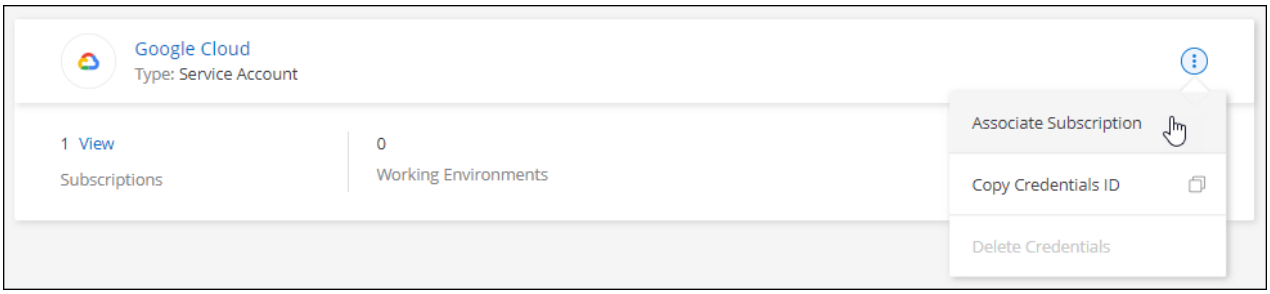
        O vídeo a seguir mostra as etapas para assinar o Azure Marketplace:

   Assine o NetApp Intelligent Services no Azure Marketplace

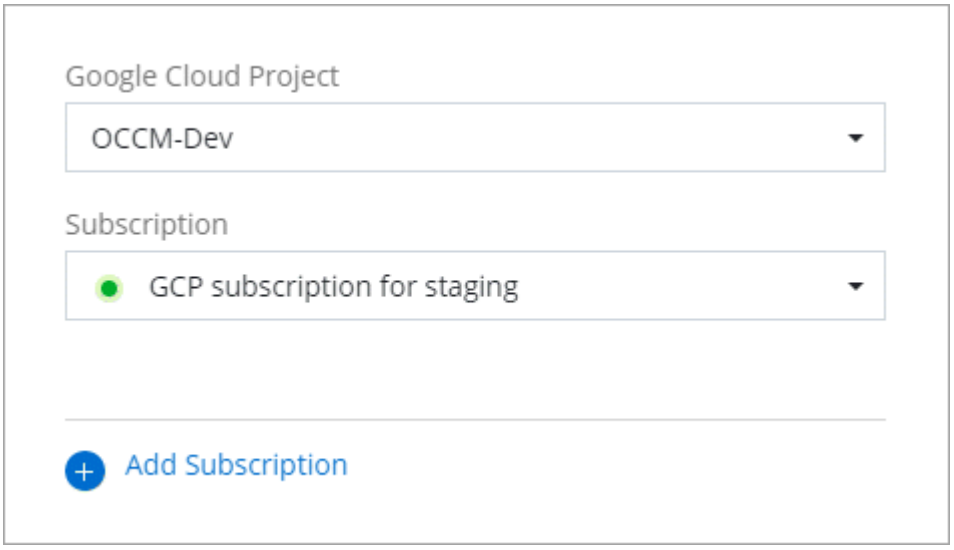
Google Cloud

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**. +nova captura de tela necessária
(TS)



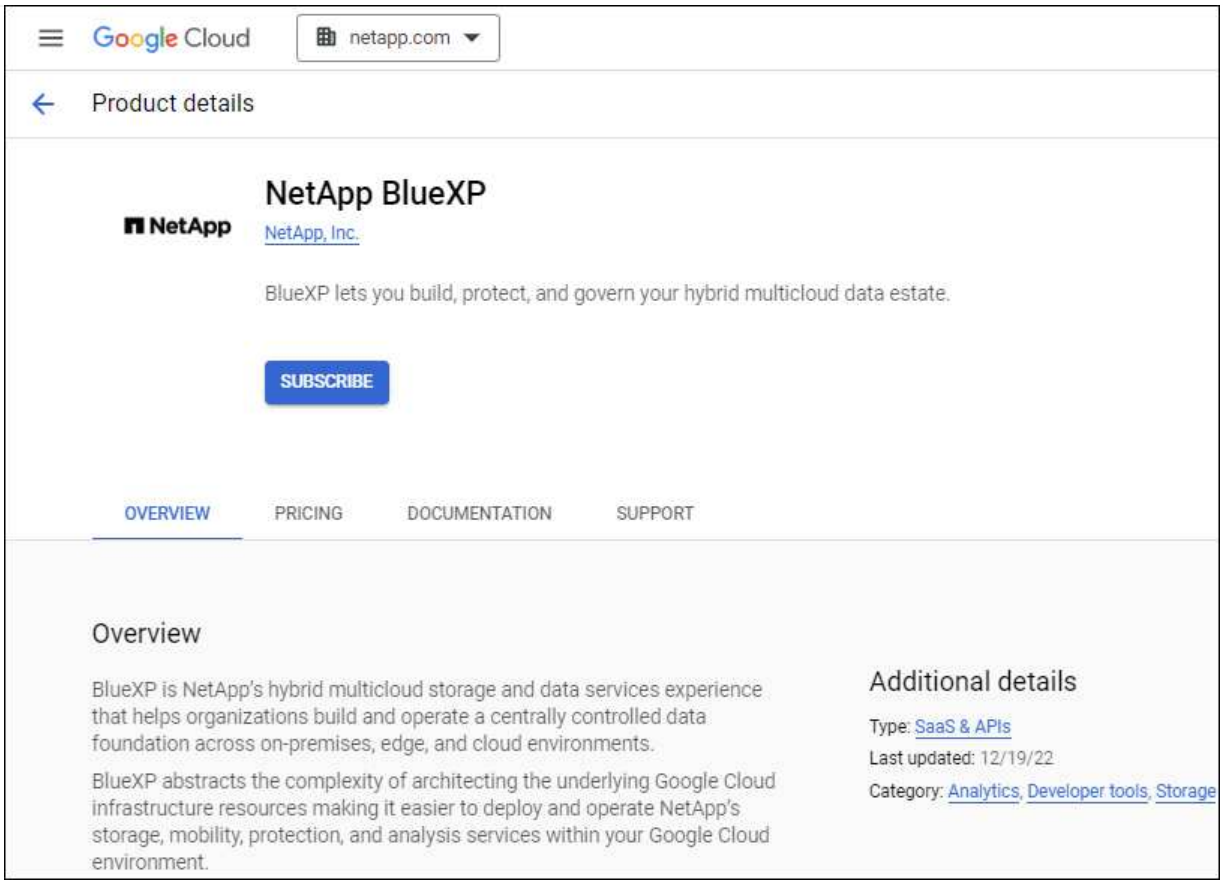
4. Para configurar uma assinatura existente com as credenciais selecionadas, selecione um projeto e uma assinatura do Google Cloud na lista suspensa e selecione **Configurar**.



5. 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 console do NetApp .

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.

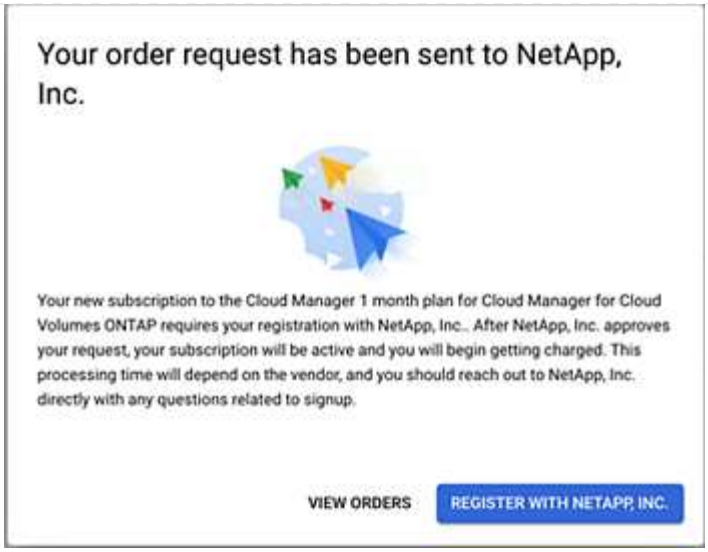


b. Selecione **Inscrever-se**.
c. Selecione a conta de cobrança apropriada e concorde com os termos e condições.
d. Selecione **Inscrever-se**.

   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 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.

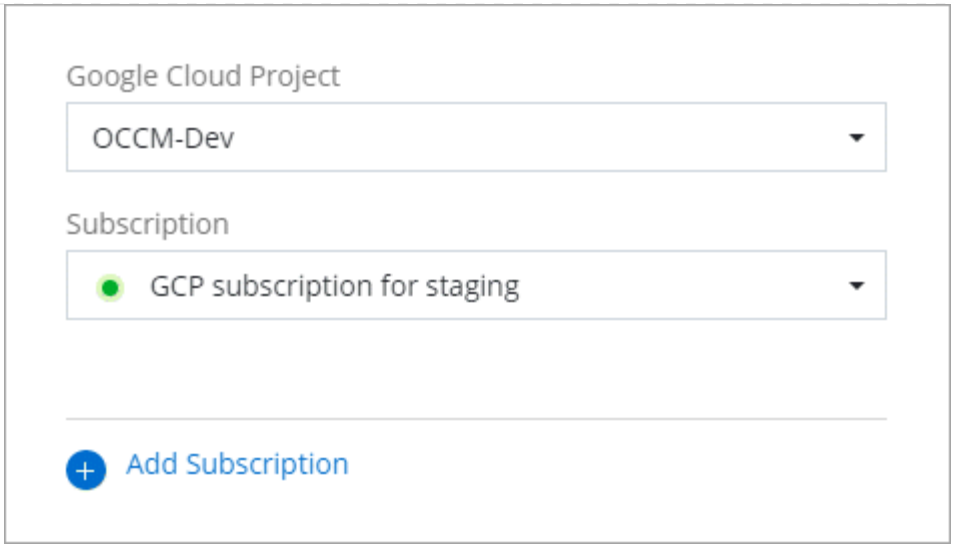
Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo essas etapas.

- Selecione **Salvar**.

  O vídeo a seguir mostra as etapas para assinar o Google Cloud Marketplace:

Assine no Google Cloud Marketplace

a. 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 padrão)

Agora que você fez login e configurou o NetApp Console no modo padrão, os usuários podem criar e descobrir sistemas de armazenamento e usar os serviços de dados do NetApp .

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

Para obter ajuda, vá para o "página inicial da documentação do NetApp Console" para visualizar a documentação do NetApp Console.

Informações relacionadas

"Modos de implantação do NetApp Console"

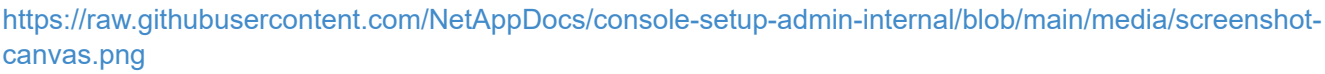
Comece com o modo restrito

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" .

1 **"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.

2 **"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 serviços inteligentes da NetApp incluem backup e recuperação da NetApp , Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience e NetApp Disaster Recovery. A classificação de dados da NetApp 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 não é suportado em um host compartilhado com outros aplicativos. O host deve ser um host dedicado. O host pode ter qualquer arquitetura que atenda aos seguintes 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 Docker ou o Podman são arquitetados para criar os contêineres dentro deste diretório. Especificamente, eles criarão contêineres no `/var/lib/containers/storage` diretório. Montagens externas ou links simbólicos não funcionam neste espaço.

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 a
Red Hat Enterprise Linux	9.1 a 9.4 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 Ver requisitos de configuração do Podman .	Suportado no modo de imposição ou no modo permissivo • O gerenciamento de sistemas Cloud Volumes ONTAP NÃO é suportado por agentes que tenham o SELinux habilitado no sistema operacional.
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

Tipo de instância AWS EC2

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

Tamanho da VM do Azure

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos Standard_D8s_v3.

Tipo de máquina do Google Cloud

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos 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"

Espaço em disco em /opt

100 GiB de espaço devem estar disponíveis

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

Espaço em disco em /var

20 GiB de espaço devem estar disponíveis

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

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 5. 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 8, verifique se sua versão do Podman está usando o DNS 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.

   Para Red Hat Enterprise Linux 9:

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

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

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<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.
6. Se estiver usando o Red Hat Enterprise:

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

   Para Red Hat Enterprise Linux 9:

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

   Para Red Hat Enterprise Linux 8:

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

7. 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.

8. 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.

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

      ```
      podman info | grep networkBackend
      ```

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

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

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

   d. 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 .
```

9. Reinicie o podman.

```
systemctl restart podman
```

10. 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.

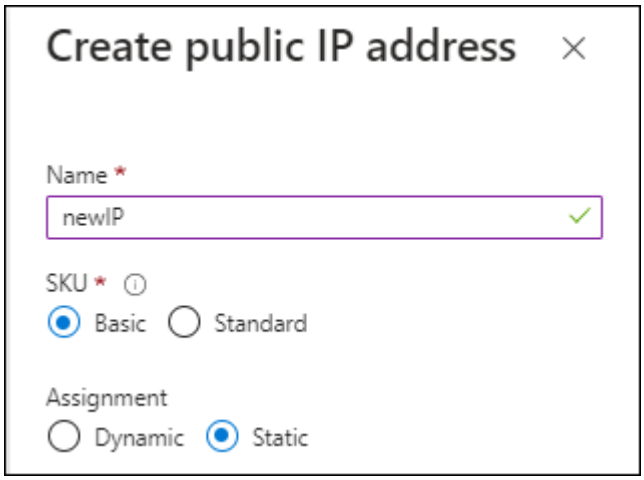
Pontos finais	Propósito
Ambientes AWS	Serviços da AWS (amazonaws.com): • CloudFormation • Nuvem de Computação Elástica (EC2) • Gerenciamento de Identidade e Acesso (IAM) • Serviço de Gerenciamento de Chaves (KMS) • Serviço de Token de Segurança (STS) • Serviço de Armazenamento Simples (S3)
Para gerenciar recursos da AWS. O ponto de extremidade depende da sua região da AWS. "Consulte a documentação da AWS para obter detalhes"	**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.

Pontos finais	Propósito
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://www.googleapis.com/deploymentmanager/v2/projects
Para gerenciar recursos no Google Cloud.	• Pontos de extremidade do console NetApp *
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://support.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://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.

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 estiver planejando usar o NetApp Data Classification para verificar suas fontes de dados corporativos, deverá habilitar 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.

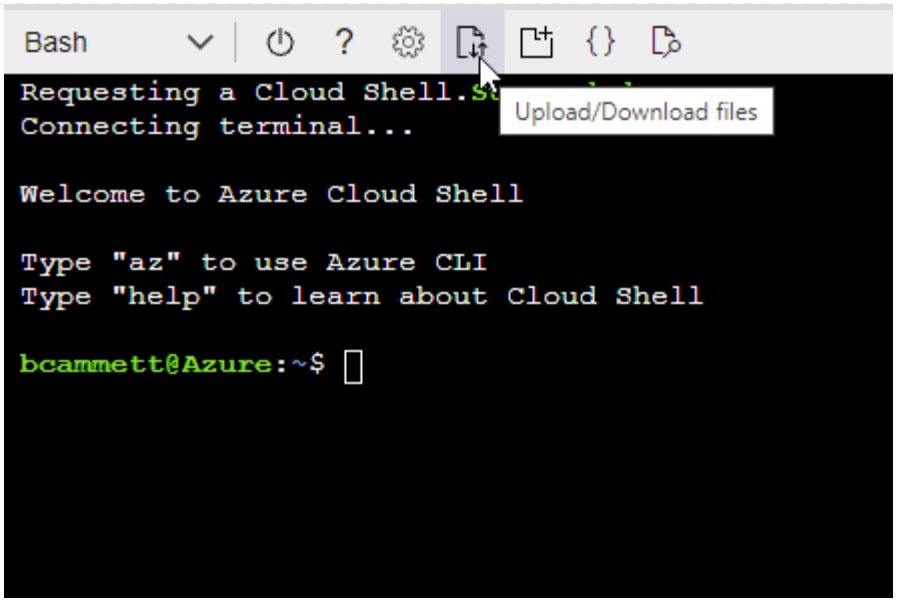
   Exemplo

   ```
   "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 Connector_Policy.json
```

Principal de serviço do Azure

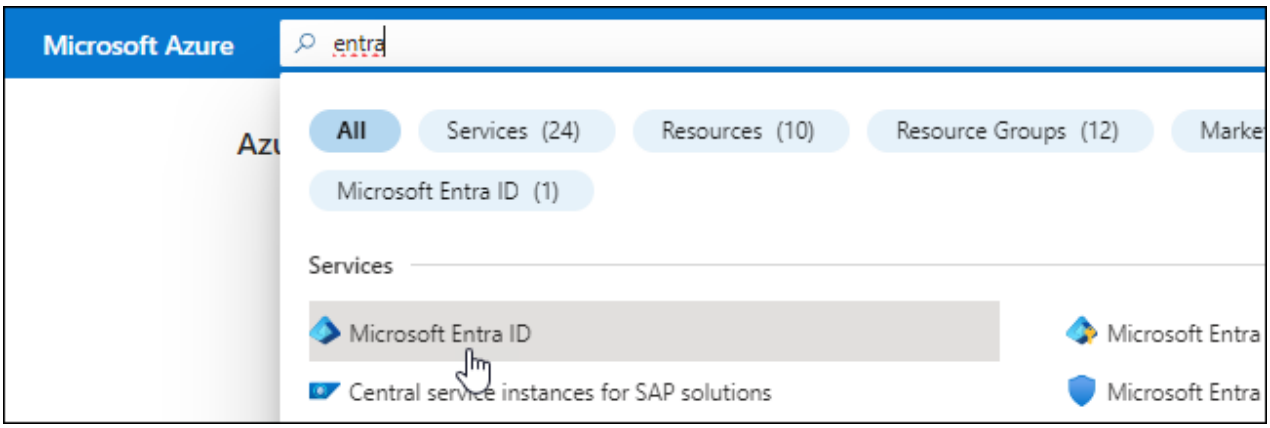
Crie e configure uma entidade de serviço no Microsoft Entra ID e obtenha as credenciais do Azure necessárias para o Console. Você precisa fornecer essas credenciais ao Console depois de instalar o agente do Console.

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 .

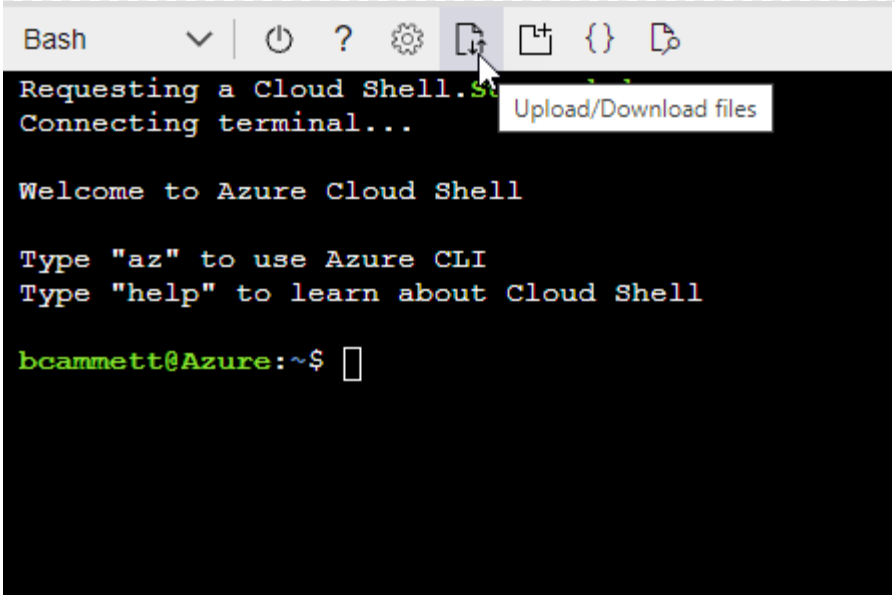
      Exemplo

      ```
      "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
Connector_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**.

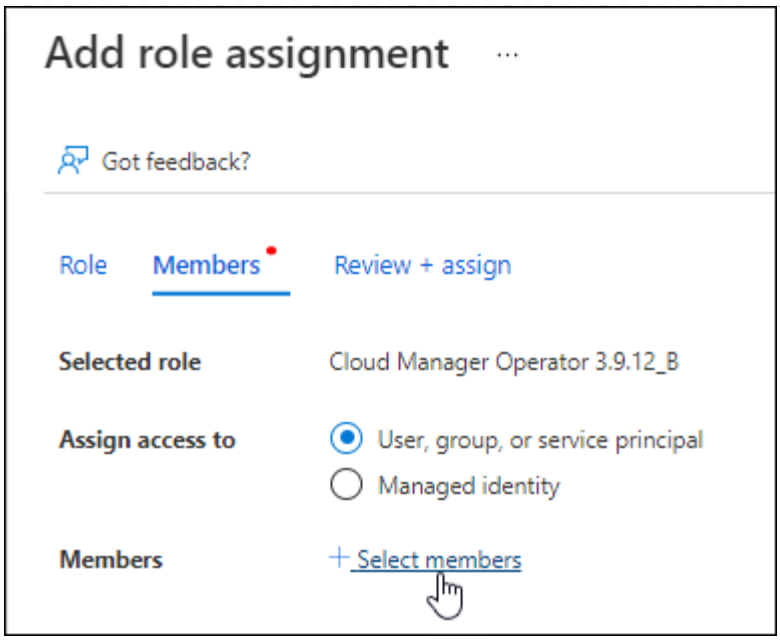
   b. Selecione a assinatura.

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

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

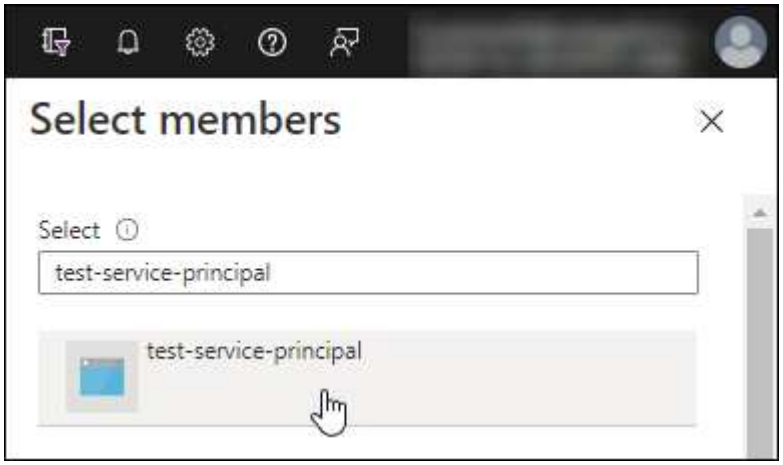
   e. Na aba **Membros**, complete os seguintes passos:

      - 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**.

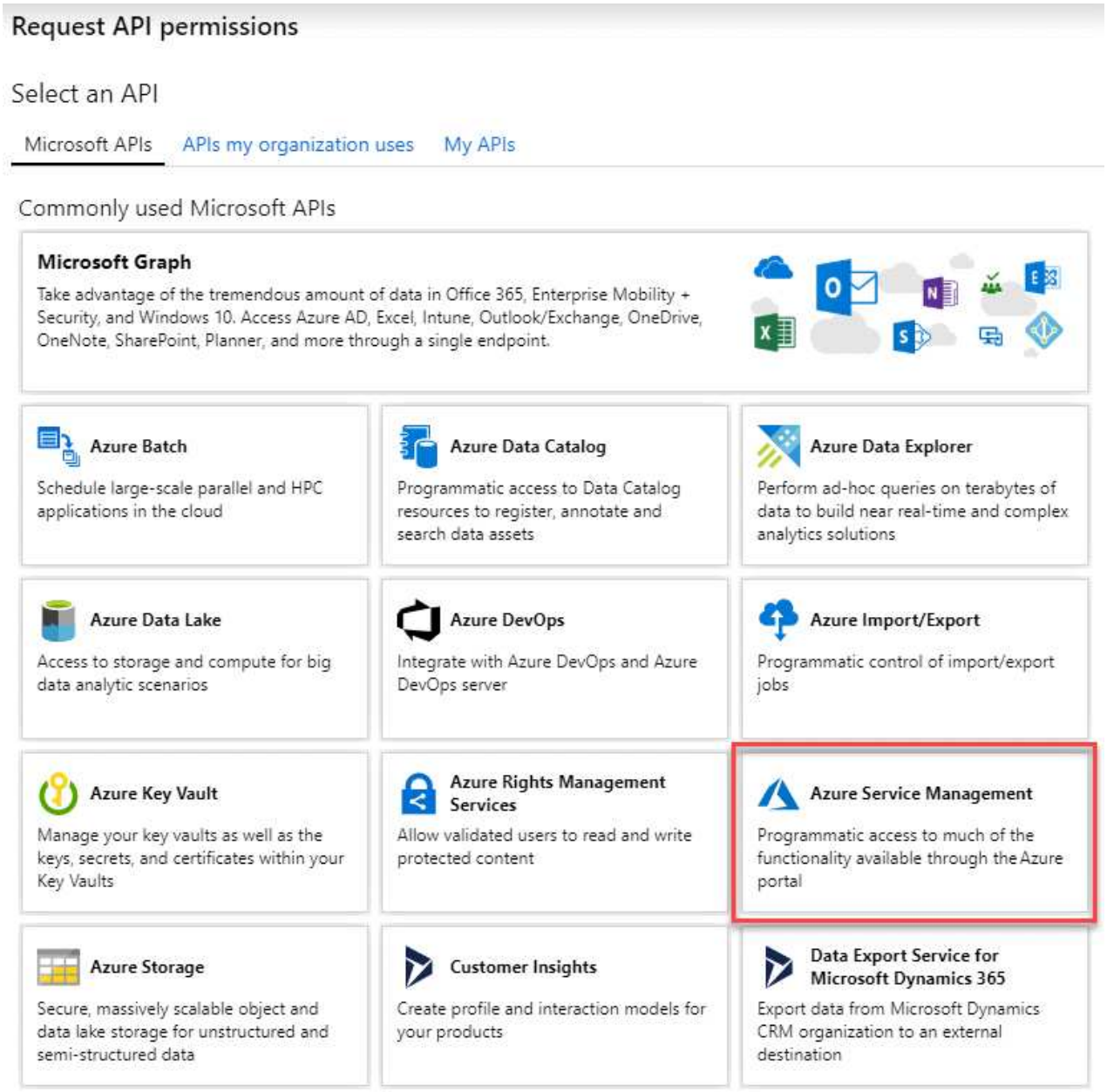
O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

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.

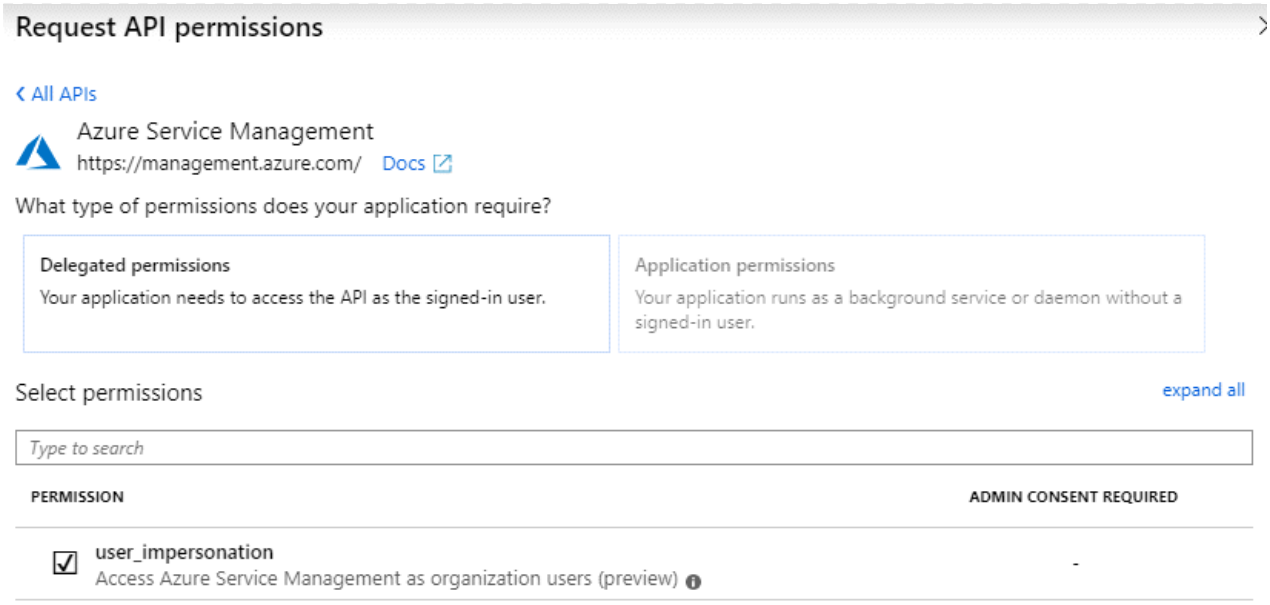
Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

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**.

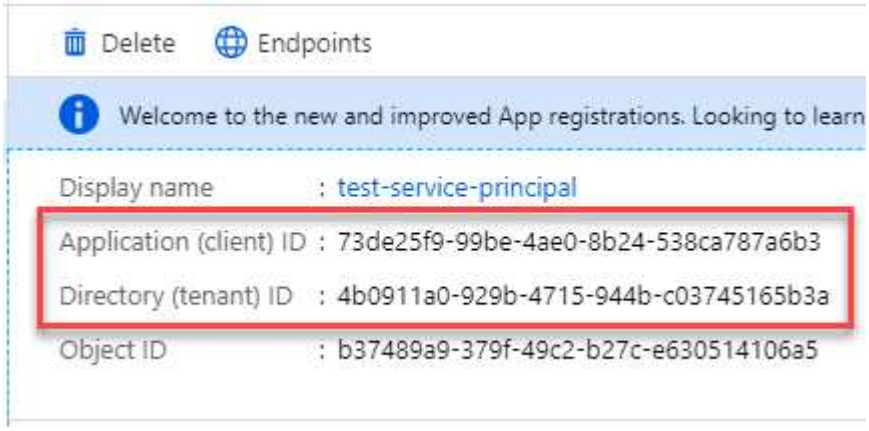


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



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 "conector" no nível do projeto:

```
gcloud iam roles create connector --project=myproject
--file=connector.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"

Resultado

Agora você tem uma conta de serviço que pode atribuir à instância de VM do agente do Console.

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 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.

Marketplace comercial da AWS

Antes de começar

Você deve ter 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 a instância.

  "Revisar requisitos de instância" .

- 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. A instância do agente do Console e o software são executados em aproximadamente cinco minutos.

O que vem a seguir?

Configure o NetApp Console.

Mercado governamental da AWS

Antes de começar

Você deve ter o seguinte:

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

  "Saiba mais sobre os requisitos de rede"

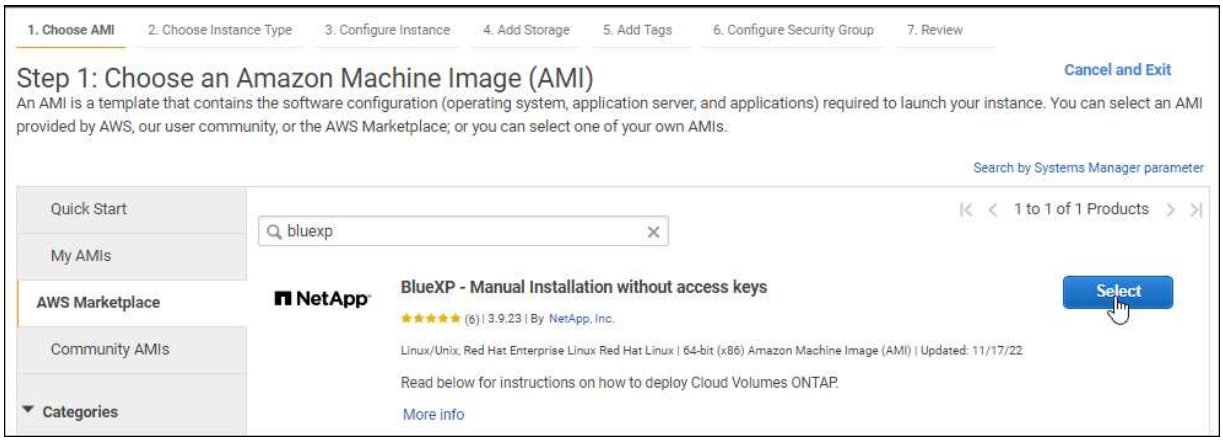
- Uma função do IAM com uma política anexada que inclui as permissões necessárias para o agente do Console.

  "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.



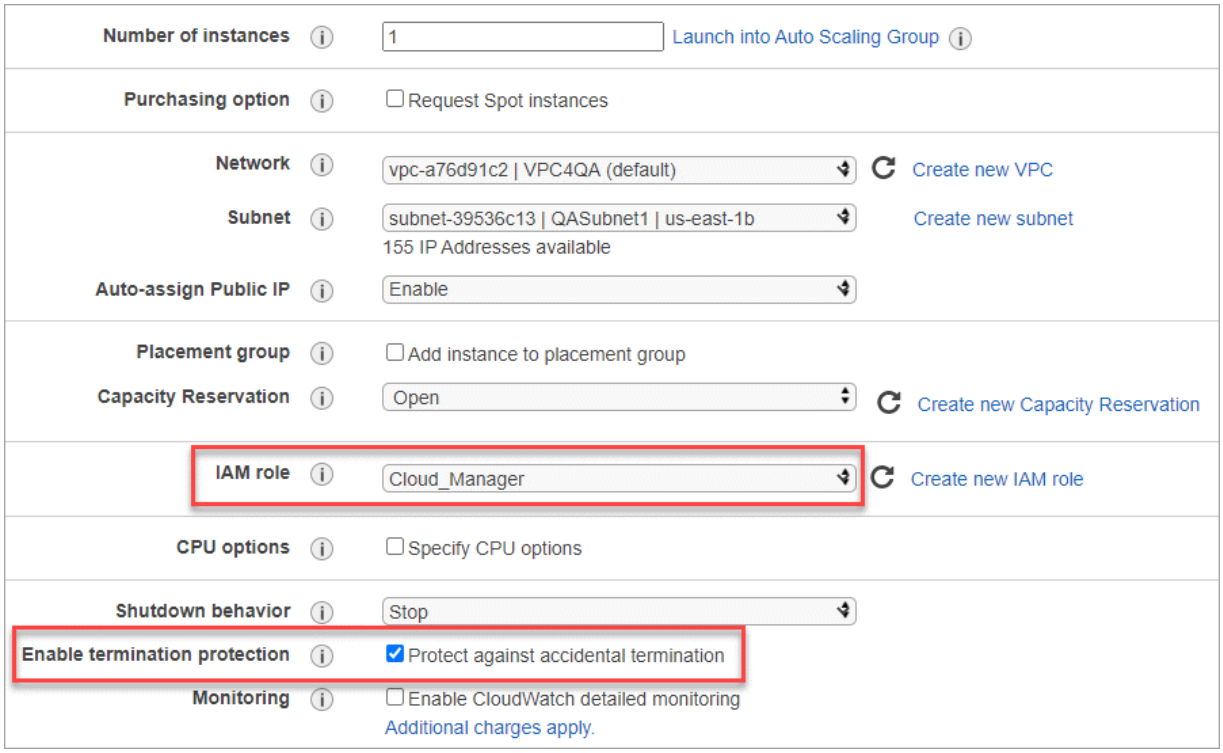
d. Selecione **Continuar**.

2. Siga as instruções para configurar e implantar 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. A instância do agente do Console e o software são executados 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.

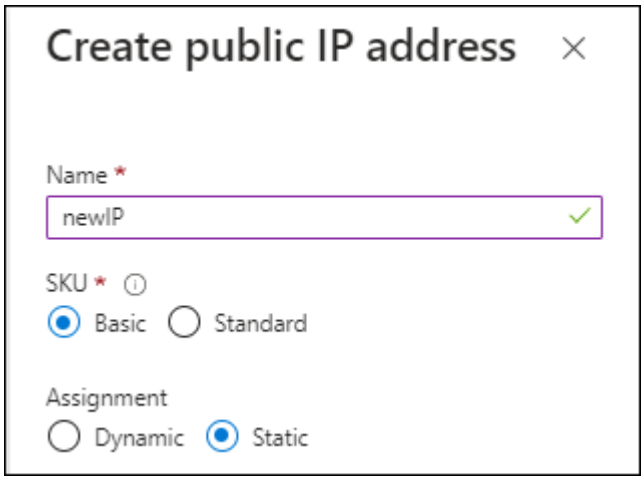
  "Aprenda a configurar permissões do Azure"

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**: se você quiser usar um endereço IP público com a VM do agente do Console, 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"

- **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**.

  Essa configuração é importante porque uma identidade gerenciada permite que a máquina virtual do agente do Console se identifique no Microsoft Entra ID sem fornecer nenhuma credencial. "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?

Configure o NetApp Console.

Instalação manual

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

O instalador disponível no site de suporte da NetApp pode ser uma versão anterior. 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 em "Site de suporte da NetApp" e, em seguida, copie-o para o host Linux.

   Você deve baixar o instalador do agente "online" destinado ao uso em sua rede ou na nuvem.

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 transparente ou explícito. Os parâmetros --proxy e --cacert são opcionais e você não será solicitado a adicioná-los. Se você tiver um servidor proxy, precisará inserir os parâmetros conforme mostrado.

   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-de-usuário:senha@endereço:porta

- http://nome-de-domínio%92nome-de-usuário:senha@endereço:porta
- https://endereço:porta
- https://nome-de-usuário:senha@endereço:porta
- https://nome-de-domínio%92nome-de-usuário:senha@endereço:porta

  Observe o seguinte:

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

    Por exemplo:

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

`--cacert`especifica um certificado assinado pela CA a ser usado para acesso HTTPS entre o agente do Console e o servidor proxy. Este parâmetro é necessário para servidores proxy HTTPS, servidores proxy de interceptação e servidores proxy transparentes.

+ Aqui está um exemplo de configuração de um servidor proxy transparente. Ao configurar um proxy transparente, você não precisa definir o servidor proxy. Você só adiciona um certificado assinado pela CA ao host do agente do Console:

+

```
 ./NetApp_Console_Agent_Cloud_v4.0.0 --cacert
/tmp/cacert/certificate.cer
```

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
...
# 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
...
Esc:wq
```

c. 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?

Configure 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 inscrever com um novo login. Caso contrário, você não verá a opção para habilitar 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. Insira 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 NetApp Console

Se você implantou o agente do Console do Azure Marketplace ou se instalou manualmente o software do agente do Console, será necessário fornecer as permissões configuradas 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:

- Backup e recuperação da NetApp
- Cloud Volumes ONTAP
- Camadas de nuvem da NetApp
- Resiliência do NetApp Ransomware
- Recuperação de desastres da NetApp

A classificação de dados da NetApp 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

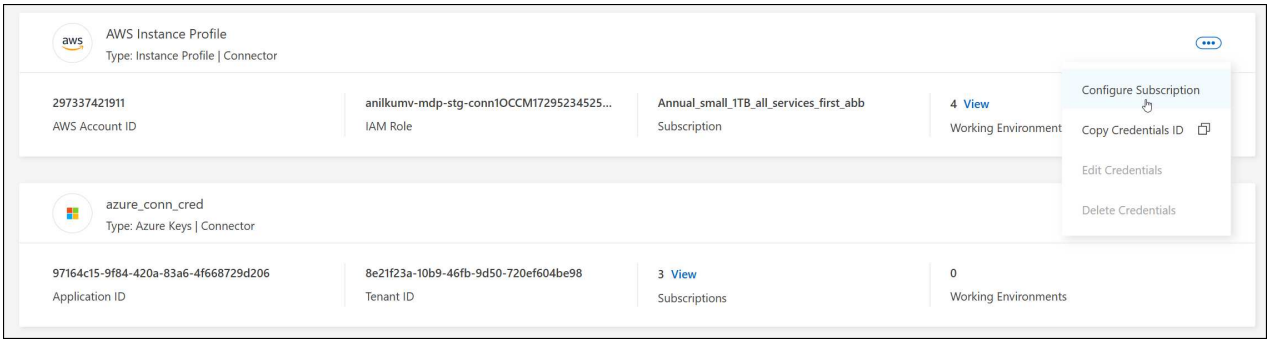
O vídeo a seguir mostra as etapas para assinar o NetApp Intelligent Services no AWS Marketplace:

Assine o NetApp Intelligent Services no AWS Marketplace

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**.

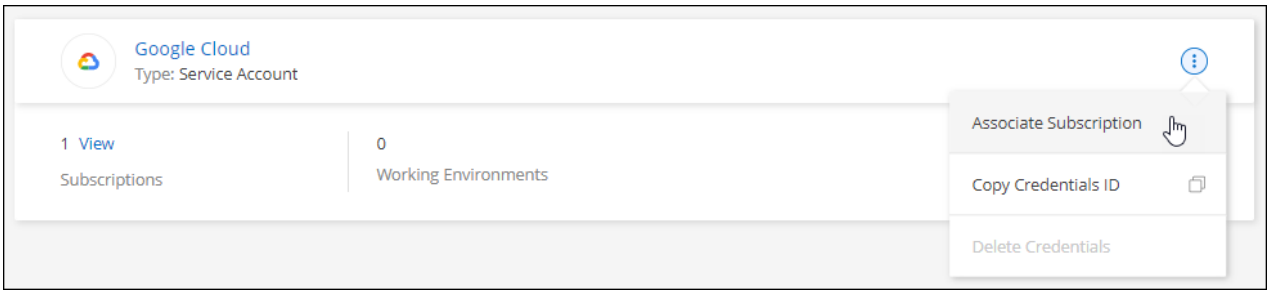
        O vídeo a seguir mostra as etapas para assinar o Azure Marketplace:

   Assine o NetApp Intelligent Services no Azure Marketplace

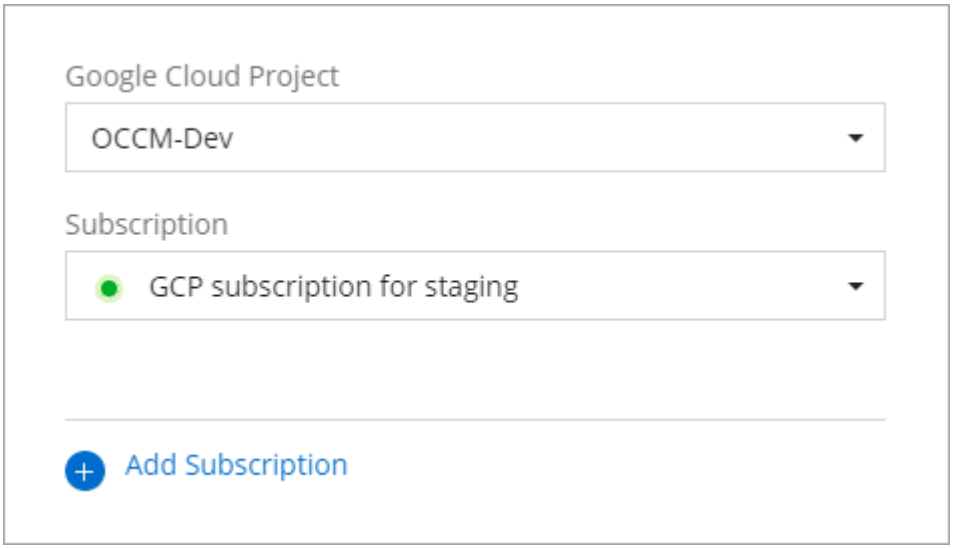
Google Cloud

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**. +nova captura de tela necessária
(TS)



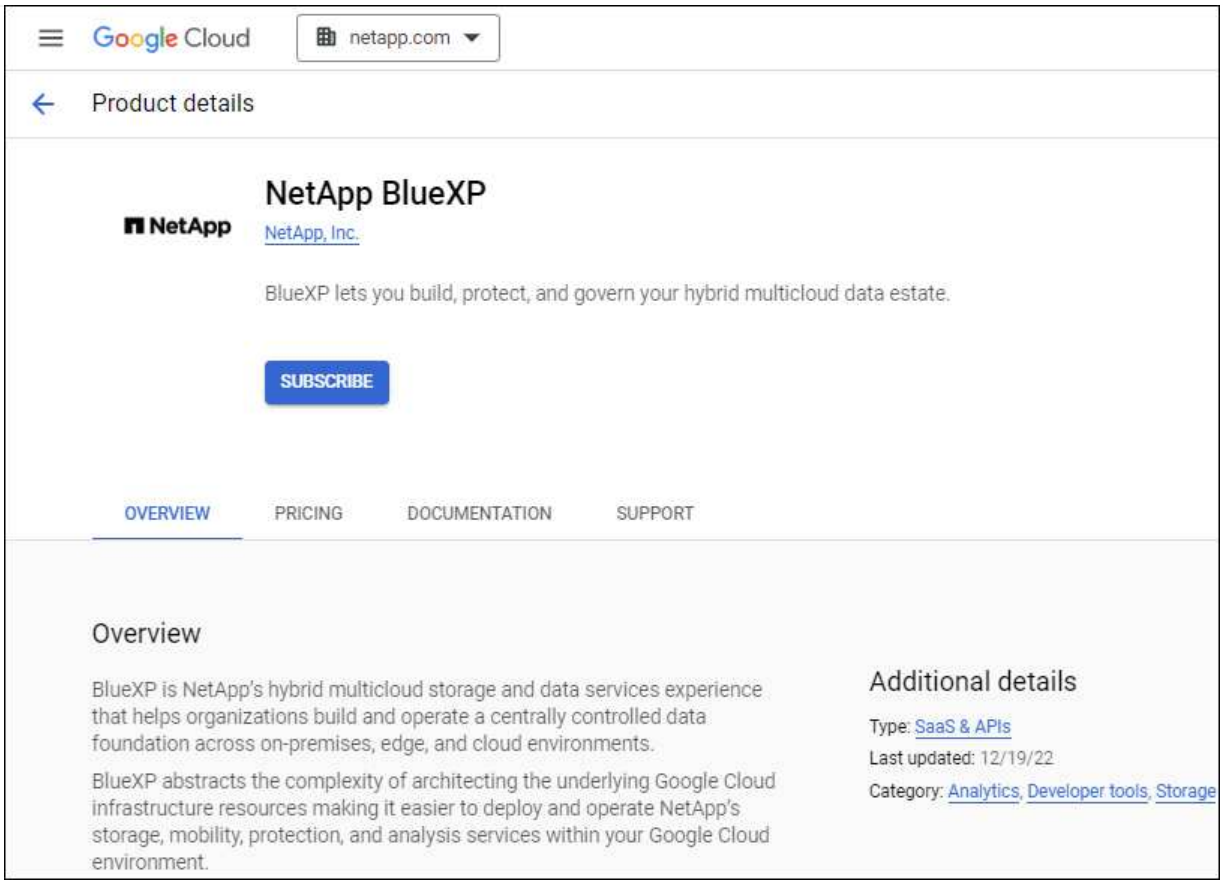
4. Para configurar uma assinatura existente com as credenciais selecionadas, selecione um projeto e uma assinatura do Google Cloud na lista suspensa e selecione **Configurar**.



5. 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 console do NetApp .

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.

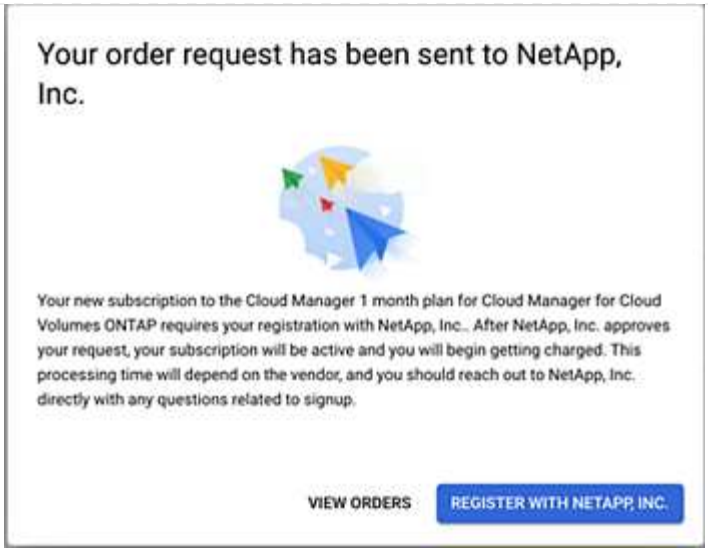


b. Selecione **Inscrever-se**.
c. Selecione a conta de cobrança apropriada e concorde com os termos e condições.
d. Selecione **Inscrever-se**.

   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 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.

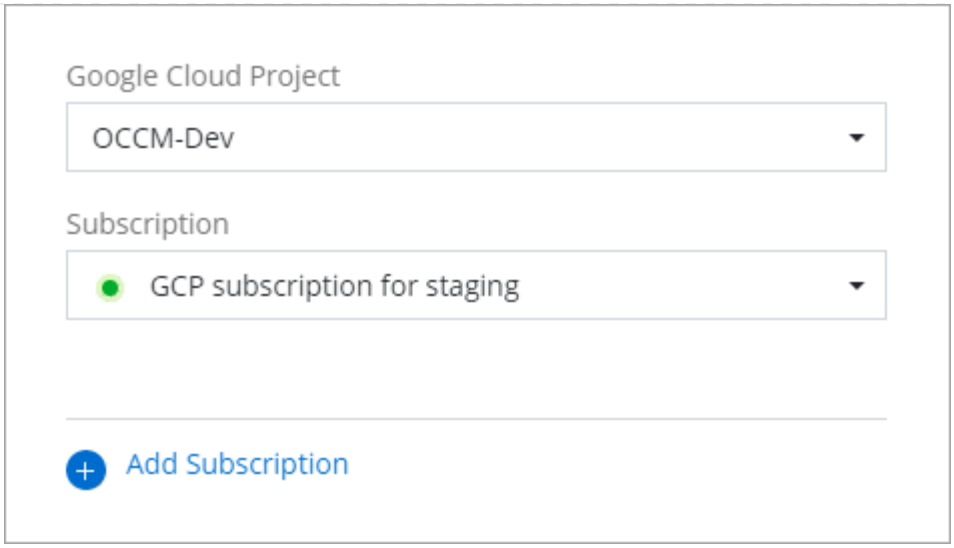
Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo essas etapas.

- Selecione **Salvar**.

  O vídeo a seguir mostra as etapas para assinar o Google Cloud Marketplace:

Assine no Google Cloud Marketplace

a. 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 com a interface legada do BlueXP (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/bluexp-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
	Proteção contra 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

Usar o console NetApp

Efetue login no console do NetApp

A maneira como você faz login no NetApp Console depende do modo de implantação que você está usando.

Você será desconectado automaticamente após 24 horas ou se fechar o navegador.

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

Modo padrão

Depois de se inscrever no NetApp Console, você pode fazer login no console baseado na Web para começar a gerenciar seus dados e infraestrutura de armazenamento.

Sobre esta tarefa

Você pode efetuar login no NetApp Console usando uma das seguintes opções:

- Suas credenciais existentes do NetApp Support Site (NSS)
- Uma conta do NetApp Console usando seu endereço de e-mail e uma senha
- Uma conexão federada

  Você pode usar o logon único para efetuar login usando credenciais do seu diretório corporativo (identidade federada). "Aprenda a configurar a federação de identidade" .

Passos

1. Abra um navegador da web e vá para o "Console NetApp"
2. Na página **Login**, insira o endereço de e-mail associado ao seu login.
3. Dependendo do método de autenticação associado ao seu login, você será solicitado a inserir suas credenciais:
   - Credenciais da nuvem NetApp : insira sua senha
   - Usuário federado: insira suas credenciais de identidade federada
   - Conta do site de suporte da NetApp : insira suas credenciais do site de suporte da NetApp

Resultado

Agora você está conectado e pode começar a usar para gerenciar sua infraestrutura de nuvem híbrida multinuvem.

Modo restrito

Ao usar o Console no modo restrito, você precisa fazer login no Console a partir da interface do usuário executada localmente no agente.

Sobre esta tarefa

O Console oferece suporte ao login com uma das seguintes opções quando estiver no modo restrito:

- Um login do NetApp Console usando seu endereço de e-mail e uma senha
- Uma conexão federada

  Você pode usar o logon único para efetuar login usando credenciais do seu diretório corporativo (identidade federada). "Aprenda a usar a federação de identidade" .

Passos

1. Abra um navegador da web e digite o endereço IP onde o agente está instalado.
2. Digite seu nome de usuário e senha para efetuar login.

Exibir métricas na página inicial do NetApp Console

Monitorar a integridade do seu depósito garante que você esteja ciente dos problemas com a proteção do armazenamento e possa tomar medidas para resolvê-los. Usando a página inicial do NetApp Console, visualize o status dos seus backups e restaurações do NetApp Backup and Recovery e o número de cargas de trabalho que correm risco de ataque de ransomware ou estão protegidas, conforme indicado pelo NetApp Ransomware Resilience. Você pode revisar a capacidade de armazenamento de clusters individuais e do Cloud Volumes ONTAP, alertas do ONTAP , capacidade de desempenho de armazenamento por cluster ou sistema Cloud Volumes ONTAP , os diferentes tipos de licenças que você tem e muito mais.

Todos os painéis na página inicial mostram dados no nível da organização. Os painéis Capacidade de armazenamento e Desempenho de armazenamento mostram sistemas associados a projetos que o usuário pode acessar com base nas permissões do IAM.

O sistema atualiza os dados na página inicial a cada cinco minutos. O armazenamento em cache pode fazer com que os dados nesta página sejam diferentes dos valores reais por até 15 minutos.

Métricas precisas na página inicial exigem agentes de console configurados e dimensionados adequadamente.

Funções necessárias do NetApp Console

Cada painel na página inicial requer funções de usuário diferentes:

- **Painel de capacidade de armazenamento**: Capacidade de ver a página de sistemas do console NetApp
- * Painel de alertas ONTAP *: Administrador de pasta ou projeto, Analista de suporte de operações, Administrador da organização, Visualizador da organização, Superadministrador, Supervisualizador
- **Painel de capacidade de desempenho de armazenamento**: Capacidade de ver a página de sistemas do console NetApp
- **Painel de licenças e assinaturas**: Administrador de pasta ou projeto, Administrador da organização, Visualizador da organização, Superadministrador, Supervisualizador
- **Painel de resiliência contra ransomware**: administrador de pasta ou projeto, administrador da organização, administrador de proteção contra ransomware, visualizador de proteção contra ransomware, superadministrador, supervisualizador
- **Painel de backup e recuperação**: Administrador de backup e recuperação, Superadministrador de backup e recuperação, Visualizador de backup e recuperação, Administrador de clone de backup e recuperação, Administrador de pasta ou projeto, Administrador de organização, Administrador de restauração de backup e recuperação, Superadministrador, Supervisualizador

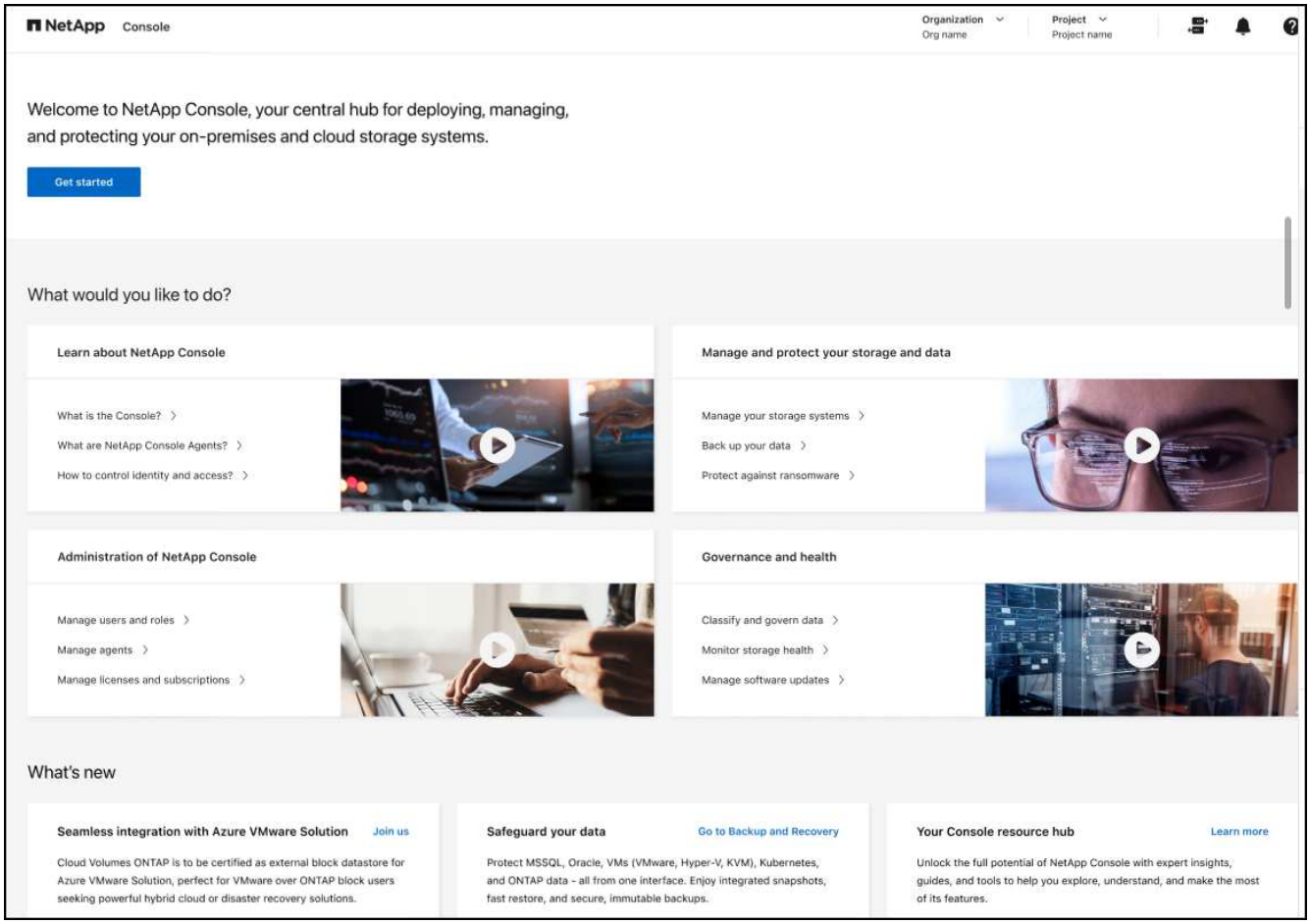
Se você não tiver permissões para acessar um painel, o painel exibirá uma mensagem indicando que você não tem permissões para usá-lo.

"Saiba mais sobre as funções de acesso do NetApp Console." .

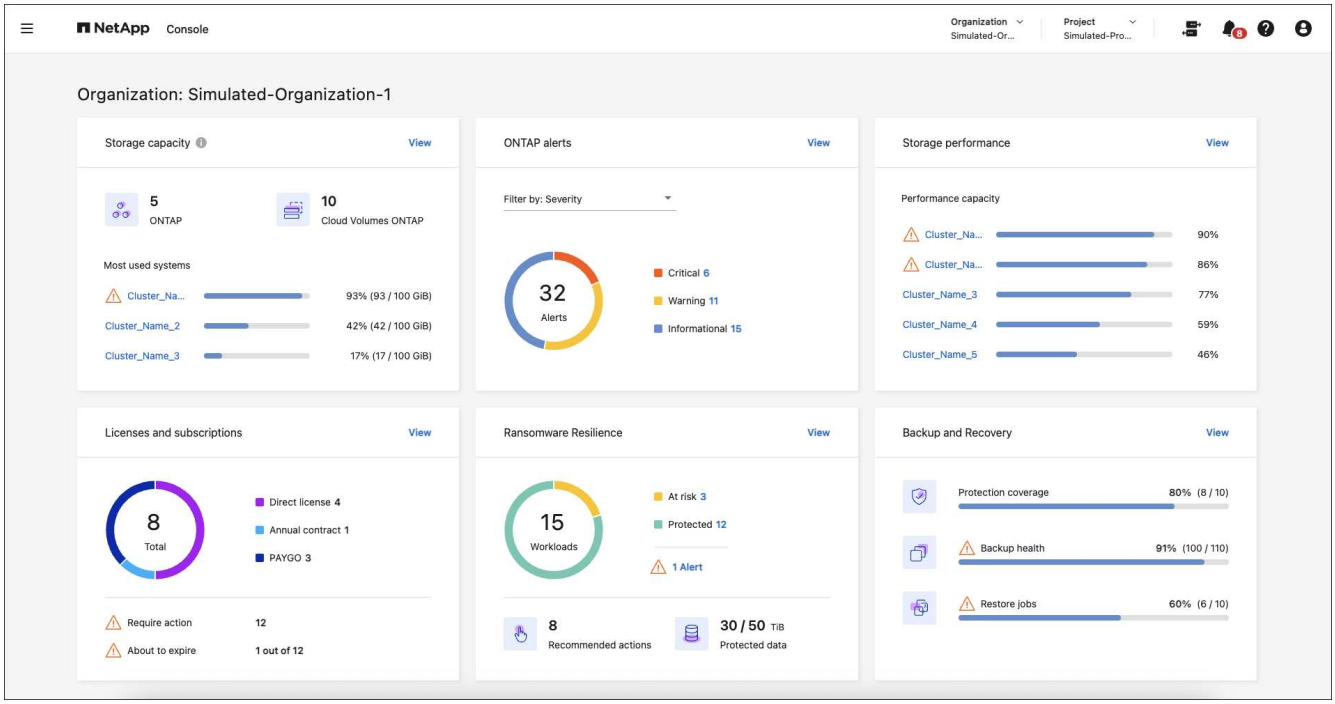
Passos

1. No menu do NetApp Console, selecione **Home**.

Se você tiver a função de administrador da organização e nenhum agente ou sistema de armazenamento estiver configurado, a página inicial exibirá informações de introdução.



Se você já configurou o NetApp Console, pelo menos um agente do Console está habilitado e pelo menos um cluster ou sistema Cloud Volumes ONTAP foi adicionado a esse agente, a página inicial mostra métricas sobre seu ambiente de armazenamento.



Habilitar que as métricas apareçam na página inicial

Você pode ver as métricas na página inicial quando as seguintes condições forem atendidas:

- Você está conectado a uma instância SaaS do NetApp Console.
- Você pertence a uma organização com recursos de armazenamento existentes (agente e cluster ou sistema Cloud Volumes ONTAP).
- Pelo menos um agente do Console está habilitado.
- Pelo menos um cluster ou sistema Cloud Volumes ONTAP foi adicionado nesse agente.

Para permitir que as métricas apareçam na página inicial, conclua as seguintes tarefas:

- Habilite pelo menos um agente do Console.
- Adicione pelo menos um cluster ou um Cloud Volumes ONTAP usando esse agente.

Veja a capacidade geral de armazenamento

O painel Capacidade de armazenamento fornece as seguintes informações sobre clusters ONTAP e sistemas Cloud Volumes ONTAP :

- Número de sistemas ONTAP descobertos no Console
- Número de sistemas Cloud Volumes ONTAP descobertos no Console
- Uso de capacidade por cluster

A ordem dos clusters ou sistemas Cloud Volumes ONTAP é baseada na quantidade de capacidade utilizada. O cluster ou sistema com maior capacidade aparece primeiro para facilitar a identificação.

Indicadores de alerta mostram clusters com capacidade de 80%, com dados atualizados a cada cinco minutos.

Se você tiver vários projetos, poderá ver dados diferentes no painel Capacidade de armazenamento em comparação à página Sistemas. Isso ocorre porque a página Sistemas mostra informações com base no nível do projeto, enquanto o painel Capacidade de armazenamento mostra informações no nível da organização. Além disso, os dados neste painel podem diferir dos valores reais por no máximo 15 minutos, porque os dados são armazenados em cache durante esse período para otimizar o desempenho.

Passos

1. No menu do NetApp Console, revise o painel Capacidade de armazenamento.
2. No painel Capacidade de armazenamento, selecione **Exibir** para ir para a página Sistemas de console.
3. Na página Sistemas, selecione o projeto que contém o cluster que você deseja visualizar.
4. Na página Sistemas, selecione um cluster para ver mais detalhes sobre ele.

Ver alertas ONTAP

Visualize problemas ou riscos potenciais em seus ambientes ONTAP locais da NetApp . Você pode ver alguns alertas não relacionados ao EMS e alguns alertas relacionados ao EMS.

Os dados são atualizados a cada 5 minutos.

Você pode ver alertas ONTAP com estas gravidades:

- Crítico
- Aviso
- Informativo

Você pode ver alertas ONTAP para estas áreas de impacto:

- Capacidade
- Desempenho
- Proteção
- Disponibilidade
- Segurança

O armazenamento em cache otimiza o desempenho, mas pode fazer com que os dados neste painel sejam diferentes dos valores reais por até 15 minutos.

Sistemas suportados

- Um sistema ONTAP NAS ou SAN local é suportado.
- Os sistemas Cloud Volumes ONTAP não são suportados.

Fontes de dados suportadas

Veja alertas sobre determinados eventos que ocorrem no ONTAP. Eles são uma combinação de EMS e alertas baseados em métricas.

Para obter detalhes sobre alertas ONTAP , consulte "Sobre alertas ONTAP" .

Para obter uma lista de alertas que você pode ver, consulte "Veja os riscos potenciais no armazenamento ONTAP" .

Passos

1. No menu do NetApp Console, revise o painel de alertas do ONTAP .
2. Opcionalmente, filtre os alertas selecionando o nível de gravidade ou altere o filtro para mostrar alertas com base na área de impacto.
3. No painel de alertas do ONTAP , selecione **Exibir** para ir para a página Alertas do Console.

Ver capacidade de desempenho de armazenamento

Analise a capacidade de desempenho de armazenamento usada por cluster ou sistema Cloud Volumes ONTAP para determinar como a capacidade de desempenho, a latência e o IOPS estão impactando suas cargas de trabalho. Por exemplo, você pode descobrir que precisa mudar as cargas de trabalho para minimizar a latência e maximizar o IOPS e a taxa de transferência para suas cargas de trabalho críticas.

O sistema organiza clusters e sistemas por capacidade de desempenho, listando primeiro a maior capacidade para facilitar a identificação.

O armazenamento em cache otimiza o desempenho, mas pode fazer com que os dados neste painel sejam diferentes dos valores reais por até 15 minutos.

Passos

1. No menu do NetApp Console, revise o painel Desempenho de armazenamento.
2. No painel Desempenho de armazenamento, selecione **Exibir** para acessar uma página Desempenho que lista todos os clusters e dados dos sistemas Cloud Volumes ONTAP para capacidade de desempenho, IOPS e latência.
3. Selecione um cluster para visualizar seus detalhes no Gerenciador do Sistema.

Visualize as licenças e assinaturas que você possui

Revise as seguintes informações no painel Licenças e assinaturas:

- O número total de licenças e assinaturas que você tem.
- O número de cada tipo de licença e assinatura que você possui (licença direta, contrato anual ou PAYGO).
- O número de licenças e assinaturas que estão ativas, exigem ação ou estão próximas do vencimento.
- O sistema exibe indicadores ao lado dos tipos de licença que exigem ação ou estão próximos de expirar.

Os dados são atualizados a cada 5 minutos.

O armazenamento em cache otimiza o desempenho, mas pode fazer com que os dados neste painel sejam diferentes dos valores reais por até 15 minutos.

Passos

1. No menu do NetApp Console, revise o painel Licenças e assinaturas.
2. No painel Licenças e assinaturas, selecione **Exibir** para ir para a página Licenças e assinaturas do console.

Ver status de resiliência do ransomware

Descubra se as cargas de trabalho correm risco de ataques de ransomware ou estão protegidas com o serviço de dados NetApp Ransomware Resilience. Você pode revisar a quantidade total de dados protegidos, visualizar o número de ações recomendadas e visualizar o número de alertas relacionados à proteção contra ransomware.

Os dados são atualizados a cada 5 minutos e correspondem aos dados mostrados no Painel de resiliência do NetApp Ransomware.

"Saiba mais sobre a resiliência do NetApp Ransomware" .

Passos

1. No menu do NetApp Console, revise o painel Resiliência contra Ransomware.
2. Execute um dos seguintes procedimentos no painel Resiliência de Ransomware:
   - Selecione **Exibir** para acessar o Painel de Resiliência do NetApp Ransomware. Para mais detalhes, consulte "Monitore a integridade da carga de trabalho usando o NetApp Ransomware Resilience Dashboard" .
   - Revise "Ações recomendadas" no Painel de resiliência do NetApp Ransomware. Para mais detalhes, consulte "Revise as recomendações de proteção no Painel de Resiliência do NetApp Ransomware" .
   - Selecione o link de alertas para revisar os alertas na página Alertas de resiliência do NetApp Ransomware. Para mais detalhes, consulte "Lide com alertas de ransomware detectados com o NetApp Ransomware Resilience" .

Ver status de backup e recuperação

Revise o status geral dos seus backups e restaurações do NetApp Backup and Recovery. Você pode ver o número de recursos protegidos e desprotegidos. Você também pode ver a porcentagem de backups e operações de restauração para proteção de suas cargas de trabalho. Uma porcentagem maior indica melhor proteção de dados.

Os dados são atualizados a cada 5 minutos.

O armazenamento em cache otimiza o desempenho, mas pode fazer com que os dados neste painel sejam diferentes dos valores reais por até 15 minutos.

Passos

1. No menu do NetApp Console, revise o painel Backup e recuperação.
2. Selecione **Exibir** para acessar o Painel de Backup e Recuperação do NetApp . Para mais detalhes, consulte "Documentação do NetApp Backup and Recovery" .

Gerencie as configurações de usuário do NetApp Console

Você pode modificar seu perfil do Console, incluindo alterar sua senha, habilitar a autenticação multifator (MFA) e ver quem é o administrador do Console.

No Console, cada usuário tem um perfil que contém informações sobre o usuário e suas configurações. Você pode visualizar e editar as configurações do seu perfil.

Alterar seu nome de exibição

Você pode alterar o nome de exibição do seu Console, que é usado para identificá-lo e fica visível para outros usuários. Seu nome de exibição não é o mesmo que seu nome de usuário ou endereço de e-mail, que não podem ser alterados.

Passos

1. Selecione o ícone de perfil no canto superior direito do Console para visualizar o painel de configurações do usuário.
2. Selecione o ícone **Editar** ao lado do seu nome.
3. Digite seu novo nome de exibição no campo **Nome**.

Configurar autenticação multifator

Configure a autenticação multifator (MFA) para melhorar a segurança exigindo um segundo método de verificação.

Usuários que usam logon único com um provedor de identidade externo ou o site de suporte da NetApp não podem habilitar o MFA. Se alguma dessas situações for verdadeira para você, você não verá a opção para habilitar o MFA nas configurações do seu perfil.

Não habilite o MFA se sua conta de usuário for usada para acesso à API. A autenticação multifator interrompe o acesso à API quando ativada para uma conta de usuário. Use contas de serviço para todo o acesso à API.

Antes de começar

- Você já deve ter baixado um aplicativo de autenticação, como o Google Authenticator ou o Microsoft Authenticator, para o seu dispositivo.
- Você precisará da sua senha para configurar o MFA.

Se você não tiver acesso ao seu aplicativo de autenticação ou perder seu código de recuperação, entre em contato com o administrador do Console para obter ajuda.

Passos

1. Selecione o ícone de perfil no canto superior direito do Console para visualizar o painel de configurações do usuário.
2. Selecione **Configurar** ao lado do cabeçalho **Autenticação multifator**.
3. Siga as instruções para configurar o MFA para sua conta.
4. Quando terminar, você será solicitado a salvar seu código de recuperação. Escolha entre copiar o código ou baixar um arquivo de texto contendo o código. Guarde esse código em algum lugar seguro. Você precisará do código de recuperação se perder o acesso ao seu aplicativo de autenticação.

   Depois de configurar o MFA, o Console solicitará que você insira um código único do seu aplicativo de autenticação sempre que fizer login.

Regenere seu código de recuperação MFA

Você só pode usar códigos de recuperação uma vez. Se você usar ou perder o seu, crie um novo.

Passos

1. Selecione o ícone de perfil no canto superior direito do Console para visualizar o painel de configurações do usuário.
2. Selecione ••• ao lado do cabeçalho **Autenticação Multifator**.
3. Selecione **Regenerar código de recuperação**.
4. Copie o código de recuperação gerado e salve-o em um local seguro.

Excluir sua configuração de MFA

Para parar de usar a autenticação multifator (MFA) para seu login, exclua sua configuração de MFA. Isso elimina a necessidade de inserir um código único no seu aplicativo de autenticação ao fazer login.

Se você não conseguir acessar seu aplicativo de autenticação ou código de recuperação, será necessário entrar em contato com o administrador da organização para redefinir sua configuração de MFA.

Passos

1. Selecione o ícone de perfil no canto superior direito do Console para visualizar o painel de configurações do usuário.
2. Selecione ••• ao lado do cabeçalho **Autenticação Multifator**.
3. Selecione **Excluir**.

Entre em contato com o administrador da sua organização

Se precisar entrar em contato com o administrador da sua organização, você pode enviar um e-mail diretamente do Console. O administrador gerencia contas de usuários e permissões dentro da sua organização.

Você deve ter um aplicativo de e-mail padrão configurado no seu navegador para usar o recurso **Entrar em contato com administradores**.

Passos

1. Selecione o ícone de perfil no canto superior direito do Console para visualizar o painel de configurações do usuário.
2. Selecione **Entrar em contato com administradores** para enviar um e-mail ao administrador da sua organização.
3. Selecione o aplicativo de e-mail a ser usado.
4. Conclua o e-mail e selecione **Enviar**.

Configurar modo escuro (tema escuro)

Você pode configurar o Console para exibir no modo escuro.

Passos

1. Selecione o ícone de perfil no canto superior direito do Console para visualizar o painel de configurações do usuário.
2. Mova o controle deslizante **Tema escuro** para ativá-lo.

Administrar o NetApp Console

Gerenciamento de identidade e acesso

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

O gerenciamento de identidade e acesso (IAM) no NetApp Console permite que você organize e controle o acesso aos seus recursos do NetApp . Você pode organizar seus recursos de acordo com a hierarquia da sua organização. Por exemplo, você pode organizar recursos por localização geográfica, site ou unidade de negócios. Você pode então atribuir funções do IAM a membros em partes específicas da hierarquia, o que impede o acesso a recursos em outras partes da hierarquia.

- "Saiba mais sobre os modos de implantação do Console"

Como funciona o IAM

O IAM permite que você conceda acesso a recursos atribuindo funções de acesso de usuários a partes específicas da hierarquia. Por exemplo, um membro pode receber a função de administrador de pasta ou projeto para um projeto com cinco recursos.

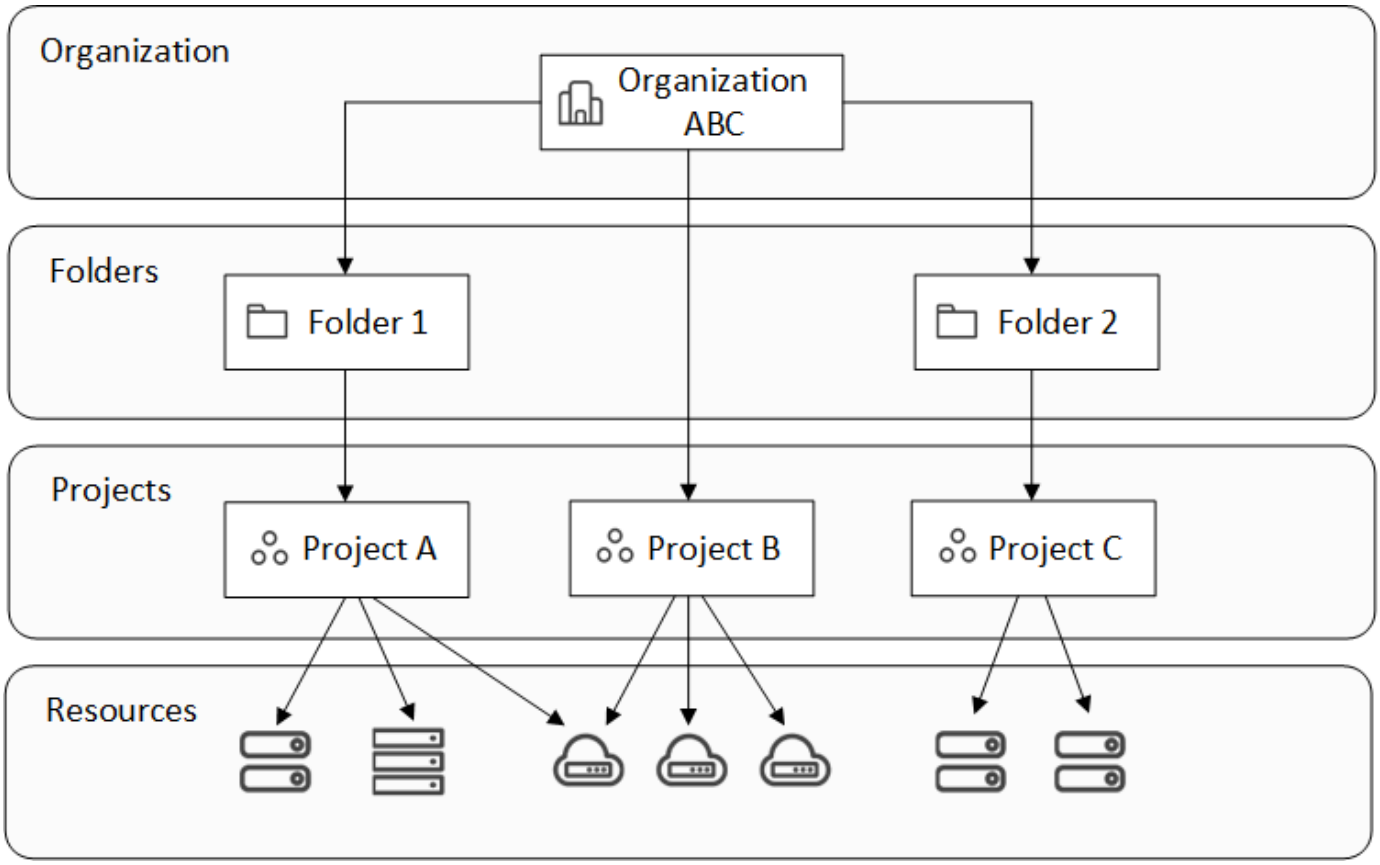
Ao usar o IAM, você gerencia os seguintes componentes:

- A organização
- Pastas
- Projetos
- Recursos
- Membros
- Funções e permissões
- Agentes de console

Os recursos são organizados hierarquicamente:

- A organização é o topo da hierarquia.
- As pastas são filhas da organização ou de outra pasta.
- Projetos são filhos da organização ou de uma pasta.
- Os recursos são associados a uma ou mais pastas ou projetos.

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



Organização

Uma *organização* é o nível superior do sistema 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.

Pastas

Uma *pasta* permite que você agrupe projetos relacionados e os separe de outros projetos na sua organização. Por exemplo, uma pasta pode representar uma localização geográfica (UE ou Leste dos EUA), um site (Londres ou Toronto) ou uma unidade de negócios (engenharia ou marketing).

Você pode organizar pastas para conter projetos, outras pastas ou ambos. Eles são opcionais.

Projetos

Um *projeto* representa um espaço de trabalho no Console que os membros da organização acessam na página **Sistemas** para gerenciar recursos. Por exemplo, um projeto pode incluir um sistema Cloud Volumes ONTAP , um cluster ONTAP local ou um sistema de arquivos FSx for ONTAP .

Uma organização pode ter um ou muitos projetos. Um projeto pode residir diretamente abaixo da organização ou dentro de uma pasta.

Recursos

Um *recurso* é um sistema que você criou ou descobriu no Console.

Quando você cria ou descobre um recurso, o recurso é associado ao projeto selecionado no momento. Esse pode ser o único projeto ao qual você deseja associar esse recurso. Mas você pode optar por associar o

recurso a projetos adicionais na sua organização.

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

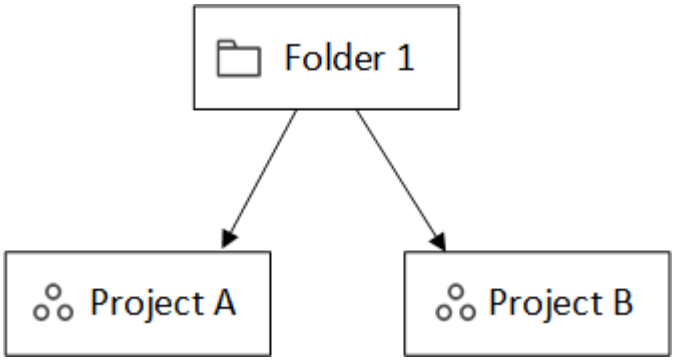
Os agentes também podem ser associados a mais de um projeto. Saiba mais sobre o uso de agentes com o IAM .

Quando associar um recurso a uma pasta

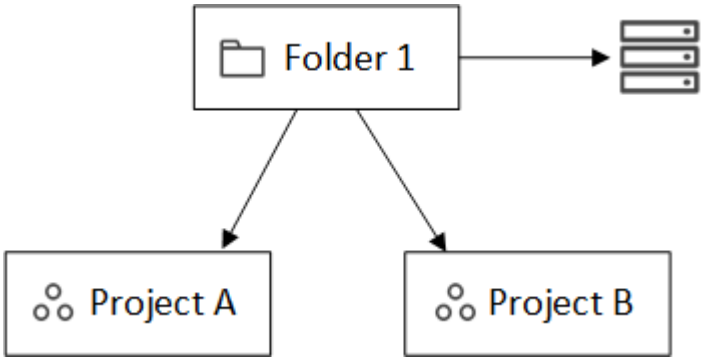
Você também tem a opção de associar um recurso a uma pasta, mas isso é opcional e atende às necessidades de um caso de uso específico.

Um *Administrador da organização* pode associar um recurso a uma pasta para que um *Administrador de pasta ou projeto* possa vinculá-lo aos projetos apropriados na pasta.

Por exemplo, digamos que você tenha uma pasta que contém dois projetos:

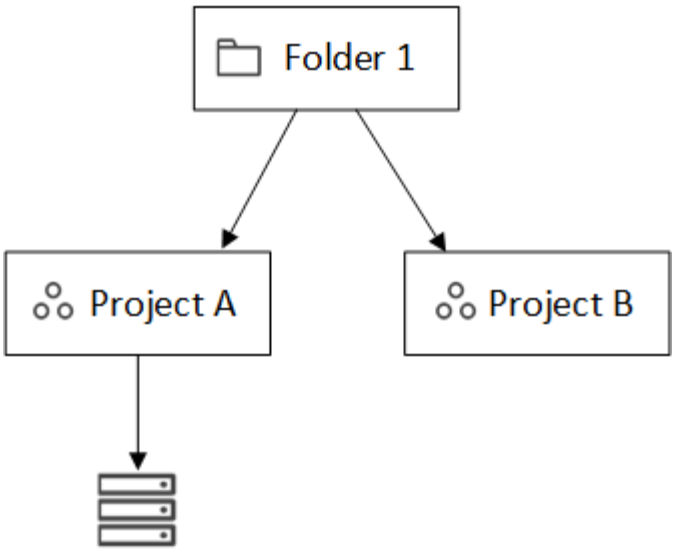


O *Administrador da organização* pode associar um recurso à pasta:



Associar um recurso a uma pasta não o torna acessível a todos os projetos; somente o *administrador da pasta ou do projeto* pode vê-lo. O *administrador de pasta ou projeto* decide quais projetos podem acessá-lo e associa o recurso aos projetos apropriados.

Neste exemplo, o administrador associa o recurso ao Projeto A:



Membros que têm permissões para o projeto A agora podem acessar o recurso.

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.

Cada organização inclui pelo menos um usuário com a função *Administrador da organização* (o Console atribui automaticamente essa função ao usuário que cria a organização). Você pode adicionar outros membros à organização e atribuir permissões diferentes em diferentes níveis da hierarquia de recursos.

Funções e permissões

Você não concede permissões diretamente aos membros da organização. Em vez disso, você concede a cada membro uma função. Uma função contém um conjunto de permissões que permite que um membro execute ações específicas em um nível específico da hierarquia de recursos.

Conceder funções em um nível de hierarquia restringe o acesso aos recursos e serviços de que um membro precisa.

Onde você pode atribuir funções na hierarquia

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

Herança de função

Quando você atribui uma função, ela é herdada na hierarquia da organização:

Organização
: Conceder a um membro uma função de acesso no nível da organização dá a ele permissões para todas as pastas, projetos e recursos.

Pastas
: Quando você concede uma função de acesso no nível da pasta, todas as pastas, projetos e recursos na pasta herdam essa função.

Por exemplo, se você atribuir uma função no nível da pasta e essa pasta tiver três projetos, o membro terá permissões para esses três projetos e quaisquer recursos associados.

Projetos

Quando você concede uma função de acesso no nível do projeto, todos os recursos associados a esse projeto herdam essa função.

Múltiplas funções

Você pode atribuir a cada membro da organização uma função em diferentes níveis da hierarquia da organização. Pode ser a mesma função ou uma função diferente. Por exemplo, você pode atribuir uma função de membro A para o projeto 1 e o projeto 2. Ou você pode atribuir uma função de membro A para o projeto 1 e uma função B para o projeto 2.

Funções de acesso

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

"Saiba mais sobre funções de acesso" .

Agentes de console

Quando um *Administrador da organização* cria um agente do Console, o Console associa automaticamente esse agente à organização e ao projeto selecionado no momento. O *Administrador da organização* tem acesso automático a esse agente de qualquer lugar da organização. Mas se você tiver outros membros na sua organização com funções diferentes, esses membros só poderão acessar esse agente a partir do projeto no qual ele foi criado, a menos que você associe esse agente a outros projetos.

Você disponibiliza um agente do Console para outro projeto nestes casos:

- Você deseja permitir que os membros da sua organização usem um agente existente para criar ou descobrir sistemas adicionais em outro projeto
- Você associou um recurso existente a outro projeto e esse recurso é gerenciado por um agente do Console

  Se um recurso que você associa a um projeto adicional for descoberto usando um agente do Console, você também precisará associar o agente ao projeto ao qual o recurso está associado. Caso contrário, o agente e seu recurso associado não poderão ser acessados na página **Sistemas** por membros que não tenham a função *Administrador da organização*.

Você pode criar uma associação na página **Agentes** no Console IAM:

- Associar um agente do Console a um projeto

  Quando você associa um agente do Console a um projeto, esse agente fica acessível na página **Sistemas** ao visualizar o projeto.

- Associar um agente do Console a uma pasta

  Associar um agente do Console a uma pasta não torna esse agente automaticamente acessível a todos os projetos na pasta. Os membros da organização não podem acessar um agente do Console de um projeto até que você associe o agente a esse projeto específico.

  Um *administrador da organização* pode associar um agente do Console a uma pasta para que o

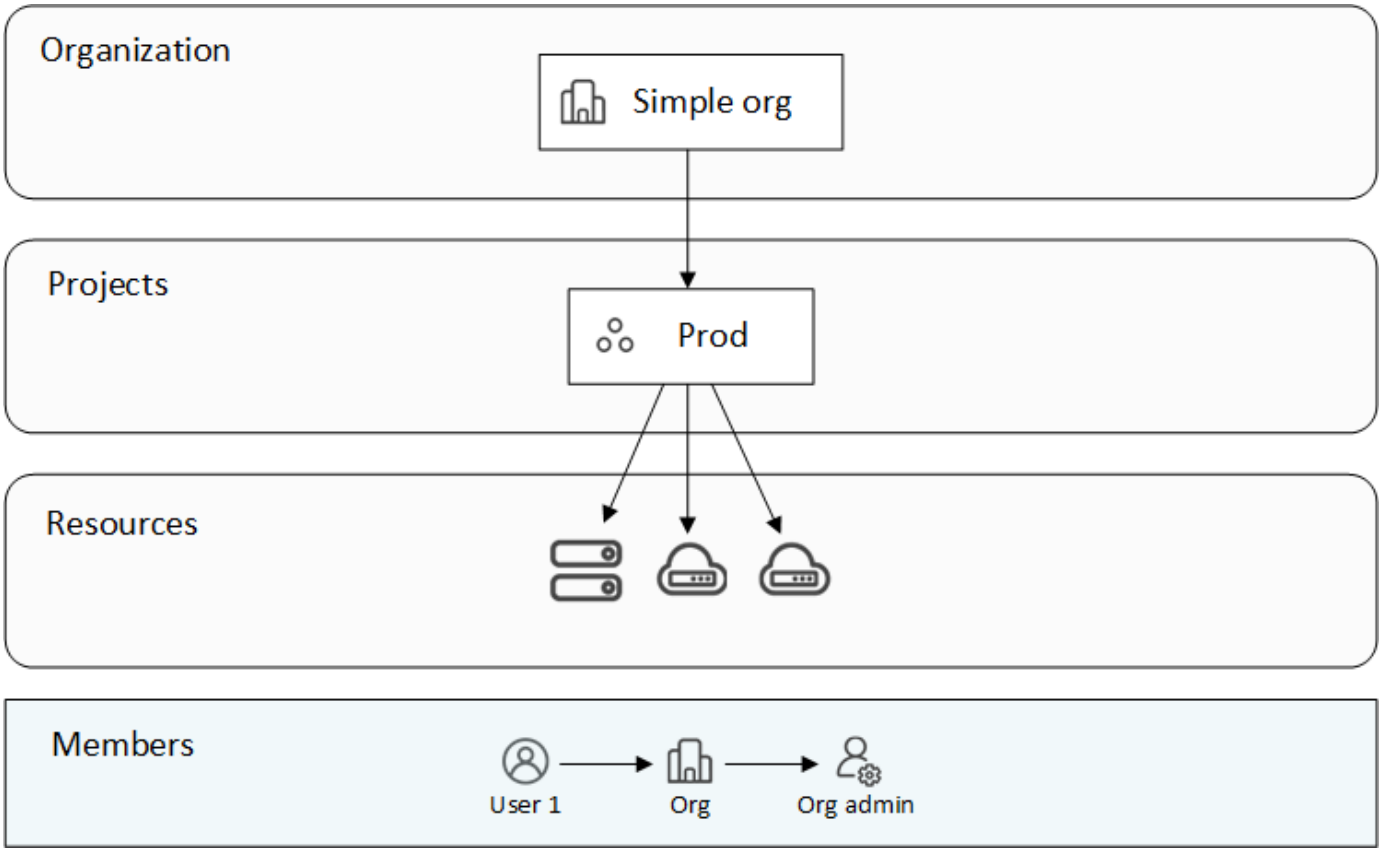
administrador da pasta ou do projeto possa tomar a decisão de associar esse agente aos projetos apropriados que residem na pasta.

Exemplos de IAM

Esses exemplos demonstram como você pode configurar sua organização.

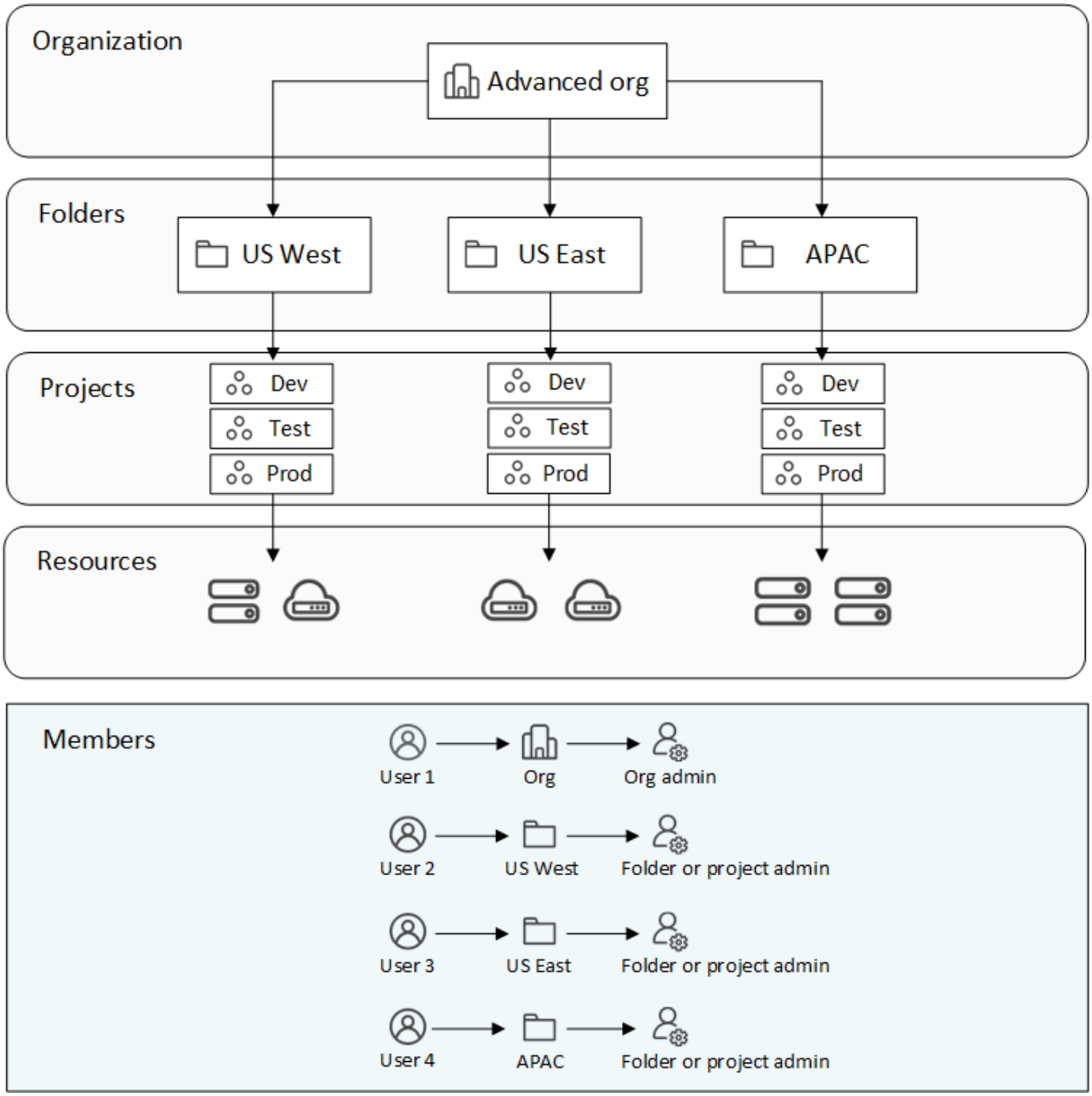
Organização simples

O diagrama a seguir mostra um exemplo simples de uma organização que usa o projeto padrão e nenhuma pasta. Um único membro gerencia toda a organização.



Organização avançada

O diagrama a seguir mostra uma organização que usa pastas para organizar os projetos de cada localização geográfica da empresa. Cada projeto tem seu próprio conjunto de recursos associados. Os membros incluem um administrador da organização e um administrador para cada pasta na organização.



O que você pode fazer com o IAM

Os exemplos a seguir descrevem como você pode usar o IAM para gerenciar sua organização do Console:

- Atribua funções específicas a membros específicos para que eles possam concluir apenas as tarefas necessárias.
- Modifique as permissões dos membros porque eles mudaram de departamento ou porque têm responsabilidades adicionais.
- Remover um usuário que saiu da empresa.
- Adicione pastas ou projetos à sua hierarquia porque uma nova unidade de negócios adicionou armazenamento NetApp .

- Associe um recurso a outro projeto porque esse recurso tem capacidade que outra equipe pode utilizar.
- Veja os recursos que um membro pode acessar.
- Veja os membros e recursos associados a um projeto específico.

Para onde ir a seguir

- "Introdução ao IAM no NetApp Console"
- "Organize seus recursos no NetApp Console com pastas e projetos"
- "Gerenciar membros do NetApp Console e suas permissões"
- "Gerencie a hierarquia de recursos na sua organização do NetApp Console"
- "Associar agentes a pastas e projetos"
- "Alternar entre projetos e organizações do NetApp Console"
- "Renomeie sua organização do NetApp Console"
- "Monitorar ou auditar a atividade do IAM"
- "Funções de acesso ao NetApp Console"
- "Saiba mais sobre a API para NetApp Console IAM"

Comece a usar identidade e acesso no NetApp Console

Ao se inscrever no NetApp Console, você será solicitado a criar uma nova organização. A organização inclui um membro (um administrador da organização) e um projeto padrão. Para configurar o gerenciamento de identidade e acesso (IAM) para atender às suas necessidades comerciais, você precisará personalizar a hierarquia da sua organização, adicionar membros adicionais, adicionar ou descobrir recursos e associar esses recursos à sua hierarquia.

Você deve ter permissões de **Administrador da organização** para administrar a identidade e o acesso de toda a sua organização. Se você tiver permissões de **Administrador de pasta ou projeto**, você só poderá administrar as pastas e projetos para os quais você tem permissões.

Siga estas etapas para configurar uma nova organização. A ordem pode variar de acordo com as necessidades da sua organização.

Edite o projeto padrão ou adicione-o à hierarquia da sua organização

Use o projeto padrão ou crie projetos e pastas adicionais que correspondam à hierarquia da sua empresa.

"Aprenda a organizar seus recursos com pastas e projetos" .

Associe membros à sua organização

Vincule contas de usuários à sua organização e atribua permissões. Você também tem a opção de adicionar contas de serviço à sua organização.

"Aprenda a gerenciar membros e suas permissões" .

3 Adicionar ou descobrir recursos

Adicione ou descubra recursos (sistemas) ao Console. Os membros da organização gerenciam sistemas de dentro de um projeto.

Aprenda como criar ou descobrir recursos:

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "Sistemas da série E"
- "Clusters ONTAP locais"
- "StorageGRID"

4 Associar recursos a projetos adicionais

Adicionar ou descobrir um sistema no Console associa automaticamente o recurso ao projeto selecionado no momento. Para disponibilizar esse recurso para outro projeto na sua organização, associe-o ao respectivo projeto. Se um agente do Console for usado para gerenciar o recurso, associe o agente do Console ao respectivo projeto.

- "Aprenda a gerenciar a hierarquia de recursos da sua organização" .
- "Aprenda como associar um agente do Console a uma pasta ou projeto" .

Informações relacionadas

- "Saiba mais sobre gerenciamento de identidade e acesso no NetApp Console"
- "Saiba mais sobre a API para identidade e acesso"

Organize seus recursos do NetApp Console com pastas e projetos

No NetApp Console, você organiza seus recursos do NetApp usando projetos e pastas. Um *projeto* representa um espaço de trabalho no Console que os membros da organização acessam para gerenciar *recursos* (por exemplo, um sistema Cloud Volumes ONTAP). Uma *pasta* agrupa projetos relacionados. Depois de organizar seus recursos em pastas e projetos, você pode conceder acesso granular aos recursos fornecendo aos membros da organização permissões para pastas e projetos específicos.

Adicionar uma pasta ou projeto

Quando você cria sua organização, ela inclui um único projeto. Adicione projetos para gerenciar recursos e pastas para agrupar projetos relacionados.

A hierarquia de recursos da sua organização pode ter até sete níveis, com pastas aninhadas em seis níveis de profundidade e projetos no sétimo.

Passos

1. Selecione **Administração > Identidade e acesso**.

2. Selecione **Organização**.
3. Na página **Organização**, selecione **Adicionar pasta ou projeto**.
4. Selecione **Pasta** ou **Projeto**.
5. Forneça detalhes sobre a pasta ou projeto:
   - **Nome e local**: Insira um nome e escolha um local na hierarquia para a pasta ou projeto. Uma pasta ou projeto pode estar diretamente abaixo da organização ou dentro de uma pasta.
   - **Recursos**: Selecione os recursos que você deseja associar a esta pasta ou projeto.

     Você pode selecionar recursos associados à pasta pai ou ao projeto.

     "Aprenda quando associar um recurso a uma pasta" .
   - **Acesso**: visualize os membros que terão acesso à pasta ou projeto com base nas permissões existentes já definidas na sua hierarquia de recursos.

     Selecione **Adicionar um membro** para atribuir acesso e uma função a membros adicionais. Uma função define as permissões que os membros têm para a pasta ou projeto.

   "Saiba mais sobre funções de acesso" .
6. Selecione **Adicionar**.

Renomear uma pasta ou projeto

Se necessário, você pode alterar o nome de suas pastas e projetos.

Passos

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, selecione ••• e então selecione **Editar pasta** ou **Editar projeto**.
2. Na página **Editar**, insira um novo nome e selecione **Aplicar**.

Excluir uma pasta ou projeto

Exclua pastas e projetos que você não precisa mais.

Antes de começar

- Certifique-se de que a pasta ou projeto não tenha recursos associados. Aprenda a desassociar recursos .
- Certifique-se de que a pasta ou projeto não tenha recursos associados.

Passos

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, selecione ••• e então selecione **Excluir**.
2. Confirme que deseja excluir a pasta ou o projeto.

Visualizar os recursos associados a uma pasta ou projeto

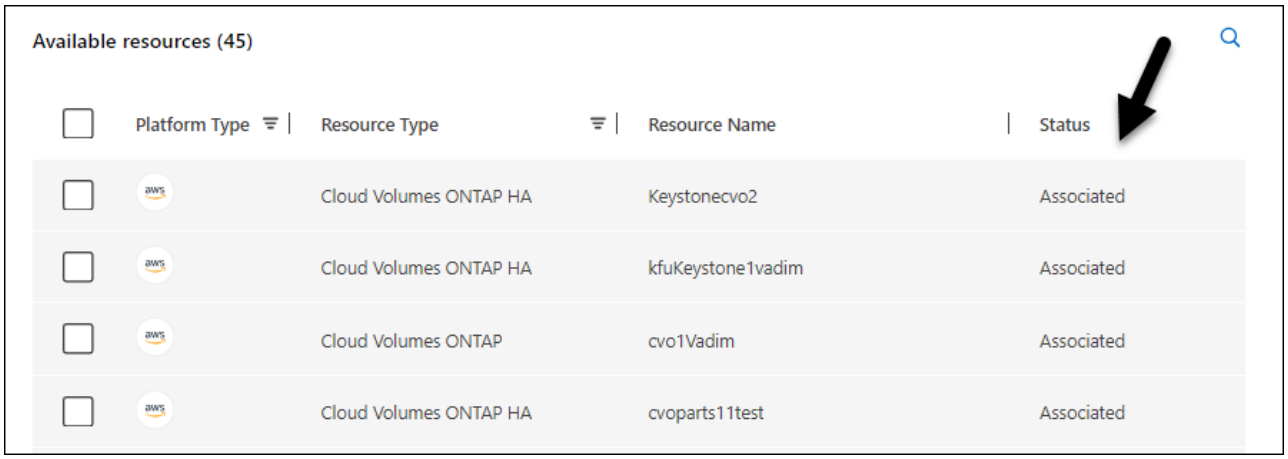
Veja quais recursos e membros estão associados a uma pasta ou projeto.

Passos

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, selecione ••• e então selecione

Editar pasta ou **Editar projeto**.

2. Na página **Editar**, você pode visualizar detalhes sobre a pasta ou projeto selecionado expandindo as seções **Recursos** ou **Acesso**.
   - Selecione **Recursos** para visualizar os recursos associados. Na tabela, a coluna **Status** identifica os recursos associados à pasta ou ao projeto.



Modificar os recursos associados a uma pasta ou projeto

Membros com permissões para uma pasta ou projeto podem acessar seus recursos associados.

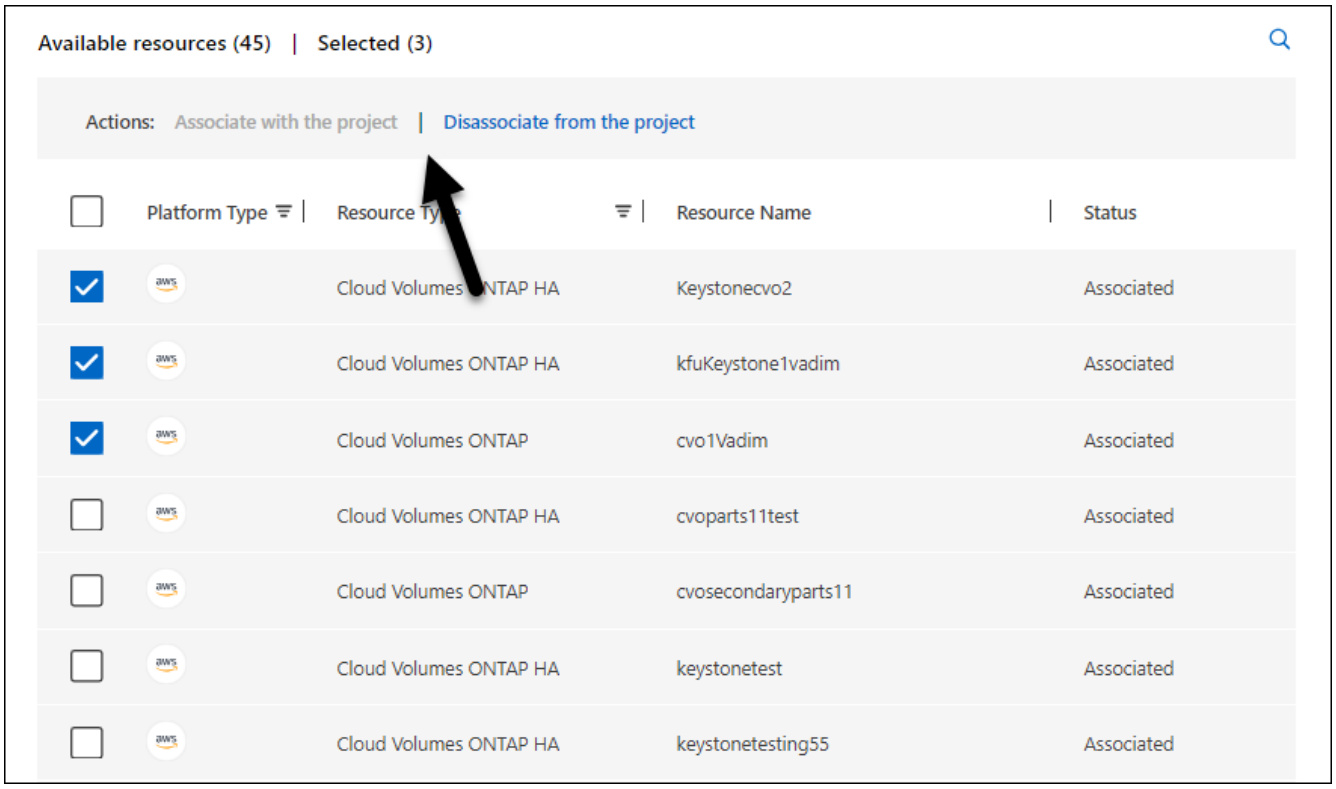
Antes de começar

"Aprenda quando associar um recurso a uma pasta" .

Passos

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, selecione ••• e então selecione **Editar pasta** ou **Editar projeto**.
2. Na página **Editar**, selecione **Recursos**.

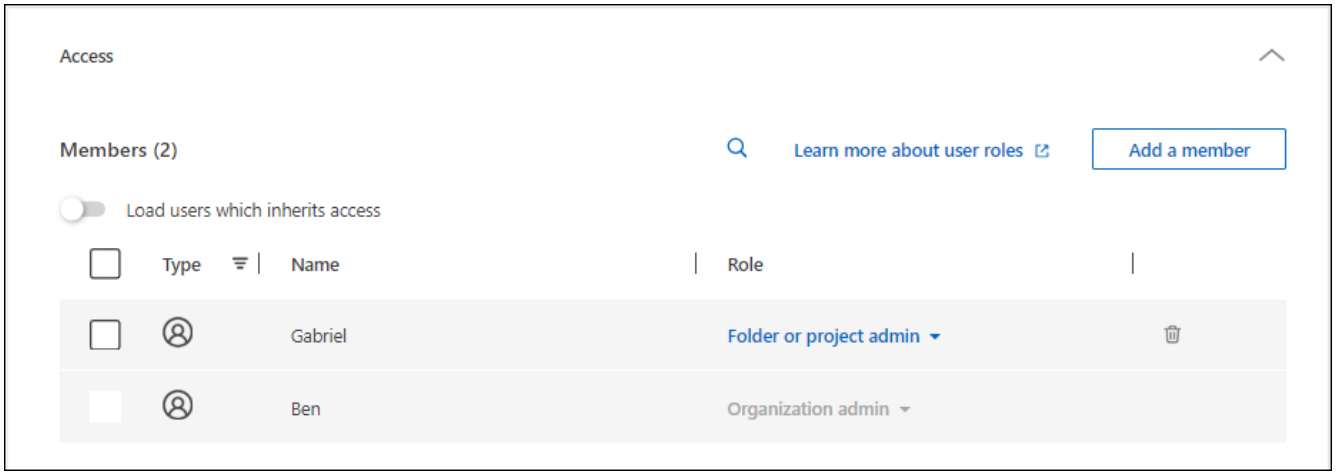
   Na tabela, a coluna **Status** identifica os recursos associados à pasta ou ao projeto.
3. Selecione os recursos que você gostaria de associar ou desassociar.
4. Dependendo dos recursos selecionados, selecione **Associar ao projeto** ou **Desassociar do projeto**.



5. Selecione **Aplicar**

Ver membros associados a uma pasta ou projeto

- Selecione **Acesso** para visualizar os membros que têm acesso à pasta ou ao projeto.



Modificar o acesso de membros a uma pasta ou projeto

Modifique o acesso dos membros para garantir que os membros certos possam acessar os recursos associados.

O acesso de membro fornecido em um nível hierárquico mais alto não pode ser alterado em níveis mais baixos. Atualize as permissões dos membros no nível hierárquico superior para alterar o acesso. Alternativamente, você pode"gerenciar permissões na página de membros" .

"Saiba mais sobre herança de funções" .

Passos

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, selecione ••• e então selecione **Editar pasta** ou **Editar projeto**.
2. Na página **Editar**, selecione **Acesso** para visualizar a lista de membros que têm acesso à pasta ou projeto selecionado.
3. Modificar acesso de membro:
   - **Adicionar um membro**: Selecione o membro que você gostaria de adicionar à pasta ou projeto e atribua uma função a ele.
   - **Alterar a função de um membro**: Para qualquer membro com uma função diferente de Administrador da Organização, selecione a função existente e escolha uma nova função.
   - **Remover acesso de membro**: Para membros que têm uma função definida na pasta ou projeto que você está visualizando, você pode remover o acesso deles.
4. Selecione **Aplicar**.

Informações relacionadas

- "Saiba mais sobre identidade e acesso no NetApp Console"
- "Comece com identidade e acesso"
- "Saiba mais sobre a API de identidade e acesso"

Adicionar membros e contas de serviço ao NetApp Console

No Console, você pode adicionar usuários e contas de serviço à sua organização e atribuir a eles uma ou mais funções na hierarquia de recursos. Uma *função* contém um conjunto de permissões que permite que um membro (usuário ou conta de serviço) execute ações específicas em um nível específico da hierarquia de recursos.

Você precisa de uma das seguintes funções para gerenciar usuários e permissões:

- Administrador da organização

  Usuários com esta função podem gerenciar todos os membros

- Administrador de pasta ou projeto

  Usuários com esta função podem gerenciar apenas membros de uma pasta ou projeto designado

  O administrador da pasta ou do projeto pode visualizar todos os membros na página **Membros**, mas gerenciar permissões apenas para pastas e projetos aos quais eles têm acesso. "Saiba mais sobre as ações que um *administrador de pasta ou projeto* pode concluir" .

Adicionar membros à sua organização

Você pode adicionar dois tipos de membros à sua organização: uma conta de usuário e uma conta de serviço. Os aplicativos usam contas de serviço para executar tarefas de API sem intervenção humana. Uma pessoa normalmente usa uma conta de usuário para fazer login e gerenciar recursos.

Os usuários devem se inscrever no NetApp Console antes que você possa adicioná-los a uma organização ou atribuir-lhes uma função. Você cria contas de serviço diretamente do Console.

Para gerenciar usuários e suas permissões, você deve ter a função **Administrador da organização** ou a função **Administrador de pasta ou projeto**. Lembre-se de que usuários com a função **Administrador de pasta ou projeto** só podem gerenciar membros da pasta ou dos projetos para os quais têm permissões de administrador.

Adicionar uma conta de usuário

Embora os usuários se inscrevam no NetApp Console por conta própria, eles precisam ser adicionados explicitamente a uma organização ou a pastas ou projetos específicos para acessar recursos no Console.

Passos

1. Direcionar o usuário para visitar "Console NetApp" para se inscrever.

   Depois que os usuários se inscrevem, eles preenchem a página **Inscrever-se**, verificam seus e-mails e efetuam login. Se o Console solicitar que os usuários criem uma organização, eles a fecham e notificam você sobre a criação da conta. Você pode então adicionar o usuário à sua organização existente.

   "Saiba como se inscrever no NetApp Console" .

2. Selecione **Administração > Identidade e acesso**.
3. Selecione **Membros**.
4. Selecione **Adicionar um membro**.
5. Para **Tipo de membro**, mantenha **Usuário** selecionado.
6. Em **E-mail do usuário**, insira o endereço de e-mail do usuário associado ao login que ele criou.
7. Use a seção **Selecione uma organização, pasta ou projeto** para escolher o nível da hierarquia de recursos para o qual o membro deve ter permissões.

   Observe o seguinte:

   - Você só pode selecionar pastas e projetos para os quais você tem permissão.
   - Selecionar uma organização ou pasta concede ao membro permissões para todo o seu conteúdo.
   - Você só pode atribuir a função **Administrador da organização** no nível da organização.
8. **Selecione uma categoria** e depois selecione uma **Função** que forneça ao membro permissões para os recursos associados à organização, pasta ou projeto que você selecionou.

   "Saiba mais sobre funções de acesso" .

9. Opcional: selecione uma função ou projeto adicional. Se você quiser fornecer acesso a pastas ou projetos adicionais dentro da sua organização ou conceder ao usuário funções adicionais na área selecionada, selecione **Adicionar função**, especifique outra pasta ou projeto ou uma categoria de função diferente e escolha uma função.
10. Selecione **Adicionar**.

    O Console envia ao usuário um e-mail com instruções.

Adicionar uma conta de serviço

Você pode automatizar tarefas e integrar com segurança as APIs do Console com contas de serviço. Ao criar uma conta de serviço, escolha entre dois métodos de autenticação: usando um ID de cliente e segredo ou usando autenticação JWT (JSON Web Token). O ID do cliente e o método secreto são adequados para

configurações simples, enquanto a autenticação JWT oferece maior segurança para ambientes automatizados ou nativos da nuvem. Escolha a opção que melhor se adapta às suas necessidades de segurança e à forma como você planeja usar o Console.

Se você quiser usar a autenticação JWT, tenha sua chave pública ou certificado pronto para uso.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.
3. Selecione **Adicionar um membro**.
4. Para **Tipo de membro**, selecione **Conta de serviço**.
5. Insira um nome para a conta de serviço.
6. Se você quiser usar a autenticação JWT, selecione **Usar autenticação JWT de chave privada** e carregue sua chave RSA pública ou certificado. Pule esta etapa se quiser usar um ID de cliente e um segredo.

   Seu certificado X.509. Deve estar no formato PEM, CRT ou CER.

7. Use a seção **Selecione uma organização, pasta ou projeto** para escolher o nível da hierarquia de recursos para o qual o membro deve ter permissões.

   Observe o seguinte:

   - Você só pode selecionar pastas e projetos para os quais você tem permissão.
   - Selecionar uma organização ou pasta concede ao membro permissões para todo o seu conteúdo.
   - Você só pode atribuir a função **Administrador da organização** no nível da organização.

8. Selecione uma **Categoria** e depois selecione uma **Função** que forneça ao membro permissões para os recursos associados à organização, pasta ou projeto que você selecionou.

   "Saiba mais sobre funções de acesso" .

9. Opcional: selecione uma função ou projeto adicional. Se você quiser fornecer acesso a pastas ou projetos adicionais dentro da sua organização ou conceder ao usuário funções adicionais na área selecionada, selecione **Adicionar função**, especifique outra pasta ou projeto ou uma categoria de função diferente e escolha uma função.
10. Se você não escolheu usar a autenticação JWT, baixe ou copie o ID do cliente e o segredo do cliente. + O Console mostra o segredo do cliente apenas uma vez. Copie-o com segurança; você pode recriá-lo mais tarde, se necessário.
11. Se você escolher a autenticação JWT, baixe ou copie o ID do cliente e o público JWT. Essas informações são exibidas apenas uma vez e não podem ser recuperadas posteriormente.
12. Selecione **Fechar**.

Ver membros da organização

Para entender quais recursos e permissões estão disponíveis para um membro, você pode visualizar as funções atribuídas ao membro em diferentes níveis da hierarquia de recursos da sua organização."Aprenda a usar funções para controlar o acesso aos recursos do Console."

Você pode visualizar contas de usuário e contas de serviço na página **Membros**.

Você também pode visualizar todos os membros associados a uma pasta ou projeto específico. "Saber mais" .

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.

   A tabela **Membros** lista os membros da sua organização.

3. Na página **Membros**, navegue até um membro na tabela, selecione ••• e então selecione **Ver detalhes**.

Remover um membro da sua organização

Pode ser necessário remover um membro da sua organização, por exemplo, se ele sair da empresa.

O sistema remove as permissões do membro, mas mantém suas contas do Console e do Site de Suporte NetApp .

Passos

1. Na página **Membros**, navegue até um membro na tabela, selecione ••• então selecione **Excluir usuário**.
2. Confirme que você deseja remover o membro da sua organização.

Recriar as credenciais para uma conta de serviço

Crie novas credenciais caso você as perca ou precise atualizá-las.

Ao recriar as credenciais, você exclui as credenciais existentes da conta de serviço e cria novas. Você não pode usar as credenciais anteriores.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.
3. Na tabela **Membros**, navegue até uma conta de serviço, selecione ••• e então selecione **Recriar segredos**.
4. Selecione **Recriar**.
5. Baixe ou copie o ID do cliente e o segredo do cliente. + O segredo do cliente é exibido apenas uma vez. Copie ou baixe e armazene com segurança.

Gerenciar a autenticação multifator (MFA) de um usuário

Se um usuário perder o acesso ao seu dispositivo MFA, você poderá remover ou desabilitar a configuração do MFA.

Os usuários devem reconfigurar o MFA no login após a remoção. Se o usuário tiver perdido o acesso ao seu dispositivo MFA apenas temporariamente, ele poderá usar o código de recuperação que salvou quando configurou o MFA para fazer login.

Caso não tenham o código de recuperação, desative temporariamente o MFA para permitir o login. Quando você desabilita o MFA para um usuário, ele é desabilitado por apenas oito horas e depois reabilitado automaticamente. O usuário tem direito a apenas um login durante esse período, sem MFA. Após as oito horas, o usuário deve usar o MFA para efetuar login.

Para gerenciar a autenticação multifator de um usuário, você deve ter um endereço de e-mail no mesmo domínio que o usuário afetado.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.

   A tabela **Membros** lista os membros da sua organização.

3. Na página **Membros**, navegue até um membro na tabela, selecione ••• e então selecione **Gerenciar autenticação multifator**.
4. Escolha se deseja remover ou desabilitar a configuração MFA do usuário.

Use funções para gerenciar o acesso do usuário aos recursos do NetApp Console

No Console, você pode atribuir funções aos usuários com base no que eles precisam fazer e onde.

Usuários com a função **Administrador da organização** ou **Administrador de pasta ou projeto** têm a responsabilidade de atribuir funções a outros usuários. Você pode atribuir funções de acesso com base em um projeto ou pasta. Por exemplo, você pode atribuir a um usuário a função de administrador de proteção contra ransomware para um projeto e a função de administrador do SnapCenter para um projeto diferente. Como alternativa, se um usuário precisar da função de administrador de classificação para todos os projetos dentro de uma pasta específica, você poderá atribuir essa função a ele no nível da pasta.

Use funções de acesso para atribuir acesso a recursos de armazenamento com base nas tarefas específicas que os usuários precisam executar. Por exemplo, se um usuário precisar interagir com serviços de proteção contra ransomware, ele deverá receber uma função de acesso que inclua permissões de visualização ou administrativas para o serviço de proteção contra ransomware do projeto para o qual a função de acesso foi concedida.

Atribua funções aos usuários com base na sua estratégia de IAM para maior segurança. As funções do IAM garantem que os usuários tenham apenas o acesso necessário.

Lembre-se de que você não pode conceder acesso direto aos recursos. Atribua recursos aos projetos primeiro. Considere configurar sua hierarquia de recursos antes de atribuir acesso aos usuários."Aprenda a organizar seus recursos com pastas e projetos."

Exibir funções atribuídas a um membro

Ao adicionar um membro à sua organização, você será solicitado a atribuir uma função a ele. Você pode permitir que os membros verifiquem quais funções estão atribuídas a eles no momento.

Se você tiver a função de *Administrador de pasta ou projeto*, a página exibirá todos os membros da organização. No entanto, você só pode visualizar e gerenciar permissões de membros para as pastas e projetos para os quais você tem permissões. "Saiba mais sobre as ações que um *administrador de pasta ou projeto* pode concluir" .

1. Na página **Membros**, navegue até um membro na tabela, selecione ••• e então selecione **Ver detalhes**.
2. Na tabela, expanda a linha respectiva da organização, pasta ou projeto onde você deseja visualizar a função atribuída ao membro e selecione **Exibir** na coluna **Função**.

Adicionar uma função de acesso a um membro

Normalmente, você atribui uma função ao adicionar um membro à sua organização, mas pode atualizá-la a qualquer momento removendo ou adicionando funções.

Você pode atribuir a um usuário uma função de acesso para sua organização, pasta ou projeto.

Os membros podem ter várias funções dentro do mesmo projeto e em projetos diferentes. Por exemplo, organizações menores podem atribuir todas as funções de acesso disponíveis ao mesmo usuário, enquanto organizações maiores podem ter usuários executando tarefas mais especializadas. Como alternativa, você também pode atribuir a um usuário a função de administrador de proteção contra ransomware para uma organização. Nesse exemplo, o usuário seria capaz de executar tarefas de proteção contra ransomware em todos os projetos da sua organização.

Sua estratégia de função de acesso deve estar alinhada à maneira como você organizou seus recursos do NetApp .

> Um membro que recebeu a função de administrador da organização não pode receber nenhuma função adicional. Eles já têm permissões em toda a organização. Um membro com a função de pasta ou projeto não pode receber nenhuma outra função dentro da pasta ou projeto em que já tenha essa função. Ambas as funções fornecem acesso a todos os serviços dentro do escopo que lhes é atribuído.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione o menu de ações ••• ao lado do membro ao qual você deseja atribuir uma função e selecione **Adicionar uma função**.
3. Para adicionar uma função, conclua as etapas na caixa de diálogo:
   - **Selecione uma organização, pasta ou projeto**: Escolha o nível da hierarquia de recursos para o qual o membro deve ter permissões.

     Se você selecionar a organização ou uma pasta, o membro terá permissões para tudo o que reside na organização ou pasta.

   - **Selecione uma categoria**: Escolha uma categoria de função. "Saiba mais sobre funções de acesso" .
   - Selecione uma **Função**: Escolha uma função que forneça ao membro permissões para os recursos associados à organização, pasta ou projeto que você selecionou.
   - **Adicionar função**: se você quiser fornecer acesso a pastas ou projetos adicionais dentro da sua organização, selecione **Adicionar função**, especifique outra pasta, projeto ou categoria de função e, em seguida, selecione uma categoria de função e uma função correspondente.
4. Selecione **Adicionar novas funções**.

Alterar a função atribuída a um membro

Você pode alterar as funções atribuídas a um membro caso precise ajustar o acesso de um usuário.

> Os usuários devem ter pelo menos uma função atribuída a eles. Não é possível remover todas as funções de um usuário. Se precisar remover todas as funções, você deverá excluir o usuário da sua organização.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Na página **Membros**, navegue até um membro na tabela, selecione ••• e então selecione **Ver detalhes**.
3. Na tabela, expanda a linha respectiva da organização, pasta ou projeto onde você deseja alterar a função atribuída ao membro e selecione **Exibir** na coluna **Função** para visualizar as funções atribuídas a este membro.
4. Você pode alterar uma função existente para um membro ou remover uma função.
   a. Para alterar a função de um membro, selecione **Alterar** ao lado da função que deseja alterar. Você só pode alterar uma função para uma função dentro da mesma categoria de função. Por exemplo, você pode mudar de uma função de serviço de dados para outra. Confirme a alteração.
   b. Para cancelar a atribuição da função de um membro, selecione 🗑 ao lado da função para remover a atribuição da respectiva função ao membro. Você será solicitado a confirmar a remoção.

Gerencie a hierarquia de recursos na sua organização do NetApp Console

Ao associar um membro à sua organização, você fornece permissões no nível da organização, pasta ou projeto. Para garantir que esses membros tenham permissões para acessar os recursos corretos, você precisará gerenciar a hierarquia de recursos da sua organização associando recursos a projetos e pastas específicos. Um *recurso* é um sistema de armazenamento ou agente do Console que o Console já gerencia ou do qual tem conhecimento.

Visualize os recursos em sua organização

Você pode visualizar recursos descobertos e não descobertos associados à sua organização. Recursos não descobertos são recursos de armazenamento identificados, mas ainda não adicionados ao Console.

ⓘ OBSERVAÇÃO: a página Recursos exclui os recursos do Amazon FSx for NetApp ONTAP porque os usuários não podem associá-los a uma função. Visualize-os na página Sistemas ou em Cargas de trabalho.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Recursos**.
3. Selecione **Pesquisa e filtragem avançadas**.
4. Use qualquer uma das opções disponíveis para encontrar o recurso que você está procurando:
   - **Pesquisar por nome do recurso**: Insira uma sequência de texto e selecione **Adicionar**.
   - **Plataforma**: Selecione uma ou mais plataformas, como Amazon Web Services.
   - **Recursos**: Selecione um ou mais recursos, como Cloud Volumes ONTAP.
   - **Organização, pasta ou projeto**: Selecione a organização inteira, uma pasta específica ou um projeto específico.
5. Selecione **Pesquisar**.

Associar um recurso a pastas e projetos

Associe um recurso a uma pasta ou projeto para torná-lo disponível.

Antes de começar

Você deve entender como funciona a associação de recursos. "Aprenda sobre recursos, incluindo quando associar um recurso a uma pasta" .

Passos

1. Na página **Recursos**, navegue até um recurso na tabela, selecione ••• e então selecione **Associar a pastas ou projetos**.
2. Selecione uma pasta ou projeto e então selecione **Aceitar**.
3. Para associar uma pasta ou projeto adicional, selecione **Adicionar pasta ou projeto** e depois selecione a pasta ou projeto.

   Observe que você só pode selecionar pastas e projetos para os quais você tem permissões de administrador.

4. Selecione **Associar recursos**.
   - Se você associou o recurso a projetos, os membros que têm permissões para esses projetos agora poderão acessar o recurso no Console.
   - Se você associou o recurso a uma pasta, um *administrador de pasta ou projeto* agora pode acessar o recurso e associá-lo a um projeto dentro da pasta. "Aprenda a associar um recurso a uma pasta" .

Depois que você terminar

Se você descobrir um recurso usando um agente do Console, associe o agente do Console ao projeto para conceder acesso. Caso contrário, o agente do Console e seu recurso associado não poderão ser acessados por membros sem a função *Administrador da organização*.

"Aprenda como associar um agente do Console a uma pasta ou projeto" .

Visualizar as pastas e projetos associados a um recurso

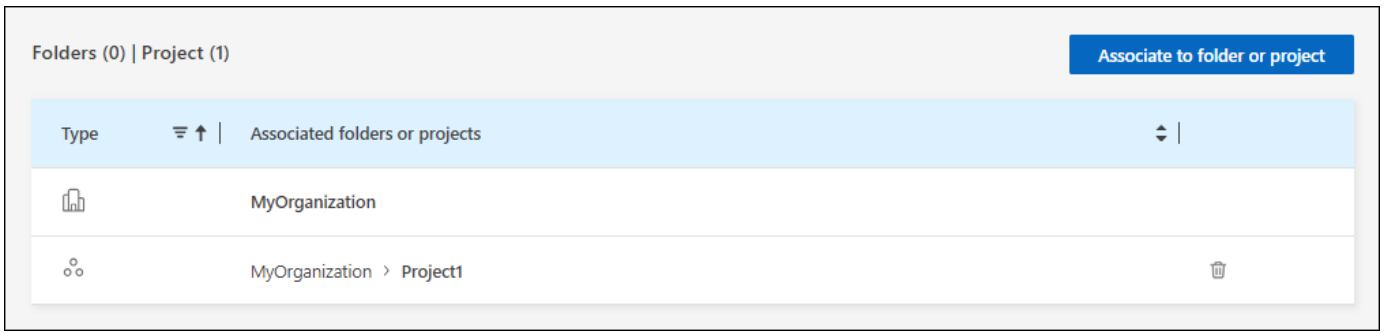
Você pode visualizar as pastas e os projetos associados a um recurso específico.

Se você precisar descobrir quais membros da organização têm acesso ao recurso, você pode"visualizar os membros que têm acesso às pastas e projetos associados ao recurso" .

Passos

1. Na página **Recursos**, navegue até um recurso na tabela, selecione ••• e então selecione **Ver detalhes**.

O exemplo a seguir mostra um recurso associado a um projeto.



Se você precisar determinar quais membros da organização têm acesso ao recurso, você pode"visualizar os membros que têm acesso às pastas e projetos associados ao recurso" .

Remover um recurso de uma pasta ou projeto

Para remover um recurso de uma pasta ou projeto, você precisa remover a associação entre a pasta ou projeto e o recurso. Quando você remove a associação, isso impede que os membros gerenciem o recurso na pasta ou no projeto.

Para remover um recurso descoberto de toda a organização, remova o sistema da página **Sistemas**.

Passos

1. Na página **Recursos**, navegue até um recurso na tabela, selecione ••• e então selecione **Ver detalhes**.
2. Para a pasta ou projeto para o qual você deseja remover o recurso, selecione 🗑
3. Confirme que deseja remover a associação selecionando **Excluir**.

Informações relacionadas

- "Saiba mais sobre identidade e acesso no NetApp Console"
- "Comece a usar identidade e acesso no NetApp Console"
- "Saiba mais sobre a API para identidade e acesso"

Associar um agente do Console a outras pastas e projetos

Quando um *Administrador da organização* cria um agente do Console, o agente do Console é automaticamente associado ao projeto selecionado na organização. Embora alguém com a função *Administrador da organização* possa acessar esse agente do Console de qualquer lugar da organização. Outros membros da sua organização só podem acessar esse agente do Console a partir do projeto no qual ele foi criado, a menos que você associe esse agente do Console a outros projetos.

Antes de começar

Revise como funciona a associação do agente do Console. "Saiba mais sobre como usar o agente do Console com Identidade e Acesso" .

Sobre esta tarefa

Um *administrador de pasta ou projeto* pode visualizar todos os agentes do Console na página **Agente**, mas só pode associar agentes do Console a pastas e projetos para os quais ele tem permissão. "Saiba mais sobre as ações que um *administrador de pasta ou projeto* pode concluir" .

Passos

1. Selecione **Administração > Identidade e acesso** > **Agentes**.
2. Na tabela, encontre o agente do Console que você deseja associar.

   Use a pesquisa acima da tabela para encontrar um agente específico do Console ou filtre a tabela por hierarquia de recursos.

3. Para visualizar as pastas e projetos vinculados ao agente do Console, selecione ••• e então selecione **Ver detalhes**.

   A página exibe detalhes sobre as pastas e projetos associados ao agente do Console.

4. Selecione **Associar à pasta ou projeto**.
5. Selecione uma pasta ou projeto e então selecione **Aceitar**.
6. Para associar o agente do Console a uma pasta ou projeto adicional, selecione **Adicionar uma pasta ou projeto** e, em seguida, selecione a pasta ou projeto.
7. Selecione **Agente Associado**.

Depois que você terminar

Associe os recursos do agente do Console às mesmas pastas e projetos da página **Recursos**.

"Aprenda a associar um recurso a pastas e projetos" .

Informações relacionadas

- "Saiba mais sobre os agentes do NetApp Console"
- "Saiba mais sobre o gerenciamento de identidade e acesso do NetApp Console"
- "Comece com identidade e acesso"
- "Saiba mais sobre a API para gerenciamento de identidade e acesso"

Alternar entre organizações, projetos e agentes do Console

Você pode pertencer a várias organizações do Console ou ter permissões para acessar vários projetos ou agentes dentro de uma organização. Quando necessário, você pode alternar facilmente entre organizações, projetos e agentes do Console para acessar os recursos associados a essa organização, projeto ou agente.

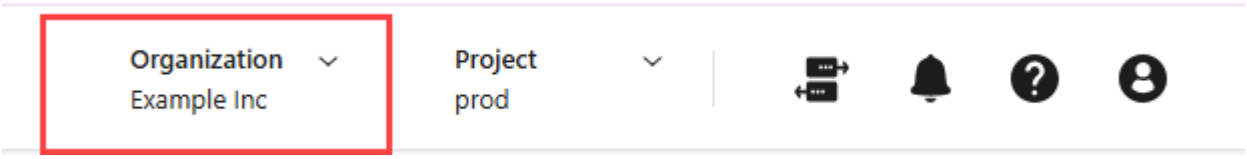
Você pode pertencer a várias organizações se outra organização o convidar para participar ou se você mesmo criar uma. Você pode criar uma organização adicional usando a API. "Aprenda a criar uma nova organização"

Alternar entre organizações

Se você for membro de várias organizações, poderá alternar entre elas a qualquer momento.

Passos

1. No cabeçalho superior do Console, selecione **Organização**.



2. Se você tiver alguma organização parceira, selecione a aba **Parceria** para ver as organizações parceiras disponíveis.

+ A aba **Parceria** não será exibida se você não tiver nenhuma organização parceira.

1. Selecione outra organização e depois selecione **Alternar**.

+ Se você tiver alguma organização parceira, selecione a aba **Parceria** para ver as organizações parceiras disponíveis.

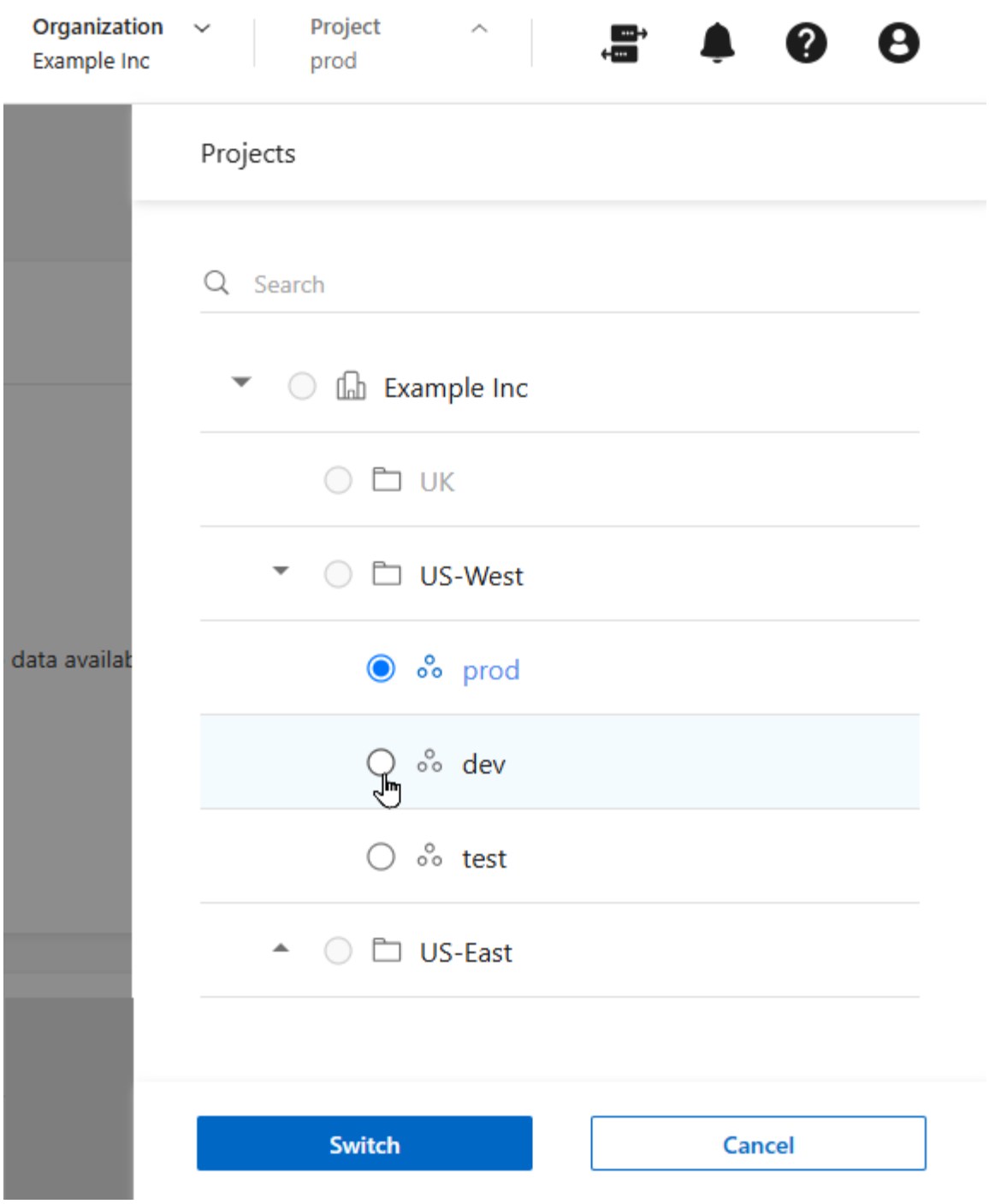
Alternar entre projetos

Se sua organização incluir vários projetos e você tiver acesso a eles, poderá alternar entre eles a qualquer momento.

> Você não pode alternar para outro projeto enquanto estiver visualizando qualquer uma das páginas de **Identidade e acesso**.

Passos

1. No cabeçalho superior do Console, selecione **Projeto**.
2. Navegue pelas pastas e projetos em sua organização, selecione o projeto desejado e, em seguida, selecione **Alternar**.



Alternar entre agentes do Console

Se você tiver vários agentes do Console, poderá alternar entre eles para ver os sistemas associados a um agente específico.

Passos

1. No cabeçalho superior do Console, selecione o ícone Agente.
2. Selecione outro agente e depois selecione **Trocar**.

Informações relacionadas

"Associar agentes a pastas e projetos" .

Informações relacionadas

- "Saiba mais sobre identidade e acesso no NetApp Console"
- "Comece com identidade e acesso"
- "Saiba mais sobre a API para identidade e acesso"

IDs de organização e projeto

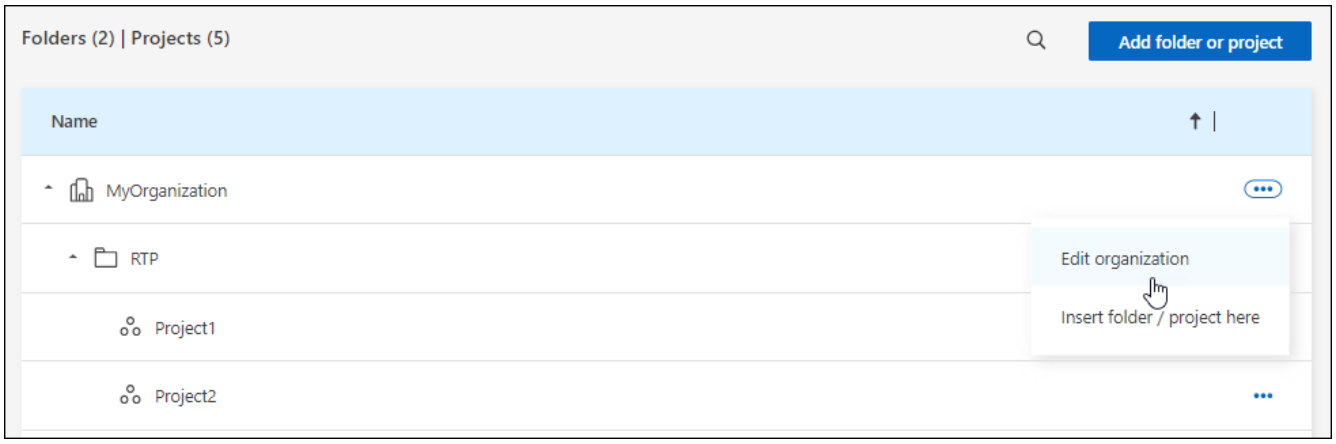
Sua organização do NetApp Console tem um nome e um ID. Você pode escolher um nome para sua organização para ajudar a identificá-la. Também pode ser necessário recuperar o ID da organização para determinadas integrações.

Renomeie sua organização

Você pode renomear sua organização. Isso é útil se você apoia mais do que apenas uma organização.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Organização**.
3. Na página **Organização**, navegue até a primeira linha da tabela e selecione ••• e então selecione **Editar organização**.



4. Digite um novo nome para a organização e selecione **Aplicar**.

Obter o ID da organização

O ID da organização é usado para determinadas integrações com o Console.

Você pode visualizar o ID da organização na página Organizações e copiá-lo para a área de transferência conforme suas necessidades.

Passos

1. Selecione **Administração > Identidade e acesso** > **Organização**.
2. Na página **Organização**, procure o ID da sua organização na barra de resumo e copie-o para a área de transferência. Você pode salvar isso para usar mais tarde ou copiá-lo diretamente para onde precisar usá-lo.

Obter o ID de um projeto

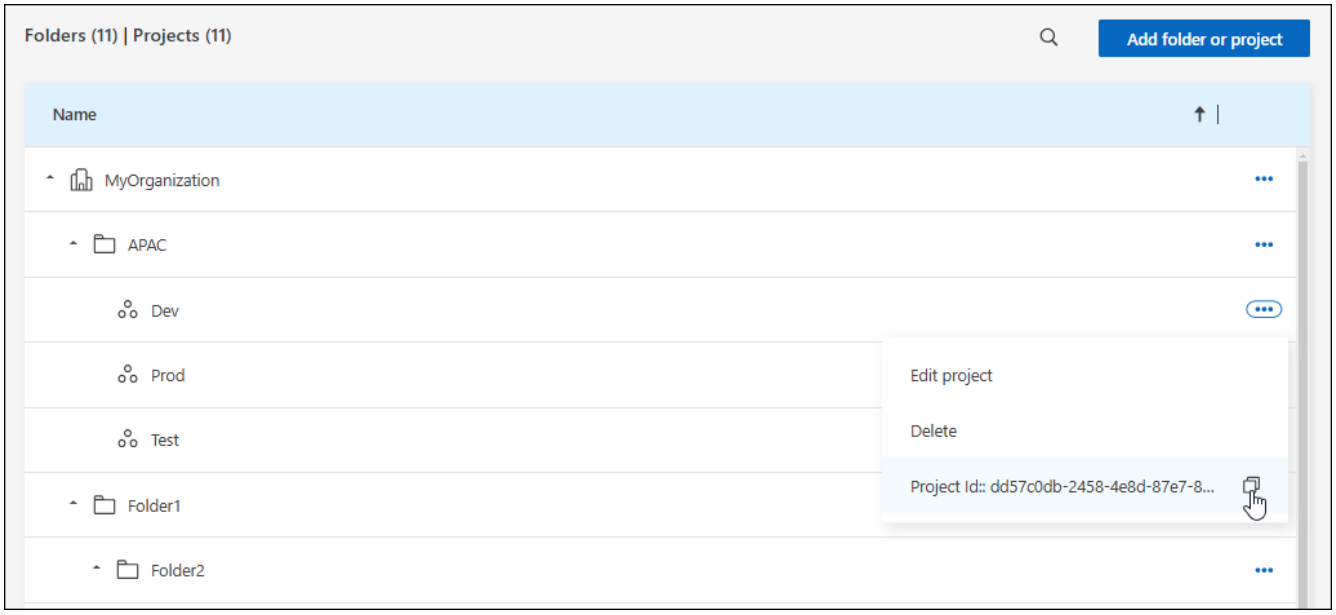
Você precisará obter o ID de um projeto se estiver usando a API. Por exemplo, ao criar um sistema Cloud Volumes ONTAP .

Passos

1. Na página **Organização**, navegue até um projeto na tabela e selecione •••

   O ID do projeto é exibido.

2. Para copiar o ID, selecione o botão copiar.



Informações relacionadas

- "Aprenda sobre gerenciamento de identidade e acesso"
- "Comece com identidade e acesso"
- "Saiba mais sobre a API para identidade e acesso"

Monitorar ou auditar a atividade do IAM

Se precisar monitorar ou auditar uma ação concluída relacionada à identidade e ao acesso, você pode visualizar os detalhes na página Auditoria. Por exemplo, você pode querer verificar quem adicionou um membro a uma organização ou se um projeto foi excluído com sucesso.

Passos

1. Selecione **Administração > Auditoria**.
2. Na página **Auditoria**, use os filtros para restringir os resultados. Selecione **Serviço** e depois selecione **Locação**.
3. Use qualquer um dos outros filtros para alterar quais ações serão exibidas na tabela.

   Por exemplo, você pode usar o filtro **Usuário** para mostrar ações relacionadas a uma conta de usuário específica.

Funções de acesso ao NetApp Console

Saiba mais sobre as funções de acesso do NetApp Console

O gerenciamento de identidade e acesso (IAM) no NetApp Console fornece funções predefinidas que você pode atribuir aos membros da sua organização em diferentes níveis da hierarquia de recursos. Antes de atribuir essas funções, você deve entender as permissões que cada função inclui. As funções se enquadram nas seguintes categorias: plataforma, aplicativo e serviço de dados.

Funções da plataforma

As funções da plataforma concedem permissões de administração do NetApp Console, incluindo atribuição de funções e gerenciamento de usuários. O Console tem várias funções de plataforma.

Função da plataforma	Responsabilidades
"Administrador da organização"	Permite que um usuário tenha acesso irrestrito a todos os projetos e pastas dentro de uma organização, adicione membros a qualquer projeto ou pasta, bem como execute qualquer tarefa e use qualquer serviço de dados que não tenha uma função explícita associada a ele. Usuários com essa função gerenciam sua organização criando pastas e projetos, atribuindo funções, adicionando usuários e gerenciando sistemas, se tiverem as credenciais adequadas. Esta é a única função de acesso que pode criar agentes do Console.
"Administrador de pasta ou projeto"	Permite ao usuário acesso irrestrito aos projetos e pastas atribuídos. Podem adicionar membros às pastas ou projetos que gerenciam, bem como executar qualquer tarefa e usar qualquer serviço de dados ou aplicativo em recursos dentro da pasta ou projeto que lhes foi atribuído. Administradores de pastas ou projetos não podem criar agentes do Console.
"Administrador da Federação"	Permite que um usuário crie e gerencie federações com o Console, o que permite logon único (SSO).
"Visualizador da Federação"	Permite que um usuário visualize federações existentes com o Console. Não é possível criar ou gerenciar federações.
"Administrador de parceria"	Permite que um usuário crie e gerencie parcerias.
"Visualizador de parceria"	Permite que um usuário visualize parcerias existentes. Não é possível criar ou gerenciar parcerias.
"Superadministrador"	Dá ao usuário um subconjunto de funções de administrador. Esta função foi projetada para organizações menores que podem não precisar distribuir responsabilidades do Console entre vários usuários.
"Super visualizador"	Dá ao usuário um subconjunto de funções de visualizador. Esta função foi projetada para organizações menores que podem não precisar distribuir responsabilidades do Console entre vários usuários.

Funções de aplicação

A seguir está uma lista de funções na categoria de aplicação. Cada função concede permissões específicas dentro de seu escopo designado. Usuários sem a função de aplicativo ou plataforma necessária não podem

acessar o respectivo aplicativo.

Função de aplicação	Responsabilidades
"Administrador do Google Cloud NetApp Volumes"	Usuários com a função Google Cloud NetApp Volumes podem descobrir e gerenciar o Google Cloud NetApp Volumes.
"Administrador Keystone"	Usuários com a função de administrador do Keystone podem criar solicitações de serviço. Permite que os usuários monitorem e visualizem o uso, os recursos e os detalhes administrativos dentro do locatário do Keystone que estão acessando.
"Visualizador Keystone"	Usuários com a função de visualizador do Keystone NÃO PODEM criar solicitações de serviço. Permite que os usuários monitorem e visualizem o consumo, os ativos e as informações administrativas dentro do locatário do Keystone que estão acessando.
Função de configuração do Mediador ONTAP	Contas de serviço com a função de configuração do ONTAP Mediator podem criar solicitações de serviço. Esta função é necessária em uma conta de serviço para configurar uma instância do"Mediador de Nuvem ONTAP" .
"Analista de suporte operacional"	Fornece acesso a alertas e ferramentas de monitoramento e capacidade de inserir e gerenciar casos de suporte.
"Administrador de armazenamento"	Administre funções de governança e integridade de armazenamento, descubra recursos de armazenamento e modifique e exclua sistemas existentes.
"Visualizador de armazenamento"	Visualize as funções de governança e integridade do armazenamento, bem como visualize os recursos de armazenamento descobertos anteriormente. Não é possível descobrir, modificar ou excluir sistemas de armazenamento existentes.
"Especialista em saúde do sistema"	Administrar funções de armazenamento, saúde e governança, todas as permissões do administrador de armazenamento, exceto não poder modificar ou excluir sistemas existentes.

Funções de serviço de dados

A seguir está uma lista de funções na categoria de serviço de dados. Cada função concede permissões específicas dentro de seu escopo designado. Usuários que não tenham a função de serviço de dados necessária ou uma função de plataforma não poderão acessar o serviço de dados.

Função de serviço de dados	Responsabilidades
"Superadministrador de Backup e Recuperação"	Execute qualquer ação no NetApp Backup and Recovery.
"Administrador de backup e recuperação"	Faça backups em snapshots locais, replique para armazenamento secundário e faça backup no armazenamento de objetos.
"Administração de restauração de backup e recuperação"	Restaure cargas de trabalho no Backup e Recuperação.
"Administrador clone de backup e recuperação"	Clone aplicativos e dados no Backup e Recuperação.

Função de serviço de dados	Responsabilidades
"Visualizador de backup e recuperação"	Ver informações de backup e recuperação.
"Administrador de recuperação de desastres"	Execute quaisquer ações no serviço NetApp Disaster Recovery.
"Administrador de failover de recuperação de desastres"	Execute failover e migrações.
"Administrador do aplicativo de recuperação de desastres"	Crie planos de replicação, altere planos de replicação e inicie failovers de teste.
"Visualizador de recuperação de desastres"	Ver apenas informações.
Visualizador de classificação	Permite que os usuários visualizem os resultados da verificação de classificação de dados do NetApp . Usuários com essa função podem visualizar informações de conformidade e gerar relatórios para recursos aos quais têm permissão de acesso. Esses usuários não podem habilitar ou desabilitar a verificação de volumes, buckets ou esquemas de banco de dados. A classificação não tem um papel de visualizador.
"Administrador de resiliência de ransomware"	Gerencie ações nas guias Proteger, Alertas, Recuperar, Configurações e Relatórios do NetApp Ransomware Resilience.
"Visualizador de resiliência de ransomware"	Visualize dados de carga de trabalho, visualize dados de alerta, baixe dados de recuperação e baixe relatórios no Ransomware Resilience.
"Comportamento do usuário de resiliência ao ransomware"	Configure, gerencie e visualize a detecção, os alertas e o monitoramento de comportamento suspeito do usuário no Ransomware Resilience.
"Visualizador de comportamento do usuário de resiliência de ransomware"	Veja alertas e insights sobre comportamento suspeito de usuários no Ransomware Resilience.
Administrador do SnapCenter	Oferece a capacidade de fazer backup de instantâneos de clusters ONTAP locais usando o NetApp Backup and Recovery para aplicativos. Um membro com essa função pode concluir as seguintes ações: * Concluir qualquer ação em Backup e recuperação > Aplicativos * Gerenciar todos os sistemas nos projetos e pastas para os quais eles têm permissões * Usar todos os serviços do NetApp Console O SnapCenter não tem uma função de visualizador.

Links relacionados

- "Saiba mais sobre o gerenciamento de identidade e acesso do NetApp Console"
- "Comece a usar o NetApp Console IAM"
- "Gerenciar membros do NetApp Console e suas permissões"
- "Saiba mais sobre a API para NetApp Console IAM"

Funções de acesso à plataforma do NetApp Console

Atribua funções de plataforma aos usuários para conceder permissões para gerenciar o NetApp Console, atribuir funções, adicionar usuários, criar agentes do Console e

gerenciar federações.

Exemplo de funções organizacionais para uma grande organização multinacional

A XYZ Corporation organiza o acesso ao armazenamento de dados por região — América do Norte, Europa e Ásia-Pacífico — fornecendo controle regional com supervisão centralizada.

O **administrador da organização** no Console da XYZ Corporation cria uma organização inicial e pastas separadas para cada região. O **administrador de pasta ou projeto** de cada região organiza projetos (com recursos associados) dentro da pasta da região.

Administradores regionais com a função **Administrador de pasta ou projeto** gerenciam ativamente suas pastas adicionando recursos e usuários. Esses administradores regionais também podem adicionar, remover ou renomear pastas e projetos que gerenciam. O **administrador da organização** herda permissões para quaisquer novos recursos, mantendo a visibilidade do uso do armazenamento em toda a organização.

Dentro da mesma organização, um usuário recebe a função **Administrador da federação** para gerenciar a federação da organização com seu IdP corporativo. Este usuário pode adicionar ou remover organizações federadas, mas não pode gerenciar usuários ou recursos dentro da organização. O **Administrador da organização** atribui a um usuário a função **Visualizador da federação** para verificar o status da federação e visualizar organizações federadas.

As tabelas a seguir indicam as ações que cada função da plataforma Console pode executar.

Funções de administração da organização

Tarefa	Administrador da organização	Administrador de pasta ou projeto
Criar agentes	Sim	Não
Criar, modificar ou excluir sistemas do Console (adicionar ou descobrir sistemas)	Sim	Sim
Crie pastas e projetos, incluindo exclusão	Sim	Não
Renomear pastas e projetos existentes	Sim	Sim
Atribuir funções e adicionar usuários	Sim	Sim
Associar recursos a pastas e projetos	Sim	Sim
Associar agentes a pastas e projetos	Sim	Não
Remover agentes de pastas e projetos	Sim	Não
Gerenciar agentes (editar certificados, configurações e assim por diante)	Sim	Não
Gerenciar credenciais em Administração > Credenciais	Sim	Sim
Criar, gerenciar e visualizar federações	Sim	Não
Registre-se para obter suporte e envie casos por meio do Console	Sim	Sim
Use serviços de dados que não estejam associados a uma função de acesso explícita	Sim	Sim
Ver a página de auditoria e notificações	Sim	Sim

Funções da Federação

Tarefa	Administrador da Federação	Visualizador da Federação
Criar uma federação	Sim	Não
Verificar um domínio	Sim	Não
Adicionar um domínio a uma federação	Sim	Não
Desabilitar e excluir federações	Sim	Não
Federações de teste	Sim	Não
Ver federações e seus detalhes	Sim	Sim

Funções de parceria

Tarefa	Administrador de parceria	Visualizador de parceria
Pode criar uma parceria	Sim	Não
Atribuir funções aos membros parceiros	Sim	Não
Pode adicionar membros a uma parceria	Sim	Não
Pode visualizar detalhes da parceria da organização	Sim	Sim

Funções de superadministrador e visualizador

A função **Superadministrador** fornece acesso total para gerenciar recursos do Console, armazenamento e serviços de dados. Essa função é adequada para aqueles que supervisionam a administração e a governança. Em contraste, a função **Super visualizador** oferece acesso somente leitura, ideal para auditores ou partes interessadas que precisam de visibilidade sem fazer alterações.

As organizações devem usar o acesso de **Superadministrador** com moderação para minimizar os riscos de segurança e se alinhar ao princípio do menor privilégio. A maioria das organizações deve atribuir funções refinadas com apenas as permissões necessárias para reduzir riscos e melhorar a capacidade de auditoria.

Exemplo para super funções

A ABC Corporation tem uma pequena equipe de cinco pessoas que utiliza o NetApp Console para serviços de dados e gerenciamento de armazenamento. Em vez de distribuir várias funções, eles atribuem a função de **Superadministrador** a dois membros seniores da equipe que lidam com todas as tarefas administrativas, incluindo gerenciamento de usuários e configuração de recursos. Os três membros restantes da equipe recebem a função de **Supervisualizador**, o que lhes permite monitorar a integridade do armazenamento e o status do serviço de dados sem a capacidade de modificar as configurações.

Papel	Funções herdadas
Superadministrador	• Administrador da organização • Administrador de pasta ou projeto • Administrador da Federação • Administrador de parceria • Administrador de resiliência de ransomware • Administrador de recuperação de desastres • Superadministrador de backup • Administrador de armazenamento • Administrador Keystone • Administrador do Google Cloud NetApp Volumes
Super visualizador	• Visualizador de organização • Visualizador da Federação • Visualizador de parceria • Visualizador de resiliência de ransomware • Visualizador de recuperação de desastres • Visualizador de backup • Visualizador de armazenamento • Visualizador Keystone • Visualizador de Google Cloud NetApp Volumes

Funções de aplicação

Funções do Google Cloud NetApp Volumes no NetApp Console

Você pode atribuir a seguinte função aos usuários para fornecer a eles acesso ao Google Cloud NetApp Volumes no NetApp Console.

O Google Cloud NetApp Volumes usa a seguinte função:

- * Administrador do Google Cloud NetApp Volumes *: Descubra e gerencie o Google Cloud NetApp Volumes no Console.

Funções de acesso Keystone no NetApp Console

As funções do Keystone fornecem acesso aos painéis do Keystone e permitem que os usuários visualizem e gerenciem sua assinatura do Keystone . Há duas funções do Keystone : administrador do Keystone e visualizador do Keystone . A principal diferença entre as duas funções são as ações que elas podem realizar no Keystone. A função de administrador do Keystone é a única função que tem permissão para criar solicitações de serviço ou modificar assinaturas.

Exemplo de funções Keystone no NetApp Console

A XYZ Corporation tem quatro engenheiros de armazenamento de diferentes departamentos que visualizam as informações de assinatura do Keystone . Embora todos esses usuários precisem monitorar a assinatura do Keystone , somente o líder da equipe tem permissão para fazer solicitações de serviço. Três membros da equipe recebem a função de *visualizador do Keystone *, enquanto o líder da equipe recebe a função de *administrador do Keystone * para que haja um ponto de controle sobre as solicitações de serviço da empresa.

A tabela a seguir indica as ações que cada função Keystone pode executar.

Recurso e ação	Administrador Keystone	Visualizador Keystone
Visualize as seguintes guias: Assinatura, Ativos, Monitor e Administração	Sim	Sim
* Página de assinatura do Keystone *:		
Ver assinaturas	Sim	Sim
Alterar ou renovar assinaturas	Sim	Não
* Página de ativos do Keystone *:		
Ver ativos	Sim	Sim
Gerenciar ativos	Sim	Não
* Página de alertas do Keystone *:		
Ver alertas	Sim	Não
Gerenciar alertas	Sim	Não
Crie alertas para si mesmo	Sim	Sim
Licenças e assinaturas:		
Pode visualizar licenças e assinaturas	Sim	Sim
*Página de relatórios do Keystone *:		
Baixar relatórios	Sim	Sim

Recurso e ação	Administrador Keystone	Visualizador Keystone
Gerenciar relatórios	Sim	Sim
Crie relatórios para si mesmo	Sim	Sim
Solicitações de serviço:		
Criar solicitações de serviço	Sim	Não
Visualizar solicitações de serviço criadas por qualquer usuário dentro da organização	Sim	Sim

Função de acesso de analista de suporte operacional para o NetApp Console

Você pode atribuir a seguinte função aos usuários para fornecer a eles acesso a alertas e monitoramento. Usuários com essa função também podem abrir casos de suporte.

Analista de suporte operacional

Tarefa	Pode executar
Gerencie suas próprias credenciais de usuário em Configurações > Credenciais	Sim
Ver recursos descobertos	Sim
Registre-se para obter suporte e envie casos por meio do Console	Sim
Sim	Ver a página de auditoria e notificações
Sim	Visualizar, baixar e configurar alertas

Funções de acesso de armazenamento para o NetApp Console

Você pode atribuir as seguintes funções aos usuários para fornecer a eles acesso aos recursos de gerenciamento de armazenamento no NetApp Console. Você pode atribuir aos usuários uma função administrativa para gerenciar o armazenamento ou uma função de visualizador para monitoramento.

Essas funções não estão disponíveis na API de parceria do NetApp Console.

Os administradores podem atribuir funções de armazenamento aos usuários para os seguintes recursos e funcionalidades de armazenamento:

Recursos de armazenamento:

- Clusters ONTAP locais
- StorageGRID
- Série E

Serviços e recursos do console:

- Consultor digital
- Atualizações de software
- Planejamento do ciclo de vida
- Sustentabilidade

Exemplo de funções de armazenamento no NetApp Console

A XYZ Corporation, uma empresa multinacional, tem uma grande equipe de engenheiros e administradores de armazenamento. Eles permitem que essa equipe gerencie ativos de armazenamento para suas regiões, ao mesmo tempo em que limitam o acesso às principais tarefas do Console, como gerenciamento de usuários, criação de agentes e gerenciamento de licenças.

Em uma equipe de 12 pessoas, dois usuários recebem a função **Visualizador de armazenamento**, que lhes permite monitorar os recursos de armazenamento associados aos projetos do Console aos quais estão atribuídos. Os nove restantes recebem a função de **Administrador de armazenamento**, que inclui a capacidade de gerenciar atualizações de software, acessar o ONTAP System Manager por meio do Console, bem como descobrir recursos de armazenamento (adicionar sistemas). Uma pessoa na equipe recebe a função de **Especialista em integridade do sistema** para que possa gerenciar a integridade dos recursos de armazenamento em sua região, mas não modificar ou excluir nenhum sistema. Essa pessoa também pode executar atualizações de software nos recursos de armazenamento para projetos aos quais ela foi atribuída.

A organização tem dois usuários adicionais com a função **Administrador da organização** que podem gerenciar todos os aspectos do Console, incluindo gerenciamento de usuários, criação de agentes e gerenciamento de licenças, bem como vários usuários com a função **Administrador de pasta ou projeto** que podem executar tarefas de administração do Console para as pastas e projetos aos quais estão atribuídos.

A tabela a seguir mostra as ações que cada função de armazenamento executa.

Recurso e ação	Administrador de armazenamento	Especialista em saúde do sistema	Visualizador de armazenamento
Gerenciamento de Armazenamento:			
Descubra novos recursos (crie sistemas)	Sim	Sim	Não
Ver sistemas descobertos	Sim	Sim	Não
Excluir sistemas do Console	Sim	Não	Não
Modificar sistemas	Sim	Não	Não
Criar agentes	Não	Não	Não
Consultor digital			
Ver todas as páginas e funções	Sim	Sim	Sim
Licenças e assinaturas			
Ver todas as páginas e funções	Não	Não	Não

Recurso e ação	Administrador de armazenamento	Especialista em saúde do sistema	Visualizador de armazenamento
Atualizações de software			
Ver página de destino e recomendações	Sim	Sim	Sim
Revise as recomendações de versões potenciais e os principais benefícios	Sim	Sim	Sim
Exibir detalhes de atualização para um cluster	Sim	Sim	Sim
Execute verificações de pré-atualização e baixe o plano de atualização	Sim	Sim	Sim
Instalar atualizações de software	Sim	Sim	Não
Planejamento do ciclo de vida			
Revisar status de planejamento de capacidade	Sim	Sim	Sim
Escolha a próxima ação (melhor prática, nível)	Sim	Não	Não
Coloque dados frios em camadas no armazenamento em nuvem e libere espaço de armazenamento	Sim	Sim	Não
Configurar lembretes	Sim	Sim	Sim
Sustentabilidade			
Ver painel e recomendações	Sim	Sim	Sim
Baixar dados do relatório	Sim	Sim	Sim
Editar porcentagem de mitigação de carbono	Sim	Sim	Não
Recomendações de correção	Sim	Sim	Não
Adiar recomendações	Sim	Sim	Não
Acesso do gerente do sistema			
Pode inserir credenciais	Sim	Sim	Não
Credenciais			
Credenciais do usuário	Sim	Sim	Não

Funções de serviços de dados

Funções de backup e recuperação do NetApp no NetApp Console

Você pode atribuir as seguintes funções aos usuários para fornecer a eles acesso ao NetApp Backup and Recovery no Console. As funções de backup e recuperação oferecem a flexibilidade de atribuir aos usuários uma função específica para as tarefas que eles precisam realizar na sua organização. A maneira como você atribui funções depende das suas próprias práticas de negócios e gerenciamento de armazenamento.

O serviço usa as seguintes funções específicas do NetApp Backup and Recovery.

- **Superadministrador de Backup e Recuperação**: Execute qualquer ação no NetApp Backup and Recovery.
- **Administrador de backup e recuperação**: execute backups em snapshots locais, replique para armazenamento secundário e faça backup em ações de armazenamento de objetos no NetApp Backup and Recovery.
- **Administrador de restauração de backup e recuperação**: restaure cargas de trabalho usando o NetApp Backup and Recovery.
- **Administrador de clones de backup e recuperação**: clone aplicativos e dados usando o NetApp Backup and Recovery.
- **Visualizador de backup e recuperação**: visualize informações no NetApp Backup and Recovery, mas não execute nenhuma ação.

Para obter detalhes sobre todas as funções de acesso do NetApp Console, consulte "a documentação de configuração e administração do Console" .

Funções usadas para ações comuns

A tabela a seguir indica as ações que cada função do NetApp Backup and Recovery pode executar para todas as cargas de trabalho.

Recurso e ação	Superadministrador de Backup e Recuperação	Administrador de backup e recuperação	Administração de restauração de backup e recuperação	Administrador clone de backup e recuperação	Visualizador de backup e recuperação
Adicionar, editar ou excluir hosts	Sim	Não	Não	Não	Não
Instalar plugins	Sim	Não	Não	Não	Não
Adicionar credenciais (host, instância, vCenter)	Sim	Não	Não	Não	Não
Ver painel e todas as guias	Sim	Sim	Sim	Sim	Sim
Iniciar teste gratuito	Sim	Não	Não	Não	Não

Recurso e ação	Superadministrador de Backup e Recuperação	Administrador de backup e recuperação	Administração de restauração de backup e recuperação	Administrador clone de backup e recuperação	Visualizador de backup e recuperação
Iniciar descoberta de cargas de trabalho	Não	Sim	Sim	Sim	Não
Ver informações da licença	Sim	Sim	Sim	Sim	Sim
Ativar licença	Sim	Não	Não	Não	Não
Ver hosts	Sim	Sim	Sim	Sim	Sim
Horários:					
Ativar agendamentos	Sim	Sim	Sim	Sim	Não
Suspender horários	Sim	Sim	Sim	Sim	Não
Políticas e proteção:					
Ver planos de proteção	Sim	Sim	Sim	Sim	Sim
Criar, modificar ou excluir planos de proteção	Sim	Sim	Não	Não	Não
Restaurar cargas de trabalho	Sim	Não	Sim	Não	Não
Criar, dividir ou excluir clones	Sim	Não	Não	Sim	Não
Criar, modificar ou excluir política	Sim	Sim	Não	Não	Não
Relatórios:					
Ver relatórios	Sim	Sim	Sim	Sim	Sim
Criar relatórios	Sim	Sim	Sim	Sim	Não
Excluir relatórios	Sim	Não	Não	Não	Não
Importar do SnapCenter e gerenciar host:					
Exibir dados importados do SnapCenter	Sim	Sim	Sim	Sim	Sim
Importar dados do SnapCenter	Sim	Sim	Não	Não	Não

Recurso e ação	Superadministrador de Backup e Recuperação	Administrador de backup e recuperação	Administração de restauração de backup e recuperação	Administrador clone de backup e recuperação	Visualizador de backup e recuperação
Gerenciar (migrar) host	Sim	Sim	Não	Não	Não
Configurar definições:					
Configurar diretório de log	Sim	Sim	Sim	Não	Não
Associar ou remover credenciais de instância	Sim	Sim	Sim	Não	Não
Baldes:					
Ver baldes	Sim	Sim	Sim	Sim	Sim
Criar, editar ou excluir bucket	Sim	Sim	Não	Não	Não

Funções usadas para ações específicas da carga de trabalho

A tabela a seguir indica as ações que cada função do NetApp Backup and Recovery pode executar para cargas de trabalho específicas.

Cargas de trabalho do Kubernetes

Esta tabela indica as ações que cada função do NetApp Backup and Recovery pode executar para ações específicas de cargas de trabalho do Kubernetes.

Recurso e ação	Superadministrador de Backup e Recuperação	Administrador de backup e recuperação	Administração de restauração de backup e recuperação	Visualizador de backup e recuperação
Exibir clusters, namespaces, classes de armazenamento e recursos de API	Sim	Sim	Sim	Sim
Adicionar novos clusters do Kubernetes	Sim	Sim	Não	Não
Atualizar configurações de cluster	Sim	Não	Não	Não
Remover clusters do gerenciamento	Sim	Não	Não	Não
Ver aplicações	Sim	Sim	Sim	Sim

Recurso e ação	Superadministrador de Backup e Recuperação	Administrador de backup e recuperação	Administração de restauração de backup e recuperação	Visualizador de backup e recuperação
Criar e definir novos aplicativos	Sim	Sim	Não	Não
Atualizar configurações do aplicativo	Sim	Sim	Não	Não
Remover aplicativos do gerenciamento	Sim	Sim	Não	Não
Exibir recursos protegidos e status de backup	Sim	Sim	Sim	Sim
Crie backups e proteja aplicativos com políticas	Sim	Sim	Não	Não
Desproteja aplicativos e exclua backups	Sim	Sim	Não	Não
Exibir pontos de recuperação e resultados do visualizador de recursos	Sim	Sim	Sim	Sim
Restaurar aplicativos de pontos de recuperação	Sim	Não	Sim	Não
Ver políticas de backup do Kubernetes	Sim	Sim	Sim	Sim
Criar políticas de backup do Kubernetes	Sim	Sim	Sim	Não
Atualizar políticas de backup	Sim	Sim	Sim	Não
Excluir políticas de backup	Sim	Sim	Sim	Não
Exibir ganchos de execução e fontes de ganchos	Sim	Sim	Sim	Sim
Crie ganchos de execução e fontes de ganchos	Sim	Sim	Sim	Não
Atualizar ganchos de execução e fontes de ganchos	Sim	Sim	Sim	Não
Excluir ganchos de execução e fontes de ganchos	Sim	Sim	Sim	Não

Recurso e ação	Superadministrador de Backup e Recuperação	Administrador de backup e recuperação	Administração de restauração de backup e recuperação	Visualizador de backup e recuperação
Exibir modelos de ganchos de execução	Sim	Sim	Sim	Sim
Criar modelos de gancho de execução	Sim	Sim	Sim	Não
Atualizar modelos de gancho de execução	Sim	Sim	Sim	Não
Excluir modelos de gancho de execução	Sim	Sim	Sim	Não
Visualizar resumo da carga de trabalho e painéis analíticos	Sim	Sim	Sim	Sim
Exibir buckets e destinos de armazenamento do StorageGRID	Sim	Sim	Sim	Sim

Funções de recuperação de desastres da NetApp no NetApp Console

Você pode atribuir as seguintes funções aos usuários para fornecer a eles acesso ao NetApp Disaster Recovery no Console. As funções de Recuperação de Desastres oferecem a flexibilidade de atribuir aos usuários uma função específica para as tarefas que eles precisam realizar na sua organização. A maneira como você atribui funções depende das suas próprias práticas de negócios e gerenciamento de armazenamento.

A recuperação de desastres utiliza as seguintes funções:

- **Administrador de recuperação de desastres**: Execute quaisquer ações.
- **Administrador de failover de recuperação de desastres**: Executa failover e migrações.
- **Administrador do aplicativo de recuperação de desastres**: Crie planos de replicação. Modificar planos de replicação. Iniciar failovers de teste.
- **Visualizador de recuperação de desastres**: Visualize somente informações.

A tabela a seguir indica as ações que cada função pode executar.

Recurso e ação	Administrador de recuperação de desastres	Administrador de failover de recuperação de desastres	Administrador do aplicativo de recuperação de desastres	Visualizador de recuperação de desastres
Ver painel e todas as guias	Sim	Sim	Sim	Sim
Iniciar teste gratuito	Sim	Não	Não	Não

Recurso e ação	Administrador de recuperação de desastres	Administrador de failover de recuperação de desastres	Administrador do aplicativo de recuperação de desastres	Visualizador de recuperação de desastres
Iniciar descoberta de cargas de trabalho	Sim	Não	Não	Não
Ver informações da licença	Sim	Sim	Sim	Sim
Ativar licença	Sim	Não	Sim	Não
Na aba Sites:				
Ver sites	Sim	Sim	Sim	Sim
Adicionar, modificar ou excluir sites	Sim	Não	Não	Não
Na aba Planos de replicação:				
Ver planos de replicação	Sim	Sim	Sim	Sim
Ver detalhes do plano de replicação	Sim	Sim	Sim	Sim
Criar ou modificar planos de replicação	Sim	Sim	Sim	Não
Criar relatórios	Sim	Não	Não	Não
Ver instantâneos	Sim	Sim	Sim	Sim
Executar testes de failover	Sim	Sim	Sim	Não
Executar failovers	Sim	Sim	Não	Não
Executar failbacks	Sim	Sim	Não	Não
Executar migrações	Sim	Sim	Não	Não
Na aba Grupos de recursos:				
Exibir grupos de recursos	Sim	Sim	Sim	Sim
Criar, modificar ou excluir grupos de recursos	Sim	Não	Sim	Não
Na aba Monitoramento de Tarefas:				
Ver empregos	Sim	Não	Sim	Sim

Recurso e ação	Administrador de recuperação de desastres	Administrador de failover de recuperação de desastres	Administrador do aplicativo de recuperação de desastres	Visualizador de recuperação de desastres
Cancelar trabalhos	Sim	Sim	Sim	Não

Funções de acesso de resiliência contra ransomware para o NetApp Console

As funções de resiliência contra ransomware fornecem aos usuários acesso à resiliência contra ransomware da NetApp . As duas funções são administrador de proteção contra ransomware e visualizador de proteção contra ransomware. A principal diferença entre as duas funções são as ações que elas podem tomar na Resiliência ao Ransomware.

A tabela a seguir mostra as ações que cada função pode executar.

Recurso e ação	Administrador de resiliência de ransomware	Visualizador de resiliência de ransomware	Comportamento do usuário de resiliência ao ransomware	Visualizador de comportamento do usuário de resiliência de ransomware
Ver painel e todas as guias	Sim	Sim	Não	Não
No painel, atualize o status da recomendação	Sim	Não	Não	Não
Iniciar teste gratuito	Sim	Não	Não	Não
Iniciar descoberta de cargas de trabalho	Sim	Não	Não	Não
Iniciar a redescoberta das cargas de trabalho	Sim	Não	Não	Não
Na aba Proteger:				
Adicionar, modificar ou excluir planos de proteção	Sim	Não	Não	Não
Proteja as cargas de trabalho	Sim	Não	Não	Não
Identificar a exposição a dados sensíveis	Sim	Não	Não	Não
Listar planos de proteção e detalhes	Sim	Sim	Não	Não
Grupos de proteção de lista	Sim	Sim	Não	Não
Ver detalhes do grupo de proteção	Sim	Sim	Não	Não

Recurso e ação	Administrador de resiliência de ransomware	Visualizador de resiliência de ransomware	Comportamento do usuário de resiliência ao ransomware	Visualizador de comportamento do usuário de resiliência de ransomware
Criar, editar ou excluir grupo de proteção	Sim	Não	Não	Não
Baixar dados	Sim	Sim	Não	Não
Na aba Alertas:				
Ver alertas e detalhes de alertas	Sim	Sim	Não	Não
Editar status do incidente	Sim	Não	Não	Não
Marcar alerta para recuperação	Sim	Não	Não	Não
Ver detalhes do incidente	Sim	Sim	Não	Não
Descartar ou resolver incidentes	Sim	Não	Não	Não
Bloquear usuário	Sim	Não	Não	Não
Obtenha a lista completa de arquivos afetados	Sim	Não	Não	Não
Baixar dados de alertas	Sim	Sim	Não	Não
Ver atividades suspeitas de usuários	Não	Não	Sim	Sim
Na aba Recuperar:				
Baixar arquivos impactados	Sim	Não	Não	Não
Restaurar carga de trabalho	Sim	Não	Não	Não
Baixar dados de recuperação	Sim	Sim	Não	Não
Baixar relatórios	Sim	Sim	Não	Não
Na aba Configurações:				
Adicionar ou modificar destinos de backup	Sim	Não	Não	Não
Listar destinos de backup	Sim	Sim	Não	Não
Exibir alvos SIEM conectados	Sim	Sim	Não	Não

Recurso e ação	Administrador de resiliência de ransomware	Visualizador de resiliência de ransomware	Comportamento do usuário de resiliência ao ransomware	Visualizador de comportamento do usuário de resiliência de ransomware
Adicionar ou modificar alvos SIEM	Sim	Não	Não	Não
Configurar exercício de prontidão	Sim	Não	Não	Não
Iniciar exercício de prontidão	Sim	Não	Não	Não
Exercício de prontidão para reinicialização	Sim	Não	Não	Não
Exercício de preparação para edição	Sim	Não	Não	Não
Revisar o status do exercício de prontidão	Sim	Sim	Não	Não
Atualizar configuração de descoberta	Sim	Não	Não	Não
Exibir configuração de descoberta	Sim	Sim	Não	Não
Configurar configurações de comportamento suspeito do usuário	Não	Não	Sim	Não
Na aba Relatórios:				
Baixar relatórios	Sim	Sim	Não	Não

Organizações parceiras

Parcerias no NetApp Console

Ao criar parcerias entre organizações, o NetApp Console permite que os parceiros gerenciem com segurança os recursos do NetApp em todos os limites organizacionais, simplificando a colaboração e aumentando a segurança.

Funções necessárias

Administrador de parceria"Saiba mais sobre funções de acesso."

As parcerias permitem o gerenciamento seguro de recursos da NetApp em todas as organizações usando relacionamentos baseados em funções no Console. A organização iniciadora concede acesso aos seus recursos, enquanto a organização aceitante fornece os usuários ou contas de serviço aos quais será concedido acesso. As parcerias são estabelecidas por meio de um fluxo de trabalho de autoatendimento, dando à organização iniciadora controle total sobre quais recursos são compartilhados, quais funções são atribuídas e a capacidade de integrar, gerenciar ou revogar o acesso do parceiro conforme necessário.

Os clientes podem autorizar MSPs ou revendedores a gerenciar ambientes NetApp sem precisar de

configurações complicadas. Os clientes podem controlar quais clusters os parceiros podem acessar e quais funções eles têm, e podem revogar o acesso a qualquer momento para manter a segurança e a conformidade.

Como parceiro, você obtém visibilidade e controle centralizados em todos os ambientes do cliente. Você pode facilmente mudar para a organização de um cliente para gerenciar recursos, executar serviços de dados e monitorar a integridade dentro de limites definidos, reduzindo ferramentas personalizadas e garantindo o alinhamento com as políticas de cada cliente.

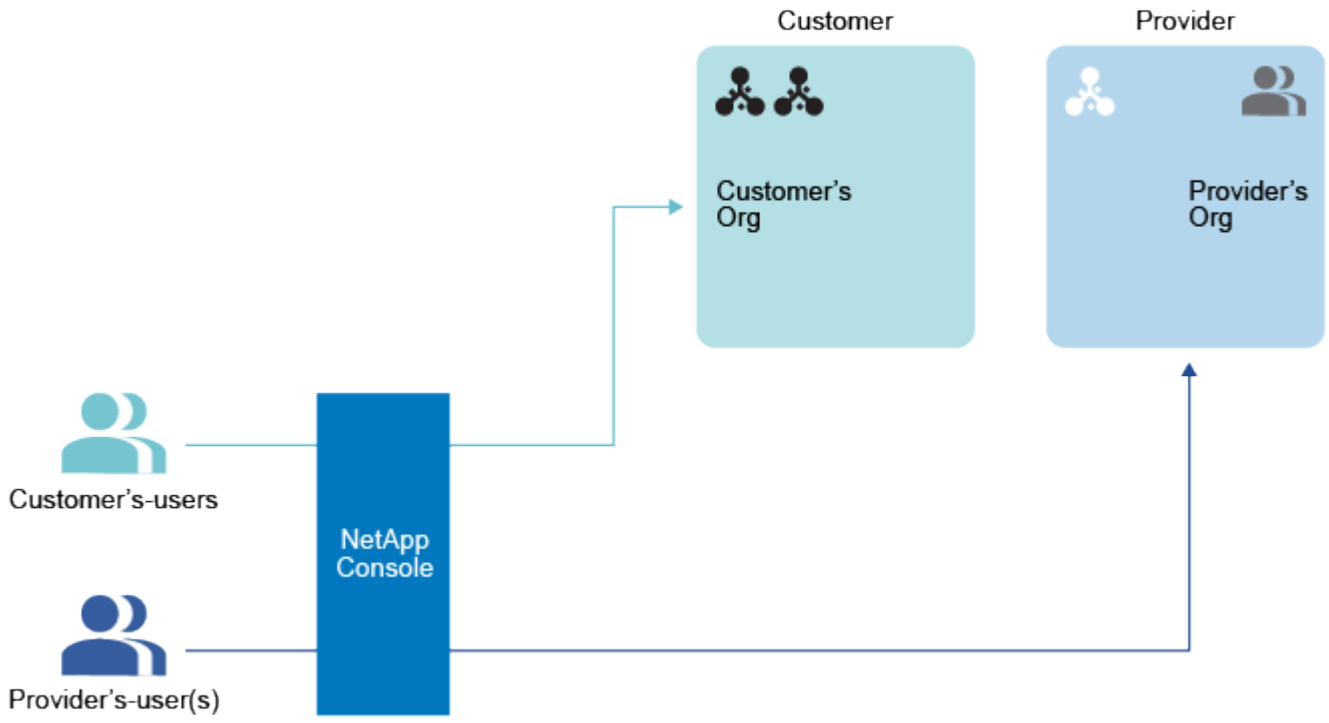
1 Atribuir a um ou mais usuários a função de administrador de parceria

Atribua a um ou mais usuários nas organizações iniciadora e receptora a função de administrador de parceria para criar e gerenciar parcerias. Você pode atribuir a função de visualizador de parceria a usuários que precisam apenas visualizar parcerias, e não gerenciá-las.

2 Compartilhe o ID da sua organização com a organização iniciadora

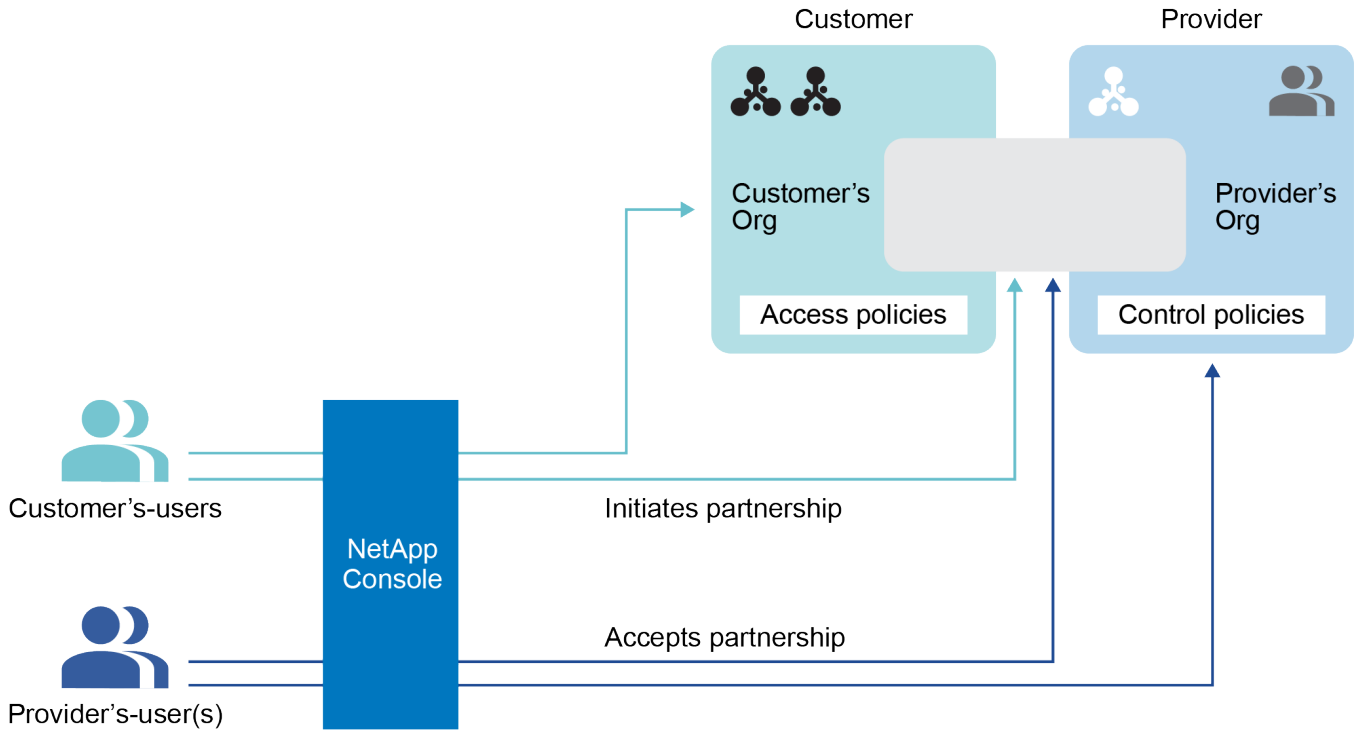
Para iniciar uma parceria, o iniciador deve saber o ID da organização alvo. Somente a respectiva organização pode acessar este ID da organização. Compartilhe-o diretamente com a organização iniciadora fora do NetApp Console por e-mail ou outro método.

A organização iniciadora é a organização que concede acesso aos seus recursos.



3 Iniciar a parceria dentro do NetApp Console

A organização que inicia a parceria o faz no NetApp Console enviando uma solicitação de parceria.



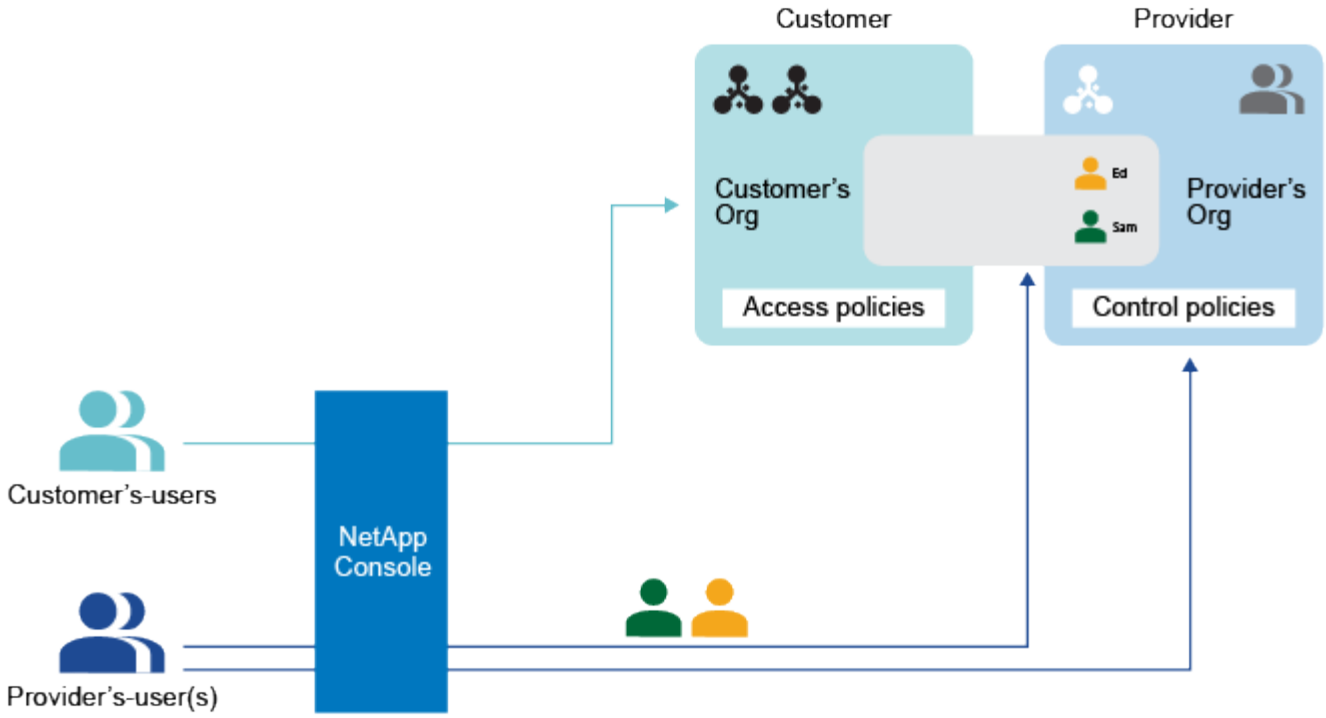
4 Aprovar a parceria

A organização receptora deve aceitar a solicitação.

A organização receptora é a organização que está recebendo acesso aos recursos.

5 Atribuir usuários à parceria

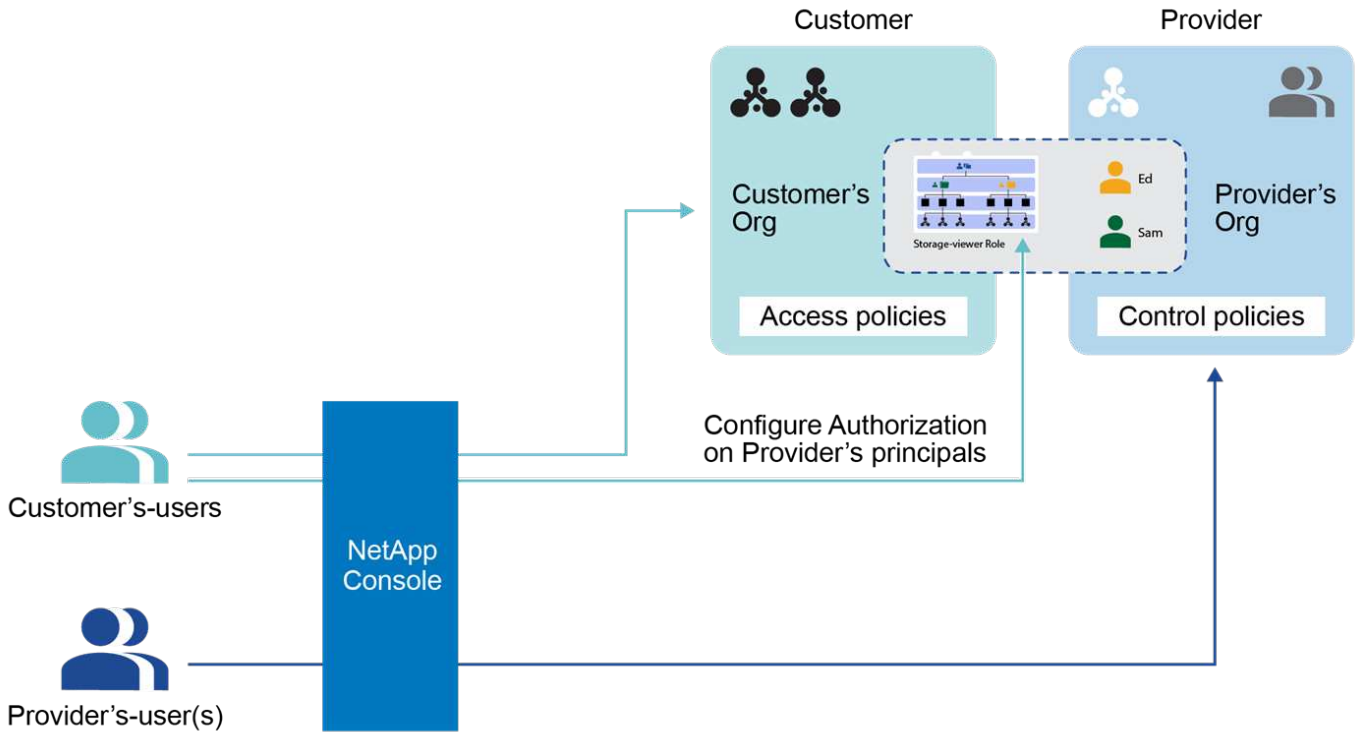
A organização receptora atribui usuários ou contas de serviço específicos da sua organização à parceria. A organização iniciadora atribui funções a esses usuários.



6 Conceder aos usuários atribuídos acesso aos recursos

Se você for a organização iniciadora, poderá conceder acesso a recursos específicos aos usuários que foram atribuídos à parceria. Você pode revogar o acesso a qualquer momento.

Você faz isso atribuindo funções para projetos ou pastas específicos dentro da sua organização.



Gerenciar parcerias no NetApp Console

Crie parcerias para estabelecer conexões seguras e gerenciadas entre sua organização e parceiros confiáveis para gerenciamento colaborativo de recursos do NetApp .

As parcerias permitem que você gerencie com segurança os recursos do NetApp em todos os limites com relacionamentos baseados em funções no Console. A organização iniciadora concede acesso aos seus recursos, enquanto a organização aceitante fornece os usuários ou contas de serviço aos quais será concedido acesso. As parcerias são estabelecidas por meio de um fluxo de trabalho de autoatendimento, dando à organização iniciadora controle total sobre quais recursos são compartilhados, quais funções são atribuídas e a capacidade de integrar, gerenciar ou revogar o acesso do parceiro conforme necessário.

Funções necessárias

A função **Administrador de parceria** é necessária para criar e gerenciar parcerias. O **Visualizador de Parcerias** pode visualizar a página Parcerias."Saiba mais sobre funções de acesso."

Iniciar uma parceria organizacional

Você pode solicitar uma parceria com outra organização se souber o ID da organização. A organização receptora aprova a solicitação antes que a parceria possa prosseguir.

Antes de começar, certifique-se de ter o ID da organização parceira e de que você recebeu a função de **Administrador da parceria**.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Parcerias**.
3. Selecione **Adicionar parceria**.
4. Na caixa de diálogo **Criar parceria**, insira o ID da organização parceira do parceiro solicitado e selecione **Adicionar**.

   A solicitação de parceria é enviada à organização parceira para aprovação. Você pode visualizar o status da solicitação de parceria na página **Parcerias**.

Aprovar uma parceria organizacional

Uma solicitação de parceria de organização deve ser aceita pela organização receptora antes que a parceria possa prosseguir. Você deve ter a função **Administrador de parceria** para aprovar e gerenciar parcerias.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Parcerias**.
3. Selecione a aba **Parceria recebida**.
4. Navegue até a parceria recebida que deseja aprovar e selecione ••• e então selecione **Aprovar**.
5. Revise os detalhes da parceria, incluindo o nome e o ID da organização que solicitou a parceria e selecione **Avançar.**
6. Opcionalmente, adicione membros da organização à parceria e selecione **Aplicar**.

   Você pode adicionar membros adicionais por meio da página **Parceria** a qualquer momento.

Todos os membros que você adicionar ficarão visíveis na organização do parceiro, onde o parceiro poderá atribuí-los aos recursos.

Resultado

A parceria que você aprovou agora mostra o status **Estabelecida**. Usuários com as funções **Administrador de parceria** ou **Visualizador de parceria** em qualquer organização podem visualizar a parceria.

Ver status da parceria

Veja o status das suas parcerias.

Função necessária

Administrador de parceria, visualizador de parceria."Saiba mais sobre funções de acesso."

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Parcerias**.
3. Selecione a aba **Parcerias iniciadas** ou **Parcerias recebidas**.
4. Revise a tabela respectiva que exibe as parcerias e seus status.

Desabilitar uma parceria de organização

Você deve ser membro da organização iniciadora para desabilitar uma parceria. Desabilitar uma parceria revoga imediatamente o acesso a quaisquer recursos na sua organização que foram compartilhados com a organização parceira.

Função necessária

Administração de parcerias."Saiba mais sobre funções de acesso."

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Parcerias**.
3. Selecione a aba **Parcerias iniciadas**.
4. Revise a tabela respectiva que exibe as parcerias e seus status.
5. Navegue até a parceria iniciada que deseja desabilitar e selecione ••• e então selecione **Desativar**.

Gerenciar membros de uma organização parceira

Você pode adicionar usuários a uma parceria adicionando-os à organização parceira. Depois de adicionar usuários, a organização parceira é responsável por atribuir a eles funções para recursos específicos em sua organização.

Funções necessárias

A função **Administrador de parceria** é necessária para criar e gerenciar parcerias. O **Visualizador de Parcerias** pode visualizar a página Parcerias."Saiba mais sobre funções de acesso."

Você pode remover usuários de uma parceria a qualquer momento. Remover um usuário de uma parceria revoga imediatamente seu acesso a quaisquer recursos na organização parceira.

Adicionar membros a uma parceria

Ao adicionar membros a uma parceria, o **administrador da parceria** da organização parceira deve atribuir a eles funções para recursos específicos na organização antes que eles possam acessá-los.

Depois de adicionar membros a uma parceria, os membros são exibidos como membros na organização parceira, onde o parceiro pode atribuí-los aos recursos.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Parcerias**.
3. Selecione a aba **Parceria recebida**.
4. Selecione o menu de ações ••• ao lado da parceria estabelecida que você deseja incluir como membros e selecione **Adicionar membros**.
5. Escolha um ou mais membros para adicionar à parceria e selecione **Adicionar**.

Remover membros de uma parceria

Você pode remover membros de uma parceria a qualquer momento. Remover um usuário de uma parceria revoga imediatamente seu acesso a quaisquer recursos na organização parceira.

Se você quiser ajustar a função de um membro ou os recursos que ele pode acessar, o administrador da Parceria da organização parceira deverá fazer essas alterações.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Parcerias**.
3. Selecione a aba **Parceria recebida**.
4. Selecione o menu de ações ••• ao lado do membro que você deseja remover e selecione **Remover associação**.
5. Confirme a ação selecionando **Remover** na caixa de diálogo.

Exibir informações de função de um usuário

Você pode visualizar a função que foi atribuída a um usuário e os recursos associados.

Você não pode alterar a função associada a um usuário. Se você tiver dúvidas sobre os recursos ou a função fornecida, entre em contato com o administrador da organização parceira.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Parcerias**.
3. Selecione a aba **Parceria recebida**.
4. Na página **Membros**, navegue até um membro na tabela, selecione ••• e então selecione **Ver detalhes**.
5. Na tabela, expanda a linha respectiva da organização, pasta ou projeto onde você deseja visualizar a função atribuída ao membro e selecione o número na coluna **Função**.

Fornecer acesso a recursos para usuários de parceria

Você pode conceder acesso a usuários de parceria atribuindo a eles funções específicas para pastas e projetos dentro da sua organização.

Funções necessárias

Administração de parcerias."Saiba mais sobre funções de acesso."

Uma organização parceira deve primeiro adicionar membros à parceria antes que você possa atribuir a eles funções para recursos em sua organização."Aprenda como adicionar membros a uma parceria."

Entenda as funções dos usuários da parceria

Você pode gerenciar funções para membros de organizações parceiras da mesma forma que faz para as suas. No entanto, nem todas as funções estão disponíveis para usuários de parceria. Em particular, você não pode conceder aos usuários parceiros uma função que permita atualizações de software. A atualização do software ONTAP geralmente requer acesso direto à rede.

Você pode atribuir as seguintes funções aos usuários parceiros:

- "Administrador da organização"
- "Administrador de pasta ou projeto"
- "Administrador da Federação"
- "Visualizador da Federação"
- "Administrador de backup e recuperação"
- "Visualizador de backup"
- "Restaurar administrador"
- "Clonar administrador"
- "Administrador de recuperação de desastres"
- "Administrador de failover de recuperação de desastres"
- "Administrador do aplicativo de recuperação de desastres"
- "Visualizador de recuperação de desastres"
- "Analista de suporte de operações"
- "Visualizador de classificação"

"Saiba mais sobre funções predefinidas"

Adicionar uma função a um usuário parceiro

Você fornece acesso aos recursos da sua organização adicionando uma função a um membro. Ao atribuir uma função, você especifica um recurso e uma função. Você pode atribuir mais de uma função a um usuário.

Por exemplo, se você tivesse dois projetos e quisesse que o mesmo usuário tivesse a função de administrador de backup e recuperação para ambos, seria necessário fornecer a função ao usuário para cada projeto. Da mesma forma, se você quisesse fornecer a um usuário duas funções diferentes para o mesmo projeto, seria necessário atribuir cada função separadamente.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Parcerias**.
3. Selecione a aba **Parceria iniciada**.
4. Selecione o menu de ações ••• ao lado da parceria estabelecida que você deseja visualizar e selecione **Ver detalhes**.

   A lista **Membros** exibe os membros que a organização parceira adicionou à parceria.

5. Selecione o menu de ações ••• ao lado do membro ao qual você deseja atribuir uma função e selecione **Adicionar uma função**.
6. Para adicionar uma função, conclua as etapas na caixa de diálogo:
   - **Selecione uma organização, pasta ou projeto**: Escolha o nível da hierarquia de recursos para o qual o membro deve ter permissões.

     Se você selecionar a organização ou uma pasta, o membro terá permissões para tudo o que reside na organização ou pasta.

   - **Selecione uma categoria**: Escolha uma categoria de função. "Saiba mais sobre funções de acesso" .
   - Selecione uma **Função**: Escolha uma função que forneça ao membro permissões para os recursos associados à organização, pasta ou projeto que você selecionou.
   - **Adicionar função**: se você quiser fornecer acesso a pastas ou projetos adicionais dentro da sua organização, selecione **Adicionar função**, especifique outra pasta, projeto ou categoria de função e, em seguida, selecione uma categoria de função e uma função correspondente.
7. Selecione **Adicionar novas funções**.

Alterar ou remover uma função de um usuário parceiro

Você pode alterar ou remover uma função que atribuiu a um membro de uma organização parceira.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Parcerias**.
3. Selecione a aba **Parceria iniciada**.
4. Selecione o menu de ações ••• ao lado da parceria estabelecida que você deseja visualizar e selecione **Ver detalhes**.

   A lista **Membros** exibe os membros que a organização parceira adicionou à parceria.

5. Na página **Membros**, navegue até um membro na tabela, selecione ••• e então selecione **Ver detalhes**.
6. Na tabela, expanda a linha respectiva da organização, pasta ou projeto onde você deseja alterar a função atribuída ao membro e selecione **Exibir** na coluna **Função** para visualizar as funções atribuídas a este membro.
7. Você pode alterar uma função existente para um membro ou remover uma função.
   a. Para alterar a função de um membro, selecione **Alterar** ao lado da função que deseja alterar. Você só pode alterar uma função para uma função dentro da mesma categoria de função. Por exemplo, você pode mudar de uma função de serviço de dados para outra. Confirme a alteração.
   b. Para cancelar a atribuição da função de um membro, selecione 🗑 ao lado da função para remover a atribuição da respectiva função ao membro. Você será solicitado a confirmar a remoção.

Trabalhar em uma organização parceira

Depois de receber uma função em uma organização parceira, você pode alternar para essa organização e executar ações para as quais tem permissão.

Use o menu Organização para alternar entre suas organizações e quaisquer organizações parceiras às quais você tenha acesso."Saiba mais sobre como mudar de organização e projeto."

Você poderá ver os recursos que foram compartilhados com você na organização parceira e executar ações com base na função que foi atribuída a você. Trabalhe com seu administrador de parceria para garantir que você tenha a função apropriada para os recursos que precisa acessar.

Federação de identidade

Habilitar logon único usando federação de identidade com o NetApp Console

O logon único (federação) simplifica o processo de login e aumenta a segurança, permitindo que os usuários façam login no NetApp Console usando suas credenciais corporativas. Você pode habilitar o logon único (SSO) com seu provedor de identidade (IdP) ou com o site de suporte da NetApp .

Função necessária

Administrador da organização, administrador da federação, visualizador da federação."Saiba mais sobre funções de acesso."

Federação de identidade com o site de suporte da NetApp

A federação com o site de suporte da NetApp permite que os usuários façam login no Console, no Active IQ Digital Advisor e em outros aplicativos associados usando as mesmas credenciais.

> Se você se federar com o Site de Suporte da NetApp , não poderá se federar também com seu provedor de gerenciamento de identidade corporativa. Escolha o que funciona melhor para sua organização.

Passos

1. Baixe e complete o "Formulário de solicitação de federação da NetApp" .
2. Envie o formulário para o endereço de e-mail especificado no formulário.

   A equipe de suporte da NetApp analisa e processa sua solicitação.

Configure uma conexão federada com seu provedor de identidade

Você pode configurar uma conexão federada com seu provedor de identidade para habilitar o logon único (SSO) para o Console. O processo envolve configurar seu provedor de identidade para confiar na NetApp como provedora de serviços e, em seguida, criar a conexão no Console.

> Se você configurou a federação anteriormente usando o NetApp Cloud Central (um aplicativo externo ao Console), será necessário importar sua federação usando a página Federação para gerenciá-la no Console."Aprenda como importar sua federação."

Provedores de identidade suportados

A NetApp oferece suporte aos seguintes protocolos e provedores de identidade para federação:

Protocolos

- Provedores de identidade de Linguagem de Marcação de Asserção de Segurança (SAML)
- Serviços de Federação do Active Directory (AD FS)

Provedores de identidade

- ID de entrada da Microsoft
- PingFederate

Federação com fluxo de trabalho do NetApp Console

O NetApp oferece suporte somente a SSO iniciado pelo provedor de serviços (iniciado pelo SP). Primeiro, você precisa configurar o provedor de identidade para confiar na NetApp como provedora de serviços. Em seguida, você pode criar uma conexão no Console que usa a configuração do provedor de identidade.

Você pode federar com seu domínio de e-mail ou com um domínio diferente que você possui. Para federar com um domínio diferente do seu domínio de e-mail, primeiro verifique se você é o proprietário do domínio.

Verifique seu domínio (se não estiver usando seu domínio de e-mail)

Para federar com um domínio diferente do seu domínio de e-mail, verifique se você é o proprietário dele. Você pode federar seu domínio de e-mail sem nenhuma etapa extra.

Configure seu IdP para confiar na NetApp como um provedor de serviços

Configure seu provedor de identidade para confiar no NetApp criando um novo aplicativo e fornecendo detalhes como URL do ACS, ID da entidade ou outras informações de credencial. As informações do provedor de serviços variam de acordo com o provedor de identidade, portanto, consulte a documentação do seu provedor de identidade específico para obter detalhes. Você precisará trabalhar com o administrador do seu IdP para concluir esta etapa.

Crie a conexão federada no Console

Forneça o URL ou arquivo de metadados SAML do seu provedor de identidade para criar a conexão. Essas informações são usadas para estabelecer a relação de confiança entre o Console e seu provedor de identidade. As informações fornecidas dependem do IdP que você está usando. Por exemplo, se estiver usando o Microsoft Entra ID, você precisará fornecer o ID do cliente, o segredo e o domínio.

Teste sua federação no Console

Teste sua conexão federada antes de habilitá-la. Use a opção de teste na página Federação no Console para verificar se o usuário de teste pode ser autenticado com sucesso. Se o teste for bem-sucedido, você poderá habilitar a conexão.

Habilite sua conexão no Console

Depois de habilitar a conexão, os usuários podem efetuar login no Console usando suas credenciais corporativas.

Revise o tópico do seu respectivo protocolo ou IdP para começar:

- "Configurar uma conexão federada com o AD FS"
- "Configurar uma conexão federada com o Microsoft Entra ID"
- "Configurar uma conexão federada com PingFederate"
- "Configurar uma conexão federada com um provedor de identidade SAML"

Verificação de domínio

Verifique o domínio de e-mail para sua conexão federada

Se você quiser federar com um domínio diferente do seu domínio de e-mail, primeiro você deve verificar se é o proprietário do domínio. Você só pode usar domínios verificados para federação.

Funções necessárias

A função de administrador da Federação é necessária para criar e gerenciar federações. O visualizador da Federação pode visualizar a página da Federação."Saiba mais sobre funções de acesso."

Verificar seu domínio envolve adicionar um registro TXT às configurações de DNS do seu domínio. Este registro é usado para provar que você é o proprietário do domínio e permite que o NetApp Console confie no domínio para federação. Talvez seja necessário coordenar com seu administrador de TI ou de rede para concluir esta etapa.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Federação** para visualizar a página **Federações**.
3. Selecione **Configurar nova federação**.
4. Selecione **Verificar propriedade do domínio**.
5. Digite o domínio que você deseja verificar e selecione **Continuar**.
6. Copie o registro TXT fornecido.
7. Acesse as configurações de DNS do seu domínio e configure o valor TXT que foi fornecido como um registro TXT para seu domínio. Trabalhe com seu administrador de TI ou de rede, se necessário.
8. Após o registro TXT ser adicionado, retorne ao Console e selecione **Verificar**.

Configurar federações

Federar o NetApp Console com os Serviços de Federação do Active Directory (AD FS)

Federe seus Serviços de Federação do Active Directory (AD FS) com o NetApp Console para habilitar o logon único (SSO) para o NetApp Console. Isso permite que os usuários façam login no Console usando suas credenciais corporativas.

Funções necessárias

A função de administrador da Federação é necessária para criar e gerenciar federações. O visualizador da Federação pode visualizar a página da Federação."Saiba mais sobre funções de acesso."

> Você pode federar com seu IdP corporativo ou com o site de suporte da NetApp . A NetApp recomenda escolher um ou outro, mas não ambos.

O NetApp oferece suporte somente a SSO iniciado pelo provedor de serviços (iniciado pelo SP). Primeiro, configure o provedor de identidade para confiar no NetApp Console como um provedor de serviços. Em seguida, crie uma conexão no Console usando a configuração do seu provedor de identidade.

Você pode configurar a federação com seu servidor AD FS para habilitar o logon único (SSO) para o NetApp Console. O processo envolve configurar o AD FS para confiar no Console como um provedor de serviços e, em seguida, criar a conexão no NetApp Console.

Antes de começar

- É necessária uma conta IdP com privilégios administrativos. Coordene com seu administrador do IdP para concluir as etapas.
- Identifique o domínio que você deseja usar para federação. Você pode usar seu domínio de e-mail ou um domínio diferente que seja seu. Se você quiser usar um domínio diferente do seu domínio de e-mail, primeiro verifique o domínio no Console. Você pode fazer isso seguindo os passos no"Verifique seu domínio no NetApp Console" tópico.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Federação** para visualizar a página **Federações**.
3. Selecione **Configurar nova federação**.
4. Insira os detalhes do seu domínio:
   a. Escolha se deseja usar um domínio verificado ou seu domínio de e-mail. O domínio de e-mail é o domínio associado à conta com a qual você está conectado.
   b. Digite o nome da federação que você está configurando.
   c. Se você escolher um domínio verificado, selecione o domínio na lista.
5. Selecione **Avançar**.
6. Para seu método de conexão, escolha **Protocolo** e depois selecione **Serviços de Federação do Active Directory (AD FS)**.
7. Selecione **Avançar**.
8. Crie uma Relying Party Trust no seu servidor AD FS. Você pode usar o PowerShell ou configurá-lo manualmente no seu servidor AD FS. Consulte a documentação do AD FS para obter detalhes sobre como criar uma confiança de terceira parte confiável.
   a. Crie a confiança usando o PowerShell usando o seguinte script:

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
auth0/master/AD FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
cloud-account.auth0.com/login/callback"
```

b. Como alternativa, você pode criar a confiança manualmente no console de gerenciamento do AD FS. Use os seguintes valores do NetApp Console ao criar a confiança:

   - Ao criar o Relying Trust Identifier, use o valor **YOUR_TENANT**: `netapp-cloud-account`
   - Ao selecionar **Ativar suporte para WS-Federation**, use o valor **YOUR_AUTH0_DOMAIN**: `netapp-cloud-account.auth0.com`

c. Depois de criar a confiança, copie o URL de metadados do seu servidor AD FS ou baixe o arquivo de metadados da federação. Você precisará deste URL ou arquivo para concluir a conexão no Console.

A NetApp recomenda usar o URL de metadados para permitir que o NetApp Console recupere automaticamente a configuração mais recente do AD FS. Se você baixar o arquivo de metadados da federação, precisará atualizá-lo manualmente no NetApp Console sempre que houver alterações na configuração do AD FS.

9. Retorne ao Console e selecione **Avançar** para criar a conexão.
10. Crie a conexão com o AD FS.
    a. Insira o **URL do AD FS** que você copiou do seu servidor AD FS na etapa anterior ou carregue o arquivo de metadados da federação que você baixou do seu servidor AD FS.
11. Selecione **Criar conexão**. A criação da conexão pode levar alguns segundos.
12. Selecione **Avançar**.
13. Selecione **Testar conexão** para testar sua conexão. Você será direcionado para uma página de login para seu servidor IdP. Efetue login com suas credenciais do IdP para concluir o teste e retorne ao Console para habilitar a conexão.
14. Selecione **Avançar**.
15. Na página **Habilitar federação**, revise os detalhes da federação e selecione **Habilitar federação**.
16. Selecione **Concluir** para finalizar o processo.

Depois de habilitar a federação, os usuários podem fazer login no NetApp Console usando suas credenciais corporativas.

Federar NetApp Console com Microsoft Entra ID

Federe com seu provedor de IdP do Microsoft Entra ID para habilitar o logon único (SSO) para o NetApp Console. Isso permite que os usuários façam login usando suas credenciais corporativas.

Funções necessárias

A função de administrador da Federação é necessária para criar e gerenciar federações. O visualizador da Federação pode visualizar a página da Federação."Saiba mais sobre funções de acesso."

Você pode federar com seu IdP corporativo ou com o site de suporte da NetApp . A NetApp recomenda escolher um ou outro, mas não ambos.

O NetApp oferece suporte somente a SSO iniciado pelo provedor de serviços (iniciado pelo SP). Primeiro, você precisa configurar o provedor de identidade para confiar na NetApp como provedora de serviços. Em seguida, você pode criar uma conexão no Console que usa a configuração do provedor de identidade.

Você pode configurar uma conexão federada com o Microsoft Entra ID para habilitar o logon único (SSO) para o Console. O processo envolve configurar seu ID do Microsoft Entra para confiar no Console como um

provedor de serviços e, em seguida, criar a conexão no Console.

Antes de começar

- É necessária uma conta IdP com privilégios administrativos. Coordene com seu administrador do IdP para concluir as etapas.
- Identifique o domínio que você deseja usar para federação. Você pode usar seu domínio de e-mail ou um domínio diferente que seja seu. Se você quiser usar um domínio diferente do seu domínio de e-mail, primeiro verifique o domínio no Console. Você pode fazer isso seguindo os passos no"Verifique seu domínio no NetApp Console" tópico.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Federação** para visualizar a página **Federações**.
3. Selecione **Configurar nova federação**.

Detalhes do domínio

1. Insira os detalhes do seu domínio:
   a. Escolha se deseja usar um domínio verificado ou seu domínio de e-mail. O domínio de e-mail é o domínio associado à conta com a qual você está conectado.
   b. Digite o nome da federação que você está configurando.
   c. Se você escolher um domínio verificado, selecione o domínio na lista.
2. Selecione **Avançar**.

Método de conexão

1. Para seu método de conexão, escolha **Provedor** e depois selecione **Microsoft Entra ID**.
2. Selecione **Avançar**.

Instruções de configuração

1. Configure seu ID Microsoft Entra para confiar na NetApp como provedora de serviços. Você precisa executar esta etapa no seu servidor Microsoft Entra ID.
   a. Use os seguintes valores ao registrar seu aplicativo Microsoft Entra ID para confiar no Console:
      - Para o **URL de redirecionamento**, use `https://services.cloud.netapp.com`
      - Para o **URL de resposta**, use `https://netapp-cloud-account.auth0.com/login/callback`
   b. Crie um segredo do cliente para seu aplicativo Microsoft Entra ID. Você precisará fornecer o ID do cliente, o segredo do cliente e o nome de domínio do Entra ID para concluir a federação.
2. Retorne ao Console e selecione **Avançar** para criar a conexão.

Criar conexão

1. Crie a conexão com o Microsoft Entra ID
   a. Insira o ID do cliente e o segredo do cliente que você criou na etapa anterior.
   b. Digite o nome de domínio do ID do Microsoft Entra.

2. Selecione **Criar conexão**. O sistema cria a conexão em poucos segundos.

Teste e habilite a conexão

1. Selecione **Avançar**.
2. Selecione **Testar conexão** para testar sua conexão. Você será direcionado para uma página de login para seu servidor IdP. Efetue login com suas credenciais do IdP para concluir o teste e retorne ao Console para habilitar a conexão.
3. Selecione **Avançar**.
4. Na página **Habilitar federação**, revise os detalhes da federação e selecione **Habilitar federação**.
5. Selecione **Concluir** para finalizar o processo.

Depois de habilitar a federação, os usuários podem fazer login no NetApp Console usando suas credenciais corporativas.

Federar o NetApp Console com o PingFederate

Federe com seu provedor PingFederate IdP para habilitar o logon único (SSO) para o NetApp Console. Isso permite que os usuários façam login usando suas credenciais corporativas.

Funções necessárias

A função de administrador da Federação é necessária para criar e gerenciar federações. O visualizador da Federação pode visualizar a página da Federação."Saiba mais sobre funções de acesso."

Você pode federar com seu IdP corporativo ou com o site de suporte da NetApp . A NetApp recomenda escolher um ou outro, mas não ambos.

O NetApp oferece suporte somente a SSO iniciado pelo provedor de serviços (iniciado pelo SP). Primeiro, você precisa configurar o provedor de identidade para confiar na NetApp como provedora de serviços. Em seguida, você pode criar uma conexão no Console que usa a configuração do provedor de identidade.

Você pode configurar uma conexão federada com o PingFederate para habilitar o logon único (SSO) para o Console. O processo envolve configurar seu servidor PingFederate para confiar no Console como um provedor de serviços e, em seguida, criar a conexão no Console.

Antes de começar

- É necessária uma conta IdP com privilégios administrativos. Coordene com seu administrador do IdP para concluir as etapas.
- Identifique o domínio que você deseja usar para federação. Você pode usar seu domínio de e-mail ou um domínio diferente que seja seu. Se você quiser usar um domínio diferente do seu domínio de e-mail, primeiro verifique o domínio no Console. Você pode fazer isso seguindo os passos no"Verifique seu domínio no NetApp Console" tópico.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Federação** para visualizar a página **Federações**.
3. Selecione **Configurar nova federação**.
4. Insira os detalhes do seu domínio:

a. Escolha se deseja usar um domínio verificado ou seu domínio de e-mail. O domínio de e-mail é o domínio associado à conta com a qual você está conectado.

b. Digite o nome da federação que você está configurando.

c. Se você escolher um domínio verificado, selecione o domínio na lista.

5. Selecione **Avançar**.
6. Para seu método de conexão, escolha **Provedor** e depois selecione **PingFederate**.
7. Selecione **Avançar**.
8. Configure seu servidor PingFederate para confiar na NetApp como provedora de serviços. Você precisa executar esta etapa no seu servidor PingFederate.

   a. Use os seguintes valores ao configurar o PingFederate para confiar no NetApp Console:

      - Para o **URL de resposta** ou **URL do serviço de consumidor de declaração (ACS)**, use `https://netapp-cloud-account.auth0.com/login/callback`
      - Para o **URL de logout**, use `https://netapp-cloud-account.auth0.com/logout`
      - Para **ID do público/entidade**, use `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` onde <fed-domain-name-pingfederate> é o nome de domínio da federação. Por exemplo, se o seu domínio for `example.com` , o ID do público/entidade seria `urn:auth0:netappcloud-account:fed-example-com-pingfederate` .

   b. Copie a URL do servidor PingFederate. Você precisará deste URL ao criar a conexão no Console.

   c. Baixe o certificado X.509 do seu servidor PingFederate. Ele precisa estar no formato PEM codificado em Base64 (.pem, .crt, .cer).

9. Retorne ao Console e selecione **Avançar** para criar a conexão.
10. Crie a conexão com PingFederate

    a. Digite a URL do servidor PingFederate que você copiou na etapa anterior.

    b. Carregue o certificado de assinatura X.509. O certificado deve estar no formato PEM, CER ou CRT.

11. Selecione **Criar conexão**. O sistema cria a conexão em poucos segundos.
12. Selecione **Avançar**.
13. Selecione **Testar conexão** para testar sua conexão. Você será direcionado para uma página de login para seu servidor IdP. Efetue login com suas credenciais do IdP para concluir o teste e retorne ao Console para habilitar a conexão.
14. Selecione **Avançar**.
15. Na página **Habilitar federação**, revise os detalhes da federação e selecione **Habilitar federação**.
16. Selecione **Concluir** para finalizar o processo.

Depois de habilitar a federação, os usuários podem fazer login no NetApp Console usando suas credenciais corporativas.

Federe com um provedor de identidade SAML

Federe com seu provedor SAML 2.0 IdP para habilitar o logon único (SSO) para o NEtApp Console. Isso permite que os usuários façam login usando suas credenciais corporativas.

Função necessária

A função de administrador da Federação é necessária para criar e gerenciar federações. O visualizador da Federação pode visualizar a página da Federação."Saiba mais sobre funções de acesso."

> Você pode federar com seu IdP corporativo ou com o site de suporte da NetApp . Você não pode federar com ambos.

O NetApp oferece suporte somente a SSO iniciado pelo provedor de serviços (iniciado pelo SP). Primeiro, você precisa configurar o provedor de identidade para confiar na NetApp como provedora de serviços. Em seguida, você pode criar uma conexão no Console que usa a configuração do provedor de identidade.

Você pode configurar uma conexão federada com seu provedor SAML 2.0 para habilitar o logon único (SSO) para o Console. O processo envolve configurar seu provedor para confiar na NetApp como provedora de serviços e, em seguida, criar a conexão no Console.

Antes de começar

- É necessária uma conta IdP com privilégios administrativos. Coordene com seu administrador do IdP para concluir as etapas.
- Identifique o domínio que você deseja usar para federação. Você pode usar seu domínio de e-mail ou um domínio diferente que seja seu. Se você quiser usar um domínio diferente do seu domínio de e-mail, primeiro verifique o domínio no Console. Você pode fazer isso seguindo os passos no"Verifique seu domínio no NetApp Console" tópico.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Federação** para visualizar a página **Federações**.
3. Selecione **Configurar nova federação**.
4. Insira os detalhes do seu domínio:
   a. Escolha se deseja usar um domínio verificado ou seu domínio de e-mail. O domínio de e-mail é o domínio associado à conta com a qual você está conectado.
   b. Digite o nome da federação que você está configurando.
   c. Se você escolher um domínio verificado, selecione o domínio na lista.
5. Selecione **Avançar**.
6. Para seu método de conexão, escolha **Protocolo** e depois selecione **Provedor de identidade SAML**.
7. Selecione **Avançar**.
8. Configure seu provedor de identidade SAML para confiar na NetApp como provedora de serviços. Você precisa executar esta etapa no servidor do seu provedor SAML.
   a. Certifique-se de que seu IdP tenha o atributo `email` definido como o endereço de e-mail do usuário. Isso é necessário para que o Console identifique os usuários corretamente:

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">
        <saml:AttributeValue xsi:type="xs:string">
email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

b. Use os seguintes valores ao registrar seu aplicativo SAML no Console:

- Para o **URL de resposta** ou **URL do serviço de consumidor de declaração (ACS)**, use `https://netapp-cloud-account.auth0.com/login/callback`
- Para o **URL de logout**, use `https://netapp-cloud-account.auth0.com/logout`
- Para **ID do público/entidade**, use `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` onde <fed-domain-name-saml> é o nome de domínio que você deseja usar para federação. Por exemplo, se o seu domínio for `example.com` , o ID do público/entidade seria `urn:auth0:netapp-cloud-account:fed-example-com-samlp` .

c. Depois de criar a confiança, copie os seguintes valores do servidor do seu provedor SAML:

- URL de login
- URL de saída (opcional)

d. Baixe o certificado X.509 do servidor do seu provedor SAML. Precisa estar no formato PEM, CER ou CRT.

9. Retorne ao Console e selecione **Avançar** para criar a conexão.
10. Crie a conexão com SAML.
    a. Digite o **URL de login** do seu servidor SAML.
    b. Faça upload do certificado X.509 que você baixou do servidor do seu provedor SAML.
    c. Opcionalmente, insira o **URL de saída** do seu servidor SAML.
11. Selecione **Criar conexão**. O sistema cria a conexão em poucos segundos.
12. Selecione **Avançar**.
13. Selecione **Testar conexão** para testar sua conexão. Você será direcionado para uma página de login para seu servidor IdP. Efetue login com suas credenciais do IdP para concluir o teste e retorne ao Console para habilitar a conexão.
14. Selecione **Avançar**.
15. Na página **Habilitar federação**, revise os detalhes da federação e selecione **Habilitar federação**.
16. Selecione **Concluir** para finalizar o processo.

Depois de habilitar a federação, os usuários podem fazer login no NetApp Console usando suas credenciais corporativas.

Gerenciar federações no NetApp Console

Você pode gerenciar sua federação no NetApp Console. Você pode desativá-lo, atualizar credenciais expiradas e também desativá-lo caso não precise mais dele.

Se você configurou a federação usando o NetApp Cloud Central, importe-a por meio da página **Federação** para gerenciá-la no Console."Aprenda como importar sua federação"

Você também pode adicionar um domínio verificado a uma federação existente, o que permite usar vários domínios para sua conexão federada.

Eventos de gerenciamento de federação, como habilitar, desabilitar e atualizar federações, são exibidos na Linha do tempo."Saiba mais sobre o monitoramento de operações no NetApp Console."

Funções necessárias

A função de administrador da Federação é necessária para criar e gerenciar federações. O visualizador da Federação pode visualizar a página da Federação."Saiba mais sobre funções de acesso."

Habilitar uma federação

Se você criou uma federação, mas ela não está habilitada, você pode habilitá-la na página **Federação**. Habilitar uma federação permite que usuários associados à federação façam login no Console usando suas credenciais corporativas. Crie e teste a federação com sucesso antes de habilitá-la.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione o menu de ações ••• ao lado da federação que você deseja habilitar e selecione **Habilitar**.

Adicionar um domínio verificado a uma federação existente

Você pode adicionar um domínio verificado a uma federação existente no Console para usar vários domínios com o mesmo provedor de identidade (IdP).

Você já deve ter verificado o domínio no Console antes de poder adicioná-lo a uma federação. Se você ainda não verificou o domínio, pode fazê-lo seguindo as etapas em"Verifique seu domínio no Console" .

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione o menu de ações ⋮ ao lado da federação à qual você deseja adicionar um domínio verificado e selecione **Atualizar domínios**. A caixa de diálogo **Atualizar domínios** exibe o domínio já associado a esta federação.
4. Selecione um domínio verificado na lista de domínios disponíveis.
5. Selecione **Atualizar**. Novos usuários de domínio podem obter acesso ao Console federado em 30 segundos.

Atualizando uma conexão federada que está expirando

Você pode atualizar os detalhes de uma federação no Console. Por exemplo, você precisará atualizar a federação se as credenciais, como um certificado ou segredo do cliente, expirarem. Quando necessário, atualize a data de notificação para lembrá-lo de atualizar a conexão antes que ela expire.

Atualize o Console antes de atualizar seu IdP para evitar problemas de login. Permaneça conectado ao Console durante o processo.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione o menu de ações (três pontos verticais) ao lado da federação que você deseja atualizar e selecione **Atualizar federação**.
4. Atualize os detalhes da federação conforme necessário.
5. Selecione **Atualizar**.

Testar uma federação existente

Teste a conexão de uma federação existente para verificar se ela funciona. Isso pode ajudar você a identificar quaisquer problemas com a federação e solucioná-los.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione o menu de ações ao lado da federação à qual você deseja adicionar um domínio verificado e selecione **Testar conexão**.
4. Selecione **Testar**. O sistema solicita que você faça login com suas credenciais corporativas. Se a conexão for bem-sucedida, você será redirecionado para o NetApp Console. Se a conexão falhar, você verá uma mensagem de erro indicando o problema com a federação.
5. Selecione **Concluído** para retornar à aba **Federação**.

Desabilitar uma federação

Se você não precisar mais de uma federação, poderá desativá-la. Isso impede que usuários associados à federação façam login no Console usando suas credenciais corporativas. Você pode reativar a federação mais tarde, se necessário.

Desabilite uma federação antes de excluí-la, como ao desativar o IdP ou descontinuar a federação. Isso permite que você o reative mais tarde, se necessário.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione o menu de ações ao lado da federação à qual você deseja adicionar um domínio verificado e selecione **Desativar**.

Excluir uma federação

Se você não precisar mais de uma federação, poderá excluí-la. Isso remove a federação e impede que qualquer usuário associado a ela faça login no Console usando suas credenciais corporativas. Por exemplo, se o IdP estiver sendo desativado ou se a federação não for mais necessária.

Não é possível recuperar uma federação após excluí-la. Você deve criar uma nova federação.

Você deve desabilitar uma federação antes de poder excluí-la. Não é possível recuperar uma federação após excluí-la.

Passos

1. Selecione **Administração > Identidade e acesso** .
2. Selecione **Federações** para visualizar a página **Federações**.
3. Selecione o menu de ações ao lado da federação à qual você deseja adicionar um domínio verificado e selecione **Excluir**.

Importe sua federação para o NetApp Console

Se você tiver configurado a federação anteriormente por meio do NetApp Cloud Central (um aplicativo externo ao NetApp Console), a página Federação solicitará que você importe sua conexão federada existente para o Console para que você possa gerenciá-la na nova interface. Você pode então aproveitar os aprimoramentos mais recentes sem precisar recriar sua conexão federada.

Depois de importar sua federação existente, você pode gerenciá-la na página **Federações** ."Saiba mais sobre como gerenciar federações."

Função necessária

Administrador da organização ou administrador da federação."Saiba mais sobre funções de acesso."

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione **Importar Federação**.

Agentes de console

Manter a VM do agente do console e o sistema operacional

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

Se você já tem um agente, você deve estar ciente de"alterações nos sistemas operacionais Linux suportados" .

Patches do sistema operacional e o agente

Aplique patches de segurança do sistema operacional sem interromper os serviços do host do agente.

Tipo de VM ou instância

Se você criar um agente do Console a partir do Console, ele implantará uma instância de VM no seu provedor de nuvem com uma configuração padrão. Depois de criar o agente, não mude para uma instância de VM menor com menos CPU ou RAM.

A tabela a seguir lista os requisitos de CPU e RAM:

CPU
: 8 núcleos ou 8 vCPUs

BATER
: 32 GB

"Saiba mais sobre a configuração padrão do agente" .

Monitore o agente

O Console notifica você quando a VM do agente não está íntegra, incluindo problemas de espaço em disco, RAM e CPU. Monitore essas notificações no Centro de Notificações do Console ou configure notificações por e-mail. Aumentos ocasionais no espaço em disco, na memória ou no uso da CPU são normais, mas se isso acontecer com frequência, você deve tomar medidas para resolver.

Por exemplo, o Console notifica você quando um recurso do agente (CPU, RAM ou espaço em disco) excede 90% de sua capacidade total por 30 minutos consecutivos. Depois, se o uso do recurso cair abaixo desse limite, a notificação será exibida como resolvida (verde) na Central de Notificações.

Entre em contato com o suporte da NetApp se tiver dúvidas sobre como modificar sua VM do agente.

"Saber mais."

Notificação	Ação necessária
O espaço em disco é muito alto	"Revise o artigo da Base de conhecimento da NetApp" .
O uso da CPU está muito alto	Aumente o tamanho da CPU da VM do agente no seu provedor de nuvem ou no local, dependendo de onde você a instalou. Como alternativa, crie agentes adicionais e distribua a carga de trabalho entre vários agentes. A utilização de RAM pode variar de acordo com seu ambiente, cargas de trabalho ONTAP , número de sistemas Cloud Volumes ONTAP e os serviços de dados que você está usando.

Notificação	Ação necessária
O uso de RAM é muito alto	Aumente a RAM da VM do agente no seu provedor de nuvem ou no local, dependendo de onde você a instalou. Como alternativa, crie agentes adicionais e distribua a carga de trabalho entre vários agentes. A utilização de RAM pode variar de acordo com seu ambiente, cargas de trabalho ONTAP , número de sistemas Cloud Volumes ONTAP e os serviços de dados que você está usando.

Parando e iniciando a VM do agente

Se necessário, pare e inicie a VM do agente usando o console do seu provedor de nuvem ou procedimentos locais padrão.

"Esteja ciente de que o agente do Console deve estar operacional o tempo todo" .

Conectar à VM Linux

Se você precisar se conectar à VM Linux na qual o agente é executado, use as opções de conectividade do seu provedor de nuvem.

AWS

Ao criar a instância do agente na AWS, forneça uma chave de acesso e uma chave secreta da AWS. Você pode usar esse par de chaves para fazer SSH na instância. Use o nome de usuário 'ubuntu' para a instância do EC2 Linux. Para agentes criados antes de maio de 2023, use o nome de usuário 'ec2-user'.

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

Azul

Ao criar a VM do agente no Azure, você especifica um nome de usuário e escolhe autenticar com uma senha ou chave pública SSH. Use o método de autenticação que você escolheu para se conectar à VM.

"Documentação do Azure: SSH na sua VM"

Google Cloud

Não é possível especificar um método de autenticação ao criar um agente no Google Cloud. No entanto, você pode se conectar à instância da VM Linux usando o Google Cloud Console ou o Google Cloud CLI (gcloud).

"Google Cloud Docs: conectar-se a VMs Linux"

Alterar o endereço IP de um agente

Você pode alterar os endereços IP internos e públicos da instância do agente atribuída pelo seu provedor de nuvem, se necessário.

Passos

1. Siga as instruções do seu provedor de nuvem para alterar o endereço IP local ou o endereço IP público (ou ambos) da instância do agente.
2. Reinicie a instância do agente para registrar um novo endereço IP público no Console.
3. Se você alterou o endereço IP privado, atualize o local de backup dos arquivos de configuração do Cloud

Volumes ONTAP para que os backups sejam enviados para o novo endereço IP privado no agente.

Atualize o local de backup para cada sistema Cloud Volumes ONTAP .

a. Na CLI do Cloud Volumes ONTAP , defina o nível de privilégio como avançado:

```
set -privilege advanced
```

b. Execute o seguinte comando para exibir o destino de backup atual:

```
system configuration backup settings show
```

c. Execute o seguinte comando para atualizar o endereço IP do destino de backup:

```
system configuration backup settings modify -destination <target-
location>
```

Editar URIs de um agente

Você pode adicionar e remover o Uniform Resource Identifier (URI) de um agente.

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione o menu de ação para um agente do Console e selecione **Editar agente**.

   O agente do Console deve estar ativo para editá-lo.

3. Expanda a barra **URIs do agente** para visualizar os URIs do agente.
4. Adicione e remova URIs e selecione **Aplicar**.

Manter um host VCenter ou ESXi para o agente do Console

Você pode fazer alterações no seu host VCenter ou ESXi existente depois de implantar o agente do Console. Por exemplo, você pode aumentar a CPU ou a RAM da instância da VM que hospeda o agente do Console.

Execute estas tarefas de manutenção usando o console da Web da VM:

- Aumentar o tamanho do disco
- Reinicie o agente
- Atualizar rotas estáticas
- Atualizar domínios de pesquisa

Limitações

A atualização do agente pelo console ainda não é suportada. Além disso, você só pode visualizar informações

sobre o endereço IP, DNS e gateways.

Acesse o console de manutenção da VM

Você pode acessar o Console de manutenção a partir do cliente VSphere.

Passos

1. Abra o cliente VSphere e faça login no seu VCenter.
2. Selecione a instância da VM que hospeda o agente do Console.
3. Selecione **Iniciar Console Web**.
4. Efetue login na instância da VM usando o nome de usuário e a senha que você especificou quando criou a instância da VM. O nome de usuário é `maint` e a senha é aquela que você especificou quando criou a instância da VM.

Alterar a senha do usuário de manutenção

Você pode alterar a senha para o `maint` usuário.

Passos

1. Abra o cliente VSphere e faça login no seu VCenter.
2. Selecione a instância da VM que hospeda o agente do Console.
3. Selecione **Iniciar Console Web**.
4. Efetue login na instância da VM usando o nome de usuário e a senha que você especificou quando criou a instância da VM. O nome de usuário é `maint` e a senha é aquela que você especificou quando criou a instância da VM.
5. Digitar `1` para ver o `System Configuration` menu.
6. Digitar `1` para alterar a senha do usuário de manutenção e seguir as instruções na tela.

Aumente a CPU ou a RAM da instância da VM

Você pode aumentar a CPU ou a RAM da instância da VM que hospeda o agente do Console.

Edite as configurações da instância da VM no seu host VCenter ou ESXi e use o Console de manutenção para aplicar as alterações.

Etapas no cliente VSphere

1. Abra o cliente VSphere e faça login no seu VCenter.
2. Selecione a instância da VM que hospeda o agente do Console.
3. Clique com o botão direito do mouse na instância da VM e selecione **Editar configurações**.
4. Aumente o espaço do disco rígido usado para /opt ou a partição /var.
   a. Selecione **Disco Rígido 2** para aumentar o espaço no disco rígido usado para /opt.
   b. Selecione **Disco Rígido 3** para aumentar o espaço no disco rígido usado para /var.
5. Salve suas alterações.

Etapas no console de manutenção

1. Abra o cliente VSphere e faça login no seu VCenter.

2. Selecione a instância da VM que hospeda o agente do Console.
3. Selecione **Iniciar Console Web**.
4. Efetue login na instância da VM usando o nome de usuário e a senha que você especificou quando criou a instância da VM. O nome de usuário é `maint` e a senha é aquela que você especificou quando criou a instância da VM.
5. Digitar `1 to view the `System Configuration` menu.
6. Digitar `2` e siga as instruções na tela. O console procura novas configurações e aumenta o tamanho das partições.

Exibir configurações de rede para a VM do agente

Visualize as configurações de rede da VM do agente no cliente VSphere para confirmar ou solucionar problemas de rede. Você só pode visualizar (não atualizar) as seguintes configurações de rede: endereço IP e detalhes de DNS.

Passos

1. Abra o cliente VSphere e faça login no seu VCenter.
2. Selecione a instância da VM que hospeda o agente do Console.
3. Selecione **Iniciar Console Web**.
4. Efetue login na instância da VM usando o nome de usuário e a senha que você especificou quando criou a instância da VM. O nome de usuário é `maint` e a senha é aquela que você especificou quando criou a instância da VM.
5. Digitar `2` para ver o `Network Configuration` menu.
6. Digite um número entre 1 e 6 para visualizar as configurações de rede correspondentes.

Atualizar as rotas estáticas para a VM do agente

Adicione, atualize ou remova rotas estáticas para a VM do agente, conforme necessário.

Passos

1. Abra o cliente VSphere e faça login no seu VCenter.
2. Selecione a instância da VM que hospeda o agente do Console.
3. Selecione **Iniciar Console Web**.
4. Efetue login na instância da VM usando o nome de usuário e a senha que você especificou quando criou a instância da VM. O nome de usuário é `maint` e a senha é aquela que você especificou quando criou a instância da VM.
5. Digitar `2` para ver o `Network Configuration` menu.
6. Digitar `7` para atualizar rotas estáticas e seguir as instruções na tela.
7. Pressione Enter.
8. Opcionalmente, faça alterações adicionais.
9. Digitar `9` para confirmar suas alterações.

Atualizar as configurações de pesquisa de domínio para a VM do agente

Você pode atualizar as configurações do domínio de pesquisa para a VM do agente.

Passos

1. Abra o cliente VSphere e faça login no seu VCenter.
2. Selecione a instância da VM que hospeda o agente do Console.
3. Selecione **Iniciar Console Web**.
4. Efetue login na instância da VM usando o nome de usuário e a senha que você especificou quando criou a instância da VM. O nome de usuário é `maint` e a senha é aquela que você especificou quando criou a instância da VM.
5. Digitar `2`` para ver o `Network Configuration` menu.
6. Digitar `8` para atualizar as configurações de pesquisa de domínio e seguir as instruções na tela.
7. Pressione Enter.
8. Opcionalmente, faça alterações adicionais.
9. Digitar `9` para confirmar suas alterações.

Acesse as ferramentas de diagnóstico do agente

Acesse ferramentas de diagnóstico para solucionar problemas com o agente do Console. O Suporte da NetApp pode solicitar que você faça isso ao solucionar problemas.

Passos

1. Abra o cliente VSphere e faça login no seu VCenter.
2. Selecione a instância da VM que hospeda o agente do Console.
3. Selecione **Iniciar Console Web**.
4. Efetue login na instância da VM usando o nome de usuário e a senha que você especificou quando criou a instância da VM. O nome de usuário é `maint` e a senha é aquela que você especificou quando criou a instância da VM.
5. Digitar `3` para visualizar o menu Suporte e Diagnóstico.
6. Digitar `1` para acessar as ferramentas de diagnóstico e seguir as instruções na tela. + Por exemplo, você pode verificar se todos os serviços do agente estão em execução. "Verifique o status do agente do Console" .

Acesse as ferramentas de diagnóstico do agente remotamente

Você pode acessar ferramentas de diagnóstico remotamente com uma ferramenta como o Putty. Habilite o acesso SSH à VM do agente atribuindo uma senha de uso único.

O acesso SSH habilita recursos avançados do terminal, como copiar e colar.

Passos

1. Abra o cliente VSphere e faça login no seu VCenter.
2. Selecione a instância da VM que hospeda o agente do Console.
3. Selecione **Iniciar Console Web**.
4. Efetue login na instância da VM usando o nome de usuário e a senha que você especificou quando criou a instância da VM. O nome de usuário é `maint` e a senha é aquela que você especificou quando criou a instância da VM.
5. Digitar `3` para ver o `Support and Diagnostics` menu.

6. Digitar `2` para acessar as ferramentas de diagnóstico e seguir as instruções na tela para configurar uma senha de uso único que expira em 24 horas.
7. Use uma ferramenta SSH como o Putty para se conectar à VM do agente usando o nome de usuário `diag` e a senha de uso único que você configurou.

Instalar um certificado assinado por CA para acesso ao console baseado na web

Quando você usa o NetApp Console no modo restrito, a interface do usuário pode ser acessada na máquina virtual do agente do Console implantada na sua região de nuvem ou no local. Por padrão, o Console usa um certificado SSL autoassinado para fornecer acesso HTTPS seguro ao console baseado na Web em execução no agente do Console.

Se exigido pela sua empresa, você pode instalar um certificado assinado por uma autoridade de certificação (CA), que fornece melhor proteção de segurança do que um certificado autoassinado. Após instalar o certificado, o Console usa o certificado assinado pela CA quando os usuários acessam o console baseado na Web.

Instalar um certificado HTTPS

Instale um certificado assinado por uma CA para acesso seguro ao console baseado na Web em execução no agente do Console.

Sobre esta tarefa

Você pode instalar o certificado usando uma das seguintes opções:

- Gere uma solicitação de assinatura de certificado (CSR) no Console, envie a solicitação de certificado para uma CA e instale o certificado assinado pela CA no agente do Console.

  O par de chaves que o Console usa para gerar o CSR é armazenado internamente no agente do Console. O Console recupera automaticamente o mesmo par de chaves (chave privada) quando você instala o certificado no agente do Console.

- Instale um certificado assinado pela CA que você já tenha.

  Com esta opção, o CSR não é gerado pelo Console. Você gera o CSR separadamente e armazena a chave privada externamente. Você fornece a chave privada ao Console quando instala o certificado.

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione o menu de ação para um agente do Console e selecione **Configuração HTTPS**.

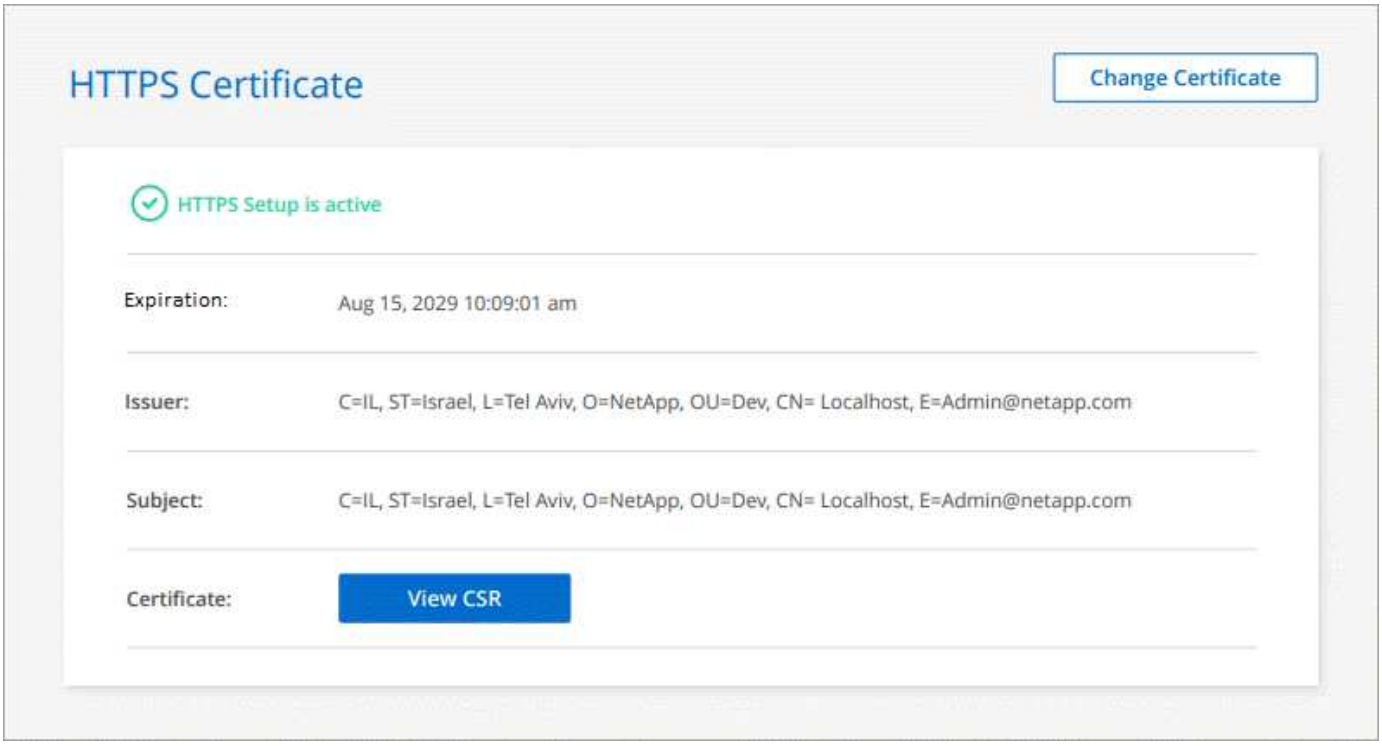
   O agente do Console deve estar ativo para editá-lo.

3. Na página Configuração de HTTPS, instale um certificado gerando uma solicitação de assinatura de certificado (CSR) ou instalando seu próprio certificado assinado pela CA:

Opção	Descrição
Gerar um CSR	a. Insira o nome do host ou DNS do host do agente do Console (seu Nome Comum) e selecione **Gerar CSR**. O Console exibe uma solicitação de assinatura de certificado. b. Use o CSR para enviar uma solicitação de certificado SSL a uma CA. O certificado deve usar o formato X.509 codificado em Base 64 do Privacy Enhanced Mail (PEM). c. Carregue o arquivo de certificado e selecione **Instalar**.
Instale seu próprio certificado assinado pela CA	a. Selecione **Instalar certificado assinado pela CA**. b. Carregue o arquivo de certificado e a chave privada e selecione **Instalar**. O certificado deve usar o formato X.509 codificado em Base 64 do Privacy Enhanced Mail (PEM).

Resultado

O agente do Console agora usa o certificado assinado pela CA para fornecer acesso HTTPS seguro. A imagem a seguir mostra um agente configurado para acesso seguro:



Renovar o certificado HTTPS do Console

Você deve renovar o certificado HTTPS do agente antes que ele expire para garantir acesso seguro. Se você não renovar o certificado antes que ele expire, um aviso será exibido quando os usuários acessarem o console da web usando HTTPS.

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione o menu de ação para um agente do Console e selecione **Configuração HTTPS**.

   Detalhes sobre o certificado são exibidos, incluindo a data de validade.

3. Selecione **Alterar certificado** e siga as etapas para gerar um CSR ou instalar seu próprio certificado assinado pela CA.

Configurar um agente de console para usar um servidor proxy

Se suas políticas corporativas exigirem que você use um servidor proxy para todas as comunicações com a Internet, será necessário configurar seus agentes para usar esse servidor proxy. Se você não configurou um agente do Console para usar um servidor proxy durante a instalação, poderá configurá-lo para usar esse servidor proxy a qualquer momento.

O servidor proxy do agente permite acesso de saída à Internet sem um IP público ou gateway NAT. O servidor proxy fornece conectividade de saída somente para o agente do Console, não para sistemas Cloud Volumes ONTAP .

Se os sistemas Cloud Volumes ONTAP não tiverem acesso de saída à Internet, o Console os configurará para usar o servidor proxy do agente do Console. Você deve garantir que o grupo de segurança do agente do Console permita conexões de entrada pela porta 3128. Abra esta porta após implantar o agente do Console.

Se o próprio agente do Console não tiver uma conexão de saída com a Internet, os sistemas Cloud Volumes ONTAP não poderão usar o servidor proxy configurado.

Configurações suportadas

- Servidores proxy transparentes são suportados por agentes que atendem sistemas Cloud Volumes ONTAP . Se você usar serviços de dados da NetApp com o Cloud Volumes ONTAP, crie um agente dedicado para o Cloud Volumes ONTAP onde você pode usar um servidor proxy transparente.
- Servidores proxy explícitos são suportados por todos os agentes, incluindo aqueles que gerenciam sistemas Cloud Volumes ONTAP e aqueles que gerenciam serviços de dados NetApp .
- HTTP e HTTPS.
- O servidor proxy pode residir na nuvem ou na sua rede.

> Depois de configurar um proxy, você não poderá alterar o tipo de proxy. Se precisar alterar o tipo de proxy, remova o agente do Console e adicione um novo agente com o novo tipo de proxy.

Habilitar um proxy explícito em um agente do Console

Quando você configura um agente do Console para usar um servidor proxy, esse agente e os sistemas Cloud Volumes ONTAP que ele gerencia (incluindo quaisquer mediadores de HA) usam o servidor proxy.

Esta operação reinicia o agente do Console. Verifique se o agente do Console está ocioso antes de prosseguir.

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione o menu de ação para um agente do Console e selecione **Editar agente**.

   O agente do Console deve estar ativo para editá-lo.

3. Selecione **Configuração de proxy HTTP**.
4. Selecione **Proxy explícito** no campo Tipo de configuração.
5. Selecione **Ativar proxy**.
6. Especifique o servidor usando a sintaxe http://address:port ou https://address:port
7. Especifique um nome de usuário e uma senha se a autenticação básica for necessária para o servidor.

   Observe o seguinte:

   - O usuário pode ser um usuário local ou de domínio.
   - Para um usuário de domínio, você deve inserir o código ASCII para \ da seguinte forma: nome-de-domínio%92nome-de-usuário

     Por exemplo: netapp%92proxy

   - O Console não suporta senhas que incluem o caractere @.
8. Selecione **Salvar**.

Habilitar um proxy transparente para um agente do Console

Somente o Cloud Volumes ONTAP oferece suporte ao uso de um proxy transparente no agente do Console. Se você usar serviços de dados da NetApp além do Cloud Volumes ONTAP, crie um agente separado para usar em serviços de dados ou para usar no Cloud Volumes ONTAP.

Antes de habilitar um proxy transparente, certifique-se de que os seguintes requisitos sejam atendidos:

- O agente é instalado na mesma rede que o servidor proxy transparente.
- A inspeção TLS está habilitada no servidor proxy.
- Você tem um certificado no formato PEM que corresponde ao usado no servidor proxy transparente.
- Não use o agente do Console para nenhum serviço de dados da NetApp além do Cloud Volumes ONTAP.

Para configurar um agente existente para usar um servidor proxy transparente, use a ferramenta de manutenção do agente do Console, disponível por meio da linha de comando no host do agente do Console.

Quando você configura um servidor proxy, o agente do Console é reiniciado. Verifique se o agente do Console está ocioso antes de prosseguir.

Passos

Certifique-se de ter um arquivo de certificado no formato PEM para o servidor proxy. Se você não tiver um certificado, entre em contato com o administrador da rede para obtê-lo.

1. Abra uma interface de linha de comando no host do agente do Console.

2. Navegue até o diretório da ferramenta de manutenção do agente do Console: `/opt/application/netapp/service-manager-2/agent-maint-console`
3. Execute o seguinte comando para habilitar o proxy transparente, onde `/home/ubuntu/<certificate-file>.pem` é o diretório e o arquivo de certificado de nome que você tem para o servidor proxy:

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

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

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

Modifique o proxy transparente para o agente do Console

Você pode atualizar o servidor proxy transparente existente de um agente do Console usando o `proxy update` comando ou remover o servidor proxy transparente usando o `proxy remove` comando. Para obter mais informações, consulte a documentação para"Console de manutenção do agente" .

Depois de configurar um proxy, você não poderá alterar o tipo de proxy. Se precisar alterar o tipo de proxy, remova o agente do Console e adicione um novo agente com o novo tipo de proxy.

Atualize o proxy do agente do Console se ele perder o acesso à Internet

Se a configuração de proxy da sua rede mudar, seu agente poderá perder o acesso à Internet. Por exemplo, se alguém alterar a senha do servidor proxy ou atualizar o certificado. Nesse caso, você precisará acessar a interface do usuário diretamente do host do agente do Console e atualizar as configurações. Certifique-se de ter acesso à rede do host do agente do Console e de poder efetuar login no Console.

Habilitar tráfego direto da API

Se você configurou um agente do Console para usar um servidor proxy, poderá habilitar o tráfego de API direto no agente do Console para enviar chamadas de API diretamente aos serviços do provedor de nuvem sem passar pelo proxy. Os agentes em execução no AWS, Azure ou Google Cloud oferecem suporte a essa opção.

Se você desabilitar o Azure Private Links com o Cloud Volumes ONTAP e usar pontos de extremidade de serviço, habilite o tráfego de API direto. Caso contrário, o tráfego não será roteado corretamente.

"Saiba mais sobre como usar um Azure Private Link ou pontos de extremidade de serviço com o Cloud Volumes ONTAP"

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione o menu de ação para um agente do Console e selecione **Editar agente**.

   O agente do Console deve estar ativo para editá-lo.

3. Selecione **Suporte ao tráfego direto da API**.
4. Marque a caixa de seleção para habilitar a opção e selecione **Salvar**.

Exigir o uso do IMDSv2 em instâncias do Amazon EC2

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

Antes de começar

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

Sobre esta tarefa

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

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

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

Passos

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

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

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

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

b. Instale a AWS CLI.

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

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

Exemplo

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

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

2. Exigir o uso do IMDSv2 em instâncias do Cloud Volumes ONTAP :
   a. Vá para o "Console Amazon EC2"
   b. No painel de navegação, selecione **Instâncias**.
   c. Selecione uma instância do Cloud Volumes ONTAP .
   d. Selecione **Ações > Configurações da instância > Modificar opções de metadados da instância**.
   e. Na caixa de diálogo **Modificar opções de metadados da instância**, selecione o seguinte:
      - Para **Serviço de metadados de instância**, selecione **Ativar**.
      - Para **IMDSv2**, selecione **Obrigatório**.
      - Selecione **Salvar**.
   f. Repita essas etapas para outras instâncias do Cloud Volumes ONTAP , incluindo o mediador HA.
   g. "Pare e inicie as instâncias do Cloud Volumes ONTAP"

Resultado

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

Gerenciar atualizações do agente do console

Quando você usa o modo padrão ou o modo restrito, o NetApp Console atualiza automaticamente o agente do Console para a versão mais recente, desde que o agente do Console tenha acesso de saída à Internet para obter a atualização do software.

Se precisar gerenciar manualmente quando o agente do Console será atualizado, você poderá desabilitar as atualizações automáticas para o modo padrão ou restrito.

Desativar atualizações automáticas

Desabilitar a atualização automática do seu agente do Console consiste em duas etapas. Primeiro, você precisa garantir que seu agente do Console esteja íntegro e atualizado. Em seguida, edite um arquivo de configuração para desativar as atualizações automáticas.

> Você só pode desabilitar atualizações automáticas se tiver um agente do Console versão 3.9.48 ou superior.

Verifique a saúde do seu agente

Você deve verificar se seu agente está estável e se todos os contêineres em execução na VM do agente estão íntegros e funcionando. Depois de desabilitar as atualizações automáticas, a VM do agente para de verificar novos serviços ou pacotes de atualização.

Use um dos seguintes comandos para verificar seu agente do Console. Todos os serviços devem ter o status *Em execução*. Se esse não for o caso, entre em contato com o suporte da NetApp antes de desabilitar a atualização automática.

Docker (para implantações do Ubuntu e VCenter)

```
docker ps -a
```

Podman

```
podman ps -a
```

Desabilitar atualização automática para o agente

Você desabilita as atualizações automáticas definindo o sinalizador *isUpgradeDisabled* no arquivo *com/opt/application/netapp/service-manager-2/config.json*. Por padrão, esse sinalizador é definido como falso e seu agente é atualizado automaticamente. Você pode definir este sinalizador como verdadeiro para desabilitar atualizações automáticas. Você deve estar familiarizado com a sintaxe JSON antes de concluir esta etapa.

Para reativar a atualização automática, siga estas etapas e defina o sinalizador *isUpgradeDisabled* como falso.

Passos

1. Certifique-se de ter verificado se seu agente está atualizado e saudável.
2. Crie uma cópia de backup do arquivo */opt/application/netapp/service-manager-2/config.json* para garantir que você possa reverter suas alterações.
3. Edite o arquivo */opt/application/netapp/service-manager-2/config.json* e altere o valor do sinalizador *isUpgradeDisabled* para true.

   ```
   "isUpgradeDisabled": true,
   ```

4. Salve seu arquivo.
5. Reinicie o serviço do gerenciador de serviços 2 executando o seguinte comando:

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

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

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

Atualizar o agente do Console

O agente do Console precisa ser reiniciado durante o processo de atualização, portanto, o NetApp Console ficará indisponível durante a atualização.

Passos

1. Baixe o software do agente do Console em "Site de suporte da NetApp" .
2. Copie o instalador para o host Linux.
3. Atribua permissões para executar o script.

```
chmod +x /path/NetApp-Console-Agent-Offline-<version>
```

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

4. Execute o script de instalação:

```
sudo /path/NetApp-Console-Agent-Offline-<version>
```

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

5. Após a conclusão da atualização, você pode verificar a versão do agente acessando **Administração > Suporte > Agentes**.

Trabalhar com vários agentes do Console

Se você usar vários agentes do Console, poderá alternar entre eles diretamente do Console para visualizar os sistemas associados.

Alternar entre agentes do Console

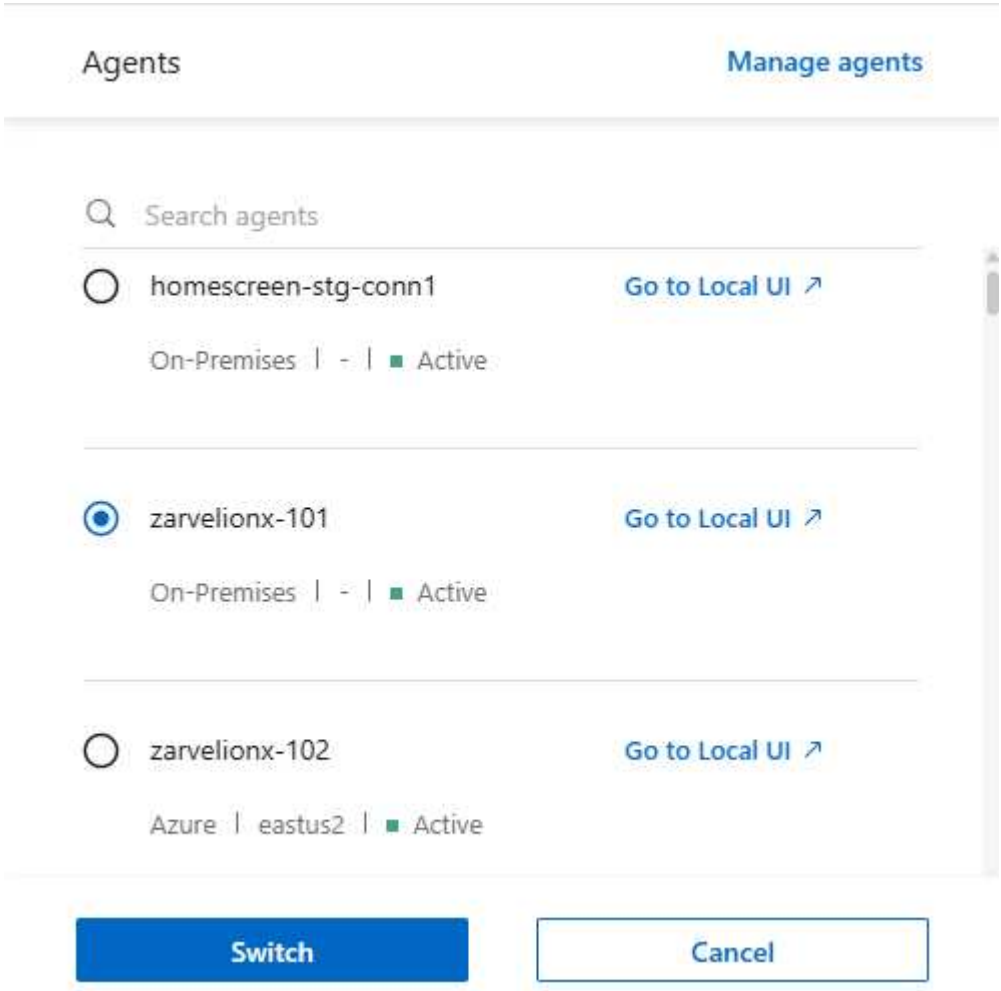
Se você tiver vários agentes do Console, poderá alternar entre eles para ver os sistemas associados a um agente específico.

Por exemplo, em um ambiente multinuvem, você pode ter um agente na AWS e outro no Google Cloud. Alterne entre esses agentes para gerenciar os sistemas Cloud Volumes ONTAP nos respectivos ambientes de nuvem.

Esta opção não está disponível ao visualizar o NetApp Console na interface de usuário local do agente

Etapa

1. Selecione o ícone de agentes do Console ( ) no canto superior direito para visualizar a lista de agentes disponíveis.



Resultado

O Console é atualizado e mostra os sistemas associados ao agente selecionado.

Configurar uma configuração de recuperação de desastres

Você pode gerenciar um sistema com vários agentes do Console ao mesmo tempo para fins de recuperação de desastres. Se um agente do Console ficar inativo, você pode alternar para o outro agente para gerenciar o sistema imediatamente.

Passos

1. Alterne para o outro agente do Console que você deseja gerenciar com o agente do Console.
2. Descubra o sistema existente.
   - "Adicionar sistemas Cloud Volumes ONTAP existentes ao Console"

- "Descubra os clusters ONTAP"

3. Se você estiver gerenciando um sistema Cloud Volumes ONTAP , ajuste o Modo de Gerenciamento de Capacidade para **Modo Manual**.

   Para evitar problemas de contenção, somente o agente principal do Console deve ser definido como **Modo Automático**.

   "Saiba mais sobre o modo de gerenciamento de capacidade"

Solucionar problemas do agente do console

Para solucionar problemas com um agente do Console, você pode verificar os problemas sozinho ou trabalhar com o Suporte da NetApp , que pode solicitar o ID do seu sistema, a versão do agente ou as mensagens mais recentes do AutoSupport .

Se você tiver uma conta no site de suporte da NetApp , também poderá visualizar o"Base de conhecimento da NetApp ."

Mensagens de erro comuns e soluções

A tabela lista mensagens de erro comuns e suas sugestões de resolução:

Mensagem de erro	Explicação	O que fazer
Não é possível carregar a interface do usuário do agente do console	A instalação do agente falhou	• Verifique se o serviço Service Manager está ativo. • Verifique se todos os contêineres estão em execução. • Certifique-se de que seu firewall permite acesso ao serviço na porta 8888. • Se o problema persistir, entre em contato com o suporte.
Não é possível acessar a interface do usuário do agente NetApp	Esta mensagem aparece ao tentar acessar o endereço IP de um agente. O agente pode falhar ao inicializar se não tiver o acesso correto à rede ou se estiver instável.	• Conecte-se ao agente do Console. • Verifique se o serviço Service Manager • Verifique se o agente tem o acesso à rede necessário."Saiba mais sobre os pontos de extremidade de acesso à rede necessários."
Não é possível carregar as configurações do agente	O Console exibe esta mensagem quando você tenta acessar a página de configurações do Agente.	• Verifique se o contêiner OCCM está em execução e funcionando. • Se o problema persistir, entre em contato com o suporte.

Mensagem de erro	Explicação	O que fazer
Não é possível carregar informações de suporte para o agente.	Esta mensagem é exibida se o agente não conseguir acessar sua conta de suporte.	• *.

Verifique o status do agente do Console

Use um dos seguintes comandos para verificar seu agente do Console. Todos os serviços devem ter o status *Em execução*. Se esse não for o caso, entre em contato com o suporte da NetApp .

Para obter informações mais detalhadas sobre como acessar o diagnóstico do agente do Console, consulte os seguintes tópicos:

- "Verifique o status do agente do console (para implantações de host Linux)"
- "Verifique o status do agente do console (para implantações do VCenter)"

Docker (para implantações do Ubuntu e VCenter)

```
docker ps -a
```

Podman (para implantações do RedHat Enterprise Linux)

```
podman ps -a
```

Ver a versão do agente do Console

Visualize a versão do agente do Console para confirmar a atualização ou compartilhe-a com seu representante da NetApp .

Passos

1. Selecione **Administração > Suporte > Agentes**.

   O Console exibe a versão no topo da página.

Verificar acesso à rede

Certifique-se de que o agente do Console tenha o acesso à rede necessário."Saiba mais sobre os pontos de acesso de rede necessários."

Problemas de instalação do agente do console

Se a instalação falhar, visualize o relatório e os logs para resolver os problemas.

Você também pode acessar o relatório de validação no formato JSON e os logs de configuração diretamente do host do agente do Console nos seguintes diretórios:

```
/tmp/netapp-console-agents/logs

/tmp/netapp-console-agents/results.json
```

- Para novas implantações de agentes, a NetApp verifica os seguintes endpoints:"listados aqui" . Esta verificação de configuração falhará com um erro se você estiver usando os endpoints anteriores usados para atualizações,"listados aqui" . A NetApp recomenda atualizar suas regras de firewall para permitir acesso aos endpoints atuais e bloquear o acesso aos endpoints anteriores o mais breve possível."Aprenda como atualizar sua rede" .
- Se você atualizar os endpoints no seu firewall, seus agentes existentes continuarão funcionando.

Desabilitar verificações de configuração para instalações manuais

Pode haver momentos em que você precise desabilitar as verificações de configuração que verificam a conectividade de saída durante a instalação. Por exemplo:

- Ao instalar manualmente um agente no seu ambiente Government Cloud, você precisa desabilitar as verificações de configuração ou a instalação falhará.
- Talvez você também queira desabilitar essas verificações se continuar usando a lista de endpoints anterior para atualizações de agentes.

Passos

Você desabilita a verificação de configuração definindo o sinalizador *skipConfigCheck* no arquivo *com/opt/application/netapp/service-manager-2/config.json*. Por padrão, esse sinalizador é definido como falso e a verificação de configuração verifica o acesso de saída do agente. Defina este sinalizador como verdadeiro para desabilitar a verificação. Você deve estar familiarizado com a sintaxe JSON antes de concluir esta etapa.

Para reativar a verificação de configuração, siga estas etapas e defina o sinalizador *skipConfigCheck* como falso.

Passos

1. Acesse o host do agente do Console como root ou com privilégios sudo.
2. Crie uma cópia de backup do arquivo */opt/application/netapp/service-manager-2/config.json* para garantir que você possa reverter suas alterações.
3. Pare o serviço do gerenciador de serviços 2 executando o seguinte comando:

```
systemctl stop netapp-service-manager.service
```

1. Edite o arquivo */opt/application/netapp/service-manager-2/config.json* e altere o valor do sinalizador *skipConfigCheck* para true.

```
  "skipConfigCheck": true,
```

2. Salve seu arquivo.

3. Reinicie o serviço do gerenciador de serviços 2 executando o seguinte comando:

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

Falha na instalação nos endpoints usados para atualizações

Se você ainda estiver usando o"pontos finais anteriores" usado para atualizações de agentes, a validação falha com um erro. Para evitar isso, desmarque a caixa de seleção **Configuração do agente de validação** ou pule a verificação de configuração ao instalar em um VCenter.

A NetApp recomenda atualizar suas regras de firewall para permitir acesso ao"pontos finais atuais" o mais breve possível. "Aprenda como atualizar seus endpoints" .

Certifique-se de verificar se o único erro está relacionado aos pontos finais anteriores:

- \ https://bluexpinfraprod.eastus2.data.azurecr.io
- \ https://bluexpinfraprod.azurecr.io

Se houver outros erros, você precisará resolvê-los antes de prosseguir.

Trabalhe com o suporte da NetApp

Se você não conseguiu resolver os problemas com seu agente do Console, entre em contato com o Suporte da NetApp . O suporte da NetApp pode solicitar o ID do agente do Console ou que você envie os logs do agente do Console, caso eles ainda não os tenham.

Encontre o ID do agente do console

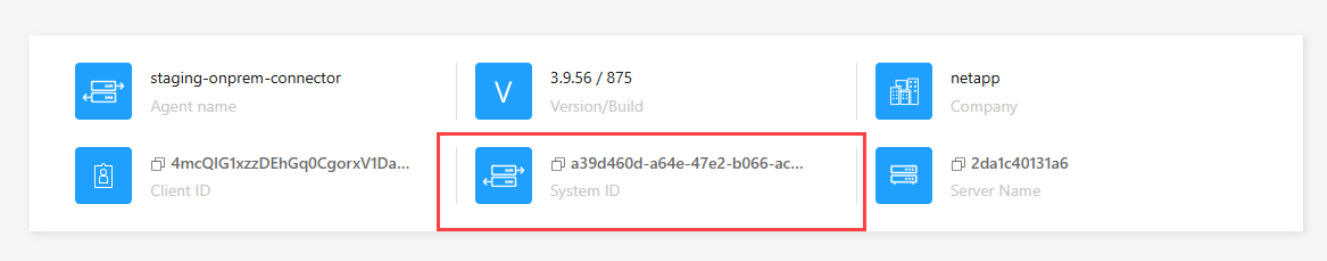
Para ajudar você a começar, você pode precisar do ID do sistema do seu agente do Console. O ID normalmente é usado para fins de licenciamento e solução de problemas.

Passos

1. Selecione **Administração > Suporte > Agentes**.

   Você pode encontrar o ID do sistema no topo da página.

   Exemplo



2. Passe o mouse e clique no ID para copiá-lo.

Baixe ou envie uma mensagem de AutoSupport

Se você estiver tendo problemas, a NetApp pode solicitar que você envie uma mensagem de AutoSupport para o suporte da NetApp para fins de solução de problemas.

O NetApp Console leva até cinco horas para enviar mensagens de AutoSupport devido ao balanceamento de carga. Para comunicação urgente, baixe o arquivo e envie-o manualmente.

Passos

1. Selecione **Administração > Suporte > Agentes**.
2. Dependendo de como você precisa enviar as informações para o suporte da NetApp , escolha uma das seguintes opções:
   a. Selecione a opção para baixar a mensagem do AutoSupport para sua máquina local. Você pode então enviá-lo ao Suporte da NetApp usando um método de sua preferência.
   b. Selecione **Enviar AutoSupport** para enviar a mensagem diretamente ao Suporte da NetApp .

Corrigir falhas de download ao usar um gateway NAT do Google Cloud

O agente do Console baixa automaticamente as atualizações de software para o Cloud Volumes ONTAP. Sua configuração pode causar falha no download se ele usar um gateway NAT do Google Cloud. Você pode corrigir esse problema limitando o número de partes em que a imagem do software é dividida. Esta etapa deve ser concluída usando a API.

Etapa

1. Envie uma solicitação PUT para /occm/config com o seguinte JSON como corpo:

```
{
  "maxDownloadSessions": 32
}
```

O valor para *maxDownloadSessions* pode ser 1 ou qualquer número inteiro maior que 1. Se o valor for 1, a imagem baixada não será dividida.

Observe que 32 é um valor de exemplo. O valor depende da sua configuração NAT e do número de sessões simultâneas.

"Saiba mais sobre a chamada de API /occm/config"

Obtenha ajuda na Base de conhecimento da NetApp

"Veja as informações de solução de problemas criadas pela equipe de suporte da NetApp" .

Desinstalar e remover um agente do Console

Desinstale o agente do Console para solucionar problemas ou removê-lo permanentemente do host. As etapas que você precisa usar dependem do modo de implantação que você está usando. Depois de remover um agente do Console do seu ambiente, você pode removê-lo do Console.

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

Desinstale o agente ao usar o modo padrão ou restrito

Se você estiver usando o modo padrão ou o modo restrito (em outras palavras, o host do agente tem conectividade de saída), siga as etapas abaixo para desinstalar o agente.

Passos

1. Conecte-se à VM Linux para o agente.
2. No host Linux, execute o script de desinstalação:

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

   silent executa o script sem solicitar sua confirmação.

Remover agentes do Console do Console

Se um agente do Console estiver inativo, você poderá removê-lo da lista de agentes. Você pode fazer isso se excluir a máquina virtual do agente ou se desinstalar o software do agente.

Observe o seguinte sobre a remoção de um agente do Console:

- Esta ação não exclui a máquina virtual.
- Esta ação não pode ser revertida: depois de remover um agente do Console, você não poderá adicioná-lo novamente.

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione o menu de ação para um agente inativo e selecione **Remover agente**.
3. Digite o nome do agente para confirmar e selecione **Remover**.

Configuração padrão para o agente do Console

Saiba mais sobre a configuração do agente do Console antes de implantá-lo.

Configuração padrão com acesso à Internet

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

Detalhes AWS

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

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

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

- A instalação inclui o Docker Engine, que é a ferramenta de orquestração de contêineres necessária.
- O nome de usuário para a instância do EC2 Linux é ubuntu (para agentes criados antes de maio de 2023,

o nome de usuário era ec2-user).

- O disco padrão do sistema é um disco gp2 de 100 GiB.

Detalhes do Azure

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

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

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

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

Detalhes do Google Cloud

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

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

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

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

Pasta de instalação

A pasta de instalação do agente está no seguinte local:

/opt/aplicativo/netapp/gerenciador de nuvem

Arquivos de log

Os arquivos de log estão contidos nas seguintes pastas:

- /opt/application/netapp/cloudmanager/log ou
- /opt/application/netapp/service-manager-2/logs (começando com novas instalações 3.9.23)

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

- /opt/aplicativo/netapp/cloudmanager/docker_occm/dados/log

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

Serviço de agente de console

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

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

Portos

O agente usa as seguintes portas no host Linux:

- 80 para acesso HTTP
- 443 para acesso HTTPS

Configuração padrão sem acesso à Internet

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

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

  /opt/aplicativo/netapp/ds

- Os arquivos de log estão contidos nas seguintes pastas:

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

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

- Todos os serviços estão sendo executados dentro de contêineres docker

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

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

Aplicar permissões ONTAP para o ONTAP Advanced View (ONTAP System Manager)

Por padrão, as credenciais do agente do Console permitem que os usuários acessem o Advanced View (ONTAP System Manager). Em vez disso, você pode solicitar aos usuários suas credenciais ONTAP . Isso garante que as permissões ONTAP de um usuário sejam aplicadas quando ele trabalha com clusters ONTAP nos clusters Cloud Volumes ONTAP e ONTAP locais.

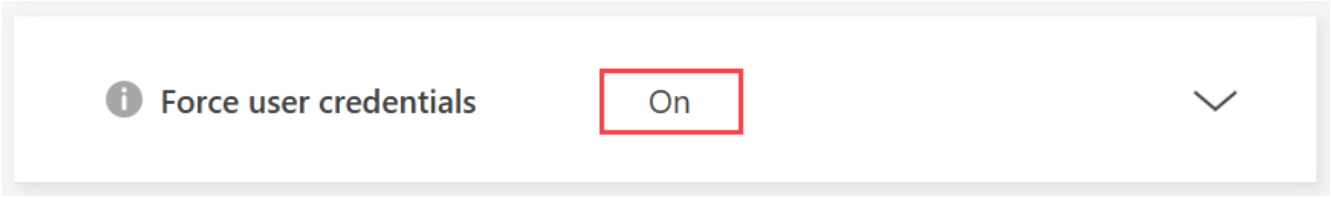
Você deve ter a função de administrador da organização para editar as configurações do agente do console.

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione o menu de ação para um agente do Console e selecione **Editar agente**.

   O agente do Console deve estar ativo para editá-lo.

3. Expanda a opção **Forçar credenciais**.
4. Marque a caixa de seleção para habilitar a opção **Forçar credenciais** e selecione **Salvar**.
5. Verifique se a opção **Forçar credenciais** está habilitada.



Credenciais e assinaturas

AWS

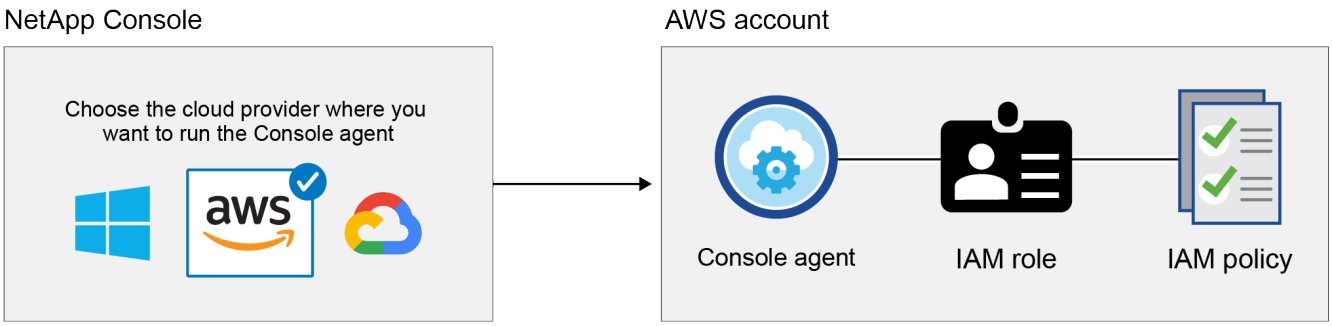
Saiba mais sobre credenciais e permissões da AWS no NetApp Console

Saiba como o NetApp Console usa credenciais da AWS para executar ações em seu nome e como essas credenciais são associadas às assinaturas do marketplace. Entender esses detalhes pode ser útil ao gerenciar as credenciais de uma ou mais contas da AWS no NetApp Console. Por exemplo, você pode querer saber quando adicionar credenciais adicionais da AWS.

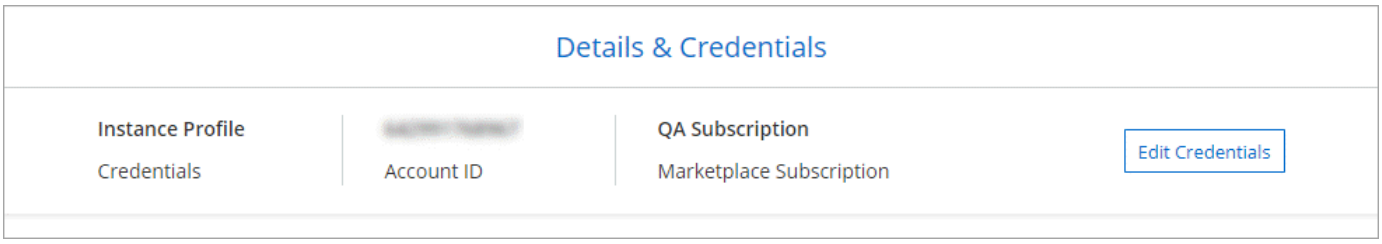
Credenciais iniciais da AWS

Ao implantar um agente do Console a partir do Console, você precisa fornecer o ARN de uma função do IAM ou chaves de acesso para um usuário do IAM. O método de autenticação deve ter permissões para implantar o Console na AWS. As permissões necessárias estão listadas no Política de implantação do agente para AWS.

Quando o Console inicia a instância do agente do Console na AWS, ele cria uma função do IAM e um perfil de instância para a instância. Ele também anexa uma política que fornece ao agente do Console permissões para gerenciar recursos e processos dentro dessa conta da AWS. "Revise como o Console usa as permissões" .



Se você adicionar um novo sistema Cloud Volumes ONTAP , o Console selecionará estas credenciais da AWS por padrão:



Implante todos os seus sistemas Cloud Volumes ONTAP usando as credenciais iniciais da AWS ou adicione credenciais adicionais.

Credenciais adicionais da AWS

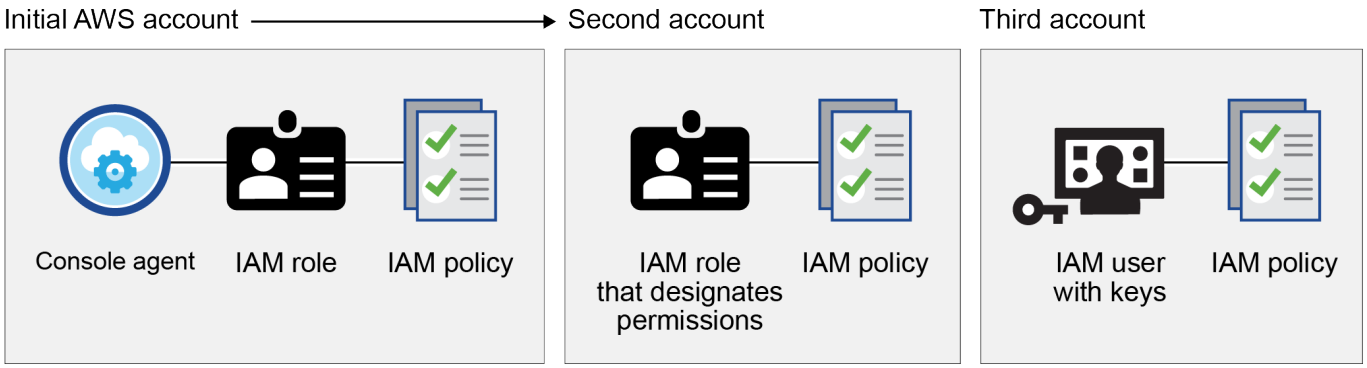
Você pode adicionar credenciais adicionais da AWS ao Console nos seguintes casos:

- Para usar o agente do Console existente com uma conta AWS adicional
- Para criar um novo agente em uma conta específica da AWS
- Para criar e gerenciar FSx para sistemas de arquivos ONTAP

Revise as seções abaixo para mais detalhes.

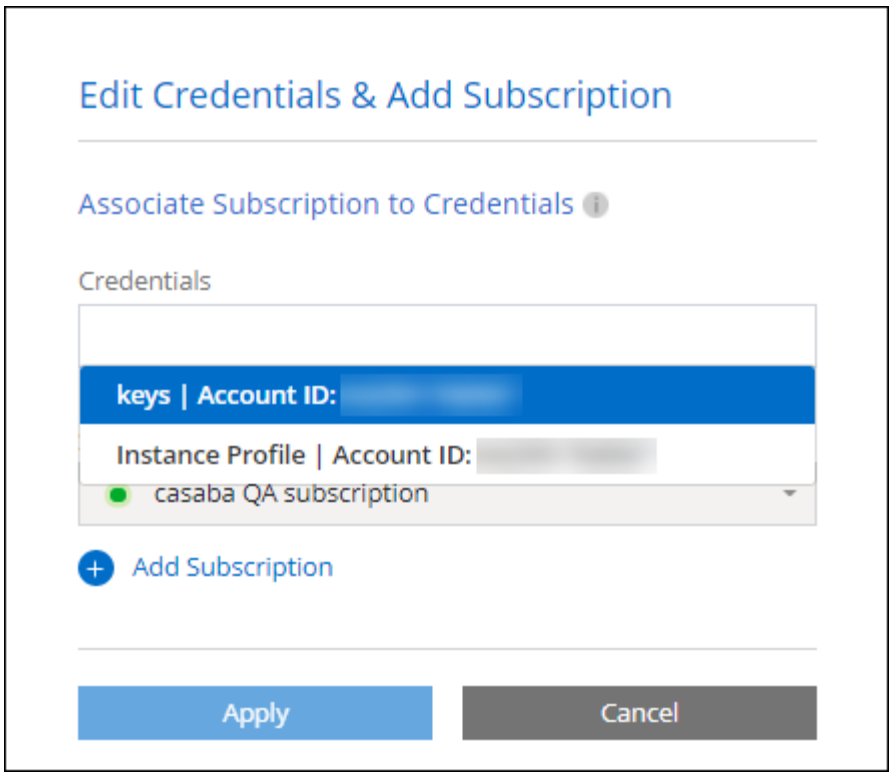
Adicione credenciais da AWS para usar um agente do Console com outra conta da AWS

Se quiser usar o Console com contas adicionais da AWS, você pode fornecer chaves da AWS para um usuário do IAM ou o ARN de uma função em uma conta confiável. A imagem a seguir mostra duas contas adicionais, uma fornecendo permissões por meio de uma função do IAM em uma conta confiável e outra por meio das chaves da AWS de um usuário do IAM:



Em seguida, você adicionaria as credenciais da conta ao Console especificando o Nome do Recurso da Amazon (ARN) da função do IAM ou as chaves da AWS para o usuário do IAM.

Por exemplo, você pode alternar entre credenciais ao criar um novo sistema Cloud Volumes ONTAP :



"Saiba como adicionar credenciais da AWS a um agente existente."

Adicione credenciais da AWS para criar um agente do Console

Adicionar novas credenciais da AWS ao Console fornece as permissões necessárias para criar um agente do Console.

"Aprenda como adicionar credenciais da AWS ao Console para criar um agente do Console"

Adicionar credenciais da AWS para FSx para ONTAP

Adicione credenciais da AWS ao Console para fornecer as permissões necessárias para criar e gerenciar um sistema FSx para ONTAP .

"Aprenda como adicionar credenciais da AWS ao Console do Amazon FSx para ONTAP"

Credenciais e assinaturas de mercado

As credenciais que você adiciona a um agente do Console devem ser associadas a uma assinatura do AWS Marketplace para que você possa pagar pelo Cloud Volumes ONTAP a uma taxa por hora (PAYGO) e outros serviços de dados da NetApp ou por meio de um contrato anual. "Aprenda como associar uma assinatura da AWS" .

Observe o seguinte sobre credenciais da AWS e assinaturas do marketplace:

- Você pode associar apenas uma assinatura do AWS Marketplace a um conjunto de credenciais da AWS
- Você pode substituir uma assinatura de mercado existente por uma nova assinatura

Perguntas frequentes

As perguntas a seguir estão relacionadas a credenciais e assinaturas.

Como posso rotacionar minhas credenciais da AWS com segurança?

Conforme descrito nas seções acima, o Console permite que você forneça credenciais da AWS de algumas maneiras: uma função do IAM associada à instância do agente do Console, assumindo uma função do IAM em uma conta confiável ou fornecendo chaves de acesso da AWS.

Com as duas primeiras opções, o Console usa o AWS Security Token Service para obter credenciais temporárias que são rotacionadas constantemente. Este processo é a melhor prática: é automático e seguro.

Se você fornecer ao Console chaves de acesso da AWS, deverá rotacionar as chaves atualizando-as no Console em intervalos regulares. Este é um processo completamente manual.

Posso alterar a assinatura do AWS Marketplace para sistemas Cloud Volumes ONTAP ?

Sim, você pode. Quando você altera a assinatura do AWS Marketplace associada a um conjunto de credenciais, todos os sistemas Cloud Volumes ONTAP existentes e novos são cobrados na nova assinatura.

"Aprenda como associar uma assinatura da AWS" .

Posso adicionar várias credenciais da AWS, cada uma com diferentes assinaturas de marketplace?

Todas as credenciais da AWS que pertencem à mesma conta da AWS serão associadas à mesma assinatura do AWS Marketplace.

Se você tiver várias credenciais da AWS que pertencem a diferentes contas da AWS, essas credenciais poderão ser associadas à mesma assinatura do AWS Marketplace ou a assinaturas diferentes.

Posso mover sistemas Cloud Volumes ONTAP existentes para uma conta AWS diferente?

Não, não é possível mover os recursos da AWS associados ao seu sistema Cloud Volumes ONTAP para uma conta diferente da AWS.

Como as credenciais funcionam para implantações de mercado e implantações locais?

As seções acima descrevem o método de implantação recomendado para o agente do Console, que é do Console. Você também pode implantar um agente na AWS a partir do AWS Marketplace e instalar manualmente o software do agente do Console no seu próprio host Linux.

Se você usar o Marketplace, as permissões serão fornecidas da mesma maneira. Você só precisa criar e configurar manualmente a função do IAM e, em seguida, fornecer permissões para quaisquer contas adicionais.

Para implantações locais, você não pode configurar uma função do IAM para o Console, mas pode fornecer permissões usando chaves de acesso da AWS.

Para saber como configurar permissões, consulte as seguintes páginas:

- Modo padrão
  - "Configurar permissões para uma implantação do AWS Marketplace"
  - "Configurar permissões para implantações locais"
- Modo restrito
  - "Configurar permissões para o modo restrito"

Gerenciar credenciais da AWS e assinaturas do marketplace para o NetApp Console

Adicione e gerencie credenciais da AWS para que você implante e gerencie recursos de nuvem em suas contas da AWS a partir do NetApp Console. Se você gerencia várias assinaturas do AWS Marketplace, pode atribuir cada uma delas a diferentes credenciais da AWS na página Credenciais.

Visão geral

Você pode adicionar credenciais da AWS a um agente do Console existente ou diretamente ao Console:

- Adicionar credenciais adicionais da AWS a um agente existente

  Adicione credenciais da AWS a um agente do Console para gerenciar recursos de nuvem. Aprenda como adicionar credenciais da AWS a um agente do Console .

- Adicione credenciais da AWS ao Console para criar um agente do Console

  Adicionar novas credenciais da AWS ao Console fornece as permissões necessárias para criar um agente do Console. Aprenda como adicionar credenciais da AWS ao NetApp Console .

- Adicionar credenciais da AWS ao Console do FSx para ONTAP

  Adicione novas credenciais da AWS ao Console para criar e gerenciar o FSx para ONTAP. "Aprenda a configurar permissões para FSx para ONTAP"

Como rotacionar credenciais

O NetApp Console permite que você forneça credenciais da AWS de algumas maneiras: uma função do IAM associada à instância do agente, assumindo uma função do IAM em uma conta confiável ou fornecendo chaves de acesso da AWS. "Saiba mais sobre credenciais e permissões da AWS" .

Com as duas primeiras opções, o Console usa o AWS Security Token Service para obter credenciais temporárias que são rotacionadas constantemente. Esse processo é a melhor prática porque é automático e seguro.

Gire manualmente as chaves de acesso da AWS atualizando-as no Console.

Adicionar credenciais adicionais a um agente do Console

Adicione credenciais adicionais da AWS a um agente do Console para que ele tenha as permissões necessárias para gerenciar recursos e processos em seu ambiente de nuvem pública. Você pode fornecer o ARN de uma função do IAM em outra conta ou fornecer chaves de acesso da AWS.

Se você está apenas começando a usar o Console,"Saiba como o NetApp Console usa credenciais e permissões da AWS" .

Conceder permissões

Conceda permissões antes de adicionar credenciais da AWS a um agente do Console. As permissões permitem que um agente do Console gerencie recursos e processos dentro dessa conta da AWS. Você pode fornecer as permissões com o ARN de uma função em uma conta confiável ou chaves da AWS.

Se você implantou um agente do Console a partir do Console, ele adicionou automaticamente credenciais da AWS para a conta na qual você implantou um agente do Console. Isso garante que as permissões necessárias estejam em vigor para gerenciar recursos. "Saiba mais sobre credenciais e permissões da AWS" .

Escolhas

- Conceder permissões assumindo uma função do IAM em outra conta
- Conceder permissões fornecendo chaves da AWS

Conceder permissões assumindo uma função do IAM em outra conta

Você pode configurar uma relação de confiança entre a conta de origem da AWS na qual você implantou uma instância do agente do Console e outras contas da AWS usando funções do IAM. Em seguida, você forneceria ao Console o ARN das funções do IAM das contas confiáveis.

Se um agente do Console estiver instalado no local, você não poderá usar esse método de autenticação. Você deve usar chaves da AWS.

Passos

1. Acesse o console do IAM na conta de destino na qual você deseja fornecer permissões ao agente do Console.
2. Em Gerenciamento de acesso, selecione **Funções > Criar função** e siga as etapas para criar a função.

   Não se esqueça de fazer o seguinte:

   - Em **Tipo de entidade confiável**, selecione **Conta AWS**.
   - Selecione **Outra conta da AWS** e insira o ID da conta onde reside uma instância do agente do Console.
   - Crie as políticas necessárias copiando e colando o conteúdo de"as políticas do IAM para um agente do Console" .
3. Copie o ARN da função do IAM para poder colá-lo no Console mais tarde.

Resultado

A conta tem as permissões necessárias. Agora você pode adicionar as credenciais a um agente do Console .

Conceder permissões fornecendo chaves da AWS

Se você quiser fornecer ao Console chaves da AWS para um usuário do IAM, precisará conceder as permissões necessárias a esse usuário. A política do Console IAM define as ações e os recursos da AWS que o Console tem permissão para usar.

Você deve usar este método de autenticação se um agente do Console estiver instalado no local. Você não pode usar uma função do IAM.

Passos

1. No console do IAM, crie políticas copiando e colando o conteúdo de"as políticas do IAM para um agente do Console" .

   "Documentação da AWS: Criando políticas do IAM"

2. Anexe as políticas a uma função do IAM ou a um usuário do IAM.
    - "Documentação da AWS: Criando funções do IAM"
    - "Documentação da AWS: Adicionando e removendo políticas do IAM"

Resultado

A conta tem as permissões necessárias. Agora você pode adicionar as credenciais a um agente do Console .

Adicione as credenciais

Depois de fornecer a uma conta da AWS as permissões necessárias, você pode adicionar as credenciais dessa conta a um agente existente. Isso permite que você inicie sistemas Cloud Volumes ONTAP nessa conta usando o mesmo agente.

```
 New credentials in your cloud provider may take a few minutes to become
available. Then, add the credentials.
.Passos
. Use a barra de navegação superior para selecionar um agente do Console
ao qual você deseja adicionar credenciais.
. Na barra de navegação à esquerda, selecione *Administração >
Credenciais*.
. Na página *Credenciais da organização*, selecione *Adicionar
credenciais* e siga as etapas do assistente.
```

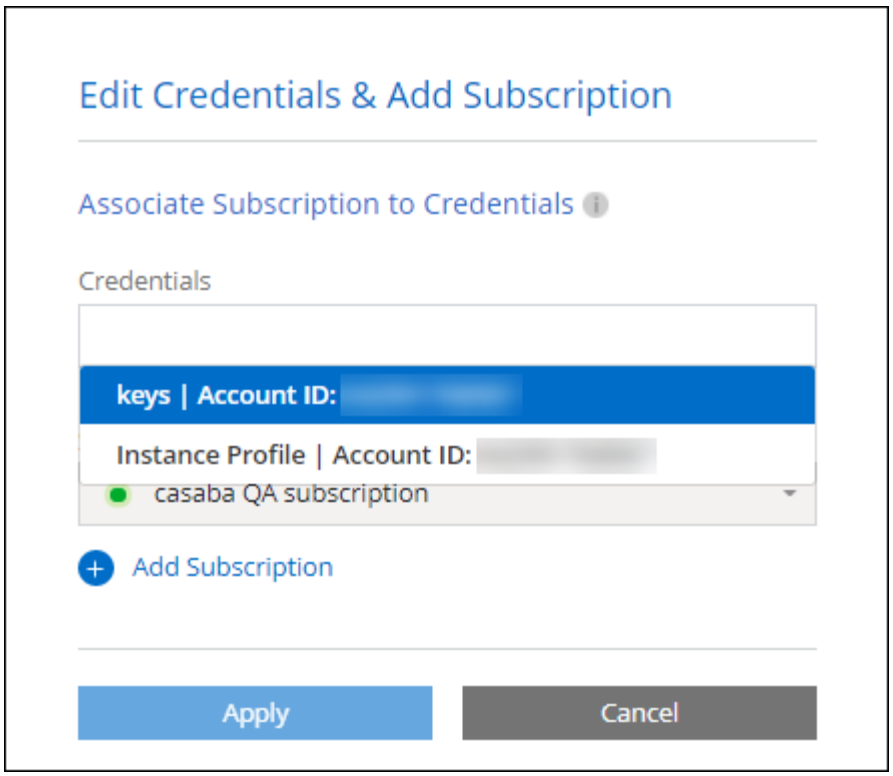
+
.. **Localização das credenciais**: Selecione **Amazon Web Services > Agente**.
.. **Definir credenciais**: forneça o ARN (Amazon Resource Name) de uma função do IAM confiável ou insira uma chave de acesso e uma chave secreta da AWS.
.. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.

+
Para pagar por serviços por hora (PAYGO) ou com um contrato anual, você deve associar as credenciais da AWS à sua assinatura do AWS Marketplace.

a. **Revisar**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

Resultado

Agora você pode alternar para um conjunto diferente de credenciais na página Detalhes e credenciais ao adicionar um sistema ao Console



Adicionar credenciais ao Console para criar um agente do Console

Adicione credenciais da AWS fornecendo o ARN de uma função do IAM que concede as permissões necessárias para criar um agente do Console. Você pode escolher essas credenciais ao criar um novo agente.

Configurar a função do IAM

Configure uma função do IAM que permita que a camada de software como serviço (SaaS) do NetApp Console assuma a função.

Passos

1. Acesse o console do IAM na conta de destino.
2. Em Gerenciamento de acesso, selecione **Funções > Criar função** e siga as etapas para criar a função.

   Não se esqueça de fazer o seguinte:

   - Em **Tipo de entidade confiável**, selecione **Conta AWS**.
   - Selecione **Outra conta AWS** e insira o ID do NetApp Console SaaS: 952013314444
   - Especificamente para o Amazon FSx for NetApp ONTAP , edite a política **Relacionamentos de confiança** para incluir "AWS": "arn:aws:iam::952013314444:root".

     Por exemplo, a política deve ficar assim:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

+
Consulte "Documentação do AWS Identity and Access Management (IAM)" para obter mais informações sobre acesso a recursos entre contas no IAM.

- Crie uma política que inclua as permissões necessárias para criar um agente do Console.
  - "Veja as permissões necessárias para o FSx para ONTAP"
  - "Exibir a política de implantação do agente"

3. Copie o ARN da função do IAM para que você possa colá-lo no Console na próxima etapa.

Resultado

A função IAM agora tem as permissões necessárias. Agora você pode adicioná-lo ao Console .

Adicione as credenciais

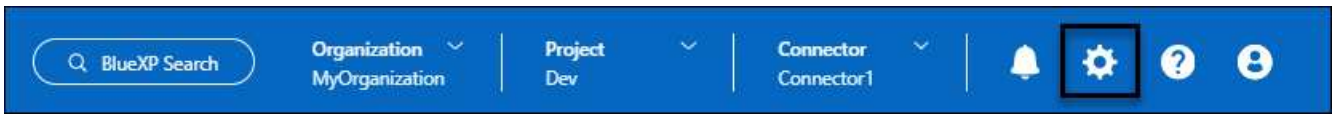
Depois de fornecer à função do IAM as permissões necessárias, adicione o ARN da função ao Console.

Antes de começar

Se você acabou de criar a função do IAM, pode levar alguns minutos até que ela esteja disponível para uso. Aguarde alguns minutos antes de adicionar as credenciais ao Console.

Passos

1. Selecione **Administração > Credenciais**.



2. Na página **Credenciais da organização** ou **Credenciais da conta**, selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Localização das credenciais**: Selecione **Amazon Web Services > NetApp Console**.
   b. **Definir credenciais**: forneça o ARN (Amazon Resource Name) da função do IAM.
   c. **Revisar**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

Adicionar credenciais ao Console do Amazon FSx para ONTAP

Para mais detalhes, consulte o "a documentação do console para Amazon FSx para ONTAP"

Configurar uma assinatura da AWS

Depois de adicionar suas credenciais da AWS, você pode configurar uma assinatura do AWS Marketplace com essas credenciais. A assinatura permite que você pague pelo Cloud Volumes ONTAP por uma taxa horária (PAYGO) ou usando um contrato anual, além de pagar por outros serviços de dados.

Há dois cenários nos quais você pode configurar uma assinatura do AWS Marketplace depois de já ter adicionado as credenciais:

- Você não configurou uma assinatura quando adicionou as credenciais inicialmente.
- Você deseja alterar a assinatura do AWS Marketplace configurada para as credenciais da AWS.

  Substituir a assinatura atual do marketplace por uma nova assinatura altera a assinatura do marketplace para todos os sistemas Cloud Volumes ONTAP existentes e todos os novos sistemas.

Antes de começar

Você precisa criar um agente do Console antes de poder configurar uma assinatura. "Aprenda a criar um agente de console" .

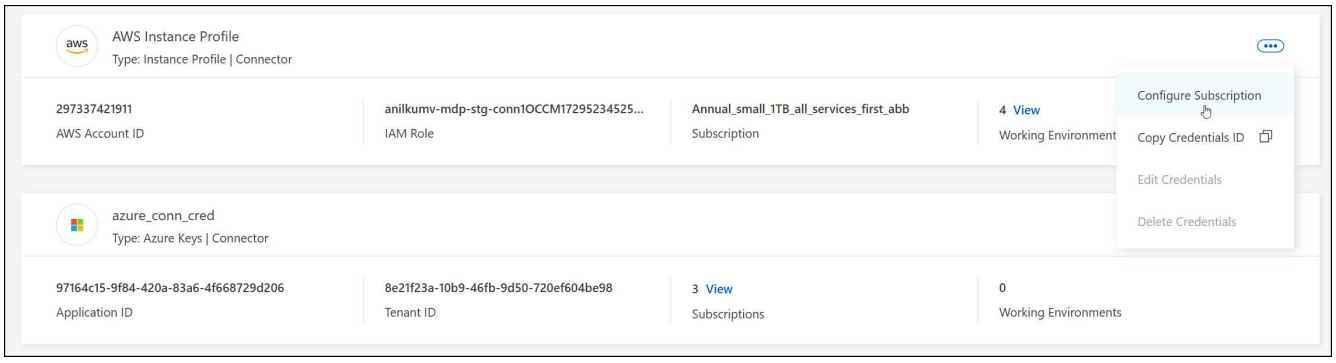
O vídeo a seguir mostra as etapas para assinar o NetApp Intelligent Services no AWS Marketplace:

Assine o NetApp Intelligent Services no AWS Marketplace

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**.

Associe uma assinatura existente à sua organização ou conta

Ao assinar no AWS Marketplace, a última etapa do processo é associar a assinatura à sua organização. Se você não concluiu esta etapa, não poderá usar a assinatura com sua organização ou conta.

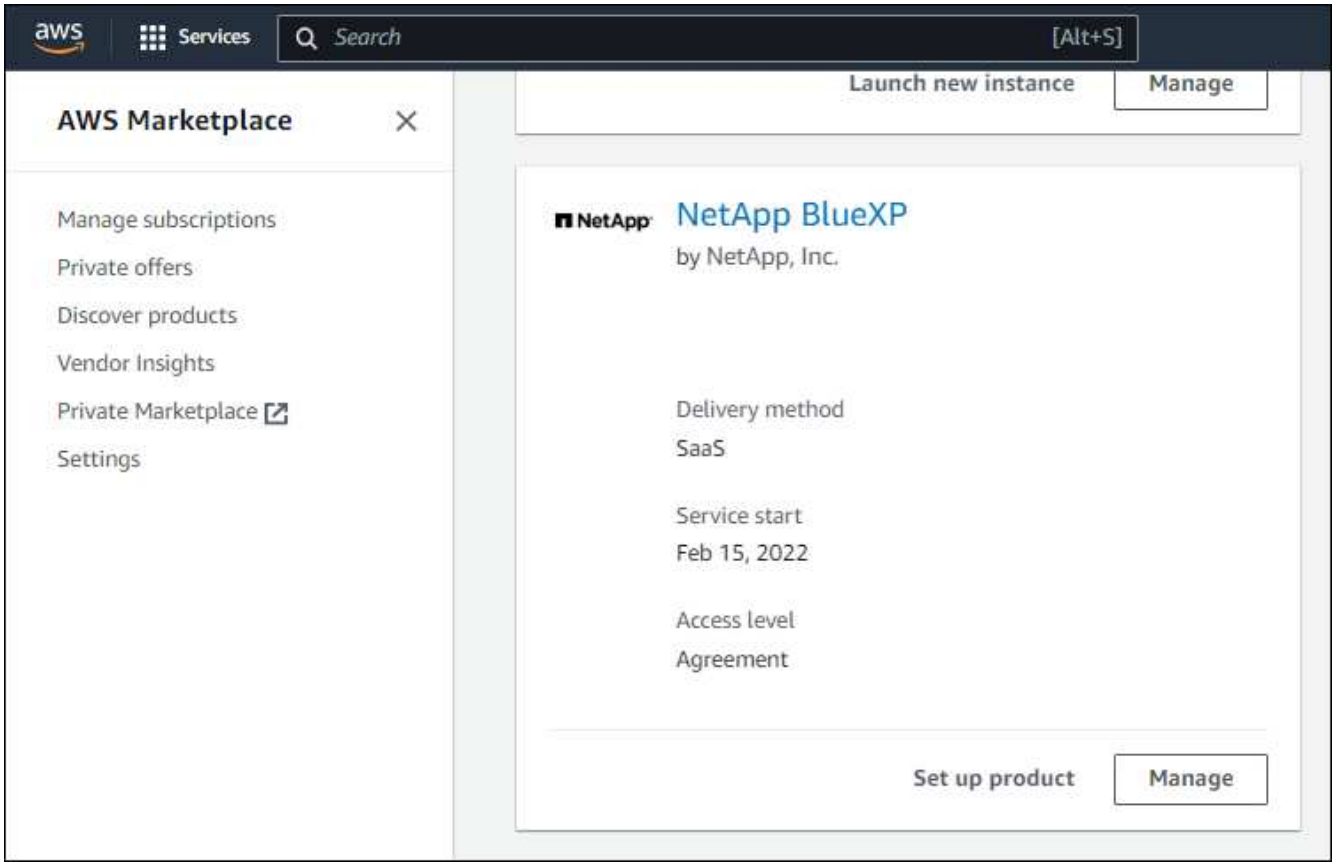
- "Saiba mais sobre os modos de implantação do Console"
- "Saiba mais sobre o gerenciamento de identidade e acesso do Console"

Siga as etapas abaixo se você assinou os serviços de dados inteligentes da NetApp no AWS Marketplace, mas perdeu a etapa para associar a assinatura à sua conta.

Passos

1. Confirme se você não associou sua assinatura à sua organização ou conta do Console.
   a. No menu de navegação, selecione **Administração > Licenças e assinaturas**.
   b. Selecione **Assinaturas**.
   c. Verifique se sua assinatura não aparece.

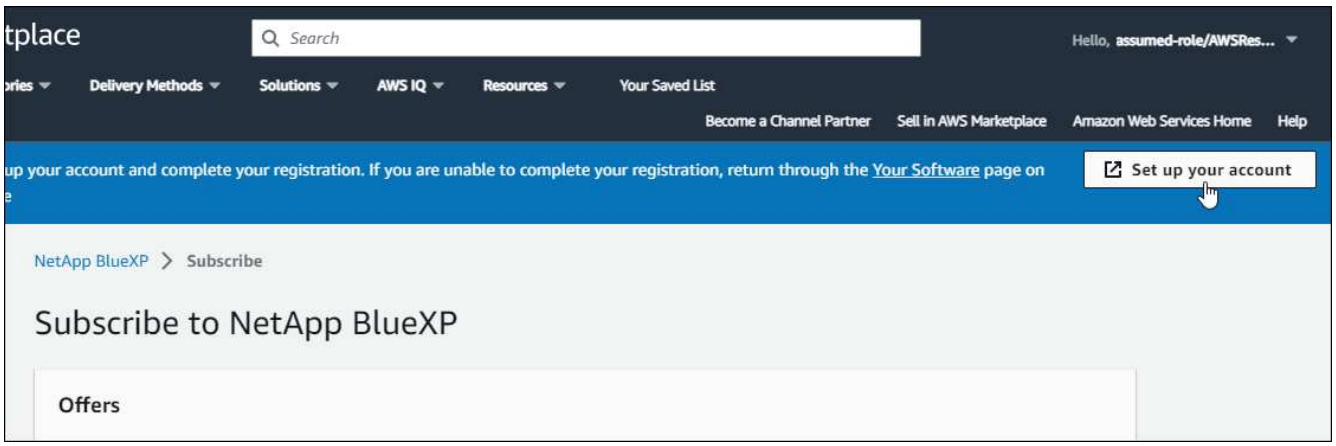
   Você verá apenas as assinaturas associadas à organização ou conta que você está visualizando no momento. Caso não veja sua assinatura, prossiga com os seguintes passos.
2. Efetue login no Console da AWS e navegue até **Assinaturas do AWS Marketplace**.
3. Encontre a assinatura.



4. Selecione **Configurar produto**.

   A página de oferta de assinatura deve ser carregada em uma nova aba ou janela do navegador.

5. Selecione **Configurar sua conta**.



   A página **Atribuição de Assinatura** no netapp.com deve ser carregada em uma nova guia ou janela do navegador.

   Observe que você pode ser solicitado a efetuar login no Console primeiro.

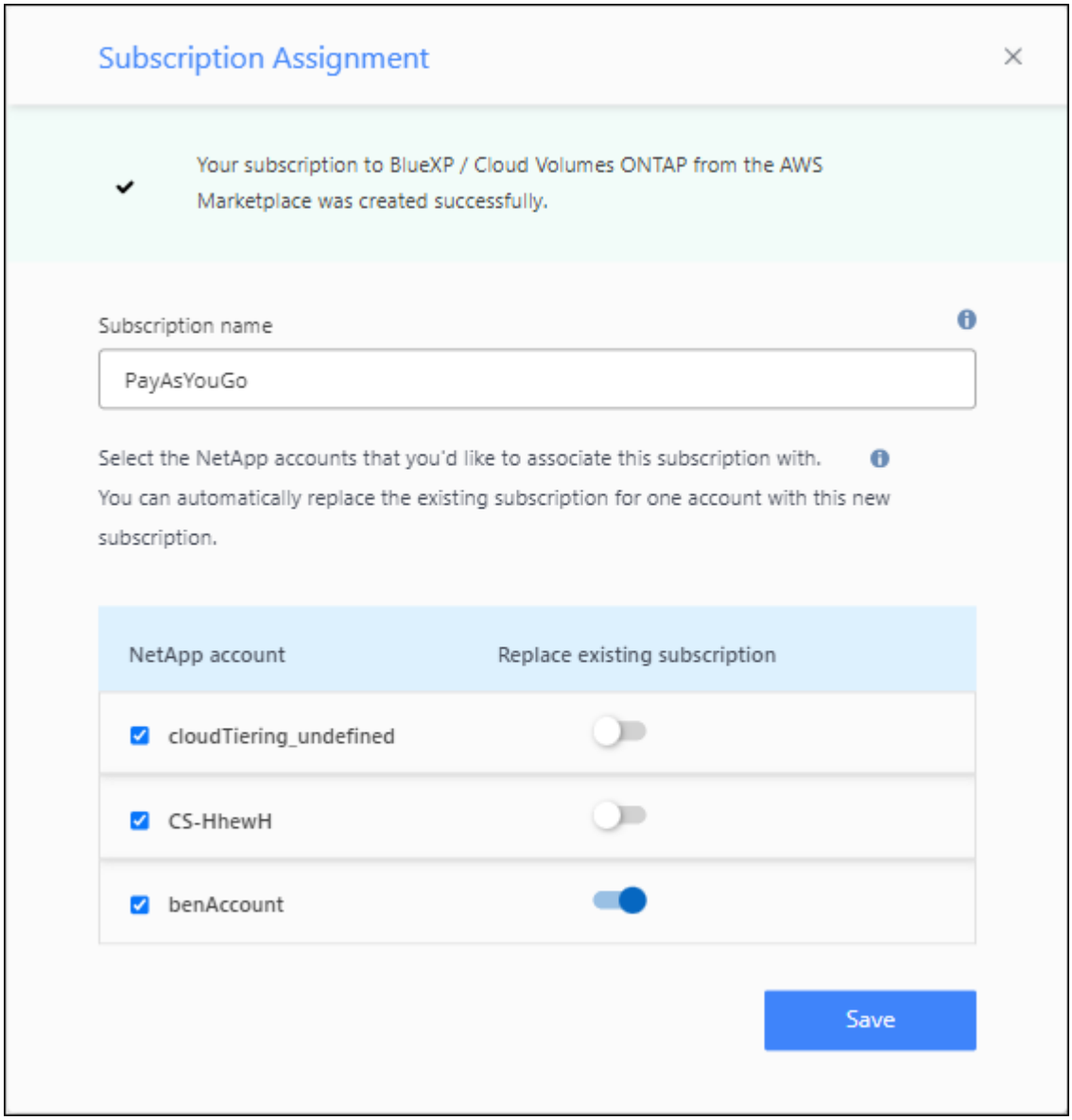
6. Na página **Atribuição de Assinatura**:

   - 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.

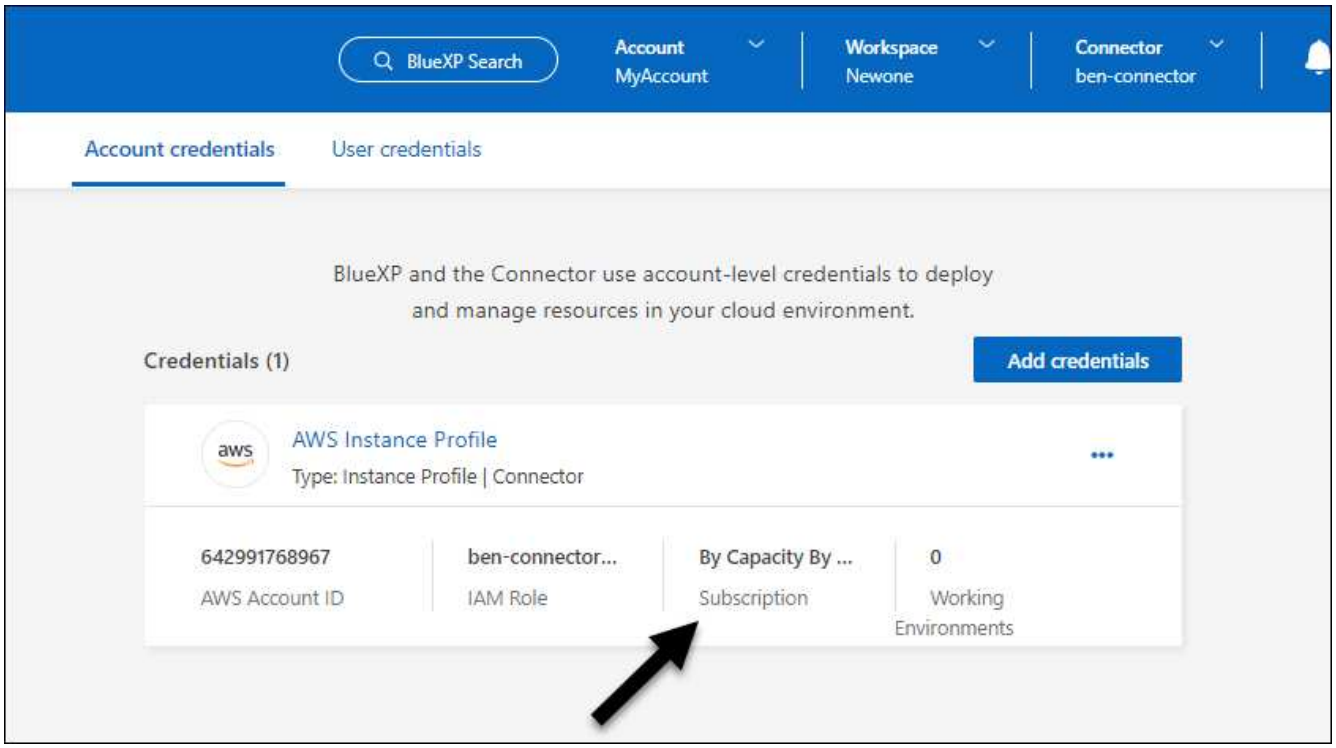


7. Confirme se a assinatura está associada à sua organização ou conta.
   a. No menu de navegação, selecione **Administração > Licença e assinaturas**.
   b. Selecione **Assinaturas**.
   c. Verifique se sua assinatura aparece.
8. Confirme se a assinatura está associada às suas credenciais da AWS.

   a. No canto superior direito do console, selecione o ícone Configurações e selecione **Credenciais**.

b. Na página **Credenciais da organização**, verifique se a assinatura está associada às suas credenciais da AWS.

Aqui está um exemplo.



Editar credenciais

Edite suas credenciais da AWS alterando o tipo de conta (chaves da AWS ou função assumida), editando o nome ou atualizando as próprias credenciais (as chaves ou o ARN da função).

Não é possível editar as credenciais de um perfil de instância associado a uma instância do agente do Console ou a uma instância do Amazon FSx for ONTAP . Você só pode renomear as credenciais de uma instância do FSx for ONTAP .

Passos

1. Selecione **Administração > Credenciais**.
2. Na página **Credenciais da organização** ou **Credenciais da conta**, selecione o menu de ações para um conjunto de credenciais e, em seguida, selecione **Editar credenciais**.
3. Faça as alterações necessárias e selecione **Aplicar**.

Excluir credenciais

Se você não precisar mais de um conjunto de credenciais, poderá excluí-las. Você só pode excluir credenciais que não estejam associadas a um sistema.

Não é possível excluir as credenciais de um perfil de instância associado a uma instância do agente do Console.

Passos

1. Selecione **Administração > Credenciais**.
2. Na página **Credenciais da organização** ou **Credenciais da conta**, selecione o menu de ações para um conjunto de credenciais e, em seguida, selecione **Excluir credenciais**.
3. Selecione **Excluir** para confirmar.

Azul

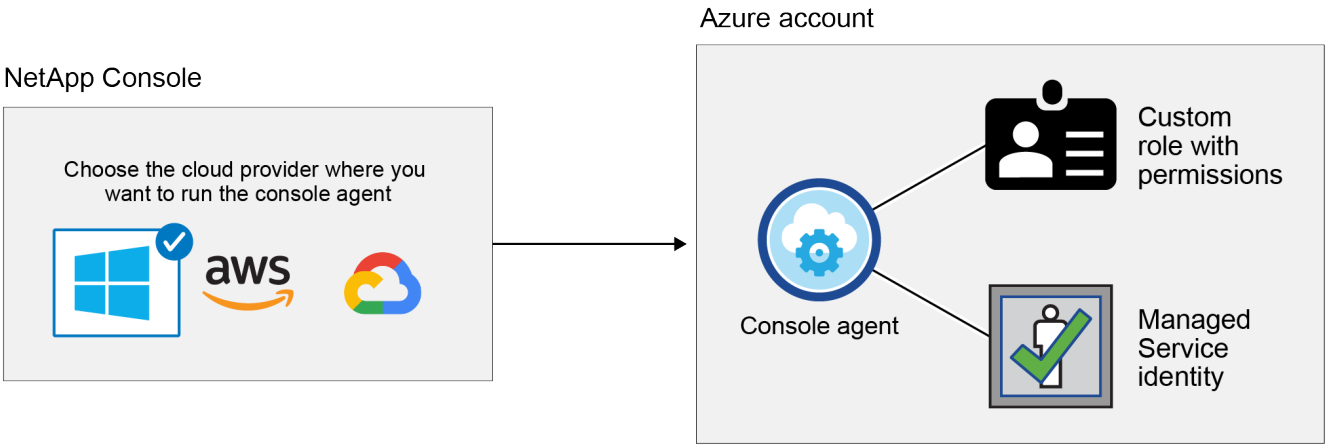
Saiba mais sobre credenciais e permissões do Azure no NetApp Console

Saiba como o NetApp Console usa credenciais do Azure para executar ações em seu nome e como essas credenciais são associadas às assinaturas do marketplace. Entender esses detalhes pode ser útil ao gerenciar as credenciais de uma ou mais assinaturas do Azure. Por exemplo, talvez você queira saber quando adicionar credenciais adicionais do Azure ao Console.

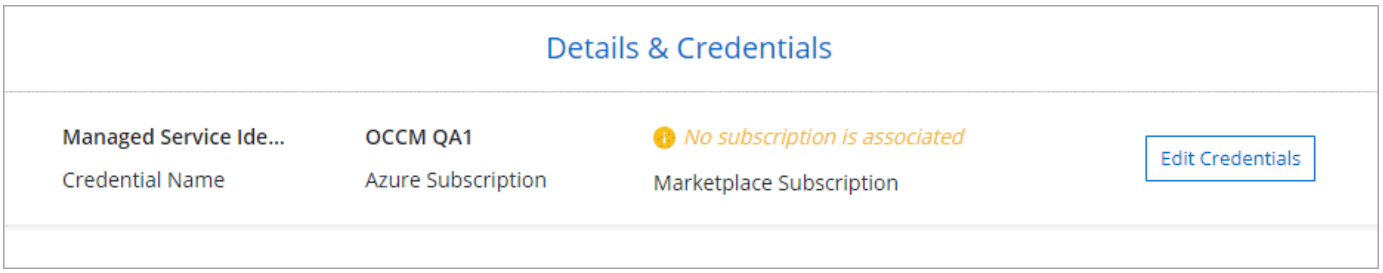
Credenciais iniciais do Azure

Ao implantar um agente do Console a partir do Console, você precisa usar uma conta do Azure ou uma entidade de serviço que tenha permissões para implantar a máquina virtual do agente do Console. As permissões necessárias estão listadas em"Política de implantação de agente para o Azure" .

Quando o Console implanta a máquina virtual do agente do Console no Azure, ele habilita um "identidade gerenciada atribuída pelo sistema" na máquina virtual, cria uma função personalizada e a atribui à máquina virtual. A função fornece ao Console as permissões necessárias para gerenciar recursos e processos dentro dessa assinatura do Azure. "Revise como o Console usa as permissões" .



Se você criar um novo sistema para o Cloud Volumes ONTAP, o Console selecionará estas credenciais do Azure por padrão:



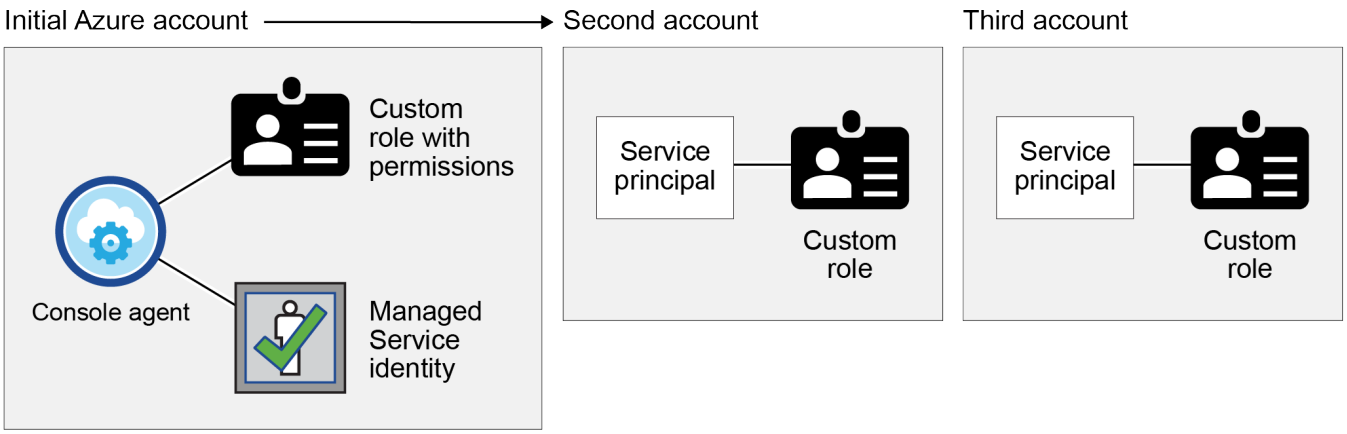
Você pode implantar todos os seus sistemas Cloud Volumes ONTAP usando as credenciais iniciais do Azure ou pode adicionar credenciais adicionais.

Assinaturas adicionais do Azure para uma identidade gerenciada

A identidade gerenciada atribuída pelo sistema à VM do agente do Console está associada à assinatura na qual você iniciou o agente do Console. Se você quiser selecionar uma assinatura diferente do Azure, será necessário"associar a identidade gerenciada a essas assinaturas" .

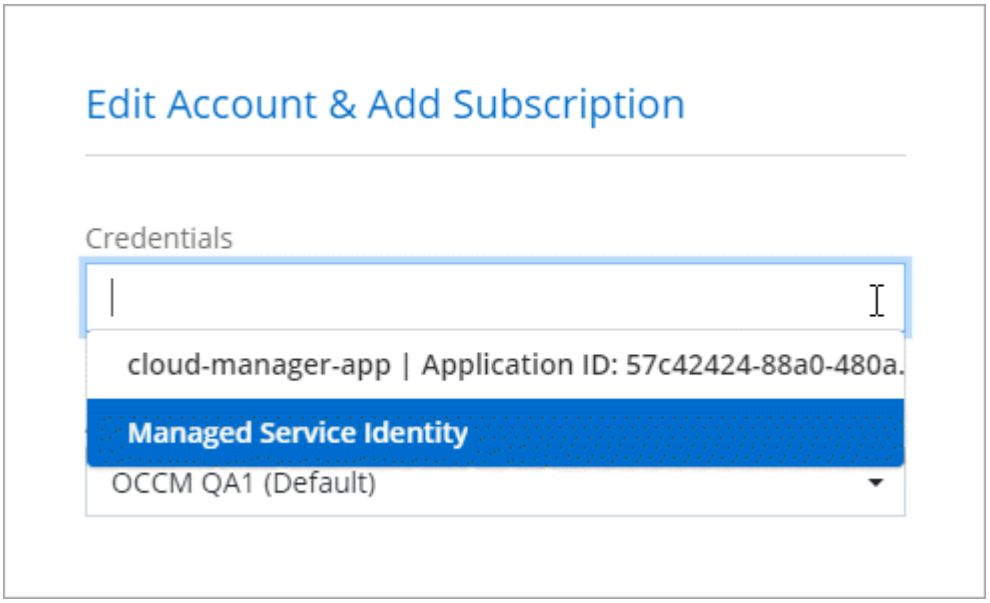
Credenciais adicionais do Azure

Se você quiser usar credenciais diferentes do Azure com o Console, deverá conceder as permissões necessárias por"criando e configurando uma entidade de serviço no Microsoft Entra ID" para cada conta do Azure. A imagem a seguir mostra duas contas adicionais, cada uma configurada com uma entidade de serviço e uma função personalizada que fornece permissões:



Você então"adicione as credenciais da conta ao Console" fornecendo detalhes sobre o principal serviço do AD.

Por exemplo, você pode alternar entre credenciais ao criar um novo sistema Cloud Volumes ONTAP :



Credenciais e assinaturas de mercado

As credenciais que você adiciona a um agente de console devem ser associadas a uma assinatura do Azure Marketplace para que você possa pagar pelo Cloud Volumes ONTAP a uma taxa por hora (PAYGO) ou pelos serviços de dados da NetApp ou por meio de um contrato anual.

"Aprenda como associar uma assinatura do Azure" .

Observe o seguinte sobre credenciais do Azure e assinaturas do marketplace:

- Você pode associar apenas uma assinatura do Azure Marketplace a um conjunto de credenciais do Azure
- Você pode substituir uma assinatura de mercado existente por uma nova assinatura

Perguntas frequentes

A pergunta a seguir está relacionada a credenciais e assinaturas.

Posso alterar a assinatura do Azure Marketplace para sistemas Cloud Volumes ONTAP ?

Sim, você pode. Quando você altera a assinatura do Azure Marketplace associada a um conjunto de credenciais do Azure, todos os sistemas Cloud Volumes ONTAP existentes e novos serão cobrados pela nova assinatura.

"Aprenda como associar uma assinatura do Azure" .

Posso adicionar várias credenciais do Azure, cada uma com diferentes assinaturas de marketplace?

Todas as credenciais do Azure que pertencem à mesma assinatura do Azure serão associadas à mesma assinatura do Azure Marketplace.

Se você tiver várias credenciais do Azure que pertencem a diferentes assinaturas do Azure, essas credenciais poderão ser associadas à mesma assinatura do Azure Marketplace ou a diferentes assinaturas do marketplace.

Posso mover sistemas Cloud Volumes ONTAP existentes para uma assinatura diferente do Azure?

Não, não é possível mover os recursos do Azure associados ao seu sistema Cloud Volumes ONTAP para uma assinatura diferente do Azure.

Como as credenciais funcionam para implantações de mercado e implantações locais?

As seções acima descrevem o método de implantação recomendado para o agente do Console, que é do Console. Você também pode implantar um agente de console no Azure a partir do Azure Marketplace e instalar o software do agente de console no seu próprio host Linux.

Se você usar o Marketplace, poderá fornecer permissões atribuindo uma função personalizada à VM do agente do Console e a uma identidade gerenciada atribuída pelo sistema, ou poderá usar uma entidade de serviço do Microsoft Entra.

Para implantações locais, você não pode configurar uma identidade gerenciada para o agente do Console, mas pode fornecer permissões usando uma entidade de serviço.

Para saber como configurar permissões, consulte as seguintes páginas:

- Modo padrão

- "Configurar permissões para uma implantação do Azure Marketplace"
- "Configurar permissões para implantações locais"

- Modo restrito
  - "Configurar permissões para o modo restrito"

Gerenciar credenciais do Azure e assinaturas do marketplace para o NetApp Console

Adicione e gerencie credenciais do Azure para que o NetApp Console tenha as permissões necessárias para implantar e gerenciar recursos de nuvem em suas assinaturas do Azure. Se você gerencia várias assinaturas do Azure Marketplace, pode atribuir cada uma delas a diferentes credenciais do Azure na página Credenciais.

Visão geral

Há duas maneiras de adicionar assinaturas e credenciais adicionais do Azure no Console.

1. Associe assinaturas adicionais do Azure à identidade gerenciada do Azure.
2. Para implantar o Cloud Volumes ONTAP usando diferentes credenciais do Azure, conceda permissões do Azure usando uma entidade de serviço e adicione suas credenciais ao Console.

Associar assinaturas adicionais do Azure a uma identidade gerenciada

O Console permite que você escolha as credenciais do Azure e a assinatura do Azure nas quais deseja implantar o Cloud Volumes ONTAP. Você não pode selecionar uma assinatura diferente do Azure para o perfil de identidade gerenciado, a menos que associe o "identidade gerenciada" com essas assinaturas.

Sobre esta tarefa

Uma identidade gerenciada é"a conta inicial do Azure" quando você implanta um agente do Console a partir do Console. Quando você implanta o agente do Console, o Console atribui a função de Operador do Console à máquina virtual do agente do Console.

Passos

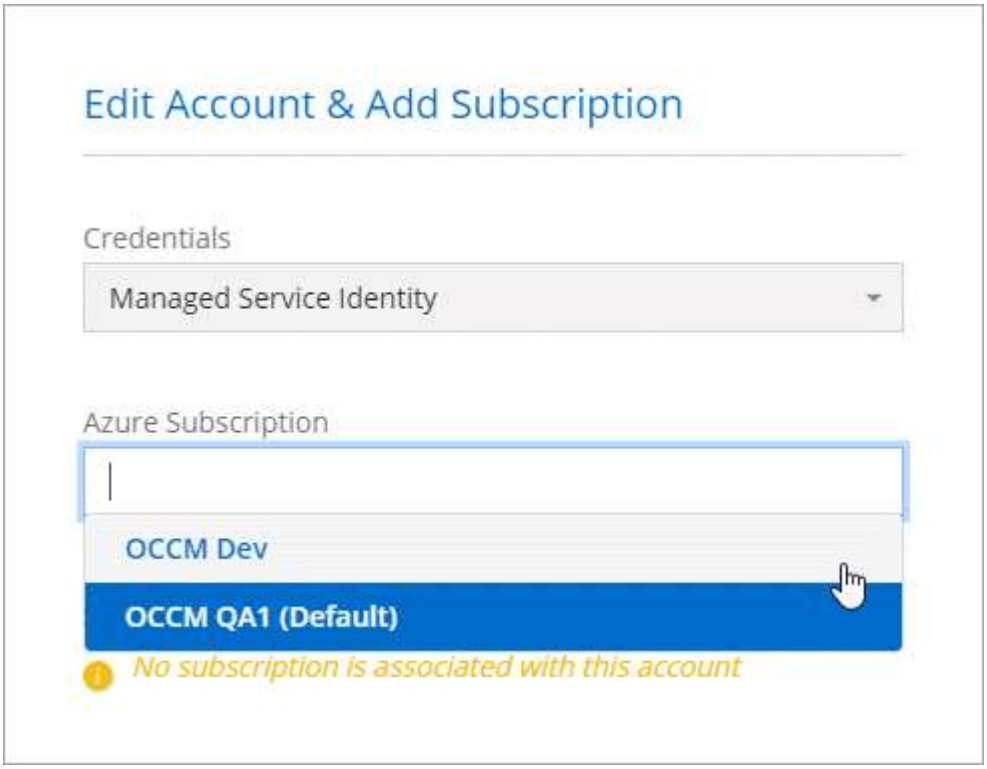
1. Efetue login no portal do Azure.
2. Abra o serviço **Assinaturas** e selecione a assinatura na qual deseja implantar o Cloud Volumes ONTAP.
3. Selecione **Controle de acesso (IAM)**.
   a. Selecione **Adicionar** > **Adicionar atribuição de função** e adicione as permissões:
      - Selecione a função **Operador de console**.

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

      - Atribuir acesso a uma **Máquina Virtual**.
      - Selecione a assinatura na qual uma máquina virtual do agente do Console foi criada.
      - Selecione uma máquina virtual do agente do Console.
      - Selecione **Salvar**.
4. Repita essas etapas para assinaturas adicionais.

Resultado

Ao criar um novo sistema, agora você pode selecionar entre várias assinaturas do Azure para o perfil de identidade gerenciado.



Adicionar credenciais adicionais do Azure ao NetApp Console

Quando você implanta um agente do Console a partir do Console, o Console habilita uma identidade gerenciada atribuída pelo sistema na máquina virtual que tem as permissões necessárias. O Console seleciona essas credenciais do Azure por padrão quando você cria um novo sistema para o Cloud Volumes ONTAP.

Um conjunto inicial de credenciais não será adicionado se você instalar manualmente um software de agente do Console em um sistema existente. "Saiba mais sobre credenciais e permissões do Azure" .

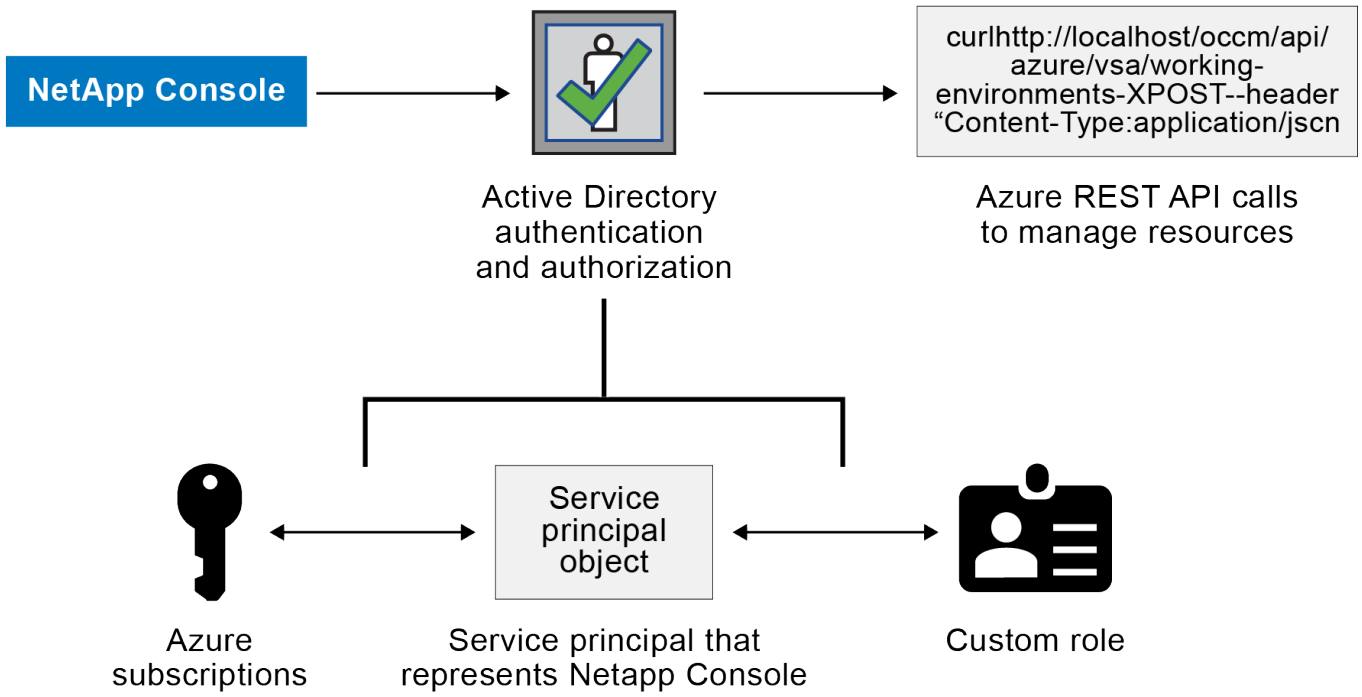
Se você quiser implantar o Cloud Volumes ONTAP usando credenciais *diferentes* do Azure, deverá conceder as permissões necessárias criando e configurando uma entidade de serviço no Microsoft Entra ID para cada conta do Azure. Você pode então adicionar as novas credenciais ao Console.

Conceder permissões do Azure usando uma entidade de serviço

O Console precisa de permissões para executar ações no Azure. Você pode conceder as permissões necessárias a uma conta do Azure criando e configurando uma entidade de serviço no Microsoft Entra ID e obtendo as credenciais do Azure necessárias para o Console.

Sobre esta tarefa

A imagem a seguir mostra como o Console obtém permissões para executar operações no Azure. Um objeto principal de serviço, que está vinculado a uma ou mais assinaturas do Azure, representa o Console no Microsoft Entra ID e é atribuído a uma função personalizada que concede as permissões necessárias.



Passos

1. Criar um aplicativo Microsoft Entra .
2. Atribuir o aplicativo a uma função .
3. Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure .
4. Obtenha o ID do aplicativo e o ID do diretório .
5. Criar um segredo do cliente .

Criar um aplicativo Microsoft Entra

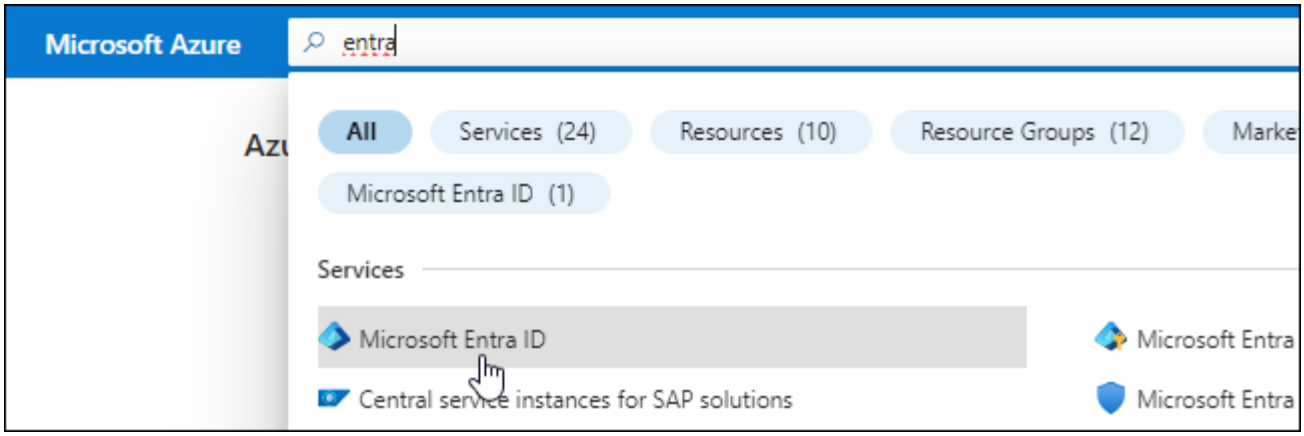
Crie um aplicativo Microsoft Entra e uma entidade de serviço que o Console possa usar para controle de acesso baseado em função.

Passos

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

Você deve vincular a entidade de serviço a uma ou mais assinaturas do Azure e atribuir a ela a função personalizada "Operador do Console" para que o Console tenha permissões no Azure.

Passos

1. Crie uma função personalizada:

   Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se 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 .

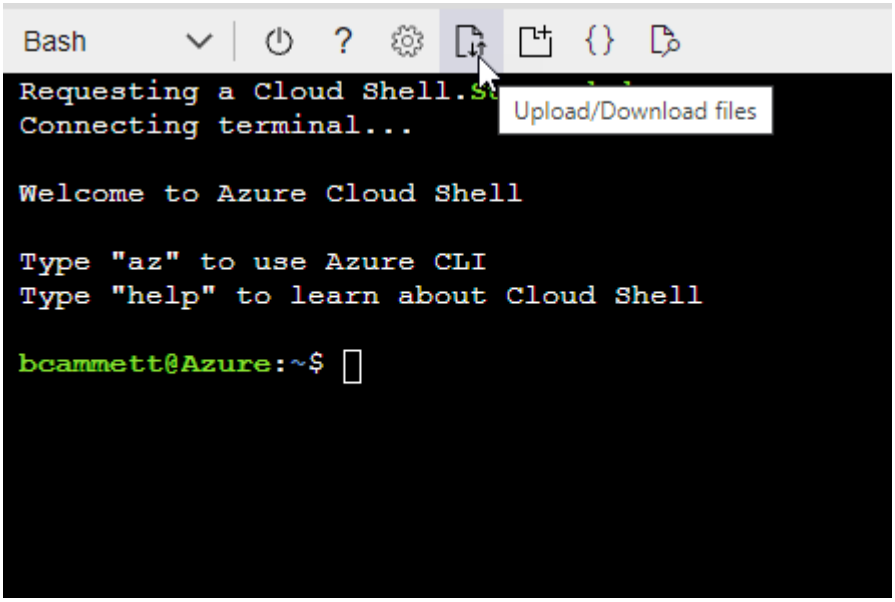
      Exemplo

```
"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:

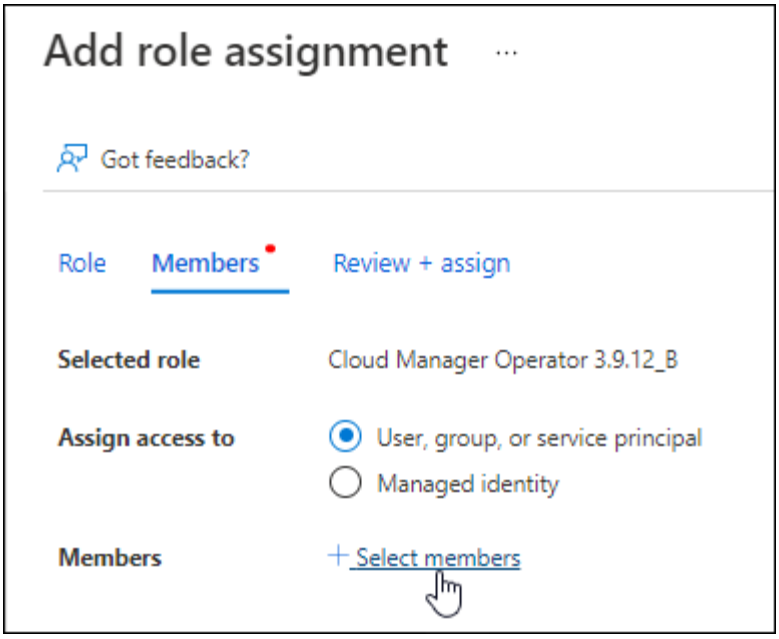
```
az role definition create --role-definition Connector_Policy.json
```

   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:

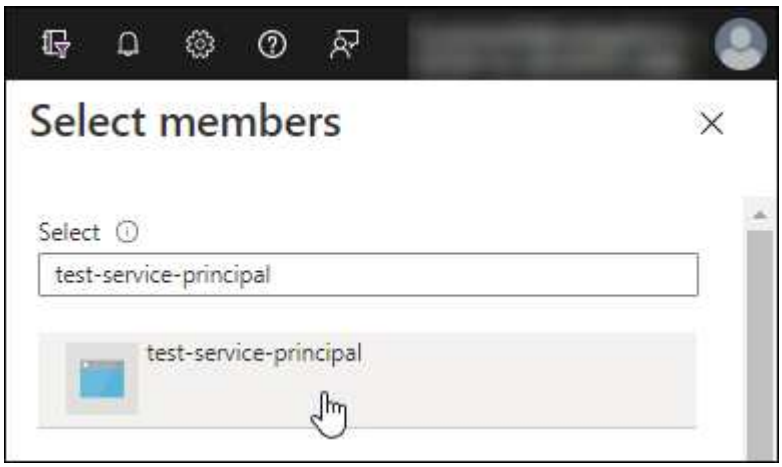
   a. No portal do Azure, abra o serviço **Assinaturas**.
   b. Selecione a assinatura.
   c. Selecione **Controle de acesso (IAM) > Adicionar > Adicionar atribuição de função**.
   d. Na guia **Função**, selecione a função **Operador de console** e selecione **Avançar**.
   e. Na aba **Membros**, complete 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.

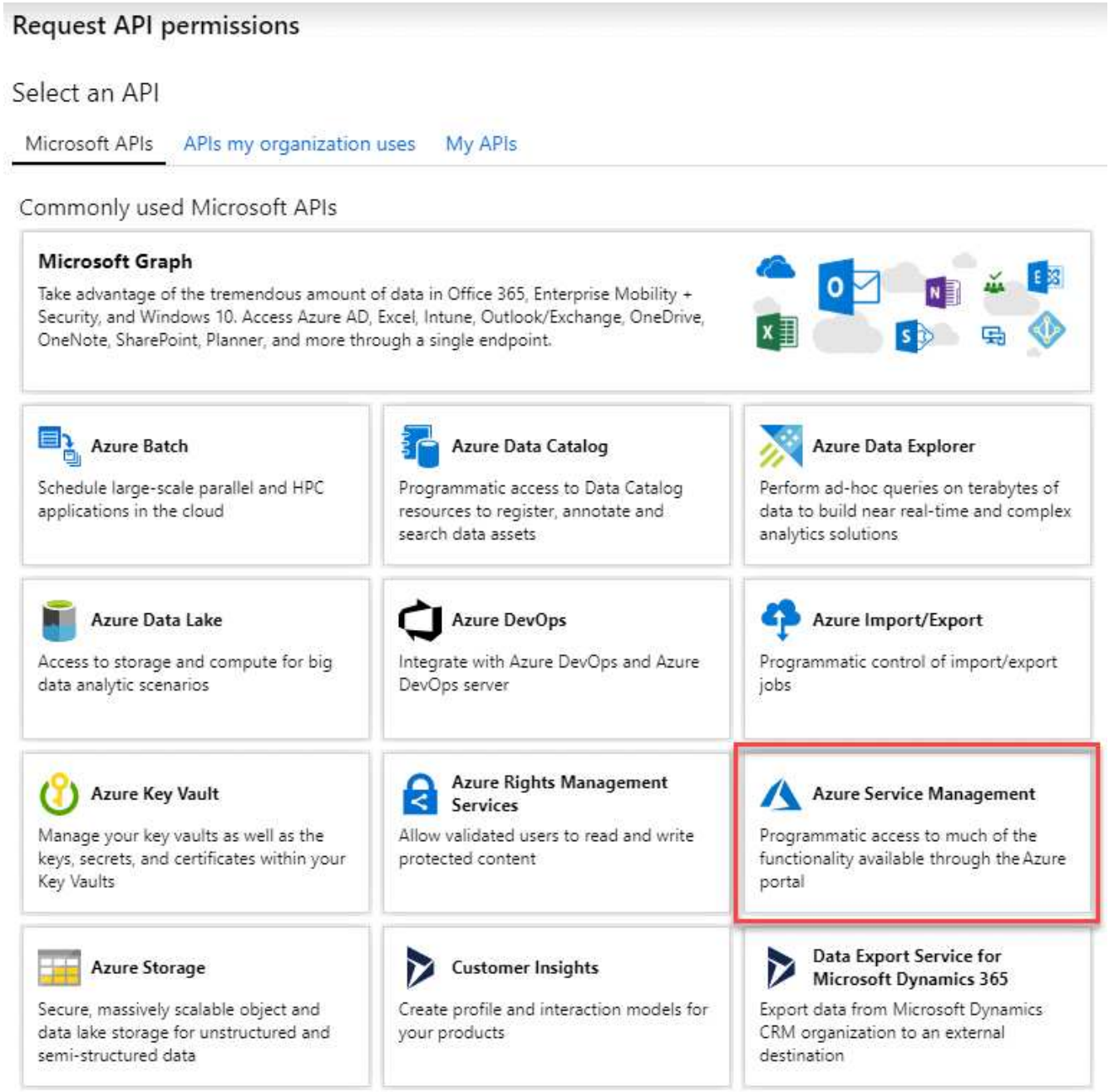
Se você quiser implantar o Cloud Volumes ONTAP de várias assinaturas do Azure, será necessário vincular a entidade de serviço a cada uma dessas assinaturas. No NetApp Console, você pode selecionar a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

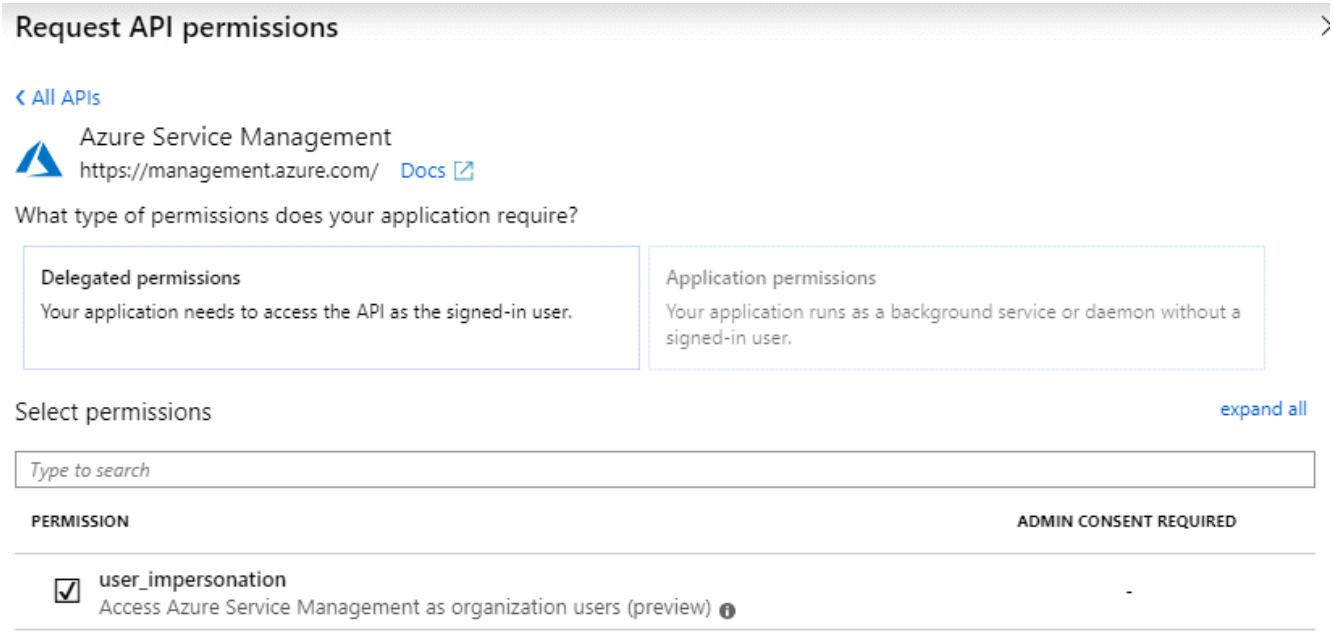
Você deve atribuir permissões "API de Gerenciamento de Serviços do Windows Azure" à entidade de serviço.

Passos

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**.

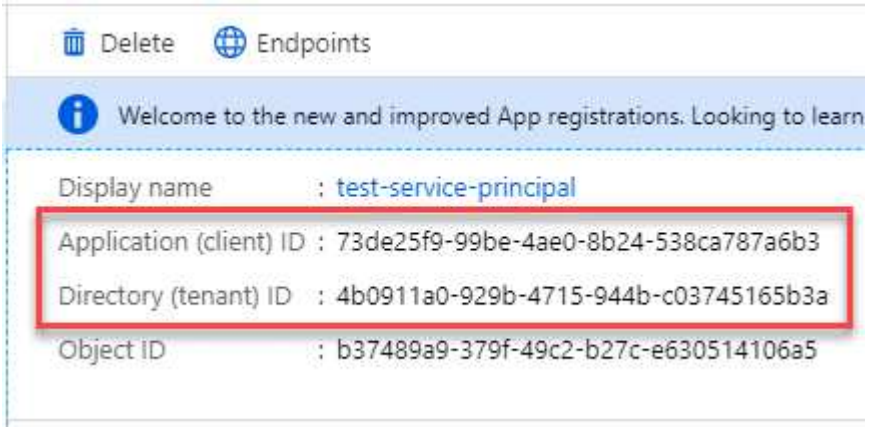


Obtenha o ID do aplicativo e o ID do diretório

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.

Passos

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

Crie um segredo do cliente e forneça seu valor ao Console para autenticação com o Microsoft Entra ID.

Passos

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.

Adicione as credenciais ao Console

Depois de fornecer uma conta do Azure com as permissões necessárias, você pode adicionar as credenciais dessa conta ao Console. Concluir esta etapa permite que você inicie o Cloud Volumes ONTAP usando diferentes credenciais do Azure.

Antes de começar

Se você acabou de criar essas credenciais no seu provedor de nuvem, pode levar alguns minutos até que elas estejam disponíveis para uso. Aguarde alguns minutos antes de adicionar as credenciais ao Console.

Antes de começar

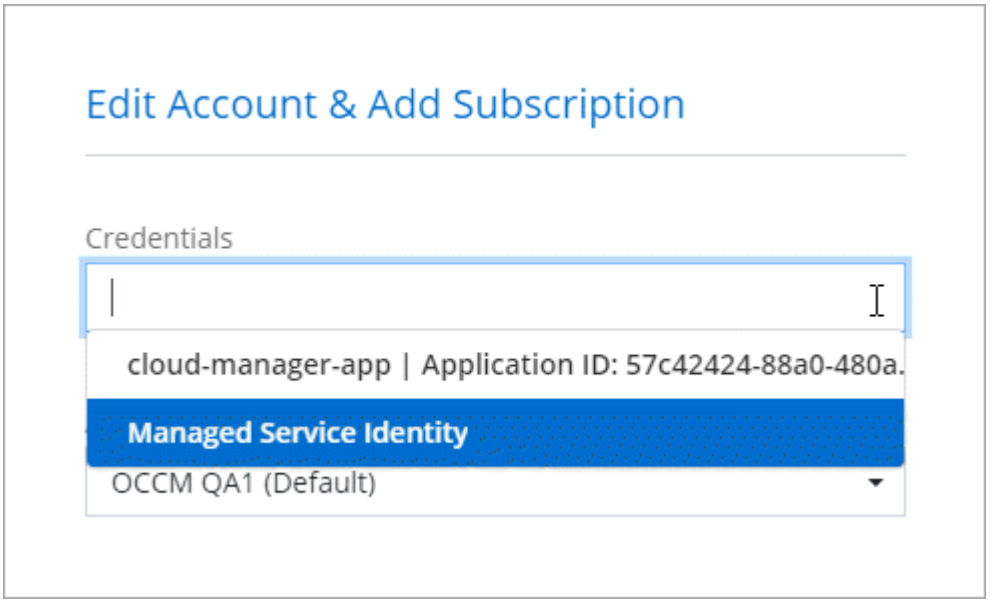
Você precisa criar um agente do Console antes de poder alterar as configurações do Console. "Aprenda a criar um agente de console" .

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

Você pode alternar para um conjunto diferente de credenciais na página Detalhes e Credenciais "ao adicionar um sistema ao Console"



Gerenciar credenciais existentes

Gerencie as credenciais do Azure que você já adicionou ao Console associando uma assinatura do Marketplace, editando credenciais e excluindo-as.

Associar uma assinatura do Azure Marketplace às credenciais

Depois de adicionar suas credenciais do Azure ao Console, você pode associar uma assinatura do Azure Marketplace a essas credenciais. Você pode usar a assinatura para criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso e acessar os serviços de dados da NetApp .

Há dois cenários nos quais você pode associar uma assinatura do Azure Marketplace depois de já ter adicionado as credenciais ao Console:

- Você não associou uma assinatura quando adicionou inicialmente as credenciais ao Console.
- Você deseja alterar a assinatura do Azure Marketplace associada às credenciais do Azure.

  A substituição da assinatura atual do marketplace a atualiza para sistemas Cloud Volumes ONTAP existentes e novos.

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**.

        O vídeo a seguir mostra as etapas para assinar o Azure Marketplace:

Assine o NetApp Intelligent Services no Azure Marketplace

Editar credenciais

Edite suas credenciais do Azure no Console. Por exemplo, você pode atualizar o segredo do cliente se um novo segredo tiver sido criado para o aplicativo principal do serviço.

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Credenciais da organização**.
3. Selecione o menu de ação para um conjunto de credenciais e, em seguida, selecione **Editar credenciais**.
4. Faça as alterações necessárias e selecione **Aplicar**.

Excluir credenciais

Se você não precisar mais de um conjunto de credenciais, poderá excluí-las. Você só pode excluir credenciais que não estejam associadas a um sistema.

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Credenciais da organização**.

3. Na página **Credenciais da organização**, selecione o menu de ações para um conjunto de credenciais e, em seguida, selecione **Excluir credenciais**.
4. Selecione **Excluir** para confirmar.

Google Cloud

Saiba mais sobre projetos e permissões do Google Cloud

Saiba como o NetApp Console usa as credenciais do Google Cloud para executar ações em seu nome e como essas credenciais são associadas às assinaturas do marketplace. Entender esses detalhes pode ser útil ao gerenciar as credenciais de um ou mais projetos do Google Cloud. Por exemplo, talvez você queira saber mais sobre a conta de serviço associada à VM do agente do Console.

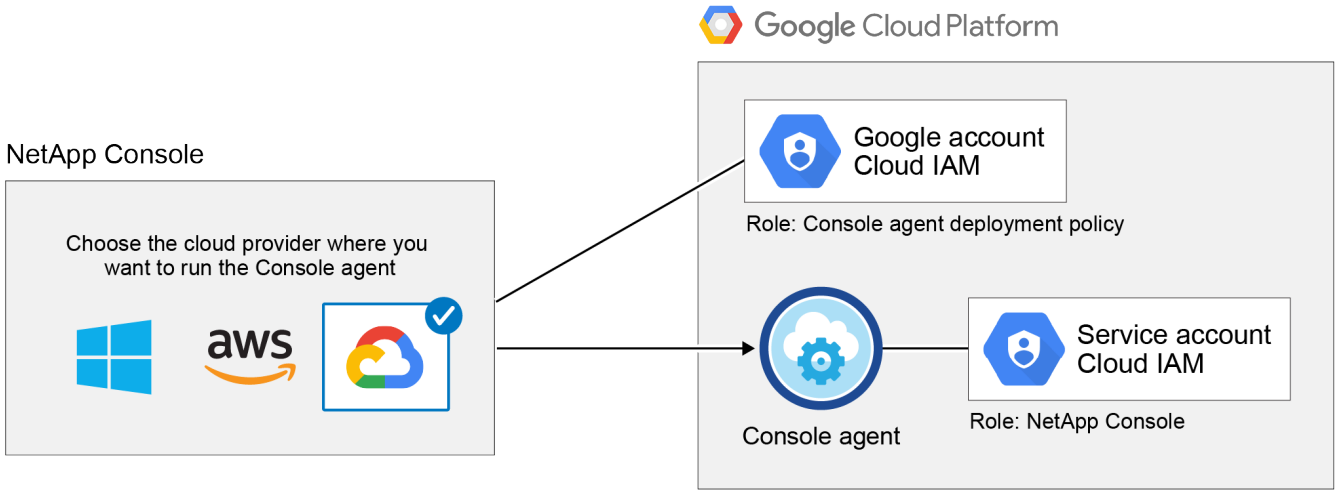
Projeto e permissões para o NetApp Console

Antes de usar o Console para gerenciar recursos no seu projeto do Google Cloud, você deve primeiro implantar um agente do Console. O agente não pode estar sendo executado em suas instalações ou em um provedor de nuvem diferente.

Dois conjuntos de permissões devem estar em vigor antes de você implantar um agente do Console diretamente do Console:

1. Você precisa implantar um agente do Console usando uma conta do Google que tenha permissões para iniciar a instância da VM do agente do Console a partir do Console.
2. Ao implantar o agente do Console, você será solicitado a selecionar um "conta de serviço" para a instância da VM. O Console obtém permissões da conta de serviço para criar e gerenciar sistemas Cloud Volumes ONTAP , gerenciar backups usando o backup e a recuperação do NetApp e muito mais. As permissões são fornecidas anexando uma função personalizada à conta de serviço.

A imagem a seguir descreve os requisitos de permissão descritos nos números 1 e 2 acima:



Para saber como configurar permissões, consulte as seguintes páginas:

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

- "Configurar permissões para o modo restrito"

Credenciais e assinaturas de mercado

Quando você implanta um agente do Console no Google Cloud, o Console cria um conjunto padrão de credenciais para a conta de serviço do Google Cloud no projeto em que o agente do Console reside. Essas credenciais devem estar associadas a uma assinatura do Google Cloud Marketplace para que você possa pagar pelos serviços de dados do Cloud Volumes ONTAP e do NetApp .

"Aprenda como associar uma assinatura do Google Cloud Marketplace" .

Observe o seguinte sobre credenciais do Google Cloud e assinaturas do marketplace:

- Apenas um conjunto de credenciais do Google Cloud pode ser associado a um agente do Console
- Você pode associar apenas uma assinatura do Google Cloud Marketplace às credenciais
- Você pode substituir uma assinatura de mercado existente por uma nova assinatura

Projeto para Cloud Volumes ONTAP

O Cloud Volumes ONTAP pode residir no mesmo projeto que o agente do Console ou em um projeto diferente. Para implantar o Cloud Volumes ONTAP em um projeto diferente, você precisa primeiro adicionar a conta de serviço e a função do agente do Console a esse projeto.

- "Aprenda a configurar a conta de serviço"
- "Aprenda a implantar o Cloud Volumes ONTAP no Google Cloud e selecione um projeto"

Gerenciar credenciais e assinaturas do Google Cloud para o NetApp Console

Você pode gerenciar as credenciais do Google Cloud associadas a uma instância de VM do agente do Console associando uma assinatura do marketplace e solucionando problemas no processo de assinatura. Ambas as tarefas garantem que você possa usar sua assinatura do marketplace para pagar por serviços de dados.

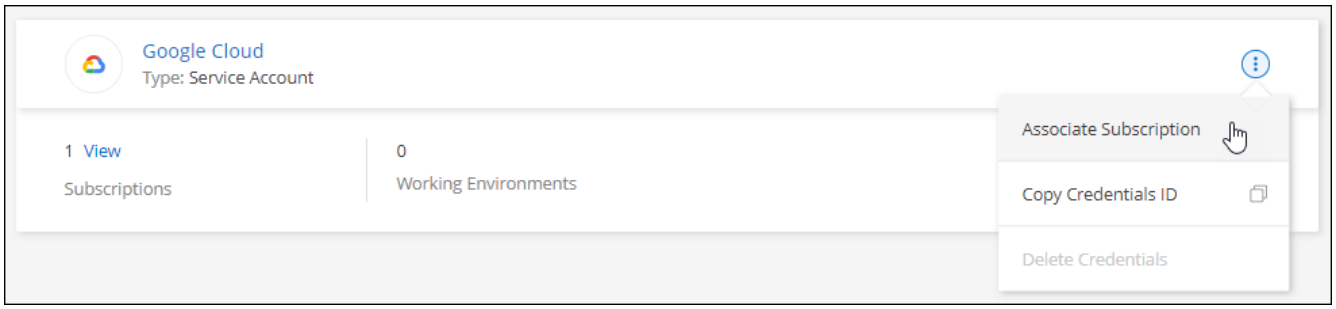
Associar uma assinatura do Marketplace às credenciais do Google Cloud

Quando você implanta um agente do Console no Google Cloud, o Console cria um conjunto padrão de credenciais associadas a uma instância de VM do agente do Console. A qualquer momento, você pode alterar a assinatura do Google Cloud Marketplace associada a essas credenciais. A assinatura permite que você crie um sistema Cloud Volumes ONTAP com pagamento conforme o uso e use outros serviços de dados.

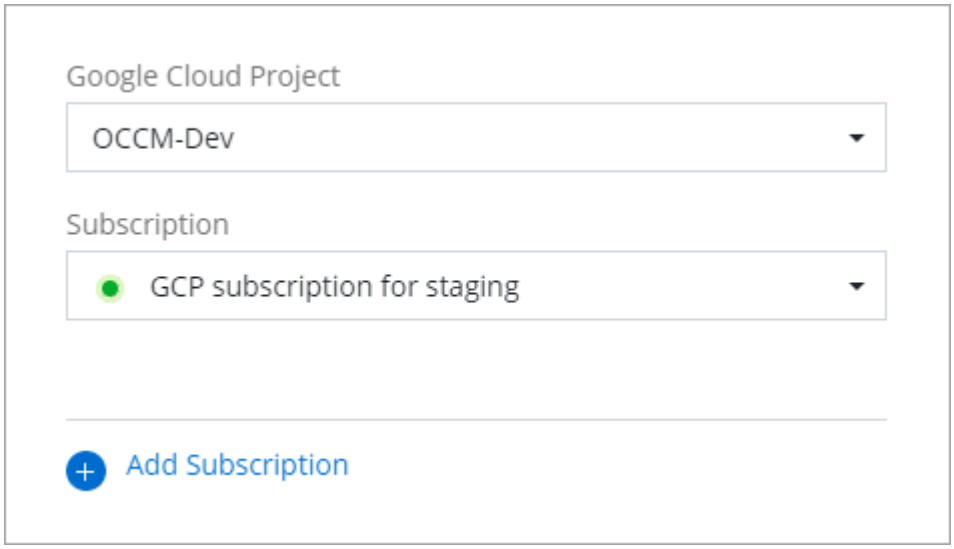
Substituir a assinatura atual do marketplace por uma nova assinatura altera a assinatura do marketplace para todos os sistemas Cloud Volumes ONTAP existentes e todos os novos sistemas.

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**. +nova captura de tela necessária
(TS)



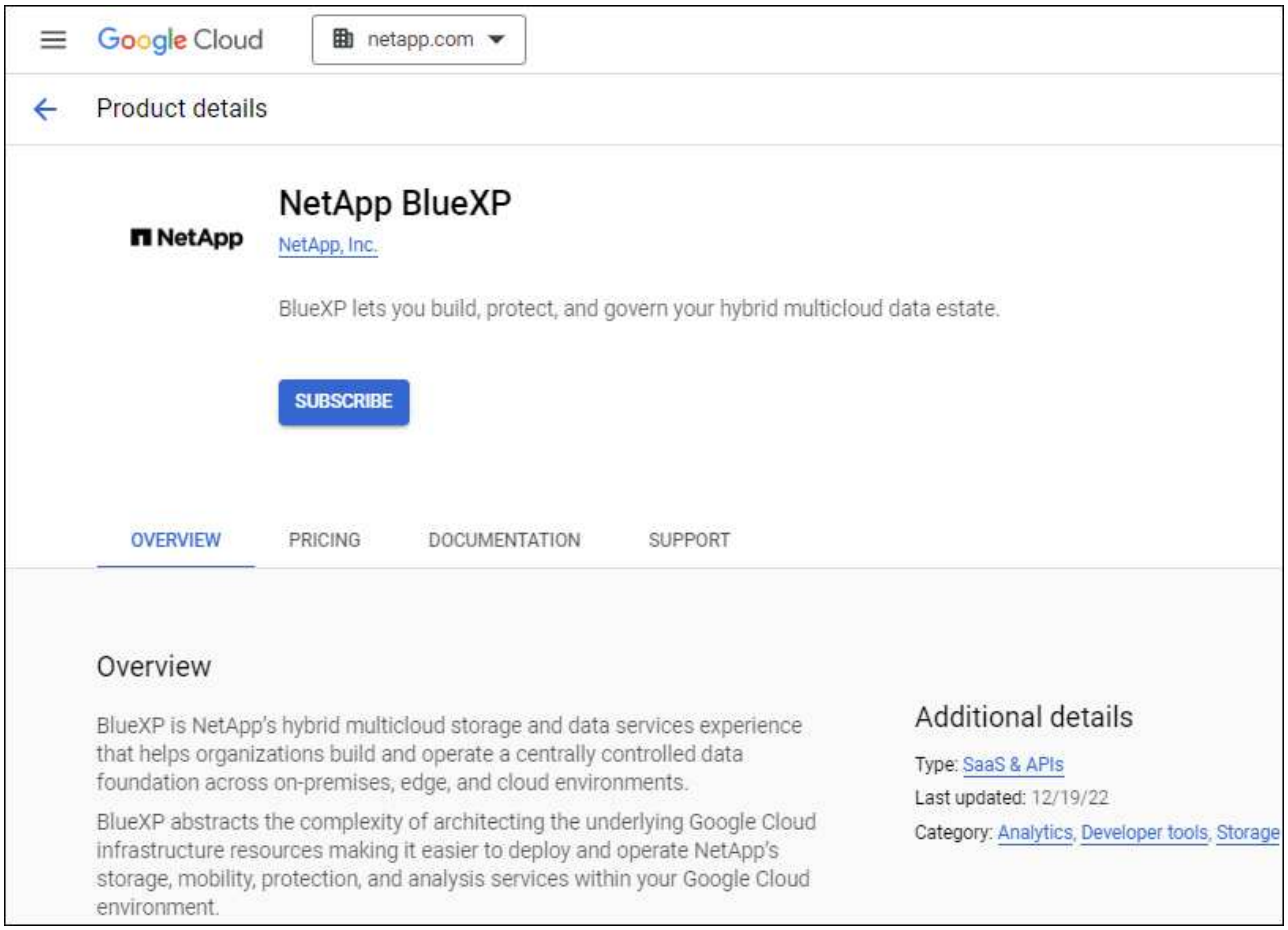
4. Para configurar uma assinatura existente com as credenciais selecionadas, selecione um projeto e uma assinatura do Google Cloud na lista suspensa e selecione **Configurar**.



5. 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 console do NetApp .

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.

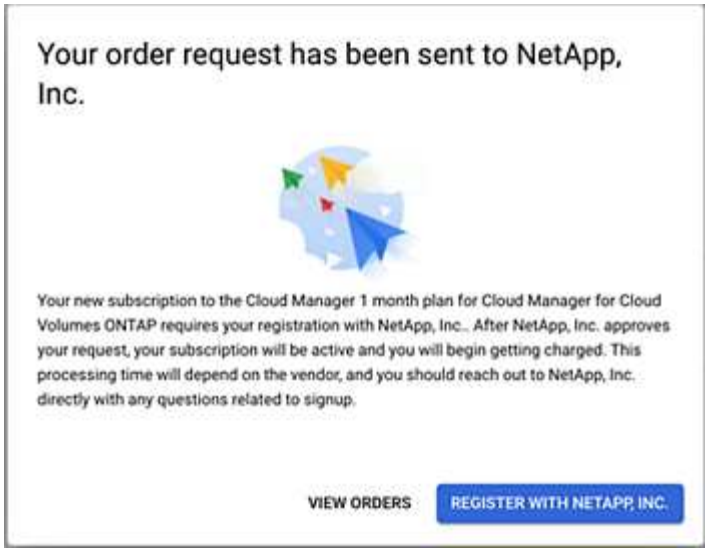


b. Selecione **Inscrever-se**.
c. Selecione a conta de cobrança apropriada e concorde com os termos e condições.
d. Selecione **Inscrever-se**.

   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 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.

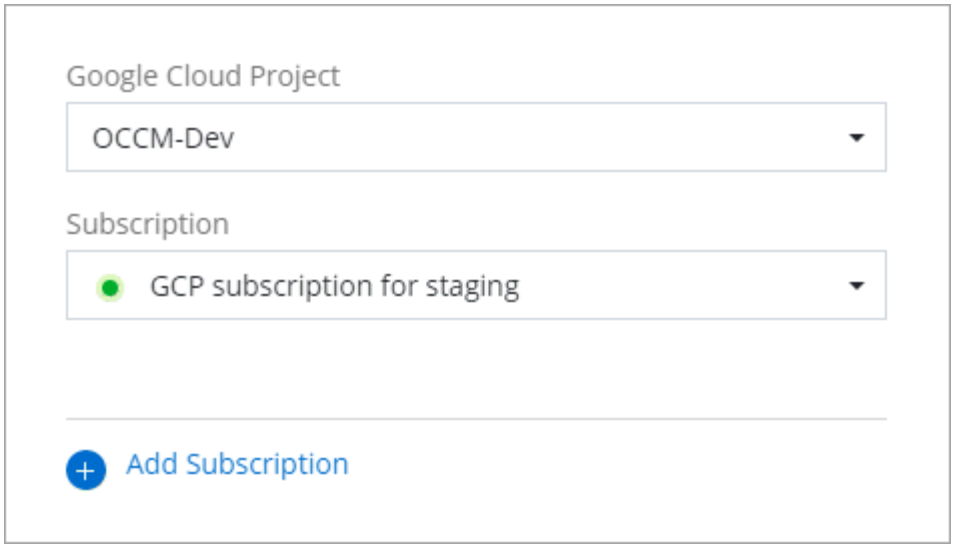
Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo essas etapas.

- Selecione **Salvar**.

  O vídeo a seguir mostra as etapas para assinar o Google Cloud Marketplace:

Assine no Google Cloud Marketplace

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

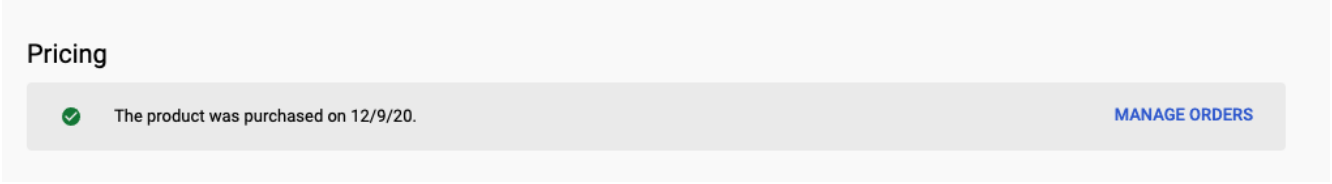


Solucionar problemas do processo de assinatura do Marketplace

Às vezes, a assinatura de serviços de dados da NetApp por meio do Google Cloud Marketplace pode ficar fragmentada devido a permissões incorretas ou ao não seguir acidentalmente o redirecionamento para o Console. Se isso acontecer, siga as etapas a seguir para concluir o processo de assinatura.

Passos

1. Navegue até o "Página da NetApp no Google Cloud Marketplace" para verificar o estado do pedido. Se a página indicar **Gerenciar no Provedor**, role para baixo e selecione **Gerenciar Pedidos**.



   - Se o pedido mostrar uma marca de seleção verde e isso for inesperado, outra pessoa da organização que usa a mesma conta de cobrança pode já estar inscrita. Se isso for inesperado ou se você precisar dos detalhes desta assinatura, entre em contato com sua equipe de vendas da NetApp .

   - Se o pedido mostrar um relógio e o status **Pendente**, volte para a página do marketplace e escolha **Gerenciar no Provedor** para concluir o processo conforme documentado acima.

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 .

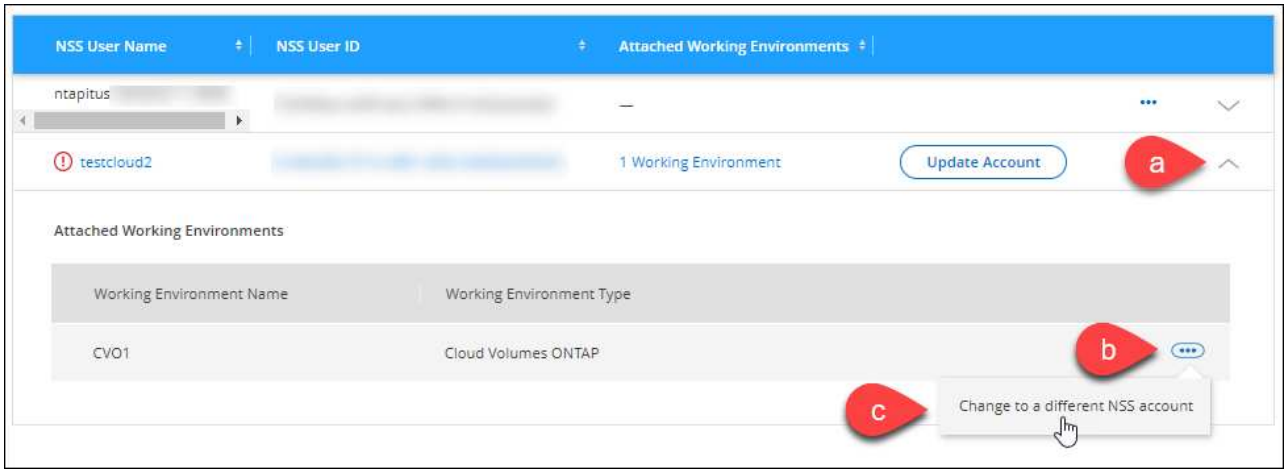
Anexar um sistema a uma conta NSS diferente

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.

Gerenciar credenciais associadas ao seu login do NetApp Console

Dependendo das ações que você realizou no Console, você pode ter associado credenciais do ONTAP e credenciais do NetApp Support Site (NSS) ao seu login de usuário. Você pode visualizar e gerenciar essas credenciais depois de associá-las. Por exemplo, se você alterar a senha dessas credenciais, será necessário atualizar a senha no Console.

Credenciais ONTAP

Os usuários precisam de credenciais de administrador do ONTAP para descobrir clusters do ONTAP no Console. No entanto, o acesso ao ONTAP System Manager depende se você está ou não usando um agente de console.

Sem um agente de console

Os usuários são solicitados a inserir suas credenciais do ONTAP para acessar o ONTAP System Manager para o cluster. Os usuários podem optar por salvar essas credenciais no Console, o que significa que não serão solicitados a inseri-las toda vez. As credenciais do usuário são visíveis apenas para o respectivo usuário e podem ser gerenciadas na página Credenciais do usuário.

Com um agente de console

Por padrão, os usuários não são solicitados a inserir suas credenciais do ONTAP para acessar o ONTAP System Manager. No entanto, um administrador do Console (com a função de administrador da organização) pode configurar o Console para solicitar que os usuários insiram suas credenciais do ONTAP . Quando essa configuração estiver habilitada, os usuários precisarão inserir suas credenciais do ONTAP sempre.

"Saber mais."

Credenciais NSS

As credenciais do NSS associadas ao seu login no NetApp Console permitem o registro de suporte, o gerenciamento de casos e o acesso ao Digital Advisor.

- Ao acessar **Suporte > Recursos** e se registrar para obter suporte, você será solicitado a associar as credenciais do NSS ao seu login.

  Isso registra sua organização ou conta para suporte e ativa o direito ao suporte. Somente um usuário em sua organização deve associar uma conta do NetApp Support Site ao seu login para se registrar para suporte e ativar o direito ao suporte. Após a conclusão, a página **Recursos** mostrará que sua conta está registrada para suporte.

  "Aprenda como se registrar para receber suporte"

- Ao acessar **Administração > Suporte > Gerenciamento de casos**, você será solicitado a inserir suas credenciais do NSS, caso ainda não tenha feito isso. Esta página permite que você crie e gerencie os casos de suporte associados à sua conta NSS e à sua empresa.
- Ao acessar o Digital Advisor no Console, você será solicitado a efetuar login no Digital Advisor inserindo

suas credenciais do NSS.

Observe o seguinte sobre a conta NSS associada ao seu login:

- A conta é gerenciada no nível do usuário, o que significa que ela não pode ser visualizada por outros usuários que efetuam login.
- Só pode haver uma conta NSS associada ao Digital Advisor e ao gerenciamento de casos de suporte por usuário.
- Se você estiver tentando associar uma conta do NetApp Support Site a um sistema Cloud Volumes ONTAP , só poderá escolher entre as contas NSS que foram adicionadas à organização da qual você é membro.

  As credenciais no nível da conta NSS são diferentes da conta NSS associada ao seu login. As credenciais de nível de conta do NSS permitem que você implante o Cloud Volumes ONTAP com BYOL, registre sistemas PAYGO e atualize seu software.

  "Saiba mais sobre como usar credenciais NSS com sua organização ou conta do NetApp Console" .

Gerencie suas credenciais de usuário

Gerencie suas credenciais de usuário atualizando o nome de usuário e a senha ou excluindo as credenciais.

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Credenciais do usuário**.
3. Se você ainda não tiver nenhuma credencial de usuário, poderá selecionar **Adicionar credenciais NSS** para adicionar sua conta do Site de Suporte NetApp .
4. Gerencie as credenciais existentes escolhendo as seguintes opções no menu Ações:
   - **Atualizar credenciais**: Atualize o nome de usuário e a senha da conta.
   - **Excluir credenciais**: Remova a conta NSS associada ao seu login do Console.

Monitorar as operações do NetApp Console

Você pode monitorar o status das operações que o Console está executando para ver se há algum problema que precisa ser resolvido. Você pode visualizar o status na página Auditoria, na Central de Notificações ou receber notificações por e-mail.

A tabela destaca os recursos da página Auditoria e do Centro de Notificações comparando-os.

Central de Notificações	Página de auditoria
Mostra status de alto nível para eventos e ações	Fornece detalhes de cada evento ou ação para investigação posterior
Mostra o status da sessão de login atual (as informações não aparecem na Central de Notificações depois que você faz logoff)	Mantém o status do último mês
Mostra apenas ações iniciadas na interface do usuário	Mostra todas as ações da IU ou APIs

Central de Notificações	Página de auditoria
Mostra ações iniciadas pelo usuário	Mostra todas as ações, sejam elas iniciadas pelo usuário ou pelo sistema
Filtrar resultados por importância	Filtrar por serviço, ação, usuário, status e muito mais
Oferece a capacidade de enviar notificações por e-mail aos usuários e a outras pessoas	Sem capacidade de e-mail

Auditar a atividade do usuário na página Auditoria

A página Auditoria mostra as ações que os usuários concluíram para gerenciar sua organização ou conta. Isso inclui ações de gerenciamento, como associação de usuários, criação de sistemas, criação de agentes e muito mais.

Use a página Auditoria para identificar quem executou uma ação ou seu status.

Passos

1. Selecione **Administração > Auditoria**.
2. Use os filtros acima da tabela para alterar quais ações serão exibidas na tabela.

   Por exemplo, você pode usar o filtro **Serviço** para mostrar ações relacionadas a um serviço específico ou pode usar o filtro **Usuário** para mostrar ações relacionadas a uma conta de usuário específica.

Baixe os logs de auditoria da página Auditoria

Você pode baixar os logs de auditoria da página Auditoria para um arquivo CSV. Isso permite que você mantenha um registro das ações que os usuários realizam na sua organização. O arquivo CSV inclui todas as colunas no arquivo CSV baixado, independentemente dos filtros ou colunas exibidas na página Auditoria.

Passos

1. Na página **Auditoria**, selecione o ícone de download no canto superior direito da tabela.

Monitore atividades usando o Centro de Notificações

As notificações rastreiam as operações do Console para confirmar o sucesso. Eles permitem que você visualize o status de muitas ações do Console que você iniciou durante sua sessão de login atual. Nem todos os serviços do Console reportam informações ao Centro de Notificações.

Você pode exibir as notificações selecionando o sino de notificação () na barra de menu. A cor da pequena bolha no sino indica o nível de gravidade mais alto que está ativo. Então, se você vir uma bolha vermelha, significa que há uma notificação importante que você deve consultar.

Você também pode configurar o Console para enviar certos tipos de notificações por e-mail para que você possa ser informado sobre atividades importantes do sistema, mesmo quando não estiver conectado ao sistema. Os e-mails podem ser enviados a qualquer usuário que faça parte da sua organização ou a qualquer outro destinatário que precise estar ciente de certos tipos de atividade do sistema. Veja comodefinir configurações de notificação por e-mail .

Comparando o Centro de Notificações com alertas

O Centro de Notificações permite que você visualize o status das operações iniciadas e configure notificações de alerta para determinados tipos de atividades do sistema. Enquanto isso, os alertas permitem que você visualize problemas ou riscos potenciais no seu ambiente de armazenamento ONTAP relacionados à capacidade, disponibilidade, desempenho, proteção e segurança.

"Saiba mais sobre os alertas do NetApp Console"

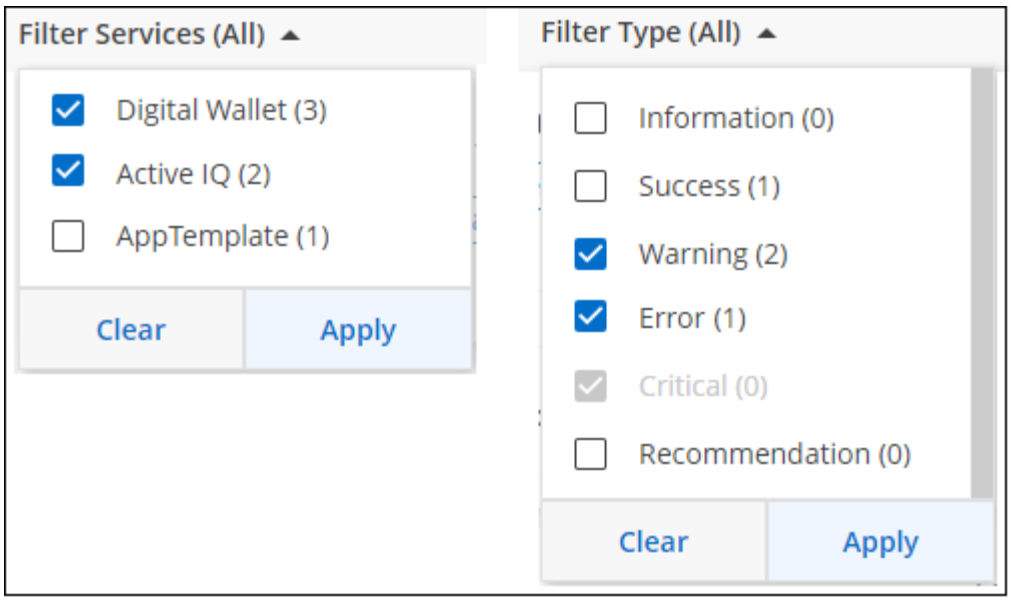
Tipos de notificação

O Console classifica as notificações nas seguintes categorias:

Tipo de notificação	Descrição
Crítico	Ocorreu um problema que pode levar à interrupção do serviço se uma ação corretiva não for tomada imediatamente.
Erro	Uma ação ou processo terminou em falha ou pode levar à falha se medidas corretivas não forem tomadas.
Aviso	Um problema que você deve estar ciente para garantir que ele não atinja a gravidade crítica. Notificações dessa gravidade não causam interrupção do serviço e pode não ser necessária ação corretiva imediata.
Recomendação	Uma recomendação do sistema para que você tome uma ação para melhorar o sistema ou um determinado serviço; por exemplo: economia de custos, sugestão de novos serviços, configuração de segurança recomendada, etc.
Informação	Uma mensagem que fornece informações adicionais sobre uma ação ou processo.
Sucesso	Uma ação ou processo concluído com sucesso.

Filtrar notificações

Por padrão, você verá todas as notificações ativas na Central de Notificações. Você pode filtrar as notificações que vê para mostrar apenas aquelas que são importantes para você. Você pode filtrar por "Serviço" e por "Tipo" de notificação.



Por exemplo, se você quiser ver apenas notificações de "Erro" e "Aviso" para operações do Console, selecione essas entradas e você verá apenas esses tipos de notificações.

Descartar notificações

Você pode remover notificações da página se não precisar mais vê-las. Você pode descartar notificações individualmente ou todas de uma vez.

Para descartar todas as notificações, na Central de Notificações, selecione ⋮ e selecione **Descartar tudo**.

Para descartar notificações individuais, passe o cursor sobre a notificação e selecione **Descartar**.

Definir configurações de notificação por e-mail

Você pode enviar tipos específicos de notificações por e-mail para ser informado sobre atividades importantes do sistema, mesmo quando não estiver conectado. Os e-mails podem ser enviados a qualquer usuário que faça parte da sua organização ou conta, ou a qualquer outro destinatário que precise estar ciente de certos tipos de atividade do sistema.

- O Console envia notificações por e-mail para o agente, licenças e assinaturas, NetApp Copy and Sync e NetApp Backup and Recovery.
- O envio de notificações por e-mail não é suportado quando o agente do Console está instalado em um site sem acesso à Internet.

Os filtros definidos na Central de Notificações não determinam os tipos de notificações que você recebe por e-mail. Por padrão, qualquer administrador da organização receberá e-mails para todas as notificações "Críticas" e "Recomendações". Essas notificações são válidas para todos os serviços. Você não pode optar por receber notificações apenas para determinados serviços, por exemplo, agentes ou NetApp Backup and Recovery.

Todos os outros usuários e destinatários estão configurados para não receber nenhum e-mail de notificação. Portanto, você precisará configurar as definições de notificação para quaisquer usuários adicionais.

Você deve ter a função de administrador da organização para personalizar as configurações de notificações.

Passos

1. Selecione **Administração > Configurações de notificações**.
2. Selecione **Usuários da organização** ou **Destinatários adicionais**.

   A página **Destinatários adicionais** permite que você configure o Console para notificar pessoas que são membros da sua organização do Console.

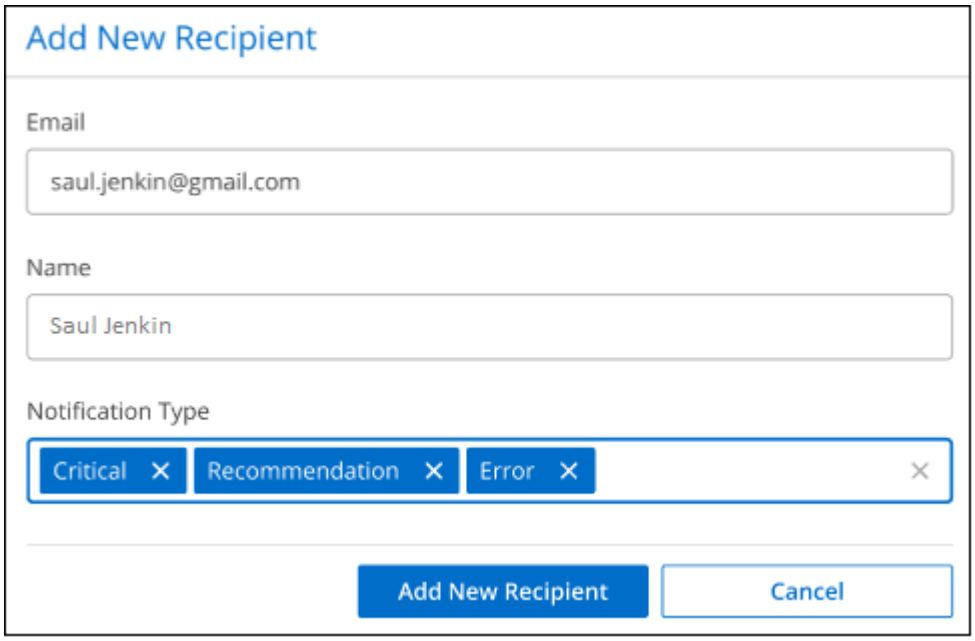
3. Selecione um usuário ou vários usuários na página *Usuários da organização* ou na página *Destinatários adicionais* e escolha o tipo de notificação a ser enviada:
   - Para fazer alterações para um único usuário, selecione o menu na coluna Notificações desse usuário, marque os tipos de Notificações a serem enviadas e selecione **Aplicar**.
   - Para fazer alterações para vários usuários, marque a caixa de cada usuário, selecione **Gerenciar notificações por e-mail**, marque os tipos de notificações a serem enviadas e selecione **Aplicar**.

Adicionar destinatários de e-mail adicionais

Os usuários que aparecem na página *Usuários da organização* são preenchidos automaticamente a partir dos usuários da sua organização ou conta. Você pode adicionar endereços de e-mail na página *Destinatários adicionais* para outras pessoas ou grupos que não têm acesso ao Console, mas que precisam ser notificados sobre determinados tipos de alertas e notificações.

Passos

1. Na página **Configurações de notificações**, selecione **Adicionar novos destinatários**.



2. Digite o nome, endereço de e-mail, selecione os tipos de notificações que o destinatário receberá e selecione **Adicionar novo destinatário**.

Referência

Console de manutenção do agente

Console de manutenção do agente do console

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

Acesse o console de manutenção do agente

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

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

Comandos de proxy transparentes

O console de manutenção do agente fornece comandos para configurar o agente para usar um servidor proxy transparente.

Visualizar a configuração atual do proxy transparente

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

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

Adicionar um servidor proxy transparente

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

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

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

Atualizar o certificado para um servidor proxy transparente

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

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

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

Remover um servidor proxy transparente

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

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

Ver ajuda para qualquer comando

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

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

Permissões

Resumo de permissões para o NetApp Console

Para usar os recursos e serviços do NetApp Console, você precisará fornecer permissões para que o Console possa executar operações no seu ambiente de nuvem. Use os links nesta página para acessar rapidamente as permissões necessárias com base no seu objetivo.

Permissões da AWS

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

Agentes de console

Meta	Descrição	Link
Implantar um agente do Console a partir do Console	O usuário que cria um agente do Console a partir do Console precisa de permissões específicas para implantar a instância na AWS.	"Configurar permissões da AWS"
Fornecer permissões para um agente do Console	Quando o Console implanta um agente do Console, ele anexa uma política à instância que fornece as permissões necessárias para gerenciar recursos e processos na sua conta da AWS. Você precisa configurar a política sozinho se implantar um agente do Console do AWS Marketplace, se instalar manualmente um agente do Console ou se"adicionar mais credenciais da AWS a um agente do Console" . Você também precisa garantir que a política esteja atualizada à medida que novas permissões forem adicionadas em versões subsequentes.	"Permissões da AWS para um agente do Console"

Backup e recuperação da NetApp

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

Cloud Volumes ONTAP

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

Cópia e sincronização da NetApp

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

FSx para ONTAP

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

Camadas de nuvem da NetApp

Meta	Descrição	Link
Clusters ONTAP locais em camadas para o Amazon S3	Quando você habilita o NetApp Cloud Tiering para AWS, o assistente solicita que você insira uma chave de acesso e uma chave secreta. Essas credenciais são passadas ao cluster ONTAP para que o ONTAP possa hierarquizar dados no bucket S3.	"Configurar permissões S3 para camadas"

Permissões do Azure

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

Agente de console

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

Backup e recuperação da NetApp

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

Meta	Descrição	Link
Fazer backup de clusters ONTAP locais no armazenamento de blobs do Azure	Ao usar o NetApp Backup and Recovery para fazer backup de clusters ONTAP locais, você precisa adicionar permissões a um agente do Console para usar a funcionalidade "Pesquisar e restaurar".	"Faça backup de dados ONTAP locais no armazenamento de Blobs do Azure com Backup e Recuperação"

Cópia e sincronização do NetApp

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

Permissões do Google Cloud

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

Agentes de console

Meta	Descrição	Link
Implantar um agente do Console a partir do Console	O usuário do Google Cloud que implanta um agente do Console a partir do Console precisa de permissões específicas para implantar um agente do Console no Google Cloud.	"Configurar permissões para criar um agente do Console"
Fornecer permissões para um agente do Console	A conta de serviço para uma instância de VM do agente do Console deve ter permissões específicas para operações diárias. Você precisa associar a conta de serviço a um agente do Console durante a implantação. Você também precisa garantir que a política esteja atualizada à medida que novas permissões forem adicionadas em versões subsequentes.	"Configurar permissões para um agente do Console"

Backup e recuperação da NetApp

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

Meta	Descrição	Link
Faça backup de clusters ONTAP locais no Google Cloud	Ao usar o NetApp Backup and Recovery para fazer backup de clusters ONTAP locais, você precisa adicionar permissões a um agente do Console para usar a funcionalidade "Pesquisar e restaurar".	"Faça backup de dados ONTAP locais no Google Cloud Storage com Backup e Recuperação"

Cópia e sincronização da NetApp

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

Permissões do StorageGRID

O Console requer permissões StorageGRID para dois serviços.

Backup e recuperação da NetApp

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

Camadas de nuvem da NetApp

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

Permissões da AWS para o agente do Console

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

Políticas de IAM

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

Observe o seguinte:

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

Selecione sua região para visualizar as políticas necessárias:

Regiões padrão

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

Política nº 1

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DescribeTags",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:CreatePlacementGroup",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
```

```
                "ec2:UnassignPrivateIpAddresses",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteRoute",
                "ec2:DeletePlacementGroup",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeVolumesModifications",
                "ec2:ModifyVolume",
                "cloudformation:CreateStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "cloudformation:DeleteStack",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:ListInstanceProfiles",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DeleteInstanceProfile",
                "iam:GetRolePolicy",
                "iam:GetRole",
                "sts:DecodeAuthorizationMessage",
                "sts:AssumeRole",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketPolicy",
                "s3:GetBucketAcl",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:PutObject",
                "s3:ListAllMyBuckets",
                "s3:GetObject",
```

```
                "s3:GetEncryptionConfiguration",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "fsx:Describe*",
                "fsx:List*",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "cvoServicePolicy"
        },
        {
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "kms:List*",
                "kms:Describe*",
                "ec2:DescribeVpcEndpoints",
                "kms:ListAliases",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
                "glue:BatchDeletePartition"
```

```
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "backupPolicy"
        },
        {
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketAcl",
                "s3:PutBucketPublicAccessBlock",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",
                "s3:DeleteBucket",
                "s3:GetObjectVersionTagging",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:PutObjectVersionTagging",
                "s3:PutObjectRetention",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketVersioning",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:PutBucketPolicy",
                "s3:PutBucketOwnershipControls"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
```

```
            ],
            "Effect": "Allow",
            "Sid": "backupS3Policy"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:DeleteBucket"
            ],
            "Resource": [
                "arn:aws:s3:::fabric-pool*"
            ],
            "Effect": "Allow",
            "Sid": "fabricPoolS3Policy"
        },
        {
            "Action": [
                "ec2:DescribeRegions"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "fabricPoolPolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/netapp-adc-manager": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
```

```
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume",
                "ec2:StopInstances",
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        }
    ]
```

```
}
```

Política nº 2

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

Regiões GovCloud (EUA)

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListInstanceProfiles",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "ec2:ModifyVolumeAttribute",
                "sts:DecodeAuthorizationMessage",
                "ec2:DescribeImages",
                "ec2:DescribeRouteTables",
                "ec2:DescribeInstances",
                "iam:PassRole",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
```

```
                "ec2:DescribeSnapshots",
                "ec2:StopInstances",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:CreateBucket",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
```

```
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::fabric-pool*"
            ]
        },
        {
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::netapp-backup-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
```

```
                "arn:aws-us-gov:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-us-gov:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Regiões secretas

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Regiões ultrasecretas

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Como as permissões da AWS são usadas

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

Amazon FSx para ONTAP

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

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

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

Descoberta de bucket do Amazon S3

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

s3:ObterConfiguração de Criptografia

Backup e recuperação da NetApp

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

- s3:ObterLocalização do Balde
- s3:ListarTodosOsMeusBuckets
- s3:ListBucket
- s3:CriarBucket
- s3:ObterConfiguração do Ciclo de Vida
- s3:PutLifecycleConfiguration
- s3:PutBucketTagging
- s3:ListBucketVersões
- s3:ObterBucketAcl
- s3:PutBucketBloco de Acesso Público
- kms:Lista*

- kms:Descreva*
- s3:ObterObjeto
- ec2:DescreverVpcEndpoints
- kms:ListAliases
- s3:PutEncryptionConfiguration

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

- s3:CriarBucket
- s3:ExcluirObjeto
- s3:ExcluirVersãoDoObjeto
- s3:ObterBucketAcl
- s3:ListBucket
- s3:ListBucketVersões
- s3:ListBucketMultipartUploads
- s3:ColocarObjeto
- s3:ColocarBucketAcl
- s3:PutLifecycleConfiguration
- s3:PutBucketBloco de Acesso Público
- s3:AbortarUploadMultipart
- s3:ListMultipartUploadParts
- athena:Execução de Consulta Inicial
- athena:ObterResultados da Consulta
- athena:GetQueryExecution
- athena:PararExecuçãoDeConsulta
- cola:CriarBancoDeDados
- cola:CriarTabela
- cola:BatchDeletePartition

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

- s3:ObterTag deVersão do Objeto
- s3:GetBucketObjectLockConfiguration
- s3:ObterVersãoDoObjetoAcl
- s3:PutObjectTagging
- s3:ExcluirObjeto
- s3:ExcluirMarcaçãoDeObjeto
- s3:ObterRetençãoDeObjeto

- s3:ExcluirMarcaçãoDeVersãoDoObjeto
- s3:ColocarObjeto
- s3:ObterObjeto
- s3:PutBucketObjectLockConfiguração
- s3:ObterConfiguração do Ciclo de Vida
- s3:ListBucketPorTags
- s3:Obter marcação de balde
- s3:ExcluirVersãoDoObjeto
- s3:ListBucketVersões
- s3:ListBucket
- s3:PutBucketTagging
- s3:ObterMarcaçãoDeObjeto
- s3:PutBucketVersionamento
- s3:PutObjectVersionTagging
- s3:GetBucketVersionamento
- s3:ObterBucketAcl
- s3:Ignorar Governança Retenção
- s3:PutObjectRetention
- s3:ObterLocalização do Balde
- s3:ObterVersãoDoObjeto

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

- s3:PolíticaPutBucket
- s3:PutBucketOwnershipControls

Classificação

O agente faz as seguintes solicitações de API para implantar a Classificação de Dados NetApp :

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

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

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

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

Cloud Volumes ONTAP

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

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

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

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

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

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

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

Registro de alterações

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

9 de setembro de 2024

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

Visualizar as permissões que foram removidas da política

```
        {
            "Action": [
                "ec2:DescribeRegions",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "iam:GetInstanceProfile"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "K8sServicePolicy"
        },
        {
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudwatch:GetMetricStatistics",
                "cloudformation:ListStacks"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "GFCservicePolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GFCInstance": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
```

9 de maio de 2024

As seguintes permissões agora são necessárias para o Cloud Volumes ONTAP:

ec2:DescreverZonasDeDisponibilidade

6 de junho de 2023

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

kms:GerarChaveDeDadosSemTextoSimples

14 de fevereiro de 2023

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

ec2:DescreverVpcEndpoints

Permissões do Azure para o agente do Console

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

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

Implantando do NetApp Console

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

Implantação manual ou do Azure Marketplace

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

Você precisará garantir que a função esteja atualizada à medida que novas permissões forem adicionadas em versões subsequentes. Se novas permissões forem necessárias, elas serão listadas nas notas de versão.

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

```
{
    "Name": "Console Operator",
    "Actions": [
                    "Microsoft.Compute/disks/delete",
                    "Microsoft.Compute/disks/read",
                    "Microsoft.Compute/disks/write",
                    "Microsoft.Compute/locations/operations/read",
                    "Microsoft.Compute/locations/vmSizes/read",
```

```
                    "Microsoft.Resources/subscriptions/locations/read",
                    "Microsoft.Compute/operations/read",
                    "Microsoft.Compute/virtualMachines/instanceView/read",
                    "Microsoft.Compute/virtualMachines/powerOff/action",
                    "Microsoft.Compute/virtualMachines/read",
                    "Microsoft.Compute/virtualMachines/restart/action",
                    "Microsoft.Compute/virtualMachines/deallocate/action",
                    "Microsoft.Compute/virtualMachines/start/action",
                    "Microsoft.Compute/virtualMachines/vmSizes/read",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/images/read",
                    "Microsoft.Network/locations/operationResults/read",
                    "Microsoft.Network/locations/operations/read",
                    "Microsoft.Network/networkInterfaces/read",
                    "Microsoft.Network/networkInterfaces/write",
                    "Microsoft.Network/networkInterfaces/join/action",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/networkSecurityGroups/write",
                    "Microsoft.Network/networkSecurityGroups/join/action",
                    "Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
                    "Microsoft.Network/virtualNetworks/subnets/read",
                    "Microsoft.Network/virtualNetworks/subnets/write",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",

"Microsoft.Network/virtualNetworks/virtualMachines/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
                    "Microsoft.Resources/deployments/operations/read",
                    "Microsoft.Resources/deployments/read",
                    "Microsoft.Resources/deployments/write",
                    "Microsoft.Resources/resources/read",

"Microsoft.Resources/subscriptions/operationresults/read",

"Microsoft.Resources/subscriptions/resourceGroups/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",
                    "Microsoft.Storage/checknameavailability/read",
                    "Microsoft.Storage/operations/read",
```

```
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Storage/storageAccounts/read",
                    "Microsoft.Storage/storageAccounts/delete",
                    "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/listAccountSas/action",
                    "Microsoft.Storage/usages/read",
                    "Microsoft.Compute/snapshots/write",
                    "Microsoft.Compute/snapshots/read",
                    "Microsoft.Compute/availabilitySets/write",
                    "Microsoft.Compute/availabilitySets/read",
                    "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write",
                    "Microsoft.Network/loadBalancers/read",
                    "Microsoft.Network/loadBalancers/write",
                    "Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/backendAddressPools/join/action",

"Microsoft.Network/loadBalancers/loadBalancingRules/read",
                    "Microsoft.Network/loadBalancers/probes/read",
                    "Microsoft.Network/loadBalancers/probes/join/action",
                    "Microsoft.Authorization/locks/*",
                    "Microsoft.Network/routeTables/join/action",
                    "Microsoft.NetApp/netAppAccounts/read",
                    "Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
                    "Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acti
on",
```

```
"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
                    "Microsoft.Network/privateEndpoints/read",
                    "Microsoft.Network/privateDnsZones/write",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
                    "Microsoft.Network/virtualNetworks/join/action",
                    "Microsoft.Network/privateDnsZones/A/write",
                    "Microsoft.Network/privateDnsZones/read",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
                    "Microsoft.Insights/Metrics/Read",
                    "Microsoft.Compute/virtualMachines/extensions/write",
                    "Microsoft.Compute/virtualMachines/extensions/delete",
                    "Microsoft.Compute/virtualMachines/extensions/read",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Network/networkInterfaces/delete",
                    "Microsoft.Network/networkSecurityGroups/delete",
                    "Microsoft.Resources/deployments/delete",
                    "Microsoft.Compute/diskEncryptionSets/read",
                    "Microsoft.Compute/snapshots/delete",
                    "Microsoft.Network/privateEndpoints/delete",
                    "Microsoft.Compute/availabilitySets/delete",
                    "Microsoft.KeyVault/vaults/read",
                    "Microsoft.KeyVault/vaults/accessPolicies/write",
                    "Microsoft.Compute/diskEncryptionSets/write",
                    "Microsoft.KeyVault/vaults/deploy/action",
                    "Microsoft.Compute/diskEncryptionSets/delete",
                    "Microsoft.Resources/tags/read",
                    "Microsoft.Resources/tags/write",
                    "Microsoft.Resources/tags/delete",
                    "Microsoft.Network/applicationSecurityGroups/write",
                    "Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

"Microsoft.Network/networkSecurityGroups/securityRules/write",
                    "Microsoft.Network/applicationSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/securityRules/delete",
                    "Microsoft.Synapse/workspaces/write",
```

```
                    "Microsoft.Synapse/workspaces/read",
                    "Microsoft.Synapse/workspaces/delete",
                    "Microsoft.Synapse/register/action",
                    "Microsoft.Synapse/checkNameAvailability/action",
                    "Microsoft.Synapse/workspaces/operationStatuses/read",
                    "Microsoft.Synapse/workspaces/firewallRules/read",

"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
                    "Microsoft.Synapse/workspaces/operationResults/read",

"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",

"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
                    "Microsoft.Compute/images/write",

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

Como as permissões do Azure são usadas

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

Azure NetApp Files

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

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

Backup e recuperação da NetApp

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

- Microsoft.Storage/storageAccounts/listkeys/ação
- Microsoft.Storage/storageAccounts/leitura
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/ação
- Microsoft.KeyVault/cofres/leitura
- Microsoft.KeyVault/vaults/accessPolicies/gravação
- Microsoft.Network/networkInterfaces/leitura
- Microsoft.Recursos/assinaturas/locais/leitura
- Microsoft.Network/redes virtuais/leitura
- Microsoft.Network/virtualNetworks/sub-redes/leitura
- Microsoft.Recursos/assinaturas/grupos de recursos/leitura
- Microsoft.Recursos/assinaturas/grupos de recursos/recursos/leitura
- Microsoft.Recursos/assinaturas/grupos de recursos/gravação
- Microsoft.Autorização/bloqueios/*
- Microsoft.Network/privateEndpoints/gravação
- Microsoft.Network/privateEndpoints/leitura
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/gravação
- Microsoft.Network/virtualNetworks/join/ação
- Microsoft.Network/privateDnsZones/A/gravação
- Microsoft.Network/privateDnsZones/leitura
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/leitura
- Microsoft.Network/networkInterfaces/excluir
- Microsoft.Network/networkSecurityGroups/excluir
- Microsoft.Recursos/implantações/excluir
- Microsoft.ManagedIdentity/userAssignedIdentities/atribuir/ação

O agente faz as seguintes solicitações de API quando você usa a funcionalidade Pesquisar e Restaurar:

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

- Microsoft.Synapse/workspaces/privateEndpointConnectionsAprovação/ação

Classificação de dados da NetApp

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

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

Ação	Usado para configuração?	Usado para operações diárias?
Microsoft.Storage/storageAccounts/blobServices/containers/read	Sim	Sim
Microsoft.Network/networkInterfaces/leitura	Sim	Sim
Microsoft.Network/networkInterfaces/escrever	Sim	Não
Microsoft.Network/networkInterfaces/join/ação	Sim	Não
Microsoft.Network/networkSecurityGroups/leitura	Sim	Sim
Microsoft.Network/networkSecurityGroups/gravação	Sim	Não
Microsoft.Recursos/assinaturas/locais/leitura	Sim	Sim
Microsoft.Network/locais/resultadosdaoperação/leitura	Sim	Sim
Microsoft.Network/locais/operações/leitura	Sim	Sim
Microsoft.Network/redes virtuais/leitura	Sim	Sim
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/ler	Sim	Sim
Microsoft.Network/virtualNetworks/sub-redes/leitura	Sim	Sim
Microsoft.Network/virtualNetworks/sub-redes/virtualMachines/leitura	Sim	Sim
Microsoft.Network/redes virtuais/máquinas virtuais/leitura	Sim	Sim
Microsoft.Network/virtualNetworks/sub-redes/juntar/ação	Sim	Não
Microsoft.Network/virtualNetworks/sub-redes/gravação	Sim	Não
Microsoft.Network/routeTables/join/ação	Sim	Não
Microsoft.Recursos/implantações/operações/leitura	Sim	Sim
Microsoft.Recursos/implantações/leitura	Sim	Sim
Microsoft.Recursos/implantações/gravação	Sim	Não

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

Cloud Volumes ONTAP

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

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

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

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

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

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

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

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

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

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

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

Hierarquização

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

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

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

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

Registro de alterações

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

9 de setembro de 2024

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

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

22 de agosto de 2024

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

- Microsoft.Compute/virtualMachineScaleSets/gravação

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

5 de dezembro de 2023

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

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

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

12 de maio de 2023

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

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

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

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

23 de março de 2023

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

Essa permissão ainda é necessária para o Cloud Volumes ONTAP.

5 de janeiro de 2023

As seguintes permissões foram adicionadas à política JSON:

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

  Essas permissões são necessárias para o NetApp Backup and Recovery.

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

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

Permissões do Google Cloud para o agente do Console

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

Permissões de conta de serviço

A função personalizada mostrada abaixo fornece as permissões que um agente do Console precisa para gerenciar recursos e processos na sua rede do Google Cloud.

Você precisará aplicar essa função personalizada a uma conta de serviço que será anexada à VM do agente do Console.

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

Você também precisa garantir que a função esteja atualizada, pois novas permissões são adicionadas em versões subsequentes. Se novas permissões forem necessárias, elas serão listadas nas notas de versão.

```
title: NetApp Console agent
description: Permissions for the service account associated with the
Console agent instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
```

```
- compute.instances.addAccessConfig
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
- compute.instanceGroups.get
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
```

```
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
```

Como as permissões do Google Cloud são usadas

Ações	Propósito
- compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use	Para criar e gerenciar discos para Cloud Volumes ONTAP.
- computar.firewalls.criar - computar.firewalls.excluir - computar.firewalls.obter - computar.firewalls.listar	Para criar regras de firewall para o Cloud Volumes ONTAP.
- computar.globalOperations.get	Para obter o status das operações.
- compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly	Para obter imagens para instâncias de VM.

Ações	Propósito
- compute.instances.attachDisk - compute.instances.detachDisk	Para anexar e desanexar discos ao Cloud Volumes ONTAP.
- computar.instâncias.criar - computar.instâncias.excluir	Para criar e excluir instâncias de VM do Cloud Volumes ONTAP .
- computar.instâncias.obter	Para listar instâncias de VM.
- compute.instances.getSerialPortOutput	Para obter logs do console.
- compute.instances.list	Para recuperar a lista de instâncias em uma zona.
- compute.instances.setDeletionProtection	Para definir a proteção contra exclusão na instância.
- compute.instances.setLabels	Para adicionar rótulos.
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	Para alterar o tipo de máquina do Cloud Volumes ONTAP.
- compute.instances.setMetadata	Para adicionar metadados.
- computar.instâncias.setTags	Para adicionar tags para regras de firewall.
- calcular.instâncias.iniciar - calcular.instâncias.parar - calcular.instâncias.atualizarDispositivoDeExibição	Para iniciar e parar o Cloud Volumes ONTAP.
- calcular.tiposdemáquina.obter	Para obter o número de núcleos para verificar cotas.
- computar.projetos.obter	Para dar suporte a multiprojetos.
- compute.snapshots.create - compute.snapshots.delete - compute.snapshots.get - compute.snapshots.list - compute.snapshots.setLabels	Para criar e gerenciar instantâneos de disco persistentes.
- compute.networks.get - compute.networks.list - compute.regions.get - compute.regions.list - compute.subnetworks.get - compute.subnetworks.list - compute.zoneOperations.get - compute.zones.get - compute.zones.list	Para obter as informações de rede necessárias para criar uma nova instância de máquina virtual do Cloud Volumes ONTAP .
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifests.get - deploymentmanager.manifests.list - deploymentmanager.operations.get - deploymentmanager.operations.list - deploymentmanager.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProviders.get - deploymentmanager.typeProviders.list - deploymentmanager.types.get - deploymentmanager.types.list	Para implantar a instância da máquina virtual do Cloud Volumes ONTAP usando o Google Cloud Deployment Manager.
- logging.logEntries.list - logging.privateLogEntries.list	Para obter unidades de log de pilha.

Ações	Propósito
- gerenciador de recursos.projetos.obter	Para dar suporte a multiprojetos.
- storage.buckets.create - storage.buckets.delete - storage.buckets.get - storage.buckets.list - storage.buckets.update	Para criar e gerenciar um bucket do Google Cloud Storage para hierarquização de dados.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.list - cloudkms.keyRings.list	Para usar chaves de criptografia gerenciadas pelo cliente do Cloud Key Management Service com o Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - storage.objects.get - storage.objects.list	Para definir uma conta de serviço na instância do Cloud Volumes ONTAP . Esta conta de serviço fornece permissões para hierarquização de dados para um bucket do Google Cloud Storage.
- computar.endereços.lista	Para recuperar os endereços em uma região ao implantar um par HA.
- compute.backendServices.create - compute.regionBackendServices.create - compute.regionBackendServices.get - compute.regionBackendServices.list	Para configurar um serviço de backend para distribuir tráfego em um par HA.
- compute.networks.updatePolicy	Para aplicar regras de firewall nas VPCs e sub-redes para um par HA.
- compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	Para habilitar a classificação de dados do NetApp .
- compute.instanceGroups.get - compute.addresses.get - compute.instances.updateNetworkInterface	Para criar e gerenciar VMs de armazenamento em pares Cloud Volumes ONTAP HA.
- monitoramento.timeSeries.list - armazenamento.buckets.getIamPolicy	Para descobrir informações sobre os buckets do Google Cloud Storage.
- cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.getIamPolicy - cloudkms.cryptoKeys.list - cloudkms.cryptoKeys.setIamPolicy - cloudkms.keyRings.get - cloudkms.keyRings.getIamPolicy - cloudkms.keyRings.list - cloudkms.keyRings.setIamPolicy	Para selecionar suas próprias chaves gerenciadas pelo cliente no assistente de ativação do NetApp Backup and Recovery em vez de usar as chaves de criptografia padrão gerenciadas pelo Google.

Registro de alterações

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

2023-02-06

A seguinte permissão foi adicionada a esta política:

- computar.instâncias.atualizarInterface de Rede

Esta permissão é necessária para o Cloud Volumes ONTAP.

2023-01-27

As seguintes permissões foram adicionadas à política:

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

Essas permissões são necessárias para o NetApp Backup and Recovery.

Portos

Regras de grupo de segurança do agente de console na AWS

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

Regras de entrada

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

Regras de saída

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

Regras básicas de saída

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

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

Regras avançadas de saída

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

O endereço IP de origem é o host do agente.

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

Regras de grupo de segurança do agente de console no Azure

O grupo de segurança do Azure para o agente requer regras de entrada e saída. O NetApp Console cria automaticamente esse grupo de segurança quando você cria um agente do Console a partir do Console. Para outras opções de instalação, você precisa configurar esse grupo de segurança manualmente.

Regras de entrada

Protocolo	Porta	Propósito
SSH	22	Fornece acesso SSH ao host do agente

Protocolo	Porta	Propósito
HTTP	80	• Fornece acesso HTTP dos navegadores da web do cliente para a interface do usuário local • Usado durante o processo de atualização do Cloud Volumes ONTAP
HTTPS	443	Fornece acesso HTTPS dos navegadores da Web do cliente à interface do usuário local e conexões da instância de classificação de dados do NetApp
TCP	3128	Fornece ao Cloud Volumes ONTAP acesso à Internet para enviar mensagens do AutoSupport ao Suporte da NetApp . Você deve abrir esta porta manualmente após a implantação. "Aprenda como o agente é usado como proxy para mensagens do AutoSupport"

Regras de saída

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

Regras básicas de saída

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

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

Regras avançadas de saída

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

O endereço IP de origem é o host do agente.

Serviço	Protocolo	Porta	Destino	Propósito
Chamadas de API e AutoSupport	HTTPS	443	Gerenciamento de cluster de Internet de saída e ONTAP LIF	Chamadas de API para o Azure, para o ONTAP, para a Classificação de Dados do NetApp e envio de mensagens de AutoSupport para o NetApp
Chamadas de API	TCP	8080	Classificação de Dados	Sondar a instância de classificação de dados durante a implantação
DNS	UDP	53	DNS	Usado para resolução de DNS pelo Console

Regras de firewall do agente no Google Cloud

As regras de firewall do Google Cloud para o agente exigem regras de entrada e saída. O NetApp Console cria automaticamente esse grupo de segurança quando você cria um agente do Console a partir do Console. Para outras opções de instalação, você precisa configurar esse grupo de segurança manualmente.

Regras de entrada

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

Regras de saída

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

Regras básicas de saída

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

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

Regras avançadas de saída

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

O endereço IP de origem é o host do agente.

Serviço	Protocolo	Porta	Destino	Propósito
Chamadas de API e AutoSupport	HTTPS	443	Gerenciamento de cluster de Internet de saída e ONTAP LIF	Chamadas de API para o Google Cloud, para o ONTAP, para a classificação de dados da NetApp e envio de mensagens de AutoSupport para a NetApp
Chamadas de API	TCP	8080	Classificação de Dados	Sondar a instância de classificação de dados durante a implantação
DNS	UDP	53	DNS	Usado para resolução de DNS por classificação de dados

Portas para o agente do Console local

O agente do Console usa portas *de entrada* quando instalado manualmente em um host Linux local. Consulte essas portas para fins de planejamento.

Essas regras de entrada se aplicam a todos os modos de implantação do NetApp Console.

Protocolo	Porta	Propósito
HTTP	80	• Fornece acesso HTTP dos navegadores da web do cliente para a interface do usuário local • Usado durante o processo de atualização do Cloud Volumes ONTAP
HTTPS	443	Fornece acesso HTTPS dos navegadores da web do cliente para a interface do usuário local

Pontos de acesso de rede necessários para 3.9.55 e abaixo

Este tópico detalha o acesso à rede necessário para versões do modo padrão do NetApp Console anteriores à versão 4.0.0 do NetApp Console, o agente do NetApp Console e o acesso de saída à Internet dos serviços de dados do NetApp , além da capacidade de contatar os endpoints necessários. Você precisa garantir que o Console e quaisquer agentes que você instalar tenham o acesso de rede correto para funcionar corretamente.

Você precisará configurar o acesso à rede para computadores que acessam o NetApp Console como software como serviço (SaaS) e para quaisquer agentes do Console que você instalar no local ou na nuvem. Você também pode precisar de endpoints adicionais para determinados serviços de dados da NetApp , incluindo o Cloud Volumes ONTAP.

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

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

A NetApp recomenda que você atualize suas regras de firewall para usar a lista de endpoints revisada. A lista revisada é menor, portanto mais segura e fácil de gerenciar.

Análise"endpoints suportados para 4.0.0 e superior"

Passos

1. Coloque os endpoints na lista de permissões em"Pontos de extremidade suportados para 4.0.0 e superior" .
2. Reinicie o serviço do gerenciador de serviços 2 em cada agente executando o seguinte comando:

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

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

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

4. Remova os endpoints antigos da sua lista de permissões.

Endpoints contatados pelo NetApp Console

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

O sistema contata esses terminais em dois cenários:

- A partir de um computador acessando o "Console NetApp" como software como serviço (SaaS).
- De um computador acessando diretamente um host do agente, para efetuar login e configurá-lo ou acessar o Console a partir do host do agente.

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

Endpoints contatados pelo agente do Console

Você instala o agente do Console no local ou na nuvem, e ele entra em contato com os endpoints para concluir as ações iniciadas pelo Console.

Os agentes do console precisam acessar os mesmos endpoints que o NetApp Console, além de endpoints adicionais se você implantar o agente no seu provedor de nuvem.

Pontos de extremidade do agente para AWS

Esses pontos de extremidade são aplicáveis aos agentes do Console anteriores à versão 4.0.0.

Pontos finais	Propósito
Serviços da AWS (amazonaws.com): CloudFormation Elastic Compute Cloud (EC2) Gerenciamento de Identidade e Acesso (IAM) Serviço de Gerenciamento de Chaves (KMS) Serviço de Token de Segurança (STS) Serviço de Armazenamento Simples (S3)	Para gerenciar recursos na AWS. O ponto final exato depende da região da AWS que você está usando. Consulte a documentação da AWS para obter detalhes sobre como obter informações de licenciamento e enviar mensagens do AutoSupport ao suporte da NetApp .
\ https://support.netapp.com \ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
Escolha entre dois conjuntos de pontos de extremidade: • Opção 1 (recomendada) \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io • Opção 2 https://*.blob.core.windows.net \ https://cloudmanagerinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. A NetApp recomenda permitir endpoints da Opção 1 no seu firewall, pois eles são mais seguros, e não permitir endpoints da Opção 2, a menos que você esteja usando o Ransomware Resilience ou o Backup and Recovery. Observe o seguinte sobre esses pontos finais: • Os endpoints da Opção 1 são suportados em 3.9.47 e superiores. Versões anteriores à 3.9.47 não oferecem suporte à compatibilidade com versões anteriores. • O agente do Console inicia o contato com os endpoints na opção 2 primeiro. Se esses pontos de extremidade não estiverem acessíveis, ele entrará em contato automaticamente com os pontos de extremidade na opção 1. • Se você usar o agente do Console com o NetApp Backup and Recovery ou o Ransomware Resilience, o sistema não oferecerá suporte aos endpoints da Opção 1. Permitir pontos de extremidade da Opção 2 e não permitir a Opção 1.

Pontos de extremidade do agente para o Azure

Esses pontos de extremidade se aplicam aos agentes do Console anteriores à versão 4.0.0.

Pontos finais	Propósito
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Para gerenciar recursos em regiões públicas do Azure.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Para gerenciar recursos nas regiões do Azure China.

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

Pontos de extremidade do agente para o Google Cloud

Esses pontos de extremidade se aplicam aos agentes do Console anteriores à versão 4.0.0.

Pontos finais	Propósito
\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://www.googleapis.com/deploymentmanager/v2/project	Para gerenciar recursos no Google Cloud.
\ https://support.netapp.com \ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .

Pontos finais	Propósito
Escolha entre dois conjuntos de pontos de extremidade: • Opção 1 (recomendada) \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io • Opção 2 https://*.blob.core.windows.net \ https://cloudmanagerinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. A NetApp recomenda permitir endpoints da Opção 1 no seu firewall, pois eles são mais seguros, e não permitir endpoints da Opção 2. Observe o seguinte sobre esses pontos finais: • A partir da versão 3.9.47 do agente do Console, o sistema oferece suporte aos endpoints listados na opção 1. Versões anteriores do agente do Console não oferecem suporte à compatibilidade com versões anteriores. • O agente do Console primeiro contata os endpoints na opção 2. Se esses pontos de extremidade não estiverem acessíveis, ele entrará em contato automaticamente com os pontos de extremidade na opção 1. • Se você usar o agente do Console com o NetApp Backup and Recovery ou o Ransomware Resilience, o sistema não oferecerá suporte aos endpoints da Opção 1. Permitir pontos de extremidade da Opção 2 e não permitir a Opção 1.

Pontos de extremidade do agente local

Conhecimento e suporte

Registre-se para obter suporte

O registro de suporte é necessário para receber suporte técnico específico para o BlueXP e suas soluções e serviços de armazenamento. O registro de suporte também é necessário para habilitar fluxos de trabalho importantes para sistemas Cloud Volumes ONTAP .

O registro para suporte não habilita o suporte da NetApp para um serviço de arquivo do provedor de nuvem. Para obter suporte técnico relacionado a um serviço de arquivo do provedor de nuvem, sua infraestrutura ou qualquer solução que use o serviço, consulte "Obter ajuda" na documentação do BlueXP para esse produto.

- "Amazon FSx para ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Visão geral do registro de suporte

Existem duas formas de registro para ativar o direito ao suporte:

- Registrando o número de série da sua conta BlueXP (seu número de série 960xxxxxxxx de 20 dígitos localizado na página Recursos de suporte no BlueXP).

  Isso serve como seu único ID de assinatura de suporte para qualquer serviço dentro do BlueXP. Cada assinatura de suporte em nível de conta BlueXP deve ser registrada.

- Registrando os números de série do Cloud Volumes ONTAP associados a uma assinatura no marketplace do seu provedor de nuvem (são números de série 909201xxxxxxxxx de 20 dígitos).

  Esses números de série são comumente chamados de *números de série PAYGO* e são gerados pelo BlueXP no momento da implantação do Cloud Volumes ONTAP .

Registrar ambos os tipos de números de série habilita recursos como abertura de tickets de suporte e geração automática de casos. O registro é concluído adicionando contas do NetApp Support Site (NSS) ao BlueXP , conforme descrito abaixo.

Registre o BlueXP para suporte da NetApp

Para se registrar para obter suporte e ativar o direito ao suporte, um usuário na sua organização BlueXP (ou conta) deve associar uma conta do Site de Suporte da NetApp ao seu login BlueXP . A maneira como você se registra para o suporte da NetApp depende se você já tem uma conta no NetApp Support Site (NSS).

Cliente existente com uma conta NSS

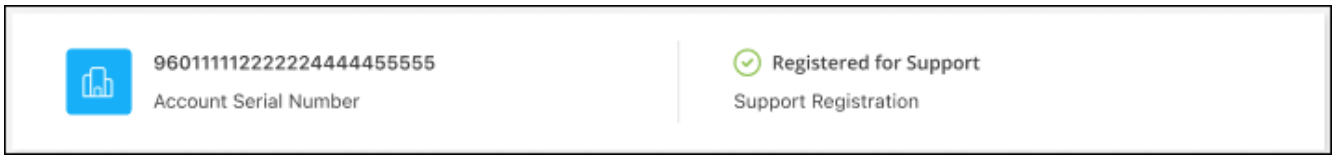
Se você for um cliente da NetApp com uma conta NSS, basta se registrar para obter suporte pelo BlueXP.

Passos

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **Credenciais**.
2. Selecione **Credenciais do usuário**.

3. Selecione **Adicionar credenciais NSS** e siga o prompt de autenticação do NetApp Support Site (NSS).
4. Para confirmar que o processo de registro foi bem-sucedido, selecione o ícone Ajuda e selecione **Suporte**.

   A página **Recursos** deve mostrar que sua organização BlueXP está registrada para suporte.



   Observe que outros usuários do BlueXP não verão o mesmo status de registro de suporte se não tiverem associado uma conta do site de suporte da NetApp ao login do BlueXP . No entanto, isso não significa que sua organização BlueXP não esteja registrada para suporte. Desde que um usuário na organização tenha seguido essas etapas, sua organização foi registrada.

Cliente existente, mas sem conta NSS

Se você já é cliente da NetApp com licenças e números de série, mas *nenhuma* conta NSS, precisa criar uma conta NSS e associá-la ao seu login do BlueXP .

Passos

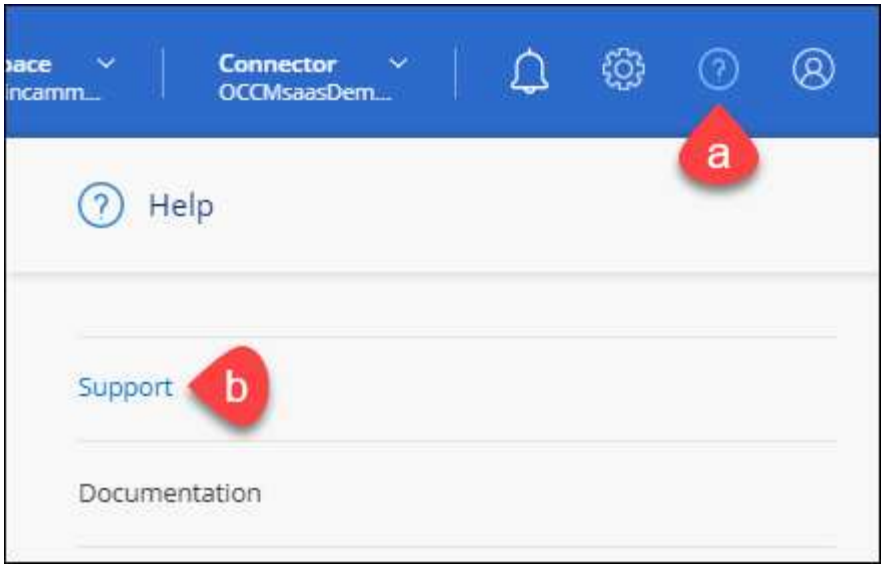
1. Crie uma conta no site de suporte da NetApp preenchendo o "Formulário de registro de usuário do site de suporte da NetApp"
   a. Certifique-se de selecionar o Nível de usuário apropriado, que normalmente é * Cliente/Usuário final da NetApp *.
   b. Certifique-se de copiar o número de série da conta BlueXP (960xxxx) usado acima para o campo de número de série. Isso acelerará o processamento da conta.
2. Associe sua nova conta NSS ao seu login BlueXP concluindo as etapas abaixoCliente existente com uma conta NSS .

Novidade na NetApp

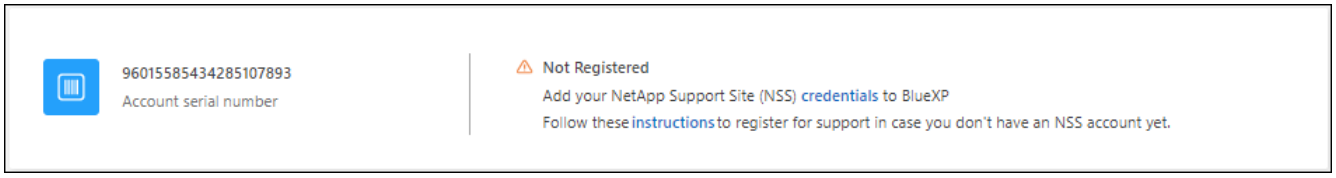
Se você é novo na NetApp e não tem uma conta NSS, siga cada etapa abaixo.

Passos

1. No canto superior direito do console BlueXP , selecione o ícone Ajuda e selecione **Suporte**.



2. Localize o número de série do seu ID de conta na página de Registro de Suporte.



3. Navegar para "Site de registro de suporte da NetApp" e selecione *Não sou um cliente registrado da NetApp *.
4. Preencha os campos obrigatórios (aqueles com asteriscos vermelhos).
5. No campo **Linha de produtos**, selecione **Cloud Manager** e, em seguida, selecione seu provedor de cobrança aplicável.
6. Copie o número de série da sua conta da etapa 2 acima, conclua a verificação de segurança e confirme que você leu a Política Global de Privacidade de Dados da NetApp.

   Um e-mail é enviado imediatamente para a caixa de correio fornecida para finalizar esta transação segura. Não deixe de verificar sua caixa de spam caso o e-mail de validação não chegue em alguns minutos.

7. Confirme a ação no e-mail.

   A confirmação envia sua solicitação à NetApp e recomenda que você crie uma conta no site de suporte da NetApp .

8. Crie uma conta no site de suporte da NetApp preenchendo o "Formulário de registro de usuário do site de suporte da NetApp"
   a. Certifique-se de selecionar o Nível de usuário apropriado, que normalmente é * Cliente/Usuário final da NetApp *.
   b. Certifique-se de copiar o número de série da conta (960xxxx) usado acima para o campo de número de série. Isso acelerará o processamento.

Depois que você terminar

A NetApp entrará em contato com você durante esse processo. Este é um exercício de integração único para novos usuários.

Depois de ter sua conta no site de suporte da NetApp , associe a conta ao seu login BlueXP concluindo as etapas emCliente existente com uma conta NSS .

Credenciais associadas do NSS para suporte do Cloud Volumes ONTAP

A associação das credenciais do NetApp Support Site à sua organização BlueXP é necessária para habilitar os seguintes fluxos de trabalho principais para o Cloud Volumes ONTAP:

- Registrando sistemas Cloud Volumes ONTAP de pagamento conforme o uso para suporte

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

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

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

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

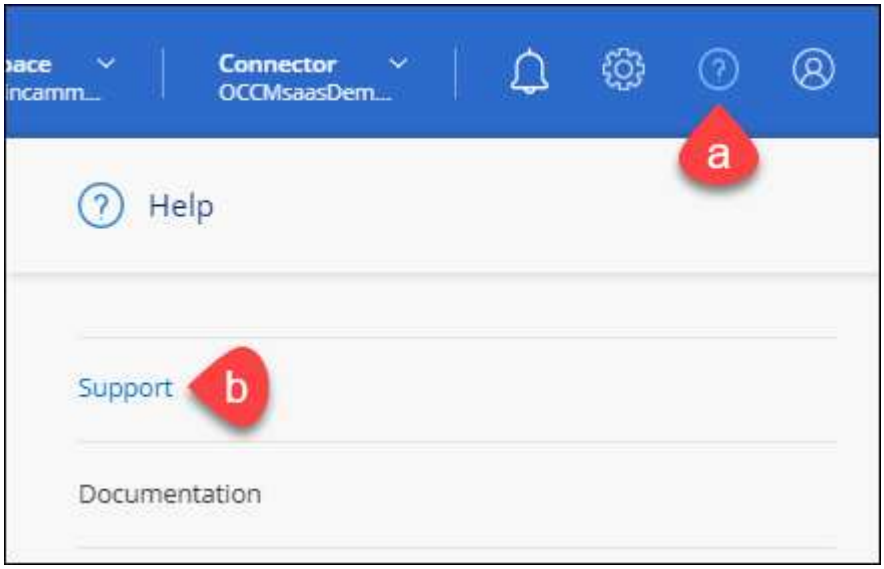
Associar credenciais do NSS à sua organização BlueXP é diferente da conta do NSS associada a um login de usuário do BlueXP .

Essas credenciais NSS estão associadas ao seu ID de organização BlueXP específico. Usuários que pertencem à organização BlueXP podem acessar essas credenciais em **Suporte > Gerenciamento NSS**.

- Se você tiver uma conta de nível de cliente, poderá adicionar uma ou mais contas NSS.
- Se você tiver uma conta de parceiro ou revendedor, poderá adicionar uma ou mais contas NSS, mas elas não poderão ser adicionadas junto com contas de nível de cliente.

Passos

1. No canto superior direito do console BlueXP , selecione o ícone Ajuda e selecione **Suporte**.



2. Selecione **Gerenciamento NSS > Adicionar conta NSS**.
3. 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 específicos para suporte e licenciamento.

4. Na página de login, forneça seu endereço de e-mail e senha registrados no Site de Suporte da NetApp para realizar o processo de autenticação.

   Essas ações permitem que o BlueXP use sua conta NSS para coisas como downloads de licenças, verificação de atualização de software e registros de suporte futuros.

   Observe o seguinte:

   - A conta NSS deve ser uma conta de nível de cliente (não uma conta de convidado ou temporária). Você pode ter várias contas NSS em nível de cliente.
   - Só pode haver uma conta NSS se essa conta for uma conta de nível de parceiro. Se você tentar adicionar contas NSS em nível de cliente e existir uma conta em nível de parceiro, você receberá a seguinte mensagem de erro:

     "O tipo de cliente NSS não é permitido para esta conta, pois já existem usuários NSS de tipos diferentes."

   O mesmo é verdadeiro se você tiver contas NSS pré-existentes em nível de cliente e tentar adicionar uma conta em nível de parceiro.

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

     Este é um ID gerado pelo sistema que mapeia para 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.

Obter ajuda

A NetApp fornece suporte para o NetApp Console e seus serviços de nuvem de diversas maneiras. Há diversas opções gratuitas de autoatendimento disponíveis 24 horas por dia, 7 dias por semana, como artigos da base de conhecimento (KB) e um fórum da comunidade. Seu cadastro no suporte inclui suporte técnico remoto por meio de tickets online.

Obtenha suporte para um serviço de arquivo de provedor de nuvem

Para obter suporte técnico relacionado a um serviço de arquivo do provedor de nuvem, sua infraestrutura ou qualquer solução que use o serviço, consulte a documentação desse produto.

- "Amazon FSx para ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Para receber suporte técnico específico para a NetApp e suas soluções de armazenamento e serviços de dados, use as opções de suporte descritas abaixo.

Use opções de autoapoio

Estas opções estão disponíveis gratuitamente, 24 horas por dia, 7 dias por semana:

- Documentação

  A documentação do NetApp Console que você está visualizando no momento.

- "Base de conhecimento"

  Pesquise na base de conhecimento da NetApp para encontrar artigos úteis para solucionar problemas.

- "Comunidades"

  Participe da comunidade do NetApp Console para acompanhar discussões em andamento ou criar novas.

Crie um caso com o suporte da NetApp

Além das opções de autossuporte acima, você pode trabalhar com um especialista em suporte da NetApp para resolver quaisquer problemas após ativar o suporte.

Antes de começar

- Para usar o recurso **Criar um caso**, você deve primeiro associar suas credenciais do site de suporte da NetApp ao seu login do console. "Aprenda a gerenciar credenciais associadas ao seu login do Console" .
- Se você estiver abrindo um caso para um sistema ONTAP que tenha um número de série, sua conta NSS deverá estar associada ao número de série desse sistema.

Passos

1. No NetApp Console, selecione **Ajuda > Suporte**.
2. Na página **Recursos**, escolha uma das opções disponíveis em Suporte Técnico:

   a. Selecione **Ligue para nós** se quiser falar com alguém por telefone. Você será direcionado para uma página no netapp.com que lista os números de telefone para os quais você pode ligar.

   b. Selecione **Criar um caso** para abrir um tíquete com um especialista de suporte da NetApp :

      - **Serviço**: Selecione o serviço ao qual o problema está associado. Por exemplo, * NetApp Console* quando específico para um problema de suporte técnico com fluxos de trabalho ou funcionalidade dentro do Console.
      - **Sistema**: Se aplicável ao armazenamento, selecione * Cloud Volumes ONTAP* ou **On-Prem** e, em seguida, o ambiente de trabalho associado.

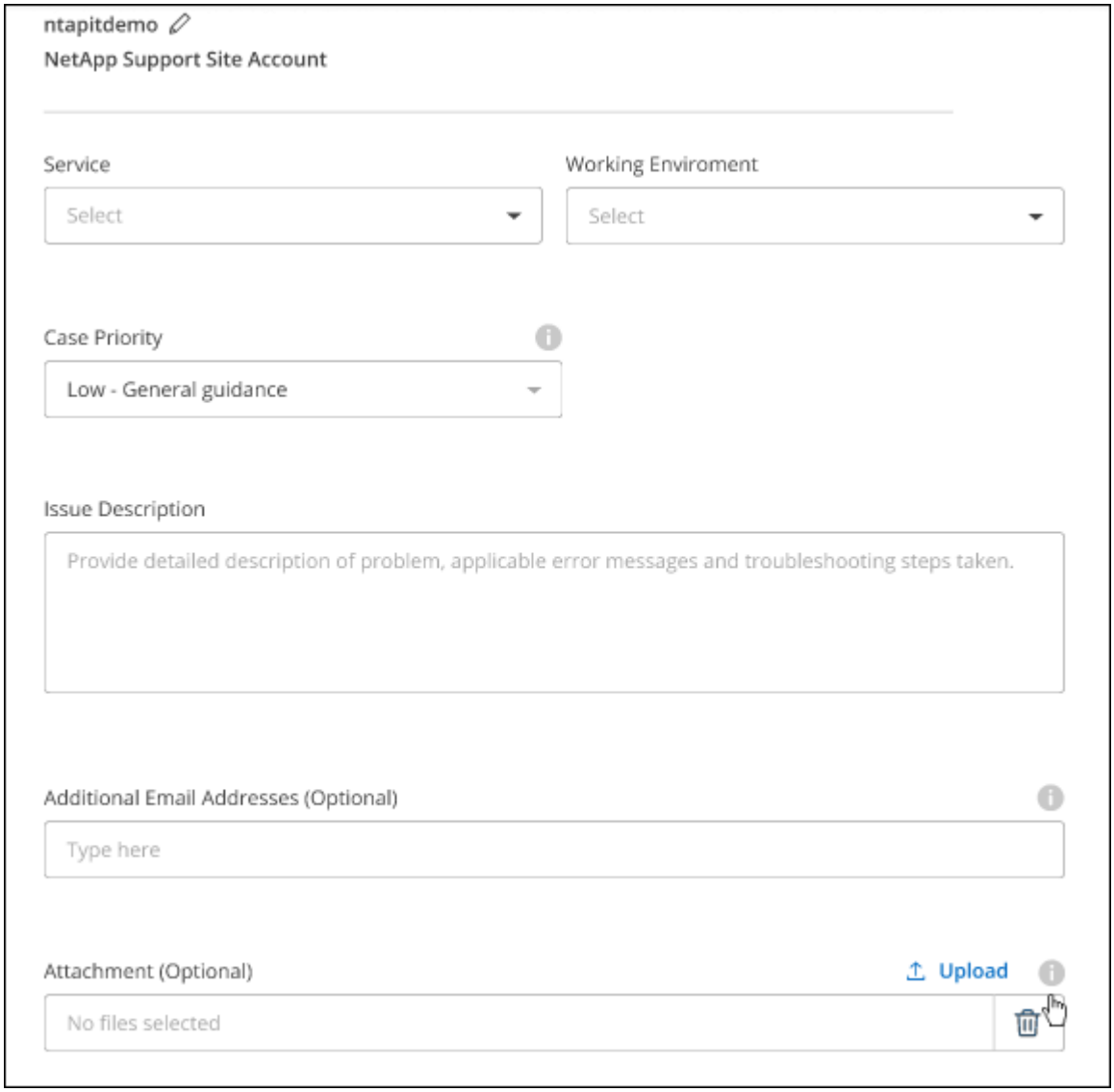
        A lista de sistemas está dentro do escopo da organização do Console e do agente do Console que você selecionou no banner superior.

      - **Prioridade do caso**: escolha a prioridade do caso, que pode ser Baixa, Média, Alta ou Crítica.

        Para saber mais detalhes sobre essas prioridades, passe o mouse sobre o ícone de informações ao lado do nome do campo.

- **Descrição do problema**: Forneça uma descrição detalhada do seu problema, incluindo quaisquer mensagens de erro aplicáveis ou etapas de solução de problemas que você executou.
- **Endereços de e-mail adicionais**: insira endereços de e-mail adicionais se quiser informar outra pessoa sobre esse problema.
- **Anexo (Opcional)**: Carregue até cinco anexos, um de cada vez.

  Os anexos são limitados a 25 MB por arquivo. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.



Depois que você terminar

Um pop-up aparecerá com o número do seu caso de suporte. Um especialista em suporte da NetApp analisará seu caso e entrará em contato com você em breve.

Para obter um histórico dos seus casos de suporte, você pode selecionar **Configurações > Linha do tempo** e procurar por ações chamadas "criar caso de suporte". Um botão na extrema direita permite expandir a ação para ver detalhes.

É possível que você encontre a seguinte mensagem de erro ao tentar criar um caso:

"Você não está autorizado a criar um caso contra o serviço selecionado"

Esse erro pode significar que a conta NSS e a empresa registrada à qual ela está associada não são a mesma empresa registrada para o número de série da conta do NetApp Console (por exemplo, 960xxxx) ou o número de série do ambiente de trabalho. Você pode buscar assistência usando uma das seguintes opções:

- Envie um caso não técnico em https://mysupport.netapp.com/site/help

Gerencie seus casos de suporte

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

Observe o seguinte:

- O painel de gerenciamento de casos na parte superior da página oferece duas visualizações:
  - A visualização à esquerda mostra o total de casos abertos nos últimos 3 meses pela conta NSS do usuário que você forneceu.
  - A visualização à direita mostra o total de casos abertos nos últimos 3 meses no nível da sua empresa com base na sua conta de usuário NSS.

  Os resultados na tabela refletem os casos relacionados à exibição que você selecionou.
- Você pode adicionar ou remover colunas de interesse e filtrar o conteúdo de colunas como Prioridade e Status. Outras colunas fornecem apenas recursos de classificação.

  Veja as etapas abaixo para mais detalhes.
- Em cada caso, oferecemos a possibilidade de atualizar notas do caso ou fechar um caso que ainda não esteja no status Fechado ou Pendente Fechado.

Passos

1. No NetApp Console, selecione **Ajuda > Suporte**.
2. Selecione **Gerenciamento de casos** e, se solicitado, adicione sua conta NSS ao Console.

   A página **Gerenciamento de casos** mostra casos abertos relacionados à conta NSS associada à sua conta de usuário do Console. Esta é a mesma conta NSS que aparece no topo da página **Gerenciamento NSS**.
3. Modifique opcionalmente as informações exibidas na tabela:
   - Em **Casos da organização**, selecione **Exibir** para visualizar todos os casos associados à sua empresa.
   - Modifique o intervalo de datas escolhendo um intervalo de datas exato ou escolhendo um período de tempo diferente.
   - Filtrar o conteúdo das colunas.
   - Altere as colunas que aparecem na tabela selecionando e então escolher as colunas que você gostaria de exibir.
4. Gerencie um caso existente selecionando e selecionando uma das opções disponíveis:
   - **Ver caso**: Veja detalhes completos sobre um caso específico.

- **Atualizar notas do caso**: Forneça detalhes adicionais sobre seu problema ou selecione **Carregar arquivos** para anexar até no máximo cinco arquivos.

  Os anexos são limitados a 25 MB por arquivo. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.

- **Fechar caso**: Forneça detalhes sobre o motivo pelo qual você está fechando o caso e selecione **Fechar caso**.

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos autorais

"https://www.netapp.com/company/legal/copyright/"

Marcas Registradas

NETAPP, o logotipo da NETAPP e as marcas listadas na página de Marcas Registradas da NetApp são marcas registradas da NetApp, Inc. Outros nomes de empresas e produtos podem ser marcas registradas de seus respectivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de Privacidade

"https://www.netapp.com/company/legal/privacy-policy/"

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais e licenças de terceiros usados no software NetApp .

"Aviso para o NetApp Console"

Informações sobre direitos autorais

Informações sobre marcas comerciais