Gerenciamento de identidade e acesso

NetApp Console setup and administration

NetApp
February 11, 2026

Índice

Gerenciamento de identidade e acesso

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

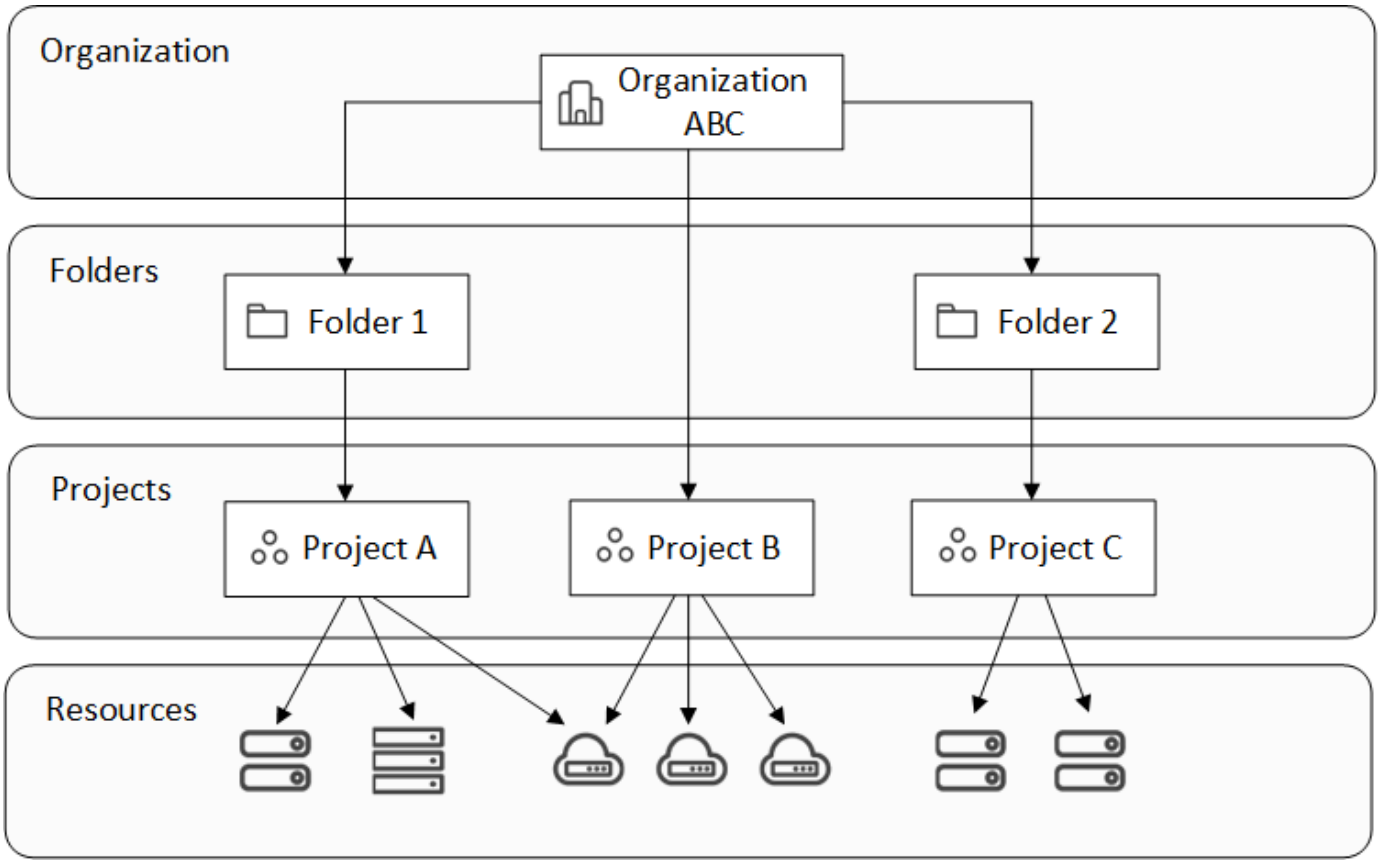
Utilize o Gerenciamento de Identidade e Acesso (IAM) do NetApp Console para organizar seus recursos NetApp e controlar o acesso de acordo com a estrutura da sua empresa — por local, departamento ou projeto.

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

Atribua funções de acesso no nível da organização, pasta ou projeto para que os usuários tenham o acesso correto aos recursos.

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

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



]

Componentes de gerenciamento de identidade e acesso

No NetApp Console, você organiza seus recursos de armazenamento usando três componentes principais:

componentes organizacionais, componentes de recursos e componentes de acesso do usuário.

Projetos e pastas dentro da sua organização

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

Organização

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

Projetos

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

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

"Aprenda como adicionar projetos à sua organização."

Pastas

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

"Aprenda como adicionar pastas à sua organização."

Recursos

Um recurso é uma entidade que o Console reconhece e que pode ser atribuída a um projeto. Recursos incluem sistemas de storage, assinaturas do Keystone, algumas cargas de trabalho do NetApp Backup and Recovery, bem como agentes do Console.

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

+

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

+

"Aprenda como associar recursos a projetos."

Sistemas de armazenamento e assinaturas Keystone

Os sistemas de storage são os principais recursos que você gerencia no NetApp Console. NetApp Console oferece suporte ao gerenciamento de sistemas de storage locais e de storage de nuvem. Você deve adicionar um sistema de storage a um projeto para que ele possa ser acessado pelas pessoas atribuídas ao projeto.

Sistemas de storage

Os sistemas de storage são associados automaticamente ao projeto em que são adicionados, mas você pode associá-los a outros projetos ou pastas na página **Resources**. Você não pode associar sistemas de storage FSx for NetApp ONTAP a projetos ou pastas, mas pode visualizá-los na página **Systems** ou em Workloads.

Assinaturas Keystone

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

Cargas de trabalho de backup e recuperação (Oracle e Microsoft SQL Server)

Algumas cargas de trabalho de Backup and Recovery também são consideradas recursos. Você pode atribuir permissões aos usuários para acessar Backup and

Agentes de console

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

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

"Aprenda como associar agentes a projetos."

Membros e funções

Membros

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

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

"Aprenda como adicionar membros à sua organização."

Funções de acesso

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

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

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

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

"Saiba mais sobre funções de acesso" .

Exemplos de estratégia IAM

Estratégia para pequenas organizações

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

Exemplo: ABC Corporation (equipe de 5 pessoas)

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

Estratégia empresarial multirregional

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

Exemplo: Corporação XYZ (empresa multinacional)

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

Estratégia de especialização departamental

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

Exemplo: TechCorp (empresa de tecnologia de médio porte)

- **Estrutura:** Organização > Pastas de departamento (TI, Segurança, Desenvolvimento) > Recursos específicos do projeto
- **Funções especializadas:**
  - Equipe de segurança: funções de **Administrador de Resiliência a Ransomware** e **Visualizador de Classificações**.
  - Equipe de backup: **Superadministrador de backup e recuperação** para operações de backup abrangentes.
  - Equipe de desenvolvimento: **Administrador de armazenamento** para gerenciamento de ambiente de teste
  - Equipe de Compliance: **Analista de suporte operacional** para monitoramento e gerenciamento de casos de suporte.
- **Estratégia de agentes:** Agentes vinculados a projetos departamentais com base na propriedade dos recursos.
- **Benefícios:** Controle de acesso personalizado, maior eficiência operacional e responsabilidade clara por tarefas especializadas.

Próximos passos com o IAM no NetApp Console

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

Comece a usar 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 precisa das permissões de **Administrador da organização** ou **Superadministrador** para gerenciar a identidade e o acesso da sua organização. Com as permissões de **Administrador de pasta ou projeto**, você só pode gerenciar as pastas e os projetos aos quais tem acesso.

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" .

2 **Associe membros à sua organização**

Após os usuários se inscreverem no NetApp Console, você deve adicioná-los explicitamente à sua organização do Console. 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"

Configure a organização do seu console.

Adicione pastas e projetos à sua organização do NetApp Console.

Adicione pastas e projetos para que correspondam à estrutura da sua empresa. Depois de criar pastas e projetos, você pode associar recursos a eles e gerenciar o acesso dos membros a esses projetos.

O Console cria automaticamente um projeto para você quando você cria uma nova organização. A maioria das organizações precisa de mais de um projeto, além de pastas para manter tudo organizado. "Saiba mais

sobre a hierarquia de recursos no NetApp Console.".

Utilizando pastas e projetos para organizar recursos

No NetApp Console, uma organização contém pastas e projetos que ajudam você a organizar seus recursos. As pastas ajudam a agrupar projetos relacionados, e os projetos ajudam a gerenciar recursos e o acesso de membros.

Pastas

As pastas ajudam você a organizar projetos relacionados. Você pode criar pastas aninhadas para representar diferentes níveis da estrutura da sua organização. Por exemplo, você pode criar uma pasta de nível superior para cada unidade de negócios e, em seguida, criar subpastas para diferentes equipes dentro dessa unidade de negócios. Em seguida, você cria projetos dentro de pastas.

As pastas também permitem gerenciar o acesso de membros de forma mais eficiente, utilizando a herança de funções. Ao atribuir funções aos membros no nível da pasta, eles herdam as permissões para todos os projetos e pastas filhos.

As pastas são uma ferramenta organizacional e não são visíveis para membros que não possuem permissões do IAM, como administrador da organização, administrador de pasta ou projeto, ou superadministrador. Os membros têm acesso a projetos, não a pastas.

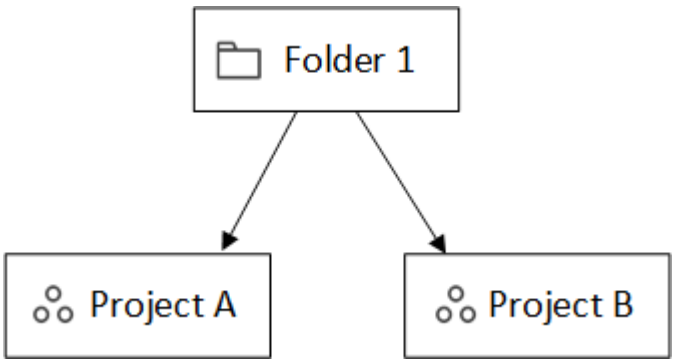
Os administradores da organização podem delegar responsabilidades administrativas criando pastas. Após criar uma pasta, um administrador da organização pode atribuir a um membro as funções de administrador da pasta ou do projeto para pastas específicas. Esses membros podem então gerenciar todos os projetos dentro dessa pasta sem ter acesso a toda a organização.

As pastas podem ter outras pastas ou projetos como filhos, mas não podem ter recursos diretamente associados a elas. Os recursos devem estar associados a um projeto.

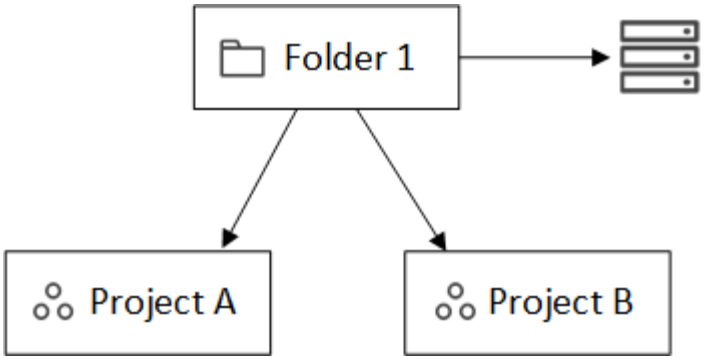
Quando associar um recurso a uma pasta

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:

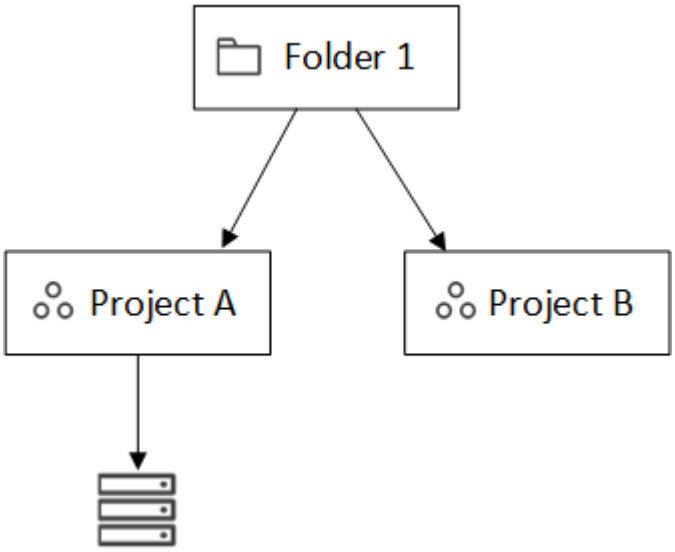


O *Administrador da organização* pode associar um recurso à pasta:



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.

Projetos

Associe recursos a projetos para permitir que os membros os gerenciem. Os recursos devem ser associados a um projeto para fins de gerenciamento e acesso do usuário.

Uma organização pode ter um ou vários projetos. Um projeto pode estar diretamente subordinado à organização ou dentro de uma pasta. Se um agente for usado para descobrir recursos dentro de um projeto, você também deverá associar o agente a esse projeto.

Os usuários navegam entre os projetos atribuídos na página **Sistemas** para gerenciar os recursos associados a cada projeto.

Adicionar uma pasta ou projeto

Adicione projetos para gerenciar recursos e pastas para agrupar projetos relacionados. Ao criar uma nova organização, o Console inclui um projeto.

Você pode criar até sete níveis de pastas e projetos na estrutura de recursos da sua organização. Crie pastas

aninhadas para organizar seus recursos conforme necessário.

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. Insira os detalhes da pasta ou do projeto:
   - **Nome e localização**: Insira um nome e escolha uma localização para a pasta ou projeto. Você pode colocar pastas ou projetos dentro da organização ou em outra pasta.
   - **Recursos**: Selecione os recursos que deseja associar a esta pasta ou projeto. Se você ainda não adicionou sistemas de armazenamento ao Console, poderá fazer isso mais tarde.

     Os membros não podem acessar os recursos em uma pasta até que esses recursos sejam atribuídos a um projeto. Utilize pastas para armazenar recursos temporariamente até que você crie os projetos necessários. Isso pode ajudar o administrador da organização a delegar a alocação de recursos a um administrador de pasta ou projeto, que então atribui recursos aos projetos dentro da pasta.

   - **Acesso**: Selecione **Adicionar um membro** para atribuir acesso e uma função. Você pode adicionar ou remover membros do projeto ou da pasta a qualquer momento.

     "Saiba mais sobre funções de acesso" .
6. Selecione **Adicionar**.

Renomear uma pasta ou projeto

Renomeie uma pasta ou projeto conforme necessário. A mudança de nome não afeta os recursos associados nem o acesso dos membros.

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, como após uma reestruturação da equipe ou a conclusão de um projeto.

Antes de excluir uma pasta ou projeto, certifique-se de que ele não contenha nenhum recurso. Aprenda como remover recursos.

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.

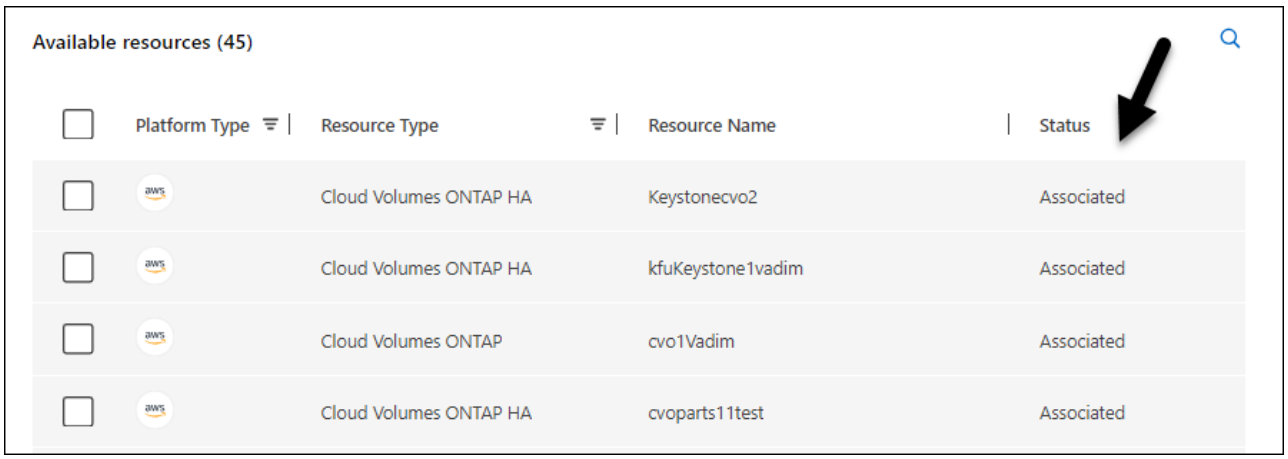
Visualizar os recursos associados a uma pasta ou projeto

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.



Alterar os recursos associados a uma pasta ou projeto

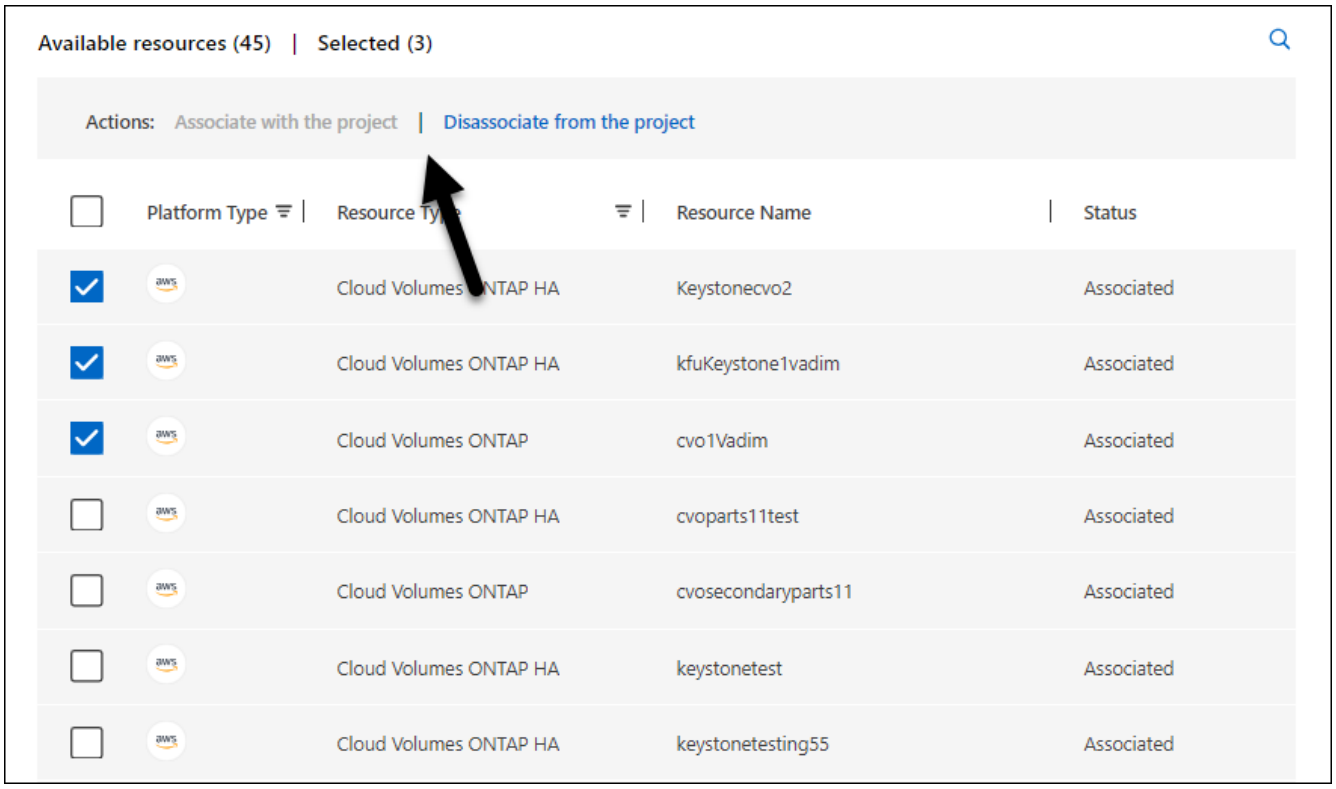
Você pode alterar os recursos associados a uma pasta ou projeto conforme as necessidades da sua organização mudam.

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. Com base nos recursos que você selecionou, escolha **Associar-se ao projeto** ou **Desassociar-se do projeto**.



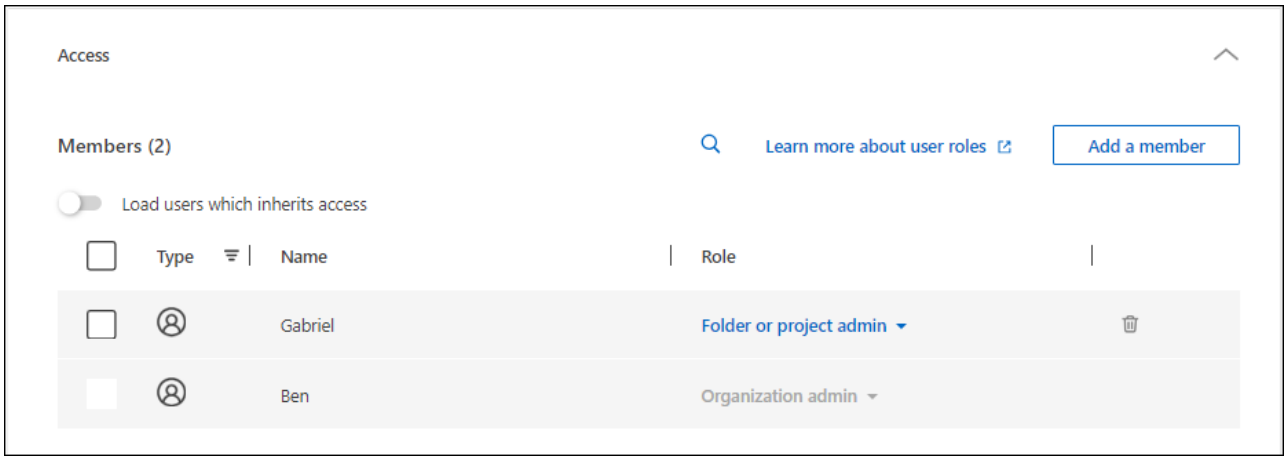
5. Selecione **Aplicar**.

Ver membros associados a uma pasta ou projeto

Você pode visualizar os membros associados a uma pasta ou projeto na página **Organização**.

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.
   - 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 controlar o acesso aos recursos. Lembre-se de que as funções atribuídas no nível da pasta são herdadas por todos os projetos e pastas filhos.

Não é possível alterar o acesso de membros em níveis inferiores se ele for herdado do nível da pasta ou da organização. Altere a permissão do membro no nível hierárquico superior para modificar o acesso. Alternativamente, você pode "gerenciar permissões na página de membros".

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"

Adicione recursos a pastas e projetos no NetApp Console.

Controle o acesso dos usuários aos recursos adicionando-os a projetos e pastas na sua organização do NetApp Console . Conceder acesso aos usuários no nível do projeto.

Um *recurso* é uma entidade da qual o Console tem conhecimento, como um recurso de armazenamento, um agente do Console ou uma carga de trabalho de Backup e Recuperação.

Você pode visualizar e gerenciar recursos na página **Recursos** do Console.

Tipos de recursos do console

Você pode associar vários tipos de recursos a projetos na sua organização do NetApp Console :

Recursos de armazenamento

Os recursos de armazenamento são o tipo de recurso mais comum em sua organização e representam sistemas de armazenamento locais e em nuvem. Ao adicionar um sistema de armazenamento ao Console, você pode adicioná-lo a uma pasta ou projeto. Até então, o Console o marca como não descoberto e não o exibe na página **Recursos**.

Agentes de console

Se você utilizou um agente de console para descobrir sistemas de armazenamento, adicione o agente à mesma pasta ou projeto. Isso permite que os usuários executem funções habilitadas por agente, como serviços de dados ou gerenciamento de armazenamento nativo do Console. Você pode adicionar agentes a pastas ou projetos na página **Agentes** do Console. "Aprenda como associar um agente do Console a uma pasta ou projeto".

Assinaturas Keystone

Se a sua organização possui assinaturas do Keystone , você pode visualizá-las na página **Recursos**. Você pode associar assinaturas do Keystone a pastas ou projetos para fornecer acesso a membros que tenham permissões para essas pastas ou projetos.

Visualize os recursos em sua organização

Você pode visualizar recursos descobertos e não descobertos associados à sua organização. O sistema localiza recursos de armazenamento e os marca como não descobertos até que você os adicione ao Console.

O Console exclui os recursos do Amazon FSx for NetApp ONTAP da página Recursos porque os usuários não podem associá-los a uma função. Você pode visualizar esses recursos 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. Utilize as opções disponíveis para encontrar um recurso:
   - **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 aos membros que têm permissões para essa pasta ou projeto.

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

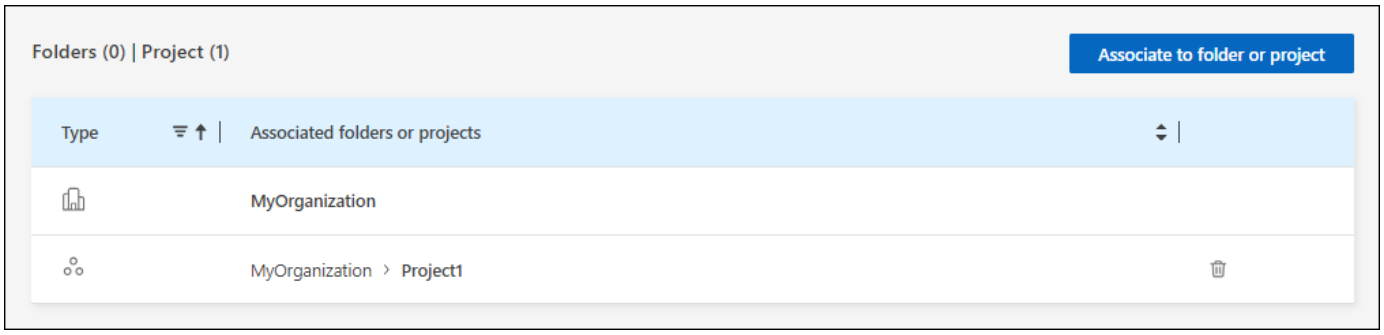
Você pode visualizar as pastas e os projetos associados a um recurso específico.

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.



Para ver quais membros da organização têm acesso ao recurso,"Veja os membros com acesso às pastas e projetos associados." .

Remover um recurso de uma pasta ou projeto

Para remover um recurso de uma pasta ou projeto, remova a sua associação. Isso impede que os membros gerenciem o recurso nessa pasta ou projeto.

Para remover um recurso detectado de toda a organização, acesse a página **Sistemas** e remova o sistema.

Passos

1. Na página **Recursos**, navegue até um recurso na tabela, selecione ••• e então selecione **Ver detalhes**.
2. Para remover um recurso de uma pasta ou projeto, selecione ao lado da pasta ou do projeto.
3. Selecione **Excluir** para remover a associação.

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

Associe agentes do Console a projetos específicos para permitir o gerenciamento de recursos e o acesso a serviços de dados. Os recursos descobertos por meio de um agente do Console exigem que tanto o recurso quanto o agente estejam associados aos mesmos projetos respectivos para que a equipe tenha acesso.

Os superadministradores e administradores da organização podem criar agentes e associar qualquer agente a qualquer projeto ou pasta. Os administradores de pastas ou projetos só podem associar agentes existentes a pastas e projetos para os quais possuem permissões. "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"

Adicione usuários à sua organização do Console.

Adicionar usuários a uma organização do NetApp Console

No Console, você concede aos usuários acesso a projetos ou pastas de acordo com uma função de acesso. Uma *função de acesso* contém um conjunto de permissões que permite a um membro (usuário ou conta de serviço) executar ações específicas no nível atribuído da hierarquia de recursos.

Funções de acesso necessárias

Superadministrador, administrador da organização ou administrador de pasta ou projeto (para pastas e projetos que eles administram). "Saiba mais sobre funções de acesso".

Entenda como o acesso é concedido no NetApp Console.

O NetApp Console utiliza o controle de acesso baseado em funções (RBAC) para gerenciar permissões. Atribua funções aos usuários individualmente ou por meio de grupos federados. Cada função define as ações permitidas para recursos específicos.

Observe o seguinte sobre como conceder acesso no NetApp Console:

- Todos os usuários devem primeiro se cadastrar no NetApp Console antes de obterem acesso aos recursos.
- Você deve atribuir explicitamente uma função a cada usuário no Console antes que ele possa acessar os recursos, mesmo que seja membro de um grupo federado ao qual já tenha sido atribuída uma função.
- Você pode adicionar contas de serviço diretamente do Console e atribuir funções a elas.

Adicionar membros à sua organização

O NetApp Console suporta três tipos de membros: contas de usuário, contas de serviço e grupos federados.

Os usuários precisam se cadastrar no NetApp Console antes que você possa adicioná-los e atribuir uma função, mesmo que estejam em um grupo federado. Crie contas de serviço diretamente no Console.

Todos os membros devem ter pelo menos uma função explicitamente atribuída a eles para poderem acessar os recursos.

Ao adicionar um membro, escolha o nível de recurso (organização, pasta ou projeto) e atribua uma ou mais funções com as permissões necessárias.

Adicionar um usuário

Os usuários se cadastram no NetApp Console, mas um administrador da organização, pasta ou projeto precisa adicioná-los à organização, pasta ou projeto para que possam acessar os recursos.

Antes de começar:

O usuário já deve ter se cadastrado no NetApp Console. Se eles ainda não se inscreveram, oriente-os a… "Inscreva-se no NetApp Console."

Se você estiver adicionando um usuário que faz parte de um grupo federado, certifique-se de que ele já tenha se cadastrado no NetApp Console e que uma função tenha sido explicitamente atribuída a ele no Console. A NetApp recomenda atribuir uma função de acesso mínima, como a de visualizador da organização.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.
3. Selecione **Adicionar um membro**.
4. Para **Tipo de membro**, mantenha **Usuário** selecionado.
5. Em **E-mail do usuário**, insira o endereço de e-mail do usuário associado ao login que ele criou.
6. 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 pode selecionar apenas as pastas e os projetos para os quais você tem permissão.
   - Ao selecionar uma organização ou pasta, você concede ao membro permissões para acessar todo o seu conteúdo.
   - Você só pode atribuir a função **Administrador da organização** no nível da organização.
7. **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" .
8. Para conceder acesso a mais pastas, projetos ou funções, selecione **Adicionar função**, escolha a categoria de pasta, projeto ou função e selecione uma função.
9. Selecione **Adicionar**.

   O console envia instruções ao usuário por e-mail.

Adicionar uma conta de serviço

As contas de serviço permitem automatizar tarefas e conectar-se com segurança às APIs do Console. Escolha um ID e um segredo do cliente para configurações simples ou um JWT (JSON Web Token) para maior segurança em ambientes automatizados ou nativos da nuvem. Selecione o método que atenda aos seus requisitos de segurança.

Antes de começar:

Para autenticação JWT, prepare sua chave pública ou certificado.

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. Para usar a autenticação JWT, selecione **Usar autenticação JWT com chave privada** e carregue sua chave ou certificado RSA público. Ignore se estiver usando ID e segredo do cliente.

   Seu certificado X.509. Deve estar no formato PEM, CRT ou CER.

   a. Configure notificações de expiração para o seu certificado. Escolha entre sete dias ou 30 dias. As notificações de expiração são enviadas por e-mail e exibidas no Console para usuários com a função de Superadministrador ou Administrador da Organização.

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, em seguida, selecione uma **Função** que conceda ao membro permissões para os recursos na organização, pasta ou projeto que você selecionou.

   "Saiba mais sobre funções de acesso" .

9. Para conceder acesso a mais pastas, projetos ou funções, selecione **Adicionar função**, escolha a categoria de pasta, projeto ou função e selecione 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 exibe o segredo do cliente apenas uma vez. Faça uma cópia segura; você poderá recriá-la mais tarde, caso a perca.

11. Se você escolheu a autenticação JWT, baixe ou copie o ID do cliente e o público-alvo do JWT. O Console exibe essas informações apenas uma vez e não permite que você as recupere posteriormente.
12. Selecione **Fechar**.

Adicione um grupo federado à sua organização.

Você pode adicionar um grupo federado do seu provedor de identidade (IdP) à sua organização e atribuir a ele uma ou mais funções. Os membros do grupo federado herdam as funções que você atribui ao grupo no Console.

Antes de atribuir uma função a um grupo federado, certifique-se do seguinte:

- Configure a federação entre seu IdP e o Console. "Aprenda como configurar a federação."
- O grupo já deve existir no seu IdP e ter recebido acesso ao Console.
- Os usuários pertencentes ao grupo já devem ter se cadastrado no NetApp Console e ter recebido uma função explicitamente atribuída no Console. A NetApp recomenda atribuir uma função de acesso mínima, como a de visualizador da organização.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.
3. Selecione **Adicionar um membro**.

4. Em **Tipo de membro**, selecione **Grupo federado**.
5. Selecione a federação à qual o grupo pertence.
6. Em **Nome do grupo**, insira o nome exato do grupo em seu IdP.
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, em seguida, selecione uma **Função** que conceda ao membro permissões para os recursos na organização, pasta ou projeto que você selecionou.

   "Saiba mais sobre funções de acesso" .
9. Para conceder acesso a mais pastas, projetos ou funções, selecione **Adicionar função**, escolha a categoria de pasta, projeto ou função e selecione uma função.

Informações relacionadas

- "Saiba mais sobre gerenciamento de identidade e acesso no NetApp Console"
- "Comece com identidade e acesso"
- "Funções de acesso ao NetApp Console"
- "Saiba mais sobre a API para identidade e acesso"

Gerenciar o acesso e a segurança do usuário

Saiba mais sobre o controle de acesso baseado em função (RBAC) do NetApp Console .

Gerencie o acesso de usuários ao NetApp Console com controle de acesso baseado em funções (RBAC), atribuindo funções predefinidas no nível da organização, pasta ou projeto. Cada função concede permissões específicas que definem quais ações os usuários podem executar dentro do escopo atribuído.

A NetApp projeta funções de console com privilégios mínimos, de forma que cada função inclua apenas as permissões necessárias para suas tarefas. Essa abordagem aumenta a segurança ao limitar o acesso apenas ao que cada membro precisa.

Depois de organizar os recursos em pastas e projetos, atribua aos membros da organização uma ou mais funções para pastas ou projetos específicos, permitindo que eles executem apenas suas responsabilidades.

Por exemplo, você pode atribuir a um membro a função de administrador de Resiliência a Ransomware para um nível de projeto específico, permitindo que ele execute operações de Resiliência a Ransomware para recursos dentro desse projeto, sem conceder a ele acesso mais amplo a toda a organização. Esse mesmo usuário pode receber a função para vários projetos dentro da sua organização.

Você pode atribuir aos usuários várias funções para o mesmo escopo ou para escopos diferentes,

dependendo de suas responsabilidades. Por exemplo, uma organização menor pode ter o mesmo usuário gerenciando as tarefas de Resiliência a Ransomware e Backup e Recuperação no nível organizacional, enquanto uma organização maior pode ter usuários diferentes atribuídos a cada função no nível do projeto.

Tipos de membros da organização Console

Existem três tipos de membros em uma organização do NetApp Console : * *Contas de usuário*: Usuários individuais que fazem login no NetApp Console para gerenciar recursos. Os usuários precisam se cadastrar no NetApp Console antes de serem adicionados a uma organização. * *Contas de serviço*: Contas não humanas usadas por aplicativos ou serviços para interagir com o NetApp Console por meio de APIs. Você pode adicionar contas de serviço diretamente à sua organização do Console. * *Grupos federados*: Grupos sincronizados do seu provedor de identidade (IdP) que permitem gerenciar o acesso de vários usuários coletivamente. Cada usuário dentro de um grupo federado deve ter se cadastrado no NetApp Console e ter sido adicionado à sua organização com uma função de acesso antes de poder acessar os recursos concedidos ao grupo.

"Aprenda como adicionar membros à sua organização."

Funções predefinidas no NetApp Console

O NetApp Console inclui funções predefinidas que você pode atribuir aos membros da organização. Cada função inclui permissões que especificam quais ações um membro pode realizar dentro do seu escopo atribuído (organização, pasta ou projeto).

As funções do NetApp Console utilizam princípios de privilégio mínimo, garantindo que os membros tenham apenas as permissões necessárias para suas tarefas, e categorizam as funções pelo tipo de acesso que fornecem:

- Funções da plataforma: Conceder permissões de administração do console
- Funções de serviços de dados: Conceder permissões para gerenciar serviços de dados específicos, como Resiliência a Ransomware e Backup e Recuperação.
- Funções do aplicativo: Conceder permissões para gerenciar o armazenamento, bem como auditar eventos e alertas do Console.

Você pode atribuir várias funções a um membro com base em suas responsabilidades. Por exemplo, você pode atribuir a um membro tanto a função de administrador de Resiliência a Ransomware quanto a função de administrador de Backup e Recuperação para um projeto específico.

"Saiba mais sobre as funções predefinidas disponíveis no NetApp Console.".

Gerencie o acesso de membros no NetApp Console.

Gerencie o acesso de membros na sua organização do Console. Atribua funções para definir permissões. Remover membros quando eles saírem.

Funções de acesso necessárias

Superadministrador, administrador da organização ou administrador de pasta ou projeto (para pastas e projetos que eles administram). Link:reference-iam-predefined-roles.html[Saiba mais sobre funções de acesso].

Você pode atribuir funções de acesso por projeto ou pasta. Por exemplo, atribua uma função a um usuário para dois projetos específicos ou atribua a função no nível da pasta para conceder a um usuário a função de administrador de Resiliência a Ransomware para todos os projetos em uma pasta.

Adicione suas pastas e projetos antes de atribuir acesso aos usuários. "Aprenda como adicionar pastas e projetos."

Entenda como o acesso é concedido no NetApp Console.

O NetApp Console utiliza um modelo de controle de acesso baseado em funções (RBAC) para gerenciar as permissões de usuário. Você pode atribuir funções predefinidas aos membros individualmente ou por meio de grupos federados. Você pode adicionar e atribuir funções a contas de serviço, bem como a grupos federados. Cada função define quais ações um membro pode executar nos recursos associados.

Observe o seguinte sobre como conceder acesso no NetApp Console:

- Todos os usuários devem primeiro se cadastrar no NetApp Console antes de obterem acesso aos recursos.
- Você deve atribuir explicitamente uma função a cada usuário no Console antes que ele possa acessar os recursos, mesmo que seja membro de um grupo federado ao qual já tenha sido atribuída uma função.
- Você pode adicionar contas de serviço diretamente do Console e atribuir funções a elas.

Utilizando a herança de funções

Ao atribuir uma função no nível da organização, pasta ou projeto no NetApp Console, essa função é automaticamente herdada por todos os recursos dentro do escopo selecionado. Por exemplo, as funções em nível de pasta aplicam-se a todos os projetos contidos nela, enquanto as funções em nível de projeto aplicam-se a todos os recursos dentro desse projeto.

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."

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**.

Exibir funções atribuídas a um membro

Você pode verificar quais funções estão atribuídas a eles atualmente.

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" .

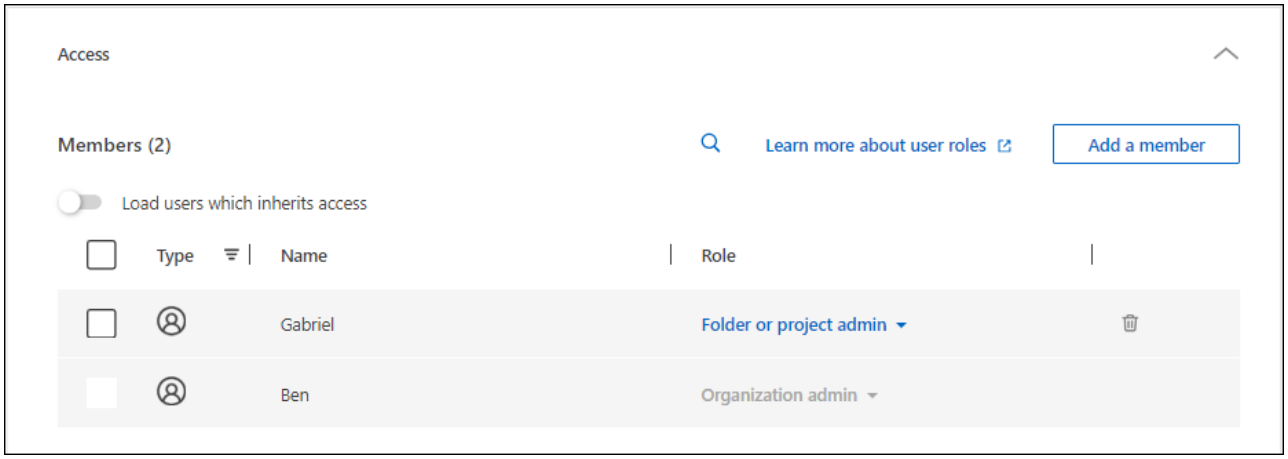
1. Na página **Membros**, navegue até um membro na tabela e selecione ••• Em seguida, selecione **Ver detalhes**.
2. Na tabela, expanda a linha respectiva da organização, pasta ou projeto onde você deseja visualizar a função atribuída ao membro e selecione **Exibir** na coluna **Função**.

Ver membros associados a uma pasta ou projeto

Você pode visualizar os membros que têm acesso a uma pasta ou projeto específico.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Organização**.
3. Na página **Organização**, navegue até um projeto ou pasta na tabela, selecione ••• e então selecione **Editar pasta** ou **Editar projeto**.
   - Selecione **Acesso** para visualizar os membros que têm acesso à pasta ou ao projeto.



Atribuir ou modificar o acesso de membros

Depois que um usuário se cadastra no NetApp Console, você pode adicioná-lo à sua organização e atribuir-lhe uma função para fornecer acesso aos recursos. "Aprenda como adicionar membros à sua organização."

Você pode ajustar o acesso de um membro adicionando ou removendo funções conforme necessário.

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 desempenhar múltiplas 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 que realizam tarefas mais especializadas. Alternativamente, você também pode atribuir a função de administrador de Resiliência a Ransomware a um usuário no nível da organização. Nesse exemplo, o usuário seria capaz de executar tarefas de resiliência a 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 .

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.

3. Selecione uma das guias de membros: **Usuários**, **Contas de serviço** ou **Grupos federados**.
4. Selecione o menu de ações ••• ao lado do membro ao qual você deseja atribuir uma função e selecione **Adicionar uma função**.
5. 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.
6. Selecione **Adicionar novas funções**.

Alterar a função atribuída a um membro

Alterar as funções de um membro para atualizar o seu acesso.

> ⓘ 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. Selecione **Membros**.
3. Selecione uma das guias de membros: **Usuários**, **Contas de serviço** ou **Grupos federados**.
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 alterar a função atribuída ao membro e selecione **Exibir** na coluna **Função** para visualizar as funções atribuídas a este membro.
6. 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 remover a função de um membro, selecione 🗑 Ao lado da função, clique para remover a respectiva função do membro. Você precisará confirmar a remoção.

Remover um membro da sua organização

Remova um membro se ele deixar sua organização.

Ao remover um membro, o sistema revoga suas permissões de Console, mas mantém suas contas de Console e do Site de Suporte da NetApp .

Membros federados

- Os usuários federados perdem automaticamente o acesso ao NetApp Console quando são removidos do seu IdP. Mas você ainda deve removê-los da sua organização no Console para manter sua lista de membros atualizada.
- Se você remover um usuário de um grupo federado em seu IdP, ele perderá o acesso ao Console associado a esse grupo. No entanto, eles ainda mantêm qualquer acesso associado a uma função explícita atribuída a eles no Console.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.
3. Selecione uma das guias de membros: **Usuários**, **Contas de serviço** ou **Grupos federados**.
4. Na página **Membros**, navegue até um membro na tabela, selecione ••• então selecione **Excluir usuário**.
5. Confirme que você deseja remover o membro da sua organização.

Segurança do usuário

Proteja o acesso dos usuários à sua organização NetApp Console gerenciando as configurações de segurança dos membros. Você pode redefinir senhas de usuários, gerenciar a autenticação multifator (MFA) e recriar credenciais de contas de serviço.

Funções de acesso necessárias

Superadministrador, administrador da organização ou administrador de pasta ou projeto (para pastas e projetos que eles administram). Link:reference-iam-predefined-roles.html[Saiba mais sobre funções de acesso].

Redefinir senhas de usuários (somente usuários locais)

Os administradores da organização não podem redefinir as senhas dos usuários locais. No entanto, eles podem instruir os usuários a redefinirem suas próprias senhas.

Instrua o usuário a redefinir sua senha na página de login do Console, selecionando **Esqueceu sua senha?**.

Essa opção não está disponível para usuários em uma organização federada.

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.

A autenticação multifator está disponível apenas para usuários locais. Usuários federados não podem ativar a autenticação multifator (MFA).

Os usuários deverão configurar a autenticação multifator (MFA) novamente ao fazerem login após a remoção. Caso o usuário perca temporariamente o acesso ao seu dispositivo MFA, ele poderá usar o código de recuperação salvo 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.

Recriar as credenciais para uma conta de serviço

Você pode criar novas credenciais para um serviço caso as perca ou precise atualizá-las.

A criação de novas credenciais exclui as antigas. Você não pode usar as credenciais antigas.

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 Console exibe o segredo do cliente apenas uma vez. Certifique-se de copiar ou baixar o arquivo e armazená-lo em local seguro.

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.
"Visualizador de Google Cloud NetApp Volumes"	Usuários com a função de usuário Google Cloud NetApp Volumes podem visualizar os 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.

Função de aplicação	Responsabilidades
"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.
"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.

Função de serviço de dados	Responsabilidades
"Visualizador de recuperação de desastres"	Ver apenas informações.
Visualizador de classificação	Permite que os usuários visualizem os resultados da verificação de NetApp Data Classification . 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 possui função administrativa.
"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

Tarefa	Administrador da Federação	Visualizador da Federação
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.
- *Visualizador de Google Cloud NetApp Volumes *: Visualize os 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	Sim
Gerenciar alertas	Sim	Não
Crie alertas para si mesmo	Sim	Sim
* Licenses and subscriptions*:		
Pode visualizar licenças e assinaturas	Sim	Sim
*Página de relatórios do Keystone *:		

Recurso e ação	Administrador Keystone	Visualizador Keystone
Baixar relatórios	Sim	Sim
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 função de analista de suporte operacional aos usuários para conceder 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
Ver a página de auditoria e notificações	Sim
Visualizar, baixar e configurar alertas	Sim

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			

Recurso e ação	Administrador de armazenamento	Especialista em saúde do sistema	Visualizador de armazenamento
Ver todas as páginas e funções	Sim	Sim	Sim
* Licenses and subscriptions*			
Ver todas as páginas e funções	Não	Não	Não
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

Recurso e ação	Administrador de armazenamento	Especialista em saúde do sistema	Visualizador de armazenamento
Credenciais			
Credenciais do usuário	Sim	Sim	Não

Funções de serviços de dados

Funções de NetApp Backup and Recovery 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 instantâneos 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 Clone 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

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 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
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

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
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
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

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
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
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

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
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
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 NetApp Disaster Recovery 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
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

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
Na aba Monitoramento de Tarefas:				
Ver empregos	Sim	Não	Sim	Sim
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 ao NetApp Ransomware Resilience. O Ransomware Resilience oferece suporte às seguintes funções:

Funções de base

- Administrador de resiliência contra ransomware - Configurar as configurações de resiliência contra ransomware; investigar e responder a alertas de criptografia
- Visualizador de resiliência de ransomware - visualize incidentes de criptografia, relatórios e configurações de descoberta

Funções de atividade de comportamento do usuário"Detecção de atividade suspeita do usuário" Os alertas fornecem visibilidade de dados como eventos de atividade de arquivo; esses alertas incluem nomes de arquivos e ações de arquivo (como Ler, Gravar, Excluir, Renomear) executadas pelo usuário. Para limitar a visibilidade desses dados, somente usuários com essas funções podem gerenciar ou visualizar esses alertas.

- Administrador de comportamento do usuário de resiliência contra ransomware - Ative a detecção de atividades suspeitas do usuário, investigue e responda a alertas de atividades suspeitas do usuário
- Visualizador de comportamento do usuário do Ransomware Resilience - Visualize alertas de atividades suspeitas do usuário

> As funções de comportamento do usuário não são funções autônomas; elas foram projetadas para serem adicionadas às funções de administrador ou visualizador do Ransomware Resilience. Para mais informações, consulte Funções de comportamento do usuário.

Consulte as tabelas a seguir para obter descrições detalhadas de cada função.

Funções de base

A tabela a seguir descreve as ações disponíveis para as funções de administrador e visualizador do Ransomware Resilience.

Recurso e ação	Administrador de resiliência de ransomware	Visualizador de resiliência de ransomware
Ver painel e todas as guias	Sim	Sim

Recurso e ação	Administrador de resiliência de ransomware	Visualizador de resiliência de ransomware
No painel, atualize o status da recomendação	Sim	Não
Iniciar teste gratuito	Sim	Não
Iniciar descoberta de cargas de trabalho	Sim	Não
Iniciar a redescoberta das cargas de trabalho	Sim	Não
Na aba Proteger:		
Adicionar, modificar ou excluir planos de proteção para políticas de *criptografia*	Sim	Não
Proteja as cargas de trabalho	Sim	Não
Identifique a exposição a dados sensíveis com a Classificação de Dados	Sim	Não
Listar planos de proteção e detalhes	Sim	Sim
Grupos de proteção de lista	Sim	Sim
Ver detalhes do grupo de proteção	Sim	Sim
Criar, editar ou excluir grupos de proteção	Sim	Não
Baixar dados	Sim	Sim
Na aba Alertas:		
Exibir alertas de criptografia e detalhes de alertas	Sim	Sim
Editar status do incidente de criptografia	Sim	Não
Marcar alerta de criptografia para recuperação	Sim	Não
Ver detalhes do incidente de criptografia	Sim	Sim
Descartar ou resolver incidentes de criptografia	Sim	Não
Obtenha a lista completa de arquivos afetados no evento de criptografia	Sim	Não
Baixar dados de alertas de eventos de criptografia	Sim	Sim

Recurso e ação	Administrador de resiliência de ransomware	Visualizador de resiliência de ransomware
Bloquear usuário (com configuração do agente de segurança de carga de trabalho)	Sim	Não
Na aba Recuperar:		
Baixar arquivos afetados pelo evento de criptografia	Sim	Não
Restaurar carga de trabalho do evento de criptografia	Sim	Não
Baixar dados de recuperação do evento de criptografia	Sim	Sim
Baixar relatórios do evento de criptografia	Sim	Sim
Na aba Configurações:		
Adicionar ou modificar destinos de backup	Sim	Não
Listar destinos de backup	Sim	Sim
Exibir alvos SIEM conectados	Sim	Sim
Adicionar ou modificar alvos SIEM	Sim	Não
Configurar exercício de prontidão	Sim	Não
Iniciar, redefinir ou editar o exercício de prontidão	Sim	Não
Revisar o status do exercício de prontidão	Sim	Sim
Atualizar configuração de descoberta	Sim	Não
Exibir configuração de descoberta	Sim	Sim
Na aba Relatórios:		
Baixar relatórios	Sim	Sim

Funções de comportamento do usuário

Para configurar configurações de comportamento suspeito do usuário e responder a alertas, um usuário deve ter a função de administrador de comportamento do usuário de resiliência ao ransomware. Para visualizar apenas alertas de comportamento suspeito do usuário, o usuário deve ter a função de visualizador de comportamento do usuário do Ransomware Resilience.

As funções de comportamento do usuário devem ser conferidas aos usuários com privilégios de administrador ou visualizador do Ransomware Resilience existentes que precisam de acesso a"configurações e alertas de

atividades suspeitas do usuário" . Um usuário com a função de administrador de Resiliência contra Ransomware, por exemplo, deve receber a função de administrador de comportamento de usuário de Resiliência contra Ransomware para configurar agentes de atividade do usuário e bloquear ou desbloquear usuários. A função de administrador de comportamento do usuário de Resiliência contra Ransomware não deve ser conferida a um visualizador de Resiliência contra Ransomware.

Para ativar a detecção de atividades suspeitas do usuário, você deve ter a função de administrador da Organização do Console.

A tabela a seguir descreve as ações disponíveis para as funções de administrador e visualizador do comportamento do usuário do Ransomware Resilience.

Recurso e ação	Comportamento do usuário de resiliência ao ransomware	Visualizador de comportamento do usuário de resiliência de ransomware
Na aba Configurações:		
Criar, modificar ou excluir agente de atividade do usuário	Sim	Não
Criar ou excluir conector de diretório de usuário	Sim	Não
Pausar ou retomar o coletor de dados	Sim	Não
Execute um exercício de preparação para violação de dados	Sim	Não
Na aba Proteger:		
Adicionar, modificar ou excluir planos de proteção para políticas de *comportamento suspeito do usuário*	Sim	Não
Na aba Alertas:		
Ver alertas de atividade do usuário e detalhes do alerta	Sim	Sim
Editar status do incidente de atividade do usuário	Sim	Não
Marcar alerta de atividade do usuário para recuperação	Sim	Não
Ver detalhes do incidente de atividade do usuário	Sim	Sim
Descartar ou resolver incidentes de atividade do usuário	Sim	Não
Obtenha a lista completa de arquivos afetados por usuários suspeitos	Sim	Sim
Baixar dados de alertas de eventos de atividade do usuário	Sim	Sim
Bloquear ou desbloquear usuário	Sim	Não

Recurso e ação	Comportamento do usuário de resiliência ao ransomware	Visualizador de comportamento do usuário de resiliência de ransomware
Na aba Recuperar:		
Baixar arquivos impactados para evento de atividade do usuário	Sim	Não
Restaurar carga de trabalho do evento de atividade do usuário	Sim	Não
Baixar dados de recuperação do evento de atividade do usuário	Sim	Sim
Baixar relatórios de eventos de atividade do usuário	Sim	Sim

API de identidade e acesso

IDs de organização e projeto

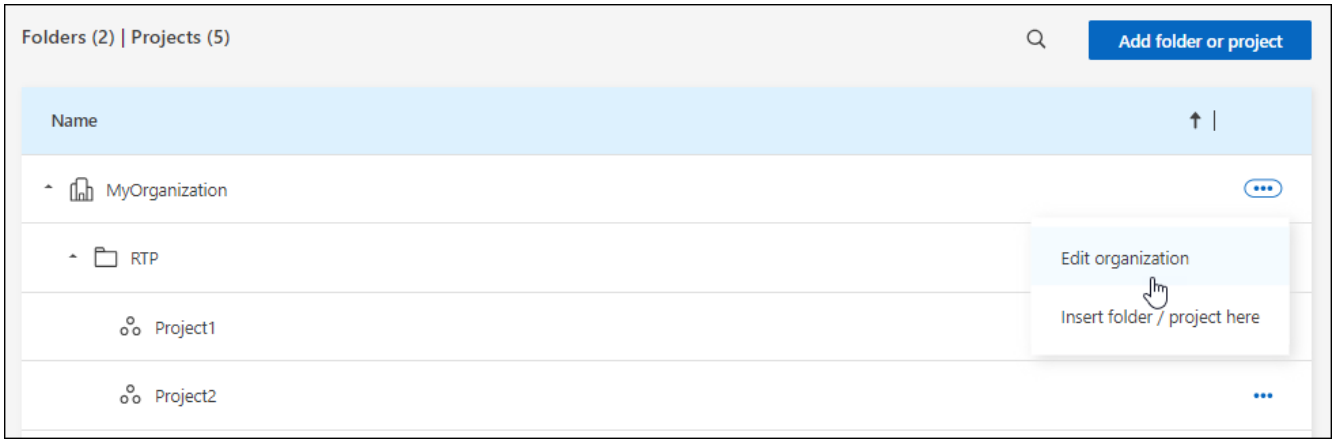
Sua organização do NetApp Console tem um nome e um ID. Você pode escolher um nome para sua organização para ajudar a identificá-la. Também pode ser necessário recuperar o ID da organização para determinadas integrações.

Renomeie sua organização

Você pode renomear sua organização. Isso é útil se você apoia mais do que 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

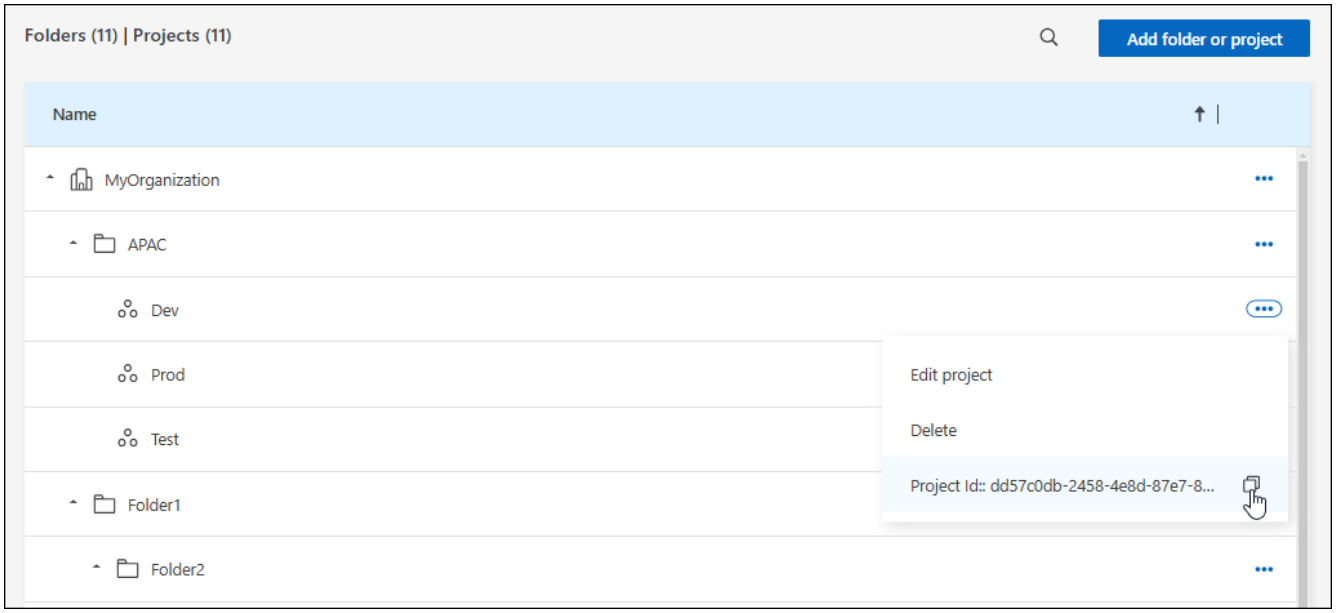
Você precisará obter o ID de um projeto se estiver usando a API. Por exemplo, ao criar um sistema Cloud Volumes ONTAP .

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"

Informações sobre direitos autorais

Informações sobre marcas comerciais