Controle de acesso baseado em funções (RBAC)

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Índice

Controle de acesso baseado em funções (RBAC)

Saiba mais sobre as ferramentas RBAC do ONTAP

O controle de acesso baseado em funções (RBAC) é uma estrutura de segurança para controlar o acesso a recursos dentro de uma organização. O RBAC simplifica a administração ao definir funções com níveis específicos de autoridade para executar ações, em vez de atribuir autorização a usuários individuais. As funções definidas são atribuídas aos usuários, o que ajuda a reduzir o risco de erro e simplifica o gerenciamento do controle de acesso em toda a sua organização.

O modelo padrão RBAC consiste em diversas tecnologias ou fases de implementação com complexidade crescente. O resultado é que as implementações reais de RBAC, baseadas nas necessidades dos fornecedores de software e de seus clientes, podem variar e ir de relativamente simples até muito complexas.

Componentes RBAC

Em linhas gerais, existem vários componentes que geralmente estão incluídos em toda implementação de RBAC. Esses componentes são interligados de diferentes maneiras como parte da definição dos processos de autorização.

Privileges

Um privilégio é uma ação ou capacidade que pode ser permitida ou negada. Pode ser algo simples, como a capacidade de ler um arquivo, ou uma operação mais abstrata específica de um determinado sistema de software. Privileges também podem ser definidos para restringir o acesso a endpoints da API REST e comandos de CLI. Toda implementação de RBAC inclui privilégios predefinidos e também pode permitir que administradores criem privilégios personalizados.

Funções

Uma *função* é um contêiner que inclui um ou mais privilégios. As funções geralmente são definidas com base em tarefas ou funções de trabalho específicas. Quando uma função é atribuída a um usuário, o usuário recebe todos os privilégios contidos nessa função. E, assim como acontece com os privilégios, as implementações incluem funções predefinidas e geralmente permitem a criação de funções personalizadas.

Objetos

Um *objeto* representa um recurso real ou abstrato identificado no ambiente RBAC. As ações definidas por meio dos privilégios são executadas sobre ou com os objetos associados. Dependendo da implementação, os privilégios podem ser concedidos a um tipo de objeto ou a uma instância de objeto específica.

Usuários e grupos

Usuários são atribuídos ou associados a uma função aplicada após a autenticação. Algumas implementações de RBAC permitem que apenas uma função seja atribuída a um usuário, enquanto outras permitem várias funções por usuário, talvez com apenas uma função ativa por vez. Atribuir funções a grupos pode simplificar ainda mais a administração de segurança.

Permissões

Uma *permissão* é uma definição que vincula um usuário ou grupo, juntamente com uma função, a um objeto. As permissões podem ser úteis em um modelo de objeto hierárquico, onde podem ser opcionalmente herdadas pelos filhos na hierarquia.

Dois ambientes RBAC

Existem dois ambientes RBAC distintos que você precisa considerar ao trabalhar com ONTAP tools for VMware vSphere 10. ONTAP tools for VMware vSphere 10 exige privilégios específicos tanto no vCenter quanto no ONTAP para executar suas operações. Embora o ONTAP tools automatize tarefas de gerenciamento de storage, ele não cria contas de usuário nem no vCenter nem no ONTAP. As contas de serviço devem ser criadas por um administrador do vSphere, conforme necessário. Esta documentação fornece orientações para que os administradores atribuam as funções e permissões necessárias para o gerenciamento eficaz do ONTAP tools.

Servidor VMware vCenter

A implementação do RBAC no VMware vCenter Server é usada para restringir o acesso a objetos expostos pela interface de usuário do vSphere Client. Como parte da instalação do ONTAP tools for VMware vSphere 10, o ambiente RBAC é estendido para incluir objetos adicionais que representam as funcionalidades do ONTAP tools. O acesso a esses objetos é fornecido por meio do plug-in remoto. Veja "vCenter Server ambiente RBAC" para mais informações.

Cluster ONTAP

ONTAP tools for VMware vSphere 10 se conecta a um cluster ONTAP por meio da API REST do ONTAP para executar operações relacionadas ao storage. O acesso aos recursos de storage é controlado por meio de uma função ONTAP associada ao usuário ONTAP fornecido durante a autenticação. Consulte "Ambiente ONTAP RBAC" para obter mais informações.

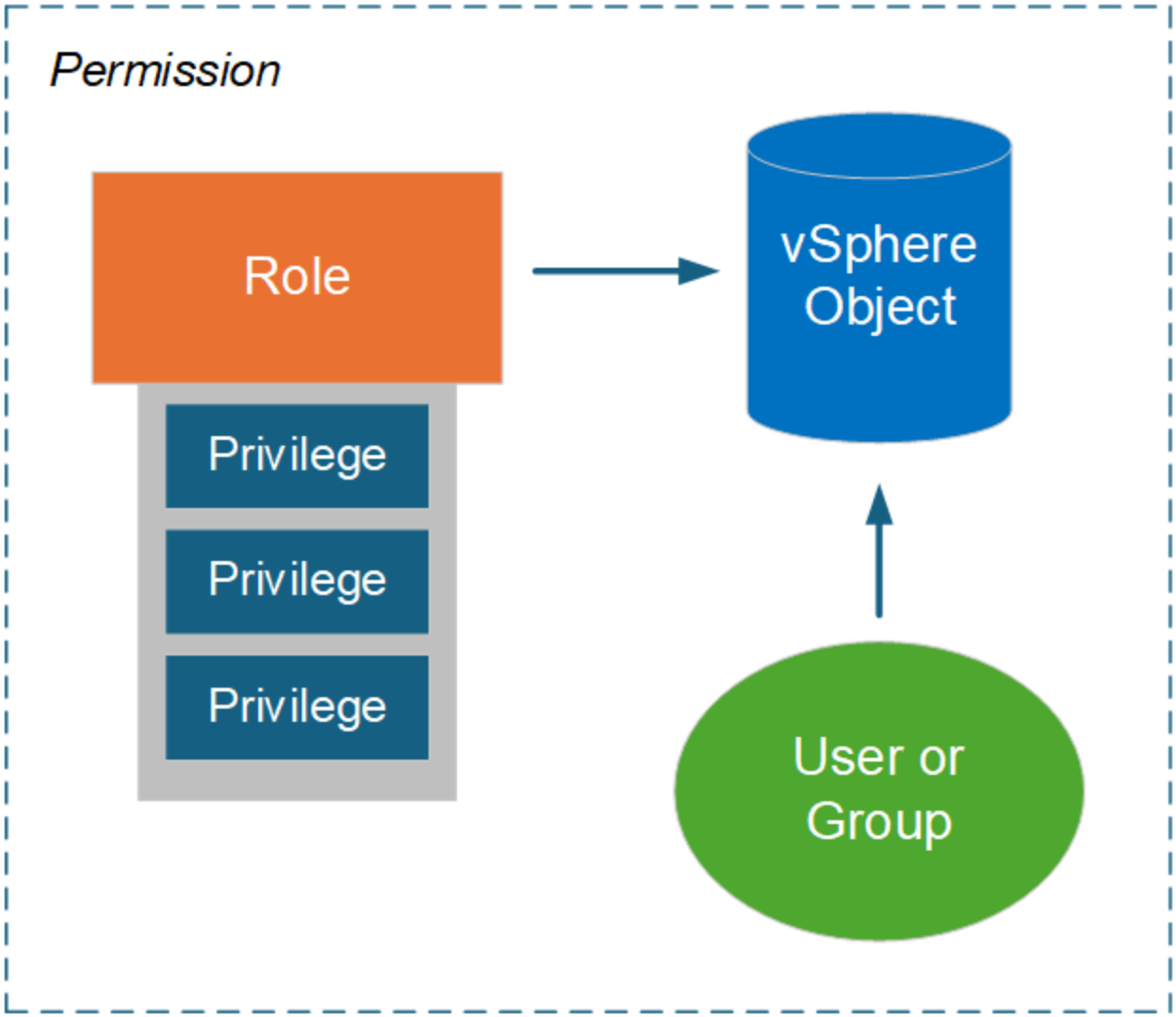
RBAC com VMware vSphere

Como o RBAC do vCenter Server funciona com as ONTAP tools

O VMware vCenter Server oferece um recurso de RBAC que permite que você controle o acesso a objetos do vSphere. É uma parte importante dos serviços de autenticação e autorização centralizados do vCenter.

Ilustração de uma permissão de servidor vCenter

Uma permissão é a base para a aplicação do controle de acesso no ambiente do vCenter Server. Ela é aplicada a um objeto vSphere com um usuário ou grupo incluído na definição da permissão. Uma ilustração de alto nível de uma permissão do vCenter é fornecida na figura abaixo.



Componentes de uma permissão de servidor vCenter

Uma permissão de vCenter Server é um pacote de vários componentes que são vinculados quando a permissão é criada.

vSphere objetos

As permissões estão associadas a objetos do vSphere, como o vCenter Server, hosts ESXi, máquinas virtuais, datastores, data centers e pastas. Com base nas permissões atribuídas ao objeto, o vCenter Server determina quais ações ou tarefas podem ser executadas no objeto por cada usuário ou grupo. Para as tarefas específicas das ONTAP tools for VMware vSphere, todas as permissões são atribuídas e validadas no nível raiz ou na pasta raiz do vCenter Server. Consulte "Use RBAC com o servidor vCenter" para mais informações.

Privileges e funções

Existem dois tipos de privilégios do vSphere usados com ONTAP tools for VMware vSphere 10. Para simplificar o trabalho com RBAC nesse ambiente, ONTAP tools fornece funções que contêm os privilégios nativos e personalizados necessários. Os privilégios incluem:

- Privilégios nativos do servidor vCenter

  Esses são os privilégios concedidos pelo vCenter Server.

- Privilégios específicos das ferramentas ONTAP

  Esses são privilégios personalizados exclusivos das ONTAP tools for VMware vSphere.

Usuários e grupos

Você pode definir usuários e grupos usando o Active Directory ou a instância local do vCenter Server. Combinado com uma função, você pode criar uma permissão em um objeto na hierarquia de objetos do vSphere. A permissão concede acesso com base nos privilégios da função associada. Observe que as funções não são atribuídas diretamente aos usuários de forma isolada. Em vez disso, usuários e grupos obtêm acesso a um objeto por meio dos privilégios de função como parte da permissão do vCenter Server.

vCenter considerações sobre RBAC do servidor para ONTAP tools

Existem vários aspectos da implementação do RBAC das ONTAP tools for VMware vSphere 10 com o vCenter Server que você deve considerar antes de usá-la em um ambiente de produção.

vCenter roles e a conta de administrador

Você só precisa definir e usar as funções personalizadas do servidor vCenter se quiser limitar o acesso aos objetos vSphere e às tarefas administrativas associadas. Se limitar o acesso não for necessário, você pode usar uma conta de administrador. Cada conta de administrador é definida com a função de Administrador no nível mais alto da hierarquia de objetos. Isso fornece acesso total aos objetos vSphere, incluindo aqueles adicionados por ONTAP tools for VMware vSphere 10.

hierarquia de objetos do vSphere

O inventário de objetos do vSphere está organizado em uma hierarquia. Por exemplo, você pode navegar pela hierarquia da seguinte forma:

`vCenter Server` → `Datacenter` → `Cluster` → `ESXi host` → `Virtual Machine`

Todas as permissões são validadas na hierarquia de objetos do vSphere, exceto as operações do plug-in VAAI, que são validadas em relação ao host ESXi de destino.

Funções incluídas nas ONTAP tools for VMware vSphere 10

Para simplificar o trabalho com o RBAC do servidor vCenter, ONTAP tools for VMware vSphere fornece funções predefinidas adaptadas a várias tarefas administrativas.

> Você pode criar novas funções personalizadas, se necessário. Para isso, clone uma das funções existentes das ferramentas ONTAP e edite-a conforme necessário. Após fazer as alterações de configuração, os usuários do cliente vSphere afetados precisam fazer logout e entrar novamente para ativar as alterações.

Para visualizar as funções das ONTAP tools for VMware vSphere, selecione **Menu** na parte superior do vSphere Client e clique em **Administração** e, em seguida, em **Funções** à esquerda. Os seguintes privilégios devem estar incluídos na função atribuída ao usuário vCenter responsável pela implantação ou processo de

ambientação do vCenter Server. Certifique-se de que esses privilégios estejam configurados como pré-requisito para a implantação ou processo de ambientação.

- Alarmes
  - Confirmar alarme
- Biblioteca de Conteúdo
  - Adicionar item da biblioteca
  - Faça check-in em um modelo
  - Confira um modelo
  - Baixar arquivos
  - Importar armazenamento
  - Leitura de storage
  - Sincronizar item da biblioteca
  - Sincronizar biblioteca assinada
  - Exibir configurações de configuração
- Datastore
  - Alocar espaço
  - Navegar no datastore
  - Operações de arquivo de baixo nível
  - Remover arquivo
  - Atualizar arquivos de máquina virtual
  - Atualizar metadados da máquina virtual
- ESX Agent Manager
  - Visualizar
- Pasta
  - Criar pasta
- Host
  - Configuração
    - Configurações avançadas
    - Alterar configurações
    - Configuração de rede
    - Recursos do sistema
    - Configuração de inicialização automática da máquina virtual
  - Operações locais
    - Criar máquina virtual
    - Excluir máquina virtual
    - Reconfigurar máquina virtual
- Rede

    - Atribuir rede
    - Configurar
- OvfManager
    - OvfConsumer Acesso
- Perfil do host
    - Visualizar
- Recurso
    - Atribua máquina virtual ao pool de recursos
- Tarefa agendada
    - Criar tarefas
    - Modificar tarefa
    - Executar tarefa
- Tarefas
    - Criar tarefa
    - Tarefa de atualização
- vApp
    - Adicionar máquina virtual
    - Atribuir pool de recursos
    - Atribuir vApp
    - Criar
    - Importar
    - Mover
    - Desligar
    - Ligar
    - Extrair da URL
    - Visualizar ambiente OVF
- Máquina virtual
    - Alterar configuração
        - Adicionar disco existente
        - Adicionar novo disco
        - Adicionar ou remover dispositivo
        - Configuração avançada
        - Alterar contagem de CPU
        - Alterar memória
        - Alterar configurações
        - Alterar recurso
        - Estender disco virtual

        - Modificar configurações do dispositivo
        - Remover disco
        - Redefinir informações do convidado
        - Atualizar a compatibilidade da máquina virtual
    - Editar inventário
        - Criar a partir de existente
        - Criar novo
        - Mover
        - Cadastre-se
        - Remover
        - Cancelar registro
    - Interação
        - Operação de backup em máquina virtual
        - Configurar mídia de CD
        - Configurar mídia de disquete
        - Conecte dispositivos
        - Interação com o console
        - Gerenciamento do sistema operacional convidado por meio da API VIX
        - Desligar
        - Ligar
        - Reiniciar
        - Suspender
    - Provisionamento
        - Permitir acesso ao disco
        - Modelo de clone
        - Personalizar convidado
        - Implantar modelo
        - Modificar especificação de personalização
        - Leia as especificações de personalização
    - Gerenciamento de Snapshot
        - Criar instantâneo
        - Remover snapshot
        - Renomear snapshot
        - Reverter para o snapshot

Existem três funções predefinidas, conforme descrito abaixo.

Administrador do NetApp ONTAP tools for VMware vSphere

Fornece todos os privilégios nativos do vCenter Server e os privilégios específicos das ferramentas ONTAP

necessários para executar tarefas administrativas essenciais das ONTAP tools for VMware vSphere.

NetApp ONTAP tools for VMware vSphere somente leitura

Fornece acesso somente leitura às ferramentas do ONTAP. Esses usuários não podem executar nenhuma ação das ferramentas do ONTAP para VMware vSphere que seja controlada por acesso.

Provisionamento do NetApp ONTAP tools for VMware vSphere

Fornece alguns dos privilégios nativos do vCenter Server e privilégios específicos das ONTAP tools que são necessários para provisionar storage. Você pode executar as seguintes tarefas:

- Criar novos datastores
- Gerenciar datastores

vSphere objetos e backends de storage ONTAP

Os dois ambientes RBAC funcionam juntos. Ao executar uma tarefa na interface do cliente vSphere, primeiro são verificadas as funções das ONTAP tools definidas para o vCenter Server. Se a operação for permitida pelo vSphere, então os privilégios da função ONTAP são examinados. Essa segunda etapa é realizada com base na função ONTAP atribuída ao usuário quando o backend de storage foi criado e configurado.

Trabalhando com RBAC do vCenter Server

Há alguns pontos a considerar ao trabalhar com os privilégios e permissões do servidor vCenter.

Privilégios necessários

Para acessar a interface de usuário do ONTAP tools for VMware vSphere 10, você precisa ter o privilégio *View* específico das ONTAP tools. Se você fizer login no vSphere sem esse privilégio e clicar no ícone NetApp, o ONTAP tools for VMware vSphere exibirá uma mensagem de erro e impedirá você de acessar a interface de usuário.

O nível de atribuição na hierarquia de objetos da vSphere determina a quais partes da interface de usuário você pode acessar. Atribuir o privilégio "Visualizar" ao objeto raiz permite que você acesse ONTAP tools for VMware vSphere clicando no ícone NetApp.

Você pode, em vez disso, atribuir o privilégio de visualização a outro nível de objeto vSphere inferior. No entanto, isso limitará os menus das ONTAP tools for VMware vSphere que você pode acessar e usar.

Atribuindo permissões

Você precisa usar permissões do vCenter Server se quiser limitar o acesso aos objetos e tarefas do vSphere. O local onde você atribui permissões na hierarquia de objetos do vSphere determina quais tarefas do ONTAP tools for VMware vSphere 10 os usuários podem executar.

A menos que você precise definir um acesso mais restritivo, geralmente é uma boa prática atribuir permissões no nível do objeto raiz ou da pasta raiz.

As permissões disponíveis com ONTAP tools for VMware vSphere 10 aplicam-se a objetos personalizados que não sejam vSphere, como sistemas de storage. Se possível, você deve atribuir essas permissões ao objeto raiz do ONTAP tools for VMware vSphere, pois não há nenhum objeto vSphere ao qual você possa atribuí-las. Por exemplo, qualquer permissão que inclua o privilégio "Adicionar/Modificar/Remover sistemas de storage" do ONTAP tools for VMware vSphere deve ser atribuída no nível do objeto raiz.

Ao definir uma permissão em um nível superior na hierarquia de objetos, você pode configurá-la para que seja

transmitida e herdada pelos objetos filhos. Se necessário, você pode atribuir permissões adicionais aos objetos filhos que substituem as permissões herdadas do pai.

Você pode modificar uma permissão a qualquer momento. Se você alterar algum dos privilégios dentro de uma permissão, os usuários associados a essa permissão precisarão fazer logout do vSphere e entrar novamente para que a alteração seja aplicada.

RBAC com ONTAP

Como o RBAC do ONTAP funciona com as ONTAP tools

ONTAP oferece um ambiente RBAC robusto e extensível. Você pode usar o recurso RBAC para controlar o acesso ao armazenamento e às operações do sistema, conforme exposto pela API REST e pela CLI. É recomendável familiarizar-se com o ambiente antes de usá-lo com uma implantação do ONTAP tools for VMware vSphere 10.

Visão geral das opções administrativas

Existem diversas opções disponíveis ao usar ONTAP RBAC, dependendo do seu ambiente e objetivos. Uma visão geral das principais decisões administrativas é apresentada abaixo. Consulte também "Automação do ONTAP: visão geral da segurança RBAC" para obter mais informações.

> O RBAC do ONTAP é otimizado para um ambiente de storage e é mais simples do que a implementação de RBAC fornecida com vCenter Server. Com ONTAP, você atribui uma função diretamente ao usuário. A configuração de permissões explícitas, como as usadas com o vCenter Server, não é necessária com o RBAC do ONTAP.

Tipos de funções e privilégios

Uma função ONTAP é necessária ao definir um usuário ONTAP. Existem dois tipos de funções ONTAP:

- REST

  As funções REST foram introduzidas no ONTAP 9.6 e geralmente são aplicadas a usuários que acessam o ONTAP por meio da API REST. Os privilégios incluídos nessas funções são definidos em termos de acesso aos endpoints da API REST do ONTAP e às ações associadas.

- Tradicional

  Essas são as funções legadas que existiam antes do ONTAP 9.6. Elas continuam sendo um aspecto fundamental do RBAC. Os privilégios são definidos em termos de acesso aos comandos da CLI do ONTAP.

Embora as funções REST tenham sido introduzidas mais recentemente, as funções tradicionais oferecem algumas vantagens. Por exemplo, parâmetros de consulta adicionais podem ser incluídos para permitir que os Privileges definam com mais precisão os objetos aos quais se aplicam.

Escopo

As funções do ONTAP podem ser definidas com um de dois escopos diferentes. Elas podem ser aplicadas a um SVM de dados específico (nível de SVM) ou a todo o cluster ONTAP (nível de cluster).

Definições de funções

ONTAP fornece um conjunto de funções predefinidas tanto no nível do cluster quanto no nível da SVM. Você também pode definir funções personalizadas.

Trabalhando com funções REST do ONTAP

Existem diversas considerações a serem feitas ao usar as funções REST do ONTAP incluídas nas ONTAP tools for VMware vSphere 10.

Mapeamento de funções

Seja usando uma função tradicional ou REST, todas as decisões de acesso do ONTAP são tomadas com base no comando CLI subjacente. Mas, como os privilégios em uma função REST são definidos em termos dos endpoints da API REST, o ONTAP precisa criar uma função tradicional mapeada para cada uma das funções REST. Portanto, cada função REST é mapeada para uma função tradicional subjacente. Isso permite que o ONTAP tome decisões de controle de acesso de forma consistente, independentemente do tipo de função. Você não pode modificar as funções mapeadas paralelamente.

Definindo uma função REST usando privilégios da CLI

Como ONTAP sempre usa os comandos da CLI para determinar o acesso em um nível básico, é possível expressar uma função REST usando privilégios de comando da CLI em vez de endpoints REST. Um dos benefícios dessa abordagem é a granularidade adicional disponível com as funções tradicionais.

Interface administrativa ao definir funções do ONTAP

Você pode criar usuários e funções com a CLI do ONTAP e a API REST. No entanto, é mais conveniente usar a interface do System Manager juntamente com o arquivo JSON disponível no ONTAP tools Manager. Veja "Use o RBAC do ONTAP com as ONTAP tools for VMware vSphere 10" para mais informações.

Considerações sobre RBAC do ONTAP para ONTAP tools

Existem vários aspectos da implementação do RBAC das ONTAP tools for VMware vSphere 10 com ONTAP que você deve considerar antes de usá-la em um ambiente de produção.

Visão geral do processo de configuração

ONTAP tools for VMware vSphere inclui suporte para criar um usuário ONTAP com uma função personalizada. As definições são fornecidas em um arquivo JSON que você pode carregar no cluster ONTAP. Você pode criar o usuário e adaptar a função para seu ambiente e necessidades de segurança.

As principais etapas de configuração são descritas em alto nível abaixo. Consulte "Configurar funções e privilégios de usuário do ONTAP" para mais detalhes.

1. Preparar

Você precisa ter credenciais administrativas tanto para o ONTAP tools Manager quanto para o ONTAP cluster.

2. Baixe o arquivo de definição JSON

Após fazer login na interface de usuário do ONTAP tools Manager, você pode baixar o arquivo JSON contendo as definições de RBAC.

3. Crie um usuário ONTAP com uma função

Após iniciar sessão no System Manager, você pode criar o usuário e a função:

1. Selecione **Cluster** à esquerda e depois **Settings**.

2. Desça até **Usuários e funções** e clique −→.
3. Selecione **Adicionar** em **Usuários** e selecione **Virtualization products**.
4. Selecione o arquivo JSON em sua estação de trabalho local e faça o upload.

4. Configure a função

Como parte da definição da função, você precisa tomar diversas decisões administrativas. Veja Configure a função usando System Manager para mais detalhes.

Configure a função usando System Manager

Após começar a criar um novo usuário e função com System Manager e carregar o arquivo JSON, você pode personalizar a função de acordo com seu ambiente e necessidades.

Configuração principal de usuários e funções

As definições de RBAC são agrupadas em diversas funcionalidades de produto, incluindo combinações de VSC, VASA Provider e SRA. Você deve selecionar o(s) ambiente(s) em que precisa de suporte a RBAC. Por exemplo, se você deseja que as funções suportem a funcionalidade de plug-in remoto, selecione VSC. Você também precisa escolher o nome de usuário e a senha associada.

Privileges

Os privilégios de função são organizados em quatro conjuntos com base no nível de acesso necessário para o armazenamento ONTAP. Os privilégios nos quais as funções se baseiam incluem:

- Descoberta

  Esta função permite adicionar sistemas de armazenamento.

- Criar storage

  Essa função permite que você crie armazenamento. Ela também inclui todos os privilégios associados à função de descoberta.

- Modificar armazenamento

  Essa função permite que você modifique o armazenamento. Ela também inclui todos os privilégios associados às funções de descoberta e criação de armazenamento.

- Destruir armazenamento

  Essa função permite destruir armazenamento. Ela também inclui todos os privilégios associados às funções de descoberta, criação e modificação de armazenamento.

Gere o usuário com uma função

Após selecionar as opções de configuração para o seu ambiente, clique em **Adicionar** e ONTAP cria o usuário e a função. O nome da função gerada é uma concatenação dos seguintes valores:

- Valor de prefixo constante definido no arquivo JSON (por exemplo "OTV_10")
- Funcionalidade do produto que você selecionou
- Lista dos conjuntos de privilégios.

Exemplo

```
OTV_10_VSC_Discovery_Create
```

O novo usuário será adicionado à lista na página 'Usuários e funções'. Observe que os métodos de login de usuário HTTP e ONTAPI são suportados.

Informações sobre direitos autorais

Informações sobre marcas comerciais