Controle de acesso baseado em função

ONTAP tools for VMware vSphere 10

NetApp
November 04, 2025

Índice

Controle de acesso baseado em função . . . 1
- Saiba mais sobre as ONTAP tools for VMware vSphere 10 RBAC . . . 1
  - Componentes RBAC . . . 1
  - Dois ambientes RBAC . . . 2
- RBAC com VMware vSphere . . . 2
  - Ambiente RBAC do vCenter Server com ONTAP tools for VMware vSphere 10 . . . 2
  - Use o vCenter Server RBAC com ONTAP tools for VMware vSphere 10 . . . 4
- RBAC com ONTAP . . . 6
  - Ambiente ONTAP RBAC com ONTAP tools for VMware vSphere 10 . . . 6
  - Use o ONTAP RBAC com ONTAP tools for VMware vSphere 10 . . . 7

Controle de acesso baseado em função

Saiba mais sobre as ONTAP tools for VMware vSphere 10 RBAC

O controle de acesso baseado em função (RBAC) é uma estrutura de segurança para controlar o acesso a recursos dentro de uma organização. O RBAC simplifica a administração definindo 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 erros e simplifica o gerenciamento do controle de acesso em toda a sua organização.

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

Componentes RBAC

Em um nível mais alto, há vários componentes que geralmente são incluídos em cada implementação do RBAC. Esses componentes são vinculados 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 CLI. Cada implementação do RBAC inclui privilégios predefinidos e também pode permitir que os 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 na função. E assim como acontece com os privilégios, as implementações incluem funções predefinidas e geralmente permitem que funções personalizadas sejam criadas.

Objetos

Um *objeto* representa um recurso real ou abstrato identificado dentro do ambiente RBAC. As ações definidas por meio dos privilégios são executadas em ou com os objetos associados. Dependendo da implementação, 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 com um modelo de objeto hierárquico, onde elas podem ser herdadas opcionalmente pelos filhos na hierarquia.

Dois ambientes RBAC

Há dois ambientes RBAC distintos que você precisa considerar ao trabalhar com ONTAP tools for VMware vSphere 10.

Servidor VMware vCenter

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

Cluster ONTAP

As ONTAP tools for VMware vSphere 10 se conectam a um cluster ONTAP por meio da API REST ONTAP para executar operações relacionadas ao armazenamento. O acesso aos recursos de armazenamento é controlado por meio de uma função ONTAP associada ao usuário ONTAP fornecido durante a autenticação. Ver "Ambiente ONTAP RBAC" para maiores informações.

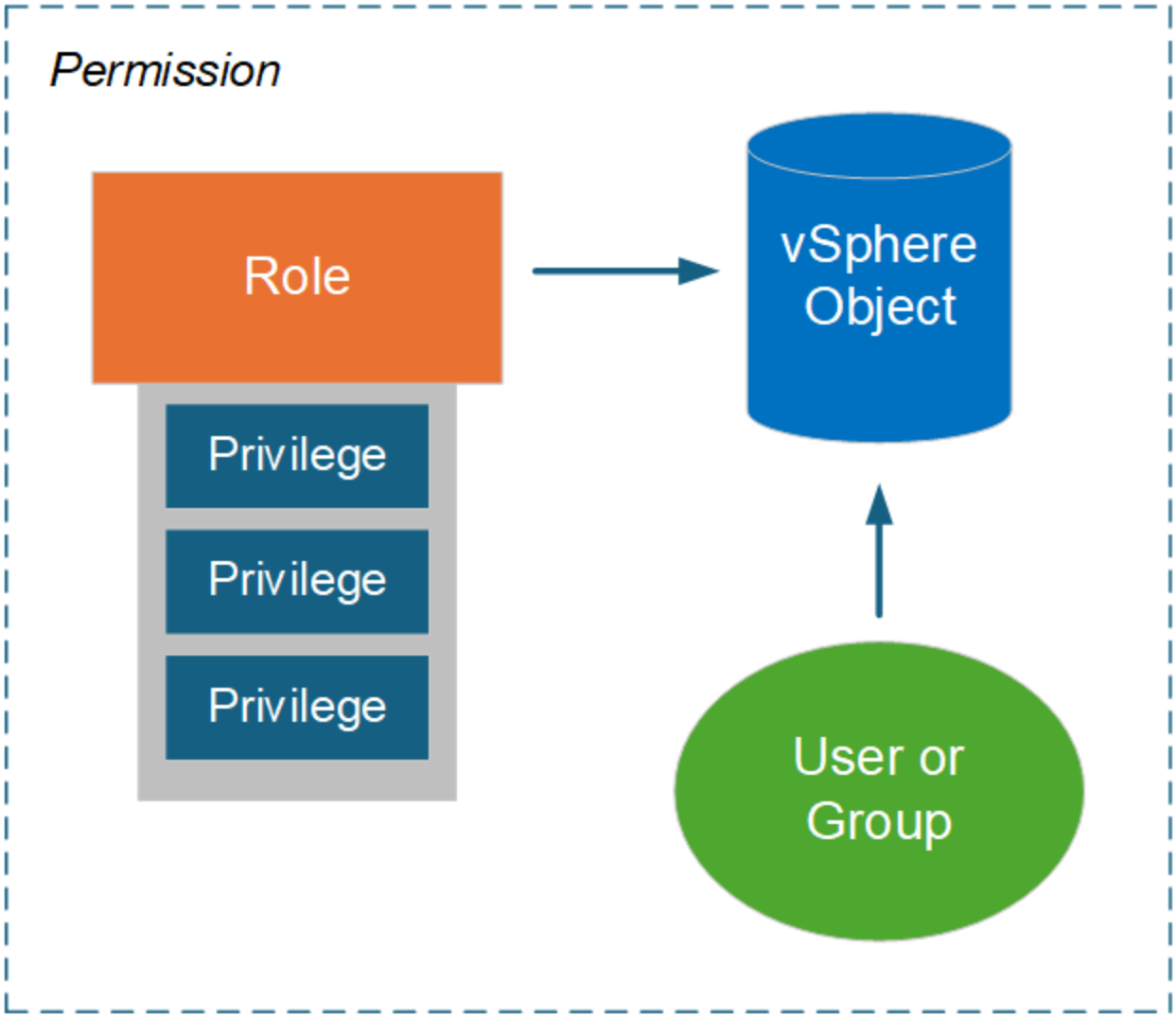
RBAC com VMware vSphere

Ambiente RBAC do vCenter Server com ONTAP tools for VMware vSphere 10

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

Ilustração de uma permissão do vCenter Server

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



Componentes de uma permissão do vCenter Server

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

Objetos vSphere

As permissões são associadas a objetos do vSphere, como o vCenter Server, hosts ESXi, máquinas virtuais, armazenamentos de dados, 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 da pasta raiz do vCenter Server. Ver "Usar RBAC com o servidor vCenter" para maiores informações.

Privileges e funções

Há dois tipos de privilégios do vSphere usados com ONTAP tools for VMware vSphere 10. Para simplificar o trabalho com o RBAC neste ambiente, as ferramentas ONTAP fornecem funções contendo os privilégios nativos e personalizados necessários. Os privilégios incluem:

- Privilégios nativos do vCenter Server

  Esses são os privilégios fornecidos 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 para 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 isoladamente. Em vez disso, usuários e grupos obtêm acesso a um objeto por meio de privilégios de função como parte da permissão mais ampla do vCenter Server.

Use o vCenter Server RBAC com ONTAP tools for VMware vSphere 10

Há vários aspectos das ONTAP tools for VMware vSphere 10 RBAC com o vCenter Server que você deve considerar antes de usá-lo em um ambiente de produção.

Funções do vCenter e a conta de administrador

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

Hierarquia de objetos do vSphere

O inventário de objetos do vSphere é organizado em uma hierarquia. Por exemplo, você pode descer na hierarquia da seguinte maneira:

`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 no host ESXi de destino.

Funções incluídas com ONTAP tools for VMware vSphere 10

Para simplificar o trabalho com o vCenter Server RBAC, as ONTAP tools for VMware vSphere fornecem funções predefinidas adaptadas a diversas tarefas de administração.

> Você pode criar novas funções personalizadas, se necessário. Nesse caso, você deve clonar uma das funções de ferramentas ONTAP existentes e editá-la conforme necessário. Após fazer as alterações de configuração, os usuários do cliente vSphere afetados precisam efetuar logout e login novamente para ativar as alterações.

Para visualizar as ONTAP tools for VMware vSphere , selecione **Menu** na parte superior do vSphere Client e clique em **Administração** e depois em **Funções** à esquerda. Há três funções predefinidas, conforme descrito abaixo.

Ferramentas NetApp ONTAP tools for VMware vSphere Administrator

Fornece todos os privilégios nativos do vCenter Server e privilégios específicos das ferramentas ONTAP necessários para executar as principais ONTAP tools for VMware vSphere .

ONTAP tools for VMware vSphere NetApp ONTAP para VMware vSphere somente leitura

Fornece acesso somente leitura às ferramentas ONTAP . Esses usuários não podem executar nenhuma ONTAP tools for VMware vSphere que sejam controladas por acesso.

ONTAP tools for VMware vSphere NetApp ONTAP para VMware vSphere Provision

Fornece alguns dos privilégios nativos do vCenter Server e privilégios específicos das ferramentas ONTAP necessários para provisionar armazenamento. Você pode executar as seguintes tarefas:

- Criar novos armazenamentos de dados
- Gerenciar armazenamentos de dados

Objetos vSphere e backends de armazenamento ONTAP

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

Trabalhando com o vCenter Server RBAC

Há algumas coisas a considerar ao trabalhar com os privilégios e permissões do vCenter Server.

Privilégios necessários

Para acessar a interface de usuário das ONTAP tools for VMware vSphere 10, você precisa ter o privilégio *View* específico das ferramentas ONTAP . Se você entrar no vSphere sem esse privilégio e clicar no ícone do NetApp , as ONTAP tools for VMware vSphere exibirão uma mensagem de erro e impedirão que você acesse a interface do usuário.

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

Em vez disso, você pode atribuir o privilégio Exibir 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 permissão na hierarquia de objetos do vSphere determina as ONTAP tools for VMware vSphere 10 que 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 se aplicam a objetos personalizados não vSphere, como sistemas de armazenamento. Se possível, você deve atribuir essas permissões às ONTAP tools for VMware vSphere, porque não há nenhum objeto vSphere ao qual você possa atribuí-las. Por

exemplo, qualquer permissão que inclua um privilégio "Adicionar/Modificar/Remover sistemas de armazenamento" das ONTAP tools for VMware vSphere deve ser atribuída no nível do objeto raiz.

Ao definir uma permissão em um nível mais alto na hierarquia de objetos, você pode configurar a permissão para que ela seja passada e herdada pelos objetos filho. 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 qualquer privilégio dentro de uma permissão, os usuários associados à permissão precisarão sair do vSphere e efetuar login novamente para habilitar a alteração.

RBAC com ONTAP

Ambiente ONTAP RBAC com ONTAP tools for VMware vSphere 10

ONTAP fornece 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 CLI. É útil estar familiarizado com o ambiente antes de usá-lo com uma implantação de ONTAP tools for VMware vSphere 10.

Visão geral das opções administrativas

Há várias opções disponíveis ao usar o ONTAP RBAC, dependendo do seu ambiente e objetivos. Uma visão geral das principais decisões administrativas é apresentada abaixo. Veja também "Automação ONTAP : Visão geral da segurança RBAC" para mais informações.

> ⓘ O ONTAP RBAC é adaptado para um ambiente de armazenamento e é mais simples do que a implementação do RBAC fornecida com o vCenter Server. Com o ONTAP, você atribui uma função diretamente ao usuário. Não é necessário configurar permissões explícitas, como aquelas usadas com o vCenter Server, com o ONTAP RBAC.

Tipos de funções e privilégios

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

- DESCANSAR

  As funções REST foram introduzidas com o 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 pontos de extremidade da API REST do ONTAP e às ações associadas.

- Tradicional

  Estas são as funções legadas incluídas antes do ONTAP 9.6. Eles 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 têm algumas vantagens. Por exemplo, parâmetros de consulta adicionais podem ser incluídos opcionalmente para que os privilégios definam com mais precisão os objetos aos quais são aplicados.

Escopo

As funções do ONTAP podem ser definidas com um de dois escopos diferentes. Eles podem ser aplicados a

um SVM de dados específico (nível SVM) ou a todo o cluster ONTAP (nível de cluster).

Definições de funções

O ONTAP fornece um conjunto de funções predefinidas no nível do cluster e do SVM. Você também pode definir funções personalizadas.

Trabalhando com funções REST do ONTAP

Há várias considerações 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 ONTAP são tomadas com base no comando CLI subjacente. Mas como os privilégios em uma função REST são definidos em termos dos pontos de extremidade 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 maneira consistente, independentemente do tipo de função. Você não pode modificar as funções mapeadas paralelamente.

Definindo uma função REST usando privilégios CLI

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

Interface administrativa ao definir funções ONTAP

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

Use o ONTAP RBAC com ONTAP tools for VMware vSphere 10

Há vários aspectos das ONTAP tools for VMware vSphere 10 RBAC com ONTAP que você deve considerar antes de usá-lo em um ambiente de produção.

Visão geral do processo de configuração

As ONTAP tools for VMware vSphere 10 incluem suporte para criar um usuário ONTAP com uma função personalizada. As definições são empacotadas em um arquivo JSON que você pode carregar no cluster ONTAP . Você pode criar o usuário e adaptar a função ao seu ambiente e às suas necessidades de segurança.

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

1. Preparar

Você precisa ter credenciais administrativas para o Gerenciador de ferramentas ONTAP e o cluster ONTAP .

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 do RBAC.

3. Crie um usuário ONTAP com uma função

Após efetuar login no Gerenciador do Sistema, você pode criar o usuário e a função:

1. Selecione **Cluster** à esquerda e depois **Configurações**.
2. Role para baixo até **Usuários e funções** e clique em −→ .
3. Selecione **Adicionar** em **Usuários** e selecione **Produtos de virtualização**.
4. Selecione o arquivo JSON na sua estação de trabalho local e carregue-o.

4. Configurar a função

Como parte da definição da função, você precisa tomar diversas decisões administrativas. VerConfigurar a função usando o Gerenciador de Sistema para mais detalhes.

Configurar a função usando o Gerenciador de Sistema

Depois de começar a criar um novo usuário e função com o System Manager e carregar o arquivo JSON, você pode personalizar a função com base no seu ambiente e necessidades.

Configuração de usuário e função principais

As definições do RBAC são agrupadas como vários recursos de produto, incluindo combinações de VSC, VASA Provider e SRA. Você deve selecionar o ambiente ou ambientes onde precisa de suporte RBAC. Por exemplo, se você quiser que as funções suportem o recurso 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 ao armazenamento ONTAP . Os privilégios nos quais as funções são baseadas incluem:

- Descoberta

  Esta função permite que você adicione sistemas de armazenamento.

- Criar armazenamento

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

- Modificar armazenamento

  Esta função permite que você modifique o armazenamento. Ele também inclui todos os privilégios associados à descoberta e criação de funções de armazenamento.

- Destruir armazenamento

  Esta função permite que você destrua o armazenamento. Ele também inclui todos os privilégios associados à descoberta, criação de armazenamento e modificação de funções de armazenamento.

Gerar o usuário com uma função

Depois de selecionar as opções de configuração para seu ambiente, clique em **Adicionar** e o ONTAP criará 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")
- Capacidade 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