Controle de acesso baseado em função

ONTAP tools for VMware vSphere 10

NetApp
August 25, 2025

Índice

Controle de acesso baseado em função

Saiba mais sobre as ferramentas do ONTAP para 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 organização.

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

Componentes RBAC

Em alto nível, existem vários componentes que geralmente são incluídos em cada implementação do RBAC. Estes componentes estão ligados de diferentes formas 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

Um *role* é um contentor que inclui um ou mais Privileges. As funções são geralmente definidas com base em tarefas específicas ou funções de trabalho. Quando uma função é atribuída a um usuário, o usuário recebe todos os Privileges contidos na função. E, como acontece com o Privileges, as implementações incluem funções pré-definidas e geralmente permitem que funções personalizadas sejam criadas.

Objetos

Um *objeto* representa um recurso real ou abstrato identificado no ambiente RBAC. As ações definidas através do Privileges são executadas em ou com os objetos associados. Dependendo da implementação, o Privileges pode ser concedido a um tipo de objeto ou a uma instância de objeto específica.

Usuários e grupos

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

Permissões

A *permission* é uma definição que liga um usuário ou grupo junto com uma função a um objeto. As permissões podem ser úteis com um modelo de objeto hierárquico onde podem ser herdadas opcionalmente pelos filhos na hierarquia.

Dois ambientes RBAC

Há dois ambientes RBAC distintos que você precisa considerar ao trabalhar com as ferramentas do ONTAP para VMware vSphere 10.

VMware vCenter Server

A implementação 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 ferramentas do ONTAP para VMware vSphere 10, o ambiente RBAC é estendido para incluir objetos adicionais que representam os recursos das ferramentas do ONTAP. O acesso a esses objetos é fornecido através do plug-in remoto. Consulte "Ambiente RBAC do vCenter Server" para obter mais informações.

Cluster DE ONTAP

As ferramentas do ONTAP para VMware vSphere 10 se conectam a um cluster do 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 do ONTAP fornecida durante a autenticação. Consulte "Ambiente RBAC do ONTAP" para obter mais informações.

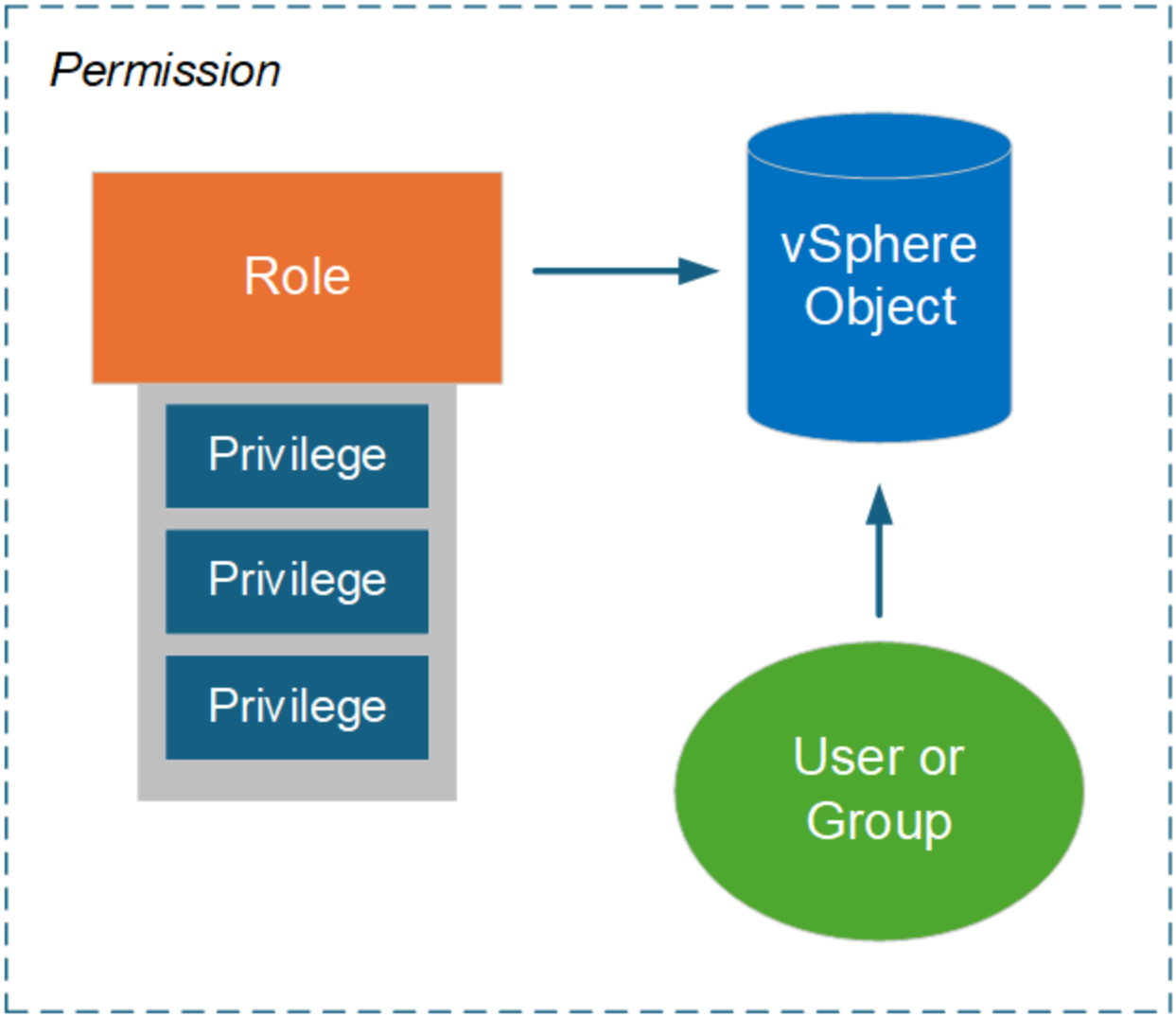
RBAC com VMware vSphere

Ambiente RBAC do vCenter Server com ferramentas do ONTAP para VMware vSphere 10

O VMware vCenter Server fornece um recurso RBAC que permite controlar o acesso a objetos 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 com a 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 vSphere, como 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 ferramentas do ONTAP para VMware vSphere, todas as permissões são atribuídas e validadas no nível da pasta raiz ou raiz do vCenter Server. Consulte "Use o RBAC com o vCenter Server" para obter mais informações.

Privileges e funções

Há dois tipos de vSphere Privileges usados com as ferramentas do ONTAP para VMware vSphere 10. Para simplificar o trabalho com o RBAC nesse ambiente, as ferramentas do ONTAP fornecem funções que contêm o Privileges personalizado e nativo necessário. Os Privileges incluem:

- Privileges nativo do vCenter Server

  Estes são os Privileges fornecidos pelo vCenter Server.

- Privileges específico de ferramentas do ONTAP

  Esses são Privileges personalizados exclusivos das ferramentas do ONTAP para 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 RBAC do vCenter Server com as ferramentas do ONTAP para VMware vSphere 10

Há vários aspetos das ferramentas do ONTAP para a implementação do RBAC do VMware vSphere 10 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 vSphere e às tarefas administrativas associadas. Se limitar o acesso não for necessário, você poderá 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 ferramentas do ONTAP para o VMware vSphere 10.

Hierarquia de objetos do vSphere

O inventário de objetos do vSphere é organizado em uma hierarquia. Por exemplo, você pode mover para baixo a hierarquia da seguinte forma:

`vCenter Server --> Datacenter --> Cluster --> Virtual Machine> ESXi host`

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

Funções incluídas nas ferramentas do ONTAP para VMware vSphere 10

Para simplificar o trabalho com o vCenter Server RBAC, as ferramentas do ONTAP para VMware vSphere fornecem funções predefinidas adaptadas a várias tarefas de administração.

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

Para exibir as ferramentas do ONTAP para as funções do VMware vSphere, selecione **Menu** na parte superior

do vSphere Client e clique em **Administration** e depois em **Roles** à esquerda. Existem três funções predefinidas, conforme descrito abaixo.

Ferramentas do NetApp ONTAP para o administrador do VMware vSphere

Fornece todas as ferramentas nativas do vCenter Server Privileges e do ONTAP específicas Privileges necessárias para executar as principais ferramentas do ONTAP para tarefas de administrador do VMware vSphere.

Ferramentas do NetApp ONTAP para VMware vSphere somente leitura

Fornece acesso somente leitura às ferramentas do ONTAP. Esses usuários não podem executar nenhuma ferramenta do ONTAP para ações do VMware vSphere controladas por acesso.

Ferramentas do NetApp ONTAP para o provisionamento do VMware vSphere

Fornece algumas das Privileges nativas específicas das ferramentas do vCenter Server Privileges e do ONTAP necessárias para provisionar o storage. Você pode executar as seguintes tarefas:

- Crie novos datastores
- Gerenciar armazenamentos de dados

Back-ends de armazenamento de objetos vSphere e ONTAP

Os dois ambientes RBAC funcionam em conjunto. Ao executar uma tarefa na interface do cliente vSphere, as funções de ferramentas do ONTAP definidas para o vCenter Server são verificadas primeiro. Se a operação for permitida pelo vSphere, o ONTAP Role Privileges será examinado. Esta segunda etapa é executada com base na função ONTAP atribuída ao usuário quando o back-end de storage foi criado e configurado.

Trabalhando com o vCenter Server RBAC

Há algumas coisas a considerar ao trabalhar com o vCenter Server Privileges e as permissões.

Privileges necessário

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

O nível de atribuição na hierarquia de objetos vSphere determina quais partes da interface de usuário você pode acessar. A atribuição do privilégio Exibir ao objeto raiz permite que você acesse as ferramentas do ONTAP para 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 as ferramentas do ONTAP para os menus do VMware vSphere que você pode acessar e usar.

Atribuindo permissões

Você precisa usar as permissões do vCenter Server se quiser limitar o acesso aos objetos e tarefas do vSphere. Quando você atribui permissão na hierarquia de objetos do vSphere determina as ferramentas do ONTAP para 10 as tarefas 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 as ferramentas do ONTAP para VMware vSphere 10 se aplicam a objetos personalizados que não sejam do vSphere, como sistemas de storage. Se possível, você deve atribuir essas permissões a ferramentas do ONTAP para o objeto raiz do VMware vSphere porque não há nenhum objeto vSphere ao qual você possa atribuí-lo. Por exemplo, qualquer permissão que inclua um privilégio "Adicionar/Modificar/Remover sistemas de armazenamento" do ONTAP 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 filho que substituem as permissões herdadas do pai.

Você pode modificar uma permissão a qualquer momento. Se você alterar qualquer um dos Privileges dentro de uma permissão, os usuários associados à permissão precisarão fazer logout do vSphere e fazer login novamente para ativar a alteração.

RBAC com ONTAP

Ambiente RBAC do ONTAP com ferramentas ONTAP para VMware vSphere 10

O ONTAP fornece um ambiente RBAC robusto e extensível. Use a funcionalidade RBAC para controlar o acesso ao storage e às operações do sistema conforme exposto pela API REST e CLI. É útil estar familiarizado com o ambiente antes de usá-lo com as ferramentas do ONTAP para a implantação do VMware vSphere 10.

Visão geral das opções administrativas

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

> ⓘ O ONTAP RBAC é personalizado para um ambiente de storage 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. A configuração de permissões explícitas, como as usadas com o vCenter Server, não é necessária com o RBAC do ONTAP.

Tipos de papéis e Privileges

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

- DESCANSO

  As funções REST foram introduzidas com o ONTAP 9.6 e geralmente são aplicadas aos usuários que acessam o ONTAP por meio da API REST. Os Privileges incluídos nessas funções são definidos em termos de acesso aos endpoints da API REST do ONTAP e às ações associadas.

- Tradicional

  Estas são as funções herdadas incluídas antes do ONTAP 9.6. Eles continuam sendo um aspeto fundamental da RBAC. Os Privileges são definidos em termos de acesso aos comandos da CLI do ONTAP.

Embora os papéis RESTANTES tenham sido introduzidos mais recentemente, os papéis tradicionais têm algumas vantagens. Por exemplo, parâmetros de consulta adicionais podem ser opcionalmente incluídos para

que o Privileges defina com mais precisão os objetos aos quais são aplicados.

Âmbito de aplicação

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

Definições de função

O ONTAP fornece um conjunto de funções pré-definidas no nível do cluster e da SVM. Você também pode definir funções personalizadas.

Trabalhando com as funções REST do ONTAP

Há várias considerações ao usar as funções REST do ONTAP incluídas nas ferramentas do ONTAP para VMware vSphere 10.

Mapeamento de funções

Seja usando uma função tradicional ou REST, todas as decisões de acesso ao ONTAP são tomadas com base no comando CLI subjacente. Mas como os Privileges 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 mapeia para um papel tradicional subjacente. Isso permite que o ONTAP tome decisões de controle de acesso de forma consistente, independentemente do tipo de função. Não é possível modificar as funções mapeadas paralelas.

Definindo uma FUNÇÃO REST usando CLI Privileges

Como o ONTAP sempre usa os comandos CLI para determinar o acesso em um nível básico, é possível expressar uma FUNÇÃO REST usando o comando CLI Privileges 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 e a API REST do ONTAP. No entanto, é mais conveniente usar a interface do Gerenciador do sistema juntamente com o arquivo JSON disponível através do Gerenciador de ferramentas do ONTAP. Consulte "Use o RBAC do ONTAP com as ferramentas do ONTAP para VMware vSphere 10" para obter mais informações.

Use o RBAC do ONTAP com as ferramentas do ONTAP para VMware vSphere 10

Há vários aspectos das ferramentas do ONTAP para a implementação do RBAC do VMware vSphere 10 com o ONTAP que você deve considerar antes de usá-lo em um ambiente de produção.

Visão geral do processo de configuração

As ferramentas do ONTAP para VMware vSphere 10 incluem suporte para criar um usuário do ONTAP com uma função personalizada. As definições são empacotadas em um arquivo JSON que você pode carregar para o cluster ONTAP. Você pode criar o usuário e adaptar a função para suas necessidades de ambiente e segurança.

Os principais passos de configuração são descritos em um nível alto abaixo. "Configurar as funções de usuário do ONTAP e o Privileges"Consulte para obter mais detalhes.

1. Prepare-se

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

ONTAP.

2. Baixe o arquivo de definição JSON

Depois de fazer login na interface de usuário do Gerenciador de ferramentas do ONTAP, você pode baixar o arquivo JSON contendo as definições RBAC.

3. Crie um usuário do ONTAP com uma função

Depois de iniciar sessão no System Manager, pode criar o utilizador e a função:

1. Selecione **Cluster** à esquerda e, em seguida, **Settings**.
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 em sua estação de trabalho local e carregue-o.

4. Configure a função

Como parte da definição do papel, você precisa tomar várias decisões administrativas. Configure a função usando o System ManagerConsulte para obter mais detalhes.

Configure a função usando o System Manager

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

Configuração principal do usuário e da função

As definições RBAC são empacotadas como várias capacidades de produto, incluindo combinações de VSC, VSA Provider e SRA. Você deve selecionar o ambiente ou os ambientes em que precisa de suporte a 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

As Privileges de função são organizadas em quatro conjuntos com base no nível de acesso necessário ao storage ONTAP. Os Privileges em que as funções são baseadas incluem:

- Detecção

  Essa função permite adicionar sistemas de storage.

- Crie armazenamento

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

- Modificar o armazenamento

  Essa função permite modificar o armazenamento. Ele também inclui todos os Privileges associados à descoberta e criação de funções de storage.

- Destrua o armazenamento

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

Gere o usuário com uma função

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