RBAC com VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
November 17, 2025

Índice

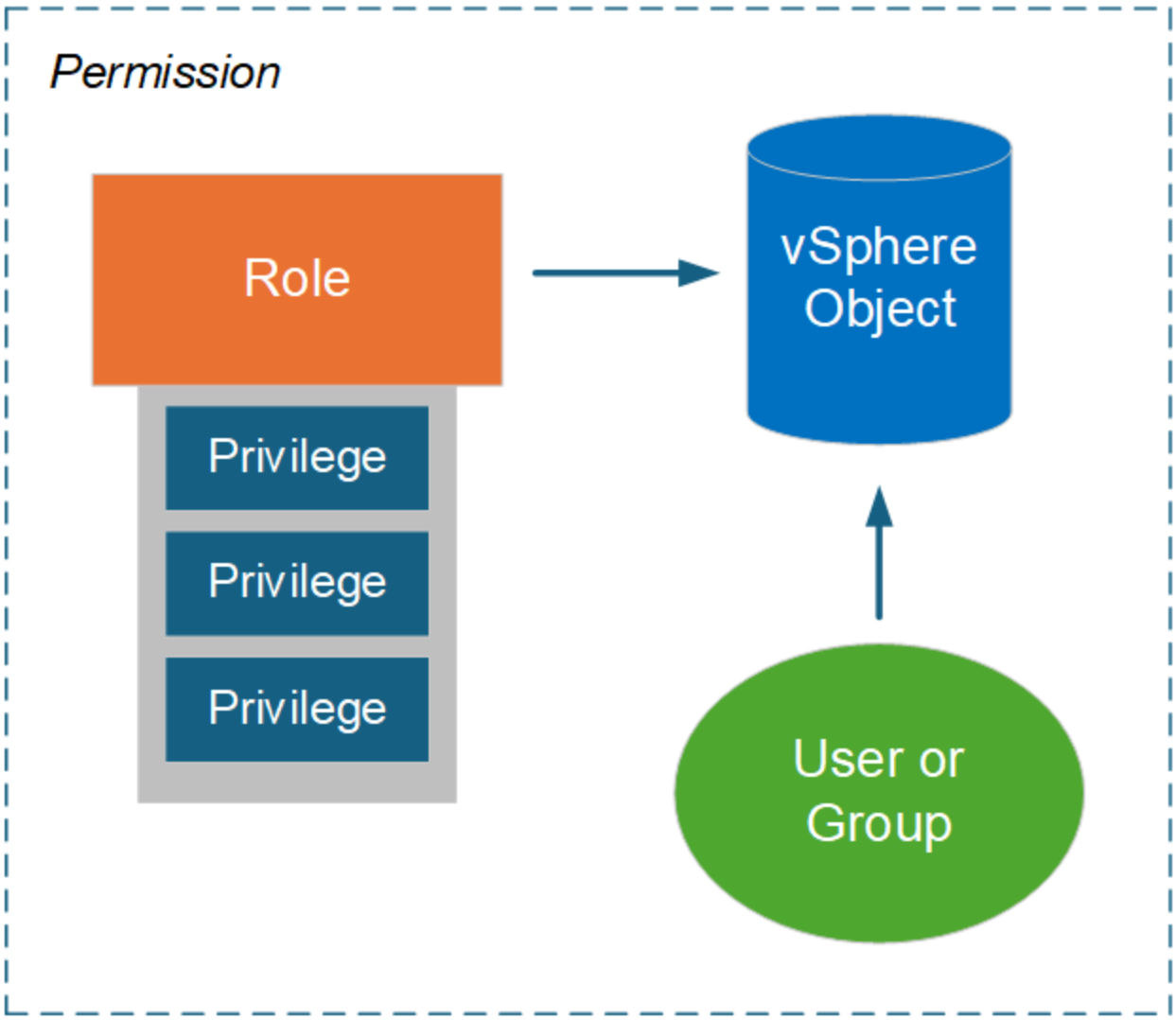
RBAC com VMware vSphere

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 ative 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 no Privileges na 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 do Role Privileges como parte da permissão maior 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.

Informações sobre direitos autorais

Informações sobre marcas comerciais