Controle de acesso baseado em função

ONTAP tools for VMware vSphere 10

NetApp
September 30, 2025

Índice

Controle de acesso baseado em função

Visão geral do controle de acesso baseado em funções nas ferramentas do ONTAP para VMware vSphere

O vCenter Server fornece controle de acesso baseado em função (RBAC) que permite controlar o acesso a objetos vSphere. O vCenter Server fornece serviços de autenticação e autorização centralizados em vários níveis diferentes em seu inventário, usando direitos de usuário e grupo com funções e Privileges. O vCenter Server possui cinco componentes principais para gerenciar o RBAC:

Componentes	Descrição
Privileges	Um privilégio habilita ou nega o acesso para executar ações no vSphere.
Funções	Uma função contém um ou mais Privileges do sistema onde cada privilégio define um direito administrativo a um determinado objeto ou tipo de objeto no sistema. Ao atribuir uma função a um usuário, o usuário herda os recursos do Privileges definidos nessa função.
Usuários e grupos	Usuários e grupos são usados em permissões para atribuir funções do ative Directory (AD). O vCenter Server tem seus próprios usuários e grupos locais que você pode usar.
Permissões	As permissões permitem que você atribua o Privileges a usuários ou grupos para executar determinadas ações e fazer alterações em objetos dentro do vCenter Server. As permissões do vCenter Server afetam apenas os usuários que fazem login no vCenter Server em vez de usuários que fazem login em um host ESXi diretamente.
Objeto	Uma entidade na qual as ações são executadas. Os objetos do VMware vCenter são data centers, pastas, pools de recursos, clusters, hosts e VMs

Para concluir uma tarefa com êxito, você deve ter as funções RBAC apropriadas do vCenter Server. Durante uma tarefa, as ferramentas do ONTAP para VMware vSphere verificam as funções do vCenter Server de um usuário antes de verificar o ONTAP Privileges do usuário.

As funções do vCenter Server se aplicam às ferramentas do ONTAP para usuários do VMware vSphere vCenter, não aos administradores. Por padrão, os administradores têm acesso total ao produto e não exigem funções atribuídas a eles.

Os usuários e grupos obtêm acesso a uma função fazendo parte de uma função do vCenter Server.

Pontos-chave sobre a atribuição e modificação de funções para o vCenter Server

Você só precisa configurar as funções do vCenter Server se quiser limitar o acesso a objetos e tarefas do vSphere. Caso contrário, você pode fazer login como administrador. Esse login permite que você acesse automaticamente todos os objetos do vSphere.

A atribuição de uma função determina as ferramentas do ONTAP para tarefas do VMware vSphere que um usuário pode executar. Você pode modificar uma função a qualquer momento. Se você alterar o Privileges em uma função, o usuário associado a essa função deve fazer logout e fazer login novamente para ativar a função atualizada.

Funções padrão empacotadas com as ferramentas do ONTAP para VMware vSphere

Para simplificar o trabalho com o vCenter Server Privileges e o RBAC, as ferramentas do ONTAP para VMware vSphere fornecem ferramentas ONTAP padrão para funções do VMware vSphere que permitem que você execute as principais ferramentas do ONTAP para tarefas do VMware vSphere. Há também uma função somente leitura que permite visualizar as informações, mas não executar nenhuma tarefa.

Você pode visualizar as ferramentas do ONTAP para as funções padrão do VMware vSphere clicando em **Roles** na página inicial do vSphere Client. As funções que as ferramentas do ONTAP para VMware vSphere fornecem permitem que você execute as seguintes tarefas:

Função	Descrição
Ferramentas do NetApp ONTAP para o administrador do VMware vSphere	Fornece todas as Privileges nativas específicas das ferramentas do vCenter Server Privileges e do ONTAP necessárias para executar algumas das ferramentas do ONTAP para tarefas 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

A função de administrador do Gerenciador de ferramentas do ONTAP não está registrada no vCenter Server. Essa função é específica do Gerenciador de ferramentas do ONTAP.

Se a sua empresa exigir que você implemente funções mais restritivas do que as ferramentas padrão do ONTAP para as funções do VMware vSphere, você poderá usar as ferramentas do ONTAP para as funções do VMware vSphere para criar novas funções.

Nesse caso, você clonaria as ferramentas do ONTAP necessárias para as funções do VMware vSphere e editaria a função clonada para que ela tenha apenas o Privileges de que seu usuário precisa.

Permissões para backends de armazenamento do ONTAP e objetos vSphere

Se a permissão do vCenter Server for suficiente, as ferramentas do ONTAP para VMware vSphere verificarão o ONTAP RBAC Privileges (sua função ONTAP) associados às credenciais de back-ends de storage (o nome de usuário e a senha) para determinar se você tem Privileges suficientes para executar as operações de storage exigidas por essas ferramentas do ONTAP para a tarefa do VMware vSphere nesse back-end de storage. Se você tiver o ONTAP Privileges correto, poderá acessar os backends de armazenamento e executar as ferramentas do ONTAP para as tarefas do VMware vSphere. As funções do ONTAP determinam as ferramentas do ONTAP para tarefas do VMware vSphere que podem ser executadas no back-end de storage.

Componentes das permissões do vCenter Server

O vCenter Server reconhece permissões, não o Privileges. Cada permissão do vCenter Server consiste em três componentes.

O vCenter Server tem os seguintes componentes:

- Um ou mais Privileges (o papel)

  O Privileges define as tarefas que um usuário pode executar.

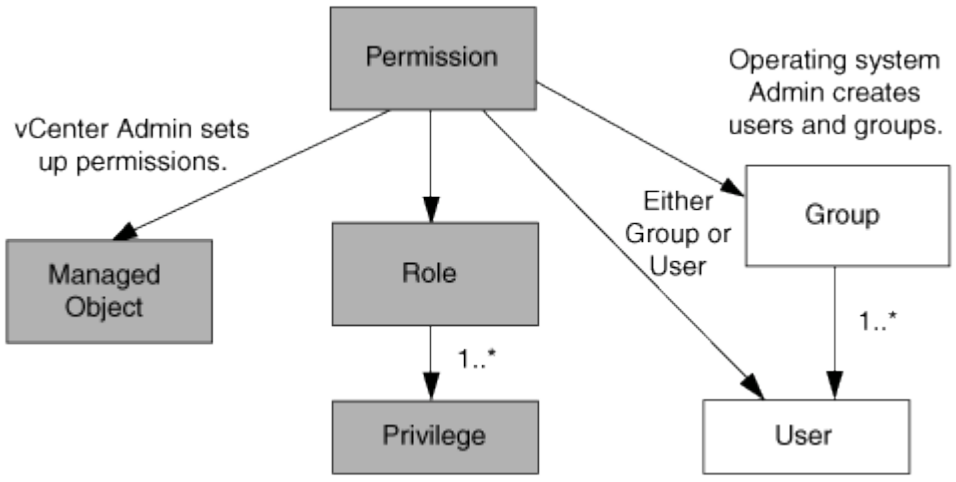
- Um objeto vSphere

  O objeto é o alvo para as tarefas.

- Um usuário ou grupo

  O usuário ou grupo define quem pode executar a tarefa.

Neste diagrama, as caixas cinza indicam os componentes que existem no vCenter Server e as caixas brancas indicam os componentes que existem no sistema operacional em que o vCenter Server está sendo executado.



Privileges

Dois tipos de Privileges estão associados às ferramentas do ONTAP para VMware vSphere:

- Privileges nativo do vCenter Server

  Esses Privileges vêm com o vCenter Server.

- Privileges específico de ferramentas do ONTAP

  Esses Privileges são definidos para ferramentas específicas do ONTAP para tarefas do VMware vSphere. Eles são exclusivos das ferramentas do ONTAP para VMware vSphere.

As ferramentas do ONTAP para as tarefas do VMware vSphere exigem o Privileges específico das ferramentas do ONTAP e o Privileges nativo do vCenter Server. Estes Privileges constituem o "papel" para o usuário. Uma permissão pode ter vários Privileges. Esses Privileges são para um usuário conetado ao vCenter Server.

> Para simplificar o trabalho com o vCenter Server RBAC, as ferramentas do ONTAP para VMware vSphere fornecem várias funções padrão que contêm todas as Privileges nativas e específicas de ferramentas do ONTAP necessárias para executar ferramentas do ONTAP para tarefas do VMware vSphere.

Se você alterar o Privileges dentro de uma permissão, o usuário que está associado a essa permissão deve fazer logout e, em seguida, fazer login para ativar a permissão atualizada.

Objetos vSphere

As permissões são associadas a objetos vSphere, como vCenter Server, hosts ESXi, máquinas virtuais, datastores, data centers e pastas. Você pode atribuir permissões a qualquer objeto vSphere. Com base na permissão atribuída a um objeto vSphere, o vCenter Server determina quem pode executar quais tarefas nesse objeto. Para as ferramentas do ONTAP para tarefas específicas do VMware vSphere, as permissões são atribuídas e validadas somente no nível da pasta raiz (vCenter Server) e não em nenhuma outra entidade. Exceto para a operação de plug-in VAAI, onde as permissões são validadas para o host ESXi em questão.

Usuários e grupos

Você pode usar o ative Directory (ou a máquina local do vCenter Server) para configurar usuários e grupos de usuários. Em seguida, você pode usar as permissões do vCenter Server para conceder acesso a esses usuários ou grupos para permitir que eles executem ferramentas específicas do ONTAP para tarefas do VMware vSphere.

> Essas permissões do vCenter Server se aplicam às ferramentas do ONTAP para usuários do VMware vSphere vCenter, e não às ferramentas do ONTAP para administradores do VMware vSphere. Por padrão, as ferramentas do ONTAP para administradores do VMware vSphere têm acesso total ao produto e não exigem permissões atribuídas a eles.

Usuários e grupos não têm funções atribuídas a eles. Eles obtêm acesso a uma função fazendo parte de uma permissão do vCenter Server.

Atribuir e modificar permissões para o vCenter Server

Há vários pontos-chave a ter em mente quando você está trabalhando com permissões do vCenter Server. Se uma tarefa do ONTAP Tools for bem-sucedida pode depender de onde você atribuiu uma permissão ou quais ações um usuário realizou após uma

permissão ser modificada.

Atribuindo permissões

Você só precisa configurar permissões do vCenter Server se quiser limitar o acesso a objetos e tarefas do vSphere. Caso contrário, você pode fazer login como administrador. Esse login permite que você acesse automaticamente todos os objetos do vSphere.

O local onde você atribui permissão determina as ferramentas do ONTAP para tarefas do VMware vSphere que um usuário pode executar.

Às vezes, para garantir a conclusão de uma tarefa, você deve atribuir permissão em um nível mais alto, como o objeto raiz. Esse é o caso quando uma tarefa requer um privilégio que não se aplica a um objeto vSphere específico (por exemplo, rastrear a tarefa) ou quando um privilégio necessário se aplica a um objeto que não seja vSphere (por exemplo, um sistema de armazenamento).

Nesses casos, você pode configurar uma permissão para que ela seja herdada pelas entidades filhos. Você também pode atribuir outras permissões às entidades filho. A permissão atribuída a uma entidade filho sempre substitui a permissão herdada da entidade pai. Isso significa que você pode conceder permissões a uma entidade filho para restringir o escopo de uma permissão atribuída a um objeto raiz e herdada pela entidade filho.

A menos que as diretivas de segurança da sua empresa exijam permissões mais restritivas, é uma boa prática atribuir permissões ao objeto raiz (também conhecido como pasta raiz).

Permissões e objetos que não sejam do vSphere

A permissão que você cria é aplicada a um objeto não vSphere. Por exemplo, um sistema de armazenamento não é um objeto vSphere. Se um privilégio se aplicar a um sistema de storage, você deve atribuir a permissão que contém esse privilégio às 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, como ferramentas do ONTAP para o privilégio "Adicionar/Modificar/Ignorar sistemas de armazenamento", deve ser atribuída no nível do objeto raiz.

Modificar permissões

Você pode modificar uma permissão a qualquer momento.

Se você alterar o Privileges dentro de uma permissão, o usuário associado a essa permissão deve fazer logout e fazer login novamente para ativar a permissão atualizada.

O Privileges é necessário para as ferramentas do ONTAP para tarefas do VMware vSphere

Diferentes ferramentas do ONTAP para tarefas do VMware vSphere exigem combinações diferentes de Privileges específicas para as ferramentas do ONTAP para VMware vSphere e vCenter Server Privileges nativo.

Para acessar as ferramentas do ONTAP para a GUI do VMware vSphere, você deve ter o privilégio de visualização específico das ferramentas do ONTAP em nível de produto atribuído no nível correto do objeto vSphere. Se você fizer login sem esse privilégio, as ferramentas do ONTAP para VMware vSphere exibirão

uma mensagem de erro ao clicar no ícone NetApp e impedir que você acesse as ferramentas do ONTAP.

No privilégio **Exibir**, você pode acessar as ferramentas do ONTAP para VMware vSphere. Esse privilégio não permite que você execute tarefas nas ferramentas do ONTAP para VMware vSphere. Para executar quaisquer ferramentas do ONTAP para tarefas do VMware vSphere, você deve ter o vCenter Server Privileges nativo e específico de ferramentas do ONTAP correto para essas tarefas.

O nível de atribuição determina quais partes da IU você pode ver. A atribuição do privilégio Exibir ao objeto raiz (pasta) permite que você entre nas ferramentas do ONTAP para VMware vSphere clicando no ícone NetApp.

Você pode atribuir o privilégio Exibir a outro nível de objeto vSphere; no entanto, isso limita as ferramentas do ONTAP para menus do VMware vSphere que você pode ver e usar.

O objeto raiz é o local recomendado para atribuir qualquer permissão que contenha o privilégio Exibir.

Funções recomendadas do ONTAP para ferramentas do ONTAP para VMware vSphere

Você pode configurar várias funções recomendadas do ONTAP para trabalhar com as ferramentas do ONTAP para VMware vSphere e com controle de acesso baseado em funções (RBAC). Essas funções contêm o ONTAP Privileges necessário para executar as operações de storage executadas pelas ferramentas do ONTAP para tarefas do VMware vSphere.

Para criar novas funções de usuário, faça login como administrador dos sistemas de storage que executam o ONTAP. Você pode criar funções do ONTAP usando o Gerenciador de sistema do ONTAP 9.8P1 ou posterior.

Cada função do ONTAP tem um par de nome de usuário e senha associados, que constituem as credenciais da função. Se você não fizer login usando essas credenciais, não poderá acessar as operações de storage associadas à função.

Como medida de segurança, as ferramentas do ONTAP para funções específicas do ONTAP do VMware vSphere são ordenadas hierarquicamente. Isso significa que a primeira função é a mais restritiva e tem apenas o Privileges associado ao conjunto mais básico de ferramentas do ONTAP para operações de storage do VMware vSphere. A próxima função inclui seu próprio Privileges e todos os Privileges associados à função anterior. Cada função adicional é menos restritiva em relação às operações de storage compatíveis.

Veja a seguir algumas das funções de RBAC do ONTAP recomendadas ao usar as ferramentas do ONTAP para VMware vSphere. Depois de criar essas funções, você pode atribuí-las a usuários que precisam executar tarefas relacionadas ao armazenamento, como provisionamento de máquinas virtuais.

Função	Privileges
Detecção	Essa função permite adicionar sistemas de storage.
Crie armazenamento	Essa função permite que você crie armazenamento. Essa função também inclui todos os Privileges associados à função descoberta.

Modificar armazenamento	Essa função permite modificar o armazenamento. Essa função também inclui todos os Privileges associados à função descoberta e à função criar armazenamento.
Destrua o armazenamento	Esta função permite que você destrua o armazenamento. Essa função também inclui todos os Privileges associados à função descoberta, à função criar armazenamento e à função Modificar armazenamento.

Se você estiver usando as ferramentas do ONTAP para VMware vSphere, também deverá configurar uma função de gerenciamento baseado em políticas (PBM). Essa função permite gerenciar o storage usando políticas de storage. Essa função requer que você também configure a função "descoberta".

Informações sobre direitos autorais

Informações sobre marcas comerciais