



RBAC com VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp

November 04, 2025

This PDF was generated from <https://docs.netapp.com/pt-br/ontap-tools-vmware-vsphere-104/concepts/rbac-vcenter-environment.html> on November 04, 2025. Always check docs.netapp.com for the latest.

Índice

- RBAC com VMware vSphere 1
 - Ambiente RBAC do vCenter Server com ONTAP tools for VMware vSphere 10 1
 - Ilustração de uma permissão do vCenter Server 1
 - Componentes de uma permissão do vCenter Server 2
 - Use o vCenter Server RBAC com ONTAP tools for VMware vSphere 10 2
 - Funções do vCenter e a conta de administrador 2
 - Hierarquia de objetos do vSphere 3
 - Funções incluídas com ONTAP tools for VMware vSphere 10 3
 - Objetos vSphere e backends de armazenamento ONTAP 3
 - Trabalhando com o vCenter Server RBAC 3

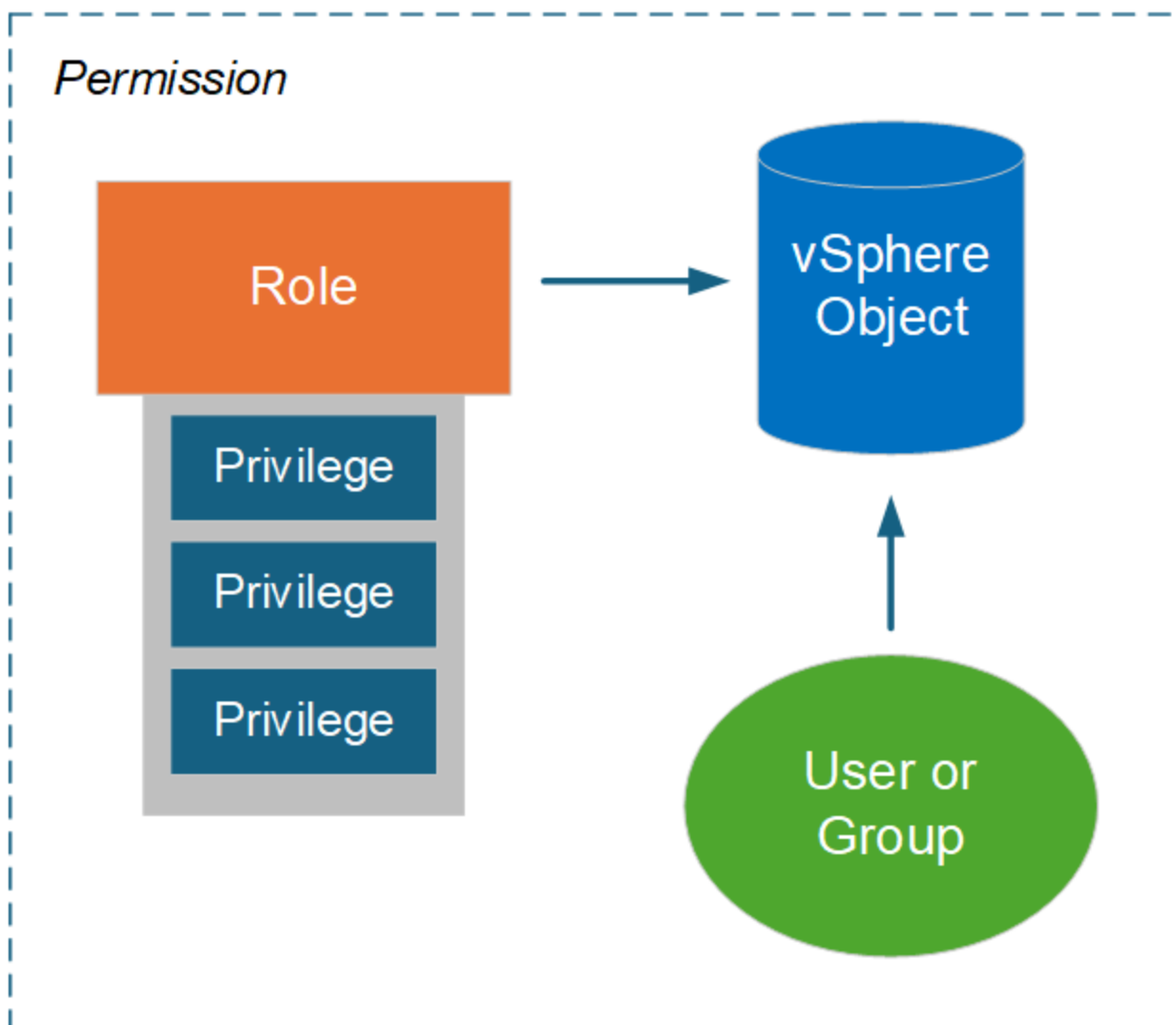
RBAC com VMware vSphere

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.

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSAIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.