Controle de acesso baseado em função

ONTAP tools for VMware vSphere 9.8

NetApp
June 20, 2025

Índice

Controle de acesso baseado em função . . . 1
Visão geral do controle de acesso baseado em funções nas ferramentas do ONTAP . . . 1
Componentes das permissões do vCenter Server . . . 1
Privileges . . . 2
Objetos vSphere . . . 3
Usuários e grupos . . . 3
Principais pontos sobre a atribuição e modificação de permissões para o vCenter Server . . . 3
Atribuindo permissões . . . 3
Permissões e objetos que não sejam do vSphere . . . 4
Modificar permissões . . . 4
Funções padrão incluídas com ferramentas ONTAP . . . 4
Diretrizes para o uso de funções padrão do VSC . . . 5
Privileges necessário para tarefas VSC . . . 5
Privilégio de nível de produto exigido pelas ferramentas do ONTAP para VMware vSphere . . . 6
Permissões para sistemas de armazenamento ONTAP e objetos vSphere . . . 6
Funções recomendadas do ONTAP ao usar as ferramentas do ONTAP para VMware vSphere . . . 8
Como configurar o controle de acesso baseado em função do ONTAP para ferramentas do ONTAP para VMware vSphere . . . 9
Funções do VSC . . . 9
Funções do Fornecedor VASA . . . 10
Funções do SRA . . . 10

Controle de acesso baseado em função

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

O vCenter Server fornece controle de acesso baseado em função (RBAC) que permite controlar o acesso a objetos vSphere. O ONTAP Server RBAC trabalha com o ONTAP RBAC para determinar quais tarefas do VSC um usuário específico pode executar em objetos em um sistema de storage específico.

Para concluir uma tarefa com êxito, você precisa ter as permissões RBAC apropriadas do vCenter Server. Durante uma tarefa, o VSC verifica as permissões do vCenter Server de um usuário antes de verificar o ONTAP Privileges do usuário.

Você pode definir as permissões do vCenter Server no objeto raiz (também conhecido como a pasta raiz). Em seguida, você pode refinar a segurança restringindo entidades filhas que não precisam dessas permissões.

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

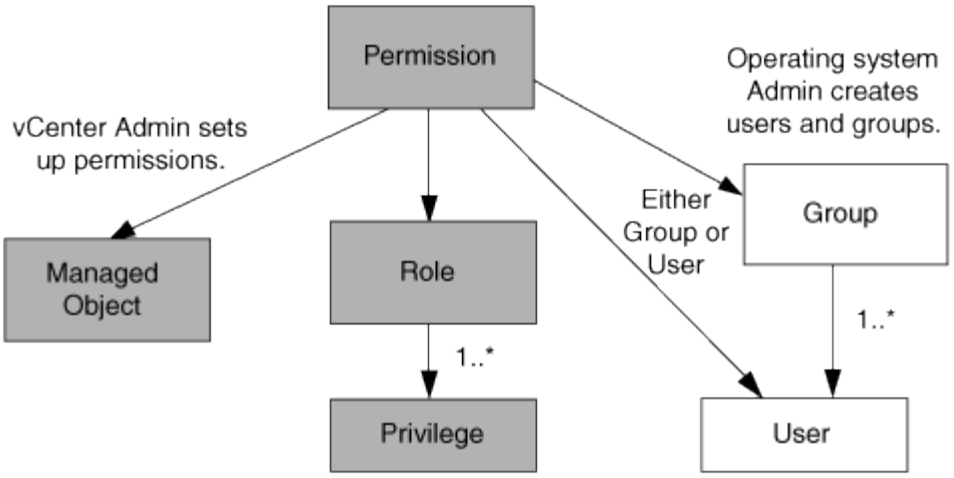
  O objeto é o alvo para as tarefas.

- Um usuário ou grupo

  O usuário ou grupo define quem pode executar a tarefa.

Como o diagrama a seguir ilustra, você deve ter todos os três elementos para ter uma permissão.

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 do VSC

  Esses Privileges são definidos para tarefas específicas do VSC. Eles são exclusivos do VSC.

As tarefas do VSC exigem Privileges específico do VSC e 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, o VSC fornece várias funções padrão que contêm todas as Privileges nativas e específicas do VSC necessárias para executar tarefas do VSC.

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.

Privilégio	Funções	Tarefas
Console de ferramentas do NetApp ONTAP > Exibir	• Administrador do VSC • Provisão de VSC • VSC somente leitura	Todas as tarefas específicas do provedor VSC e VASA requerem o privilégio de exibição.
Consola de armazenamento virtual NetApp > Gestão baseada em políticas > Gestão ou privilege.nvpfVSC.VASAGroup.com.NetApp.nvpf.label > Gestão	Administrador do VSC	Tarefas do fornecedor VSC e VASA relacionadas com perfis de capacidade de armazenamento e definições de limite.

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 tarefas específicas do VSC, as permissões são atribuídas e validadas somente no nível da pasta raiz (vCenter Server) e não em nenhuma outra entidade. Exceto para a operação do plugin VAAI, onde as permissões são validadas em relação ao 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 permissões do vCenter Server para conceder acesso a esses usuários ou grupos para permitir que eles executem tarefas específicas do VSC.

Essas permissões do vCenter Server se aplicam aos usuários do VSC vCenter, não aos administradores do VSC. Por padrão, os administradores do VSC 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.

Principais pontos sobre a atribuição e modificação de 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.

Quando você atribui uma permissão determina as tarefas do VSC que um usuário pode executar.

Às vezes, para garantir a conclusão de uma tarefa, você deve atribuir a 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 permissões para uma entidade filho como uma forma de restringir o escopo de uma permissão que foi 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 que não seja vSphere. Por exemplo, um sistema de armazenamento não é um objeto vSphere. Se um privilégio se aplicar a um sistema de armazenamento, você deve atribuir a permissão que contém esse privilégio ao objeto raiz do VSC porque não há nenhum objeto vSphere ao qual você possa atribuí-lo.

Por exemplo, qualquer permissão que inclua um privilégio como o privilégio VSC "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.

Funções padrão incluídas com ferramentas ONTAP

Para simplificar o trabalho com o vCenter Server Privileges e o controle de acesso baseado em funções (RBAC), o VSC (Virtual Storage Console) fornece funções VSC padrão que permitem executar tarefas importantes do VSC. Há também uma função somente leitura que permite exibir informações do VSC, mas não executar nenhuma tarefa.

As funções padrão do VSC têm o Privileges específico do VSC necessário e o vCenter Server Privileges nativo necessários para que os usuários executem tarefas do VSC. Além disso, as funções são configuradas para que tenham o Privileges necessário em todas as versões com suporte do vCenter Server.

Como administrador, você pode atribuir essas funções aos usuários, conforme necessário.

> Quando você atualiza o VSC para a versão mais recente, as funções padrão são atualizadas automaticamente para funcionar com a nova versão do VSC.

Você pode visualizar as funções padrão do VSC clicando em **Roles** na página inicial do vSphere Client.

As funções que o VSC fornece permitem que você execute as seguintes tarefas:

Função	Descrição
Administrador do VSC	Fornece todas as Privileges nativas do vCenter Server Privileges e do VSC que são necessárias para executar todas as tarefas do VSC.
VSC somente leitura	Fornece acesso somente leitura ao VSC. Esses usuários não podem executar nenhuma ação VSC controlada pelo acesso.

Provisão de VSC	Fornece todo o vCenter Server Privileges nativo e o Privileges específico do VSC necessários para provisionar o storage. Você pode executar as seguintes tarefas: • Crie novos datastores • Destrua armazenamentos de dados • Ver informações sobre perfis de capacidade de armazenamento

Diretrizes para o uso de funções padrão do VSC

Quando você trabalha com ferramentas padrão do ONTAP para funções do VMware vSphere, há certas diretrizes que você deve seguir.

Você não deve modificar diretamente as funções padrão. Se o fizer, o VSC substituirá as alterações sempre que atualizar o VSC. O instalador atualiza as definições de função padrão cada vez que você atualiza o VSC. Isso garante que as funções sejam atuais para sua versão do VSC, bem como para todas as versões com suporte do vCenter Server.

No entanto, você pode usar as funções padrão para criar funções adaptadas ao seu ambiente. Para fazer isso, você deve copiar a função padrão do VSC e, em seguida, editar a função copiada. Ao criar uma nova função, você pode manter essa função mesmo quando você reiniciar ou atualizar o serviço VSC Windows.

Algumas das maneiras pelas quais você pode usar as funções padrão do VSC incluem o seguinte:

- Use as funções VSC padrão para todas as tarefas VSC.

  Nesse cenário, as funções padrão fornecem todas as Privileges que um usuário precisa para executar as tarefas do VSC.

- Combine funções para expandir as tarefas que um usuário pode executar.

  Se as funções padrão do VSC oferecerem muita granularidade para o seu ambiente, você poderá expandir as funções criando grupos de nível mais alto que contenham várias funções.

  Se um usuário precisar executar outras tarefas que não sejam do VSC que exijam o vCenter Server Privileges nativo adicional, você poderá criar uma função que forneça esses Privileges e adicioná-los ao grupo também.

- Crie papéis mais refinados.

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

  Nesse caso, você clonaria as funções VSC necessárias e editaria a função clonada para que ela tenha apenas o Privileges que seu usuário precisa.

Privileges necessário para tarefas VSC

Diferentes ferramentas do ONTAP para tarefas do VMware vSphere exigem

combinações diferentes de Privileges específicas para o VSC (Virtual Storage Console) e o vCenter Server Privileges nativo.

As informações sobre o Privileges necessário para as tarefas do VSC estão disponíveis no artigo 1032542 da base de conhecimento do NetApp.

"Como configurar o RBAC para o Virtual Storage Console"

Privilégio de nível de produto exigido pelas ferramentas do ONTAP para VMware vSphere

Para acessar as ferramentas do ONTAP para a GUI do VMware vSphere, você deve ter o privilégio de exibição específico do VSC no nível do produto atribuído no nível correto do objeto vSphere. Se você fizer login sem esse privilégio, o VSC exibirá uma mensagem de erro quando você clicar no ícone NetApp e impedirá que você acesse o VSC.

As informações a seguir descrevem o privilégio visualização em nível de produto VSC:

Privilégio	Descrição	Nível de atribuição
Vista	Você pode acessar a GUI do VSC. Este privilégio não lhe permite executar tarefas no VSC. Para executar quaisquer tarefas do VSC, você precisa ter o vCenter Server Privileges nativo e específico do VSC correto para essas tarefas.	O nível de atribuição determina quais partes da IU você pode ver. A atribuição do privilégio Exibir no objeto raiz (pasta) permite que você entre no VSC clicando no ícone NetApp. Você pode atribuir o privilégio Exibir a outro nível de objeto vSphere; no entanto, isso limita os menus VSC que você pode ver e usar. O objeto raiz é o local recomendado para atribuir qualquer permissão que contenha o privilégio Exibir.

Permissões para sistemas de armazenamento ONTAP e objetos vSphere

Os controles de acesso baseados em função (RBAC) do ONTAP permitem controlar o acesso a sistemas de storage específicos e controlar as ações que um usuário pode executar nesses sistemas de storage. Nas ferramentas do ONTAP vSphere, o ONTAP RBAC trabalha com o vCenter Server RBAC para determinar quais tarefas do console de armazenamento virtual (VSC) um usuário específico pode executar nos objetos em um sistema de storage específico.

O VSC usa as credenciais (nome de usuário e senha) que você configurou no VSC para autenticar cada sistema de armazenamento e determinar quais operações de armazenamento podem ser executadas nesse sistema de armazenamento. O VSC usa um conjunto de credenciais para cada sistema de storage. Essas

credenciais determinam quais tarefas do VSC podem ser executadas nesse sistema de armazenamento; em outras palavras, as credenciais são para o VSC, não para um usuário VSC individual.

O RBAC do ONTAP se aplica apenas a sistemas de storage e a executar tarefas de VSC relacionadas ao storage, como provisionamento de máquinas virtuais. Se você não tiver o ONTAP RBAC Privileges apropriado para um sistema de storage específico, não poderá executar nenhuma tarefa em um objeto vSphere hospedado nesse sistema de storage. Você pode usar o ONTAP RBAC em conjunto com o Privileges específico do VSC para controlar quais tarefas do VSC um usuário pode executar:

- Monitoramento e configuração de objetos de armazenamento ou do vCenter Server que residem em um sistema de armazenamento
- Provisionamento de objetos vSphere que residem em um sistema de storage

O uso do RBAC do ONTAP com o Privileges específico do VSC fornece uma camada de segurança orientada ao storage que o administrador de storage pode gerenciar. Como resultado, você tem controle de acesso mais refinado do que o que o ONTAP RBAC sozinho ou o vCenter Server RBAC sozinho suporta. Por exemplo, com o vCenter Server RBAC, você pode permitir que o vCenterUserB provisione um datastore no armazenamento do NetApp enquanto impede que o vCenterUserA provisione datastores. Se as credenciais do sistema de armazenamento para um sistema de armazenamento específico não suportarem a criação de armazenamento, então nem o vCenterUserB nem o vCenterUserA poderão provisionar um armazenamento de dados nesse sistema de armazenamento.

Quando você inicia uma tarefa VSC, o VSC primeiro verifica se você tem a permissão correta do vCenter Server para essa tarefa. Se a permissão do vCenter Server não for suficiente para permitir que você execute a tarefa, o VSC não precisará verificar o ONTAP Privileges para esse sistema de armazenamento porque você não passou na verificação de segurança inicial do vCenter Server. Como resultado, você não pode acessar o sistema de armazenamento.

Se a permissão do vCenter Server for suficiente, o VSC verificará o ONTAP RBAC Privileges (sua função ONTAP) associado às credenciais do sistema de storage (nome de usuário e senha) para determinar se você tem Privileges suficientes para executar as operações de storage exigidas por essa tarefa no sistema de storage. Se tiver o ONTAP Privileges correto, pode aceder ao sistema de armazenamento e executar a tarefa VSC. As funções do ONTAP determinam as tarefas do VSC que você pode executar no sistema de storage.

Cada sistema de storage tem um conjunto de ONTAP Privileges associado.

O RBAC do ONTAP e o vCenter Server oferece os seguintes benefícios:

- Segurança

  O administrador pode controlar quais usuários podem executar quais tarefas em um nível refinado de objeto do vCenter Server e em um nível de sistema de armazenamento.

- Informações de auditoria

  Em muitos casos, o VSC fornece uma trilha de auditoria no sistema de armazenamento que permite rastrear eventos de volta para o usuário do vCenter Server que realizou as modificações de armazenamento.

- Usabilidade

  Você pode manter todas as credenciais do controlador em um só lugar.

Funções recomendadas do ONTAP ao usar as 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 controle de acesso baseado em funções (RBAC). Essas funções contêm o ONTAP Privileges necessário para executar as operações de storage necessárias executadas pelas tarefas do console de storage virtual (VSC).

Para criar novas funções de usuário, faça login como administrador em sistemas de storage que executam o ONTAP. Você pode criar funções do ONTAP usando uma das seguintes opções:

- Gerenciador de sistema ONTAP 9,7 ou posterior

  "Configurar funções de usuário e Privileges"

Cada função do ONTAP tem um nome de usuário e um par de senhas 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 funções ONTAP específicas do VSC são ordenadas hierarquicamente. Isso significa que a primeira função é a função mais restritiva e tem apenas os Privileges associados ao conjunto mais básico de operações de storage VSC. A próxima função inclui o 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 RBAC recomendadas do ONTAP ao usar o VSC. Depois de criar essas funções, você pode atribuir as funções aos usuários que precisam executar tarefas relacionadas ao storage, como o provisionamento de máquinas virtuais.

1. Detecção

   Essa função permite adicionar sistemas de storage.

2. Crie armazenamento

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

3. Modificar armazenamento

   Essa função permite modificar o armazenamento. Essa função também inclui todos os Privileges associados à função descoberta e à função criar armazenamento.

4. 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 o provedor VASA para ONTAP, você também deve 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".

Como configurar o controle de acesso baseado em função do ONTAP para ferramentas do ONTAP para VMware vSphere

Você deve configurar o controle de acesso baseado em função (RBAC) do ONTAP no sistema de storage se quiser usar os controles de acesso baseados em função com as ferramentas do ONTAP para VMware vSphere. Você pode criar uma ou mais contas de usuário personalizadas com Privileges de acesso limitado com o recurso RBAC do ONTAP.

O VSC e o SRA podem acessar sistemas de storage no nível do cluster ou no nível da SVM (Storage Virtual Machine) SVM. Se você estiver adicionando sistemas de storage no nível do cluster, forneça as credenciais do usuário admin para fornecer todas as funcionalidades necessárias. Se você estiver adicionando sistemas de storage diretamente detalhes da SVM, você deve estar ciente de que o usuário "vsadmin" não tem todas as funções e recursos necessários para executar determinadas tarefas.

O VASA Provider só pode acessar sistemas de armazenamento no nível do cluster. Se o Fornecedor VASA for necessário para um controlador de armazenamento específico, o sistema de armazenamento deve ser adicionado ao VSC no nível do cluster, mesmo que você esteja usando VSC ou SRA.

Para criar um novo usuário e conectar um cluster ou um SVM às ferramentas do ONTAP, faça o seguinte:

- Crie uma função de administrador de cluster ou de administrador do SVM

  Você pode usar uma das seguintes opções para criar essas funções:

  - Gerenciador de sistemas ONTAP 9,8

    "Configurar funções de usuário e Privileges"

- Crie usuários com a função atribuída e o conjunto de aplicativos apropriado usando o ONTAP

  Você precisa dessas credenciais do sistema de storage para configurar os sistemas de storage do VSC. Você pode configurar sistemas de armazenamento para VSC inserindo as credenciais no VSC. Cada vez que você fizer login em um sistema de storage com essas credenciais, terá permissões para as funções do VSC configuradas no ONTAP enquanto cria as credenciais.

- Adicione o sistema de storage ao VSC e forneça as credenciais do usuário que você acabou de criar

Funções do VSC

O VSC classifica o ONTAP Privileges no seguinte conjunto de funções do VSC:

- Detecção

  Permite a descoberta de todos os controladores de storage conectados

- Crie armazenamento

  Permite a criação de volumes e número de unidade lógica (LUNs)

- Modificar armazenamento

Permite o redimensionamento e a deduplicação de sistemas de armazenamento

- Destrua o armazenamento

  Permite a destruição de volumes e LUNs

Funções do Fornecedor VASA

Você pode criar somente Gerenciamento baseado em políticas no nível do cluster. Essa função permite o gerenciamento baseado em políticas do storage usando perfis de recursos de storage.

Funções do SRA

O SRA classifica o ONTAP Privileges em uma função SAN ou nas no nível do cluster ou do SVM. Isto permite que os utilizadores executem operações SRM.

O VSC executa uma validação de privilégio inicial das funções RBAC do ONTAP quando você adiciona o cluster ao VSC. Se você tiver adicionado um IP de storage direto da SVM, o VSC não realizará a validação inicial. O VSC verifica e aplica o Privileges posteriormente no fluxo de trabalho da tarefa.

Informações sobre direitos autorais

Informações sobre marcas comerciais