Controle de acesso baseado em função

ONTAP tools for VMware vSphere 10.0

NetApp
October 23, 2024

Índice

Controle de acesso baseado em função 1
Visão geral do controle de acesso baseado em funções nas ferramentas do ONTAP 1
Funções recomendadas do ONTAP ao usar as ferramentas do ONTAP para VMware vSphere 3

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 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 AD (ative Directory) ou de usuários/grupos potencialmente locais de janelas também (não recomendado)
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 precisa ter as funções RBAC apropriadas do vCenter Server. Durante uma tarefa, as ferramentas do ONTAP verificam as funções do vCenter Server de um usuário antes de verificar o ONTAP Privileges do usuário.

> As funções do vCenter Server se aplicam a usuários do ONTAP Tools vCenter, não a 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.

Quando você atribui uma função determina as tarefas das ferramentas do ONTAP 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 incluídas com ferramentas ONTAP

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

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

Função	Descrição
Administrador de ferramentas do NetApp ONTAP	Fornece todas as Privileges nativas específicas das ferramentas do vCenter Server Privileges e do ONTAP necessárias para executar algumas das tarefas das ferramentas do ONTAP.
Ferramentas NetApp ONTAP somente leitura	Fornece acesso somente leitura às ferramentas do ONTAP. Esses usuários não podem executar nenhuma ação de ferramentas do ONTAP controlada pelo acesso.
Provisionamento de ferramentas do NetApp ONTAP	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 da IU do Manager não está registrada no vCenter. Esta função é específica para a IU do gerente.

Se a sua empresa exigir que você implemente funções mais restritivas do que as funções de ferramentas padrão do ONTAP, use as funções de ferramentas do ONTAP para criar novas funções.

Nesse caso, você clonaria as funções necessárias das ferramentas do ONTAP e editaria a função clonada para que ela tenha apenas o Privileges 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 verificarão o ONTAP RBAC Privileges (sua função ONTAP) associado às credenciais de back-ends de storage (nome de usuário e senha)

para determinar se você tem Privileges suficientes para executar as operações de storage exigidas por essa tarefa de ferramentas do ONTAP nesse back-end de storage. Se você tiver o ONTAP Privileges correto, poderá acessar os backends de armazenamento e executar a tarefa de ferramentas do ONTAP. As funções do ONTAP determinam as tarefas de ferramentas do ONTAP que você pode executar no back-end de storage.

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 com controle de acesso baseado em funções (RBAC). Essas funções contêm o ONTAP Privileges necessário para executar as operações de storage necessárias executadas pelas tarefas de ferramentas do ONTAP.

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 o Gerenciador de sistema do ONTAP 9.8P1 ou posterior. Consulte "Lista de Privileges mínimo necessário para usuário de cluster com escopo global não administrador" para obter mais informações.

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 das ferramentas do ONTAP 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 de ferramentas ONTAP. 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 de RBAC do ONTAP recomendadas ao usar ferramentas do ONTAP. 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".

Informações sobre direitos autorais

Informações sobre marcas comerciais