Controles de acesso baseados em função do SnapCenter (RBAC)

SnapCenter Software 6.0

NetApp
December 19, 2024

Índice

Controles de acesso baseados em função do SnapCenter (RBAC)

Tipos de RBAC

As permissões de controle de acesso baseado em função (RBAC) e ONTAP do SnapCenter permitem que os administradores do SnapCenter delegem o controle de recursos do SnapCenter a diferentes usuários ou grupos de usuários. Esse acesso gerenciado centralmente capacita os administradores de aplicativos a trabalhar com segurança em ambientes delegados.

Você pode criar e modificar funções e adicionar acesso a recursos aos usuários a qualquer momento, mas quando você estiver configurando o SnapCenter pela primeira vez, você deve pelo menos adicionar usuários ou grupo do ative Directory a funções e, em seguida, adicionar acesso a recursos a esses usuários ou grupos.

> Você não pode usar o SnapCenter para criar contas de usuário ou grupo. Você deve criar contas de usuário ou grupo no ative Directory do sistema operacional ou banco de dados.

O SnapCenter usa os seguintes tipos de controle de acesso baseado em função:

- SnapCenter RBAC
- Plug-in RBAC do SnapCenter (para alguns plug-ins)
- RBAC no nível da aplicação
- Permissões da ONTAP

SnapCenter RBAC

Funções e permissões

O SnapCenter é fornecido com funções predefinidas com permissões já atribuídas. Você pode atribuir usuários ou grupos de usuários a essas funções. Você também pode criar novas funções e gerenciar permissões e usuários.

Atribuindo permissões a usuários ou grupos

Você pode atribuir permissões a usuários ou grupos para acessar objetos do SnapCenter, como hosts, conexões de storage e grupos de recursos. Não é possível alterar as permissões da função SnapCenterAdmin.

É possível atribuir permissões RBAC a usuários e grupos dentro da mesma floresta e a usuários pertencentes a diferentes florestas. Não é possível atribuir permissões RBAC a usuários pertencentes a grupos aninhados entre florestas.

> Se você criar uma função personalizada, ela deverá conter todas as permissões da função de administrador do SnapCenter. Se você copiar apenas algumas das permissões, por exemplo, Host add ou Host remove, não será possível executar essas operações.

Autenticação

Os usuários são obrigados a fornecer autenticação durante o login, por meio da interface gráfica do usuário (GUI) ou usando cmdlets do PowerShell. Se os usuários forem membros de mais de uma função, depois de inserir credenciais de login, eles serão solicitados a especificar a função que desejam usar. Os usuários também são obrigados a fornecer autenticação para executar as APIs.

RBAC no nível da aplicação

O SnapCenter usa credenciais para verificar se os usuários autorizados do SnapCenter também têm permissões no nível do aplicativo.

Por exemplo, se você quiser executar operações de Snapshot e proteção de dados em um ambiente SQL Server, você deve definir credenciais com as credenciais Windows ou SQL adequadas. O servidor SnapCenter autentica o conjunto de credenciais usando qualquer um dos métodos. Se você quiser executar operações de snapshot e proteção de dados em um ambiente de sistema de arquivos do Windows no storage ONTAP, a função de administrador do SnapCenter deve ter admin Privileges no host do Windows.

Da mesma forma, se você deseja executar operações de proteção de dados em um banco de dados Oracle e se a autenticação do sistema operacional (os) estiver desativada no host do banco de dados, você deve definir credenciais com o banco de dados Oracle ou as credenciais Oracle ASM. O servidor SnapCenter autentica as credenciais definidas usando um desses métodos, dependendo da operação.

Plug-in do SnapCenter para VMware vSphere RBAC

Se você estiver usando o plug-in SnapCenter VMware para proteção de dados consistente com VM, o vCenter Server fornecerá um nível adicional de RBAC. O plug-in SnapCenter VMware é compatível com o vCenter Server RBAC e o Data ONTAP RBAC.

Para obter informações, consulte "Plug-in do SnapCenter para VMware vSphere RBAC"

Permissões da ONTAP

Você deve criar uma conta vsadmin com as permissões necessárias para acessar o sistema de armazenamento.

Para obter informações sobre como criar a conta e atribuir permissões, consulte "Crie uma função de cluster do ONTAP com Privileges mínimo"

Permissões e funções do RBAC

O controle de acesso baseado em função (RBAC) do SnapCenter permite criar funções e atribuir permissões a essas funções e, em seguida, atribuir usuários ou grupos de usuários às funções. Isso permite que os administradores do SnapCenter criem um ambiente gerenciado centralmente, enquanto os administradores de aplicativos podem gerenciar tarefas de proteção de dados. O SnapCenter é fornecido com algumas funções e permissões predefinidas.

Funções do SnapCenter

O SnapCenter é fornecido com as seguintes funções predefinidas. Você pode atribuir usuários e grupos a essas funções ou criar novas funções.

Quando você atribui uma função a um usuário, somente os trabalhos relevantes a esse usuário são visíveis na página trabalhos, a menos que você tenha atribuído a função Administrador do SnapCenter.

- App Backup e Clone Admin
- Visualizador de cópias de segurança e clones
- Administrador de infraestrutura
- SnapCenterAdmin

Plug-in do SnapCenter para funções do VMware vSphere

Para gerenciar a proteção de dados consistente com VM de VMs, VMDKs e armazenamentos de dados, as funções a seguir são criadas no vCenter pelo plug-in do SnapCenter para VMware vSphere:

- Administrador do SCV
- Vista SCV
- Backup da VCR
- Restauração da VCR
- Restauração do arquivo convidado SCV

Para obter mais informações, consulte "Tipos de plug-in RBAC para SnapCenter para usuários do VMware vSphere"

Prática recomendada: a NetApp recomenda que você crie uma função do ONTAP para o plug-in do SnapCenter para operações do VMware vSphere e atribua a ele todos os Privileges necessários.

Permissões do SnapCenter

O SnapCenter fornece as seguintes permissões:

- Grupo recursos
- Política
- Backup
- Host
- Ligação de armazenamento
- Clone
- Provisionamento (apenas para banco de dados Microsoft SQL)
- Painel de instrumentos
- Relatórios
- Restaurar
  - Restauração completa de volume (somente para plug-ins personalizados)
- Recurso

  Os plug-in Privileges são necessários do administrador para que não administradores realizem operações de descoberta de recursos.

- Instalação ou desinstalação do plug-in

  Quando você ativa permissões de instalação de plug-in, você também deve modificar a permissão de host para habilitar leituras e atualizações.

- Migração
- Montar (apenas para banco de dados Oracle)
- Desmontar (apenas para banco de dados Oracle)
- Monitor de trabalho

  A permissão Monitor de tarefas permite que membros de diferentes funções vejam as operações em todos os objetos aos quais são atribuídos.

Funções e permissões do SnapCenter predefinidas

O SnapCenter é fornecido com funções predefinidas, cada uma com um conjunto de permissões já ativadas. Ao configurar e administrar o controle de acesso baseado em funções (RBAC), você pode usar essas funções predefinidas ou criar novas.

O SnapCenter inclui as seguintes funções predefinidas:

- Função de administrador do SnapCenter
- Função de Administrador de cópia de Segurança e Clonagem de aplicações
- Função Visualizador de cópia de Segurança e Clonagem
- Função de administrador de infraestrutura

Ao adicionar um usuário a uma função, você deve atribuir a permissão StorageConnection para habilitar a comunicação de máquina virtual de armazenamento (SVM) ou atribuir um SVM ao usuário para habilitar a permissão para usar o SVM. A permissão Storage Connection permite que os usuários criem conexões SVM.

Por exemplo, um usuário com a função Administrador do SnapCenter pode criar conexões SVM e atribuí-las a um usuário com a função Administrador de Backup e Clonagem de aplicativos, que por padrão não tem permissão para criar ou editar conexões SVM. Sem uma conexão com o SVM, os usuários não podem concluir operações de backup, clonagem ou restauração.

Função de administrador do SnapCenter

A função de administrador do SnapCenter tem todas as permissões ativadas. Não é possível modificar as permissões para esta função. Você pode adicionar usuários e grupos à função ou removê-los.

Função de Administrador de cópia de Segurança e Clonagem de aplicações

A função App Backup and Clone Admin tem as permissões necessárias para executar ações administrativas para backups de aplicativos e tarefas relacionadas a clones. Essa função não tem permissões para gerenciamento de host, provisionamento, gerenciamento de conexão de storage ou instalação remota.

Permissões	Ativado	Criar	Leia	Atualização	Eliminar
Grupo recursos	Não aplicável	Sim	Sim	Sim	Sim
Política	Não aplicável	Sim	Sim	Sim	Sim
Backup	Não aplicável	Sim	Sim	Sim	Sim
Host	Não aplicável	Sim	Sim	Sim	Sim
Ligação de armazenamento	Não aplicável	Não	Sim	Não	Não
Clone	Não aplicável	Sim	Sim	Sim	Sim
Provisionamento	Não aplicável	Não	Sim	Não	Não
Painel de instrumentos	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Relatórios	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restaurar	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Recurso	Sim	Sim	Sim	Sim	Sim
Instalação/desinstalação do plug-in	Não	Não aplicável		Não aplicável	Não aplicável
Migração	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Montagem	Sim	Sim	Não aplicável	Não aplicável	Não aplicável
Desmontar	Sim	Sim	Não aplicável	Não aplicável	Não aplicável
Restauração completa do volume	Não	Não	Não aplicável	Não aplicável	Não aplicável
Monitor de trabalho	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Função Visualizador de cópia de Segurança e Clonagem

A função Visualizador de cópia de Segurança e Clonagem tem uma vista só de leitura de todas as permissões. Essa função também tem permissões habilitadas para descoberta, geração de relatórios e

acesso ao Dashboard.

Permissões	Ativado	Criar	Leia	Atualização	Eliminar
Grupo recursos	Não aplicável	Não	Sim	Não	Não
Política	Não aplicável	Não	Sim	Não	Não
Backup	Não aplicável	Não	Sim	Não	Não
Host	Não aplicável	Não	Sim	Não	Não
Ligação de armazenamento	Não aplicável	Não	Sim	Não	Não
Clone	Não aplicável	Não	Sim	Não	Não
Provisionamento	Não aplicável	Não	Sim	Não	Não
Painel de instrumentos	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Relatórios	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restaurar	Não	Não	Não aplicável	Não aplicável	Não aplicável
Recurso	Não	Não	Sim	Sim	Não
Instalação/desinstalação do plug-in	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Migração	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Montagem	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Desmontar	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restauração completa do volume	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Monitor de trabalho	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Função de administrador de infraestrutura

A função Administrador de infraestrutura tem permissões habilitadas para gerenciamento de host, gerenciamento de storage, provisionamento, grupos de recursos, relatórios de instalação remota e acesso ao Dashboard.

Permissões	Ativado	Criar	Leia	Atualização	Eliminar
Grupo recursos	Não aplicável	Sim	Sim	Sim	Sim
Política	Não aplicável	Não	Sim	Sim	Sim
Backup	Não aplicável	Sim	Sim	Sim	Sim
Host	Não aplicável	Sim	Sim	Sim	Sim
Ligação de armazenamento	Não aplicável	Sim	Sim	Sim	Sim
Clone	Não aplicável	Não	Sim	Não	Não
Provisionamento	Não aplicável	Sim	Sim	Sim	Sim
Painel de instrumentos	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Relatórios	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restaurar	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Recurso	Sim	Sim	Sim	Sim	Sim
Instalação/desinstalação do plug-in	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Migração	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Montagem	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Desmontar	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restauração completa do volume	Não	Não	Não aplicável	Não aplicável	Não aplicável

Permissões	Ativado	Criar	Leia	Atualização	Eliminar
Monitor de trabalho	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Informações sobre direitos autorais

Informações sobre marcas comerciais