Configurar controles de acesso baseados em função (RBAC)

SnapCenter Software 6.0

NetApp
December 19, 2024

Índice

Configurar controles de acesso baseados em função (RBAC)

Adicione um usuário ou grupo e atribua funções e ativos

Para configurar o controle de acesso baseado em função para usuários do SnapCenter, você pode adicionar usuários ou grupos e atribuir função. A função determina as opções que os usuários do SnapCenter podem acessar.

Antes de começar

- Você deve ter feito login como a função "SnapCenterAdmin".
- Você deve ter criado as contas de usuário ou grupo no ative Directory no sistema operacional ou banco de dados. Você não pode usar o SnapCenter para criar essas contas.

  Você pode incluir apenas os seguintes carateres especiais em nomes de usuário e nomes de grupo: Espaço ( ), hífen (-), sublinhado (_) e dois pontos (:).

- O SnapCenter inclui várias funções predefinidas.

  Você pode atribuir essas funções ao usuário ou criar novas funções.

- Os usuários DE ANÚNCIOS e grupos de AD adicionados ao RBAC do SnapCenter devem ter a permissão DE LEITURA no contentor usuários e no contentor computadores no ative Directory.
- Depois de atribuir uma função a um usuário ou grupo que contenha as permissões apropriadas, você deve atribuir o acesso do usuário aos ativos do SnapCenter, como hosts e conexões de armazenamento.

  Isso permite que os usuários executem as ações para as quais eles têm permissões nos ativos que são atribuídos a eles.

- Você deve atribuir uma função ao usuário ou grupo em algum momento para aproveitar as permissões e eficiências do RBAC.
- Você pode atribuir ativos como host, grupos de recursos, política, conexão de armazenamento, plug-in e credencial ao usuário ao criar o usuário ou grupo.
- Os ativos mínimos que você deve atribuir a um usuário para executar determinadas operações são os seguintes:

Operação	Atribuição de ativos
Proteger recursos	host, política
Backup	host, grupo de recursos, política
Restaurar	host, grupo de recursos
Clone	host, grupo de recursos, política
Ciclo de vida do clone	host

Operação	Atribuição de ativos
Crie um Grupo de recursos	host

- Quando um novo nó é adicionado a um cluster do Windows ou a um ativo DAG (Exchange Server Database Availability Group) e se esse novo nó for atribuído a um usuário, você deve reatribuir o ativo ao usuário ou grupo para incluir o novo nó ao usuário ou grupo.

  Você deve reatribuir o usuário ou grupo RBAC ao cluster ou DAG para incluir o novo nó ao usuário ou grupo RBAC. Por exemplo, você tem um cluster de dois nós e atribuiu um usuário ou grupo RBAC ao cluster. Ao adicionar outro nó ao cluster, você deve reatribuir o usuário ou grupo RBAC ao cluster para incluir o novo nó para o usuário ou grupo RBAC.

- Se você estiver planejando replicar snapshots, atribua a conexão de armazenamento para o volume de origem e destino ao usuário que executa a operação.

  Você deve adicionar ativos antes de atribuir acesso aos usuários.

Se você estiver usando o plug-in do SnapCenter para funções do VMware vSphere para proteger VMs, VMDKs ou datastores, use a GUI do VMware vSphere para adicionar um usuário do vCenter a uma função do SnapCenter Plug-in para VMware vSphere. Para obter informações sobre as funções do VMware vSphere, "Funções predefinidas empacotadas com o plug-in SnapCenter para VMware vSphere" consulte .

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **usuários e acesse** > * *.
3. Na página Adicionar usuários/grupos do ative Directory ou grupo de trabalho:

Para este campo…	Faça isso…
Tipo de acesso	Selecione domínio ou grupo de trabalho Para o tipo de autenticação de domínio, você deve especificar o nome de domínio do usuário ou grupo ao qual deseja adicionar o usuário a uma função. Por padrão, ele é pré-preenchido com o nome de domínio conetado. Tem de registar o domínio não fidedigno na na página **Definições** > **Definições globais** > **Definições de domínio**.

Para este campo…	Faça isso…
Tipo	Selecione Usuário ou Grupo O SnapCenter suporta apenas o grupo de segurança e não o grupo de distribuição.
Nome de utilizador	a. Digite o nome de usuário parcial e clique em **Add**. O nome de usuário diferencia maiúsculas de minúsculas. b. Selecione o nome de utilizador na lista de pesquisa. Quando você adiciona usuários de um domínio diferente ou de um domínio não confiável, você deve digitar o nome de usuário totalmente porque não há lista de pesquisa para usuários de vários domínios. Repita esta etapa para adicionar usuários ou grupos adicionais à função selecionada.
Funções	Selecione a função à qual deseja adicionar o usuário.

4. Clique em **Assign** e, em seguida, na página Assign Assets (atribuir ativos):
   a. Selecione o tipo de ativo na lista suspensa **Ativo**.
   b. Na tabela Ativo, selecione o ativo.

      Os ativos são listados somente se o usuário tiver adicionado os ativos ao SnapCenter.

   c. Repita este procedimento para todos os ativos necessários.
   d. Clique em **Salvar**.
5. Clique em **Enviar**.

Depois de adicionar usuários ou grupos e atribuir funções, atualize a lista recursos.

Crie uma função

Além de usar as funções existentes do SnapCenter, você pode criar suas próprias funções e personalizar as permissões.

Você deve ter feito login como a função "SnapCenterAdmin".

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **funções**.
3. Clique em .
4. Na página Adicionar função, especifique um nome e uma descrição para a nova função.

   Você pode incluir apenas os seguintes carateres especiais em nomes de usuário e nomes de grupo: Espaço ( ), hífen (-), sublinhado (_) e dois pontos (:).

5. Selecione **todos os membros desta função podem ver objetos de outros membros** para permitir que outros membros da função vejam recursos como volumes e hosts depois que eles atualizarem a lista de recursos.

   Você deve desmarcar essa opção se não quiser que os membros dessa função vejam objetos aos quais outros membros são atribuídos.

   Quando essa opção está ativada, a atribuição de acesso aos usuários a objetos ou recursos não é necessária se os usuários pertencerem à mesma função que o usuário que criou os objetos ou recursos.

6. Na página permissões, selecione as permissões que você deseja atribuir à função ou clique em **Selecionar tudo** para conceder todas as permissões à função.
7. Clique em **Enviar**.

Adicione uma função ONTAP RBAC usando comandos de login de segurança

Use os comandos de login de segurança para adicionar uma função RBAC do ONTAP quando seus sistemas de storage estiverem executando o Clustered ONTAP.

Antes de começar

- Antes de criar uma função RBAC do ONTAP para sistemas de storage que executam o Clustered ONTAP, é necessário identificar o seguinte:
  - A tarefa (ou tarefas) que você deseja executar
  - O Privileges necessário para executar essas tarefas
- A configuração de uma função RBAC exige que você execute as seguintes ações:
  - Conceda Privileges aos comandos e/ou diretórios de comando.

    Existem dois níveis de acesso para cada diretório de comando/comando: All-Access e somente leitura.

    Você deve sempre atribuir primeiro o All-Access Privileges.

  - Atribua funções aos usuários.
  - Varie a configuração dependendo se os plug-ins do SnapCenter estão conetados ao IP do administrador de cluster para todo o cluster ou diretamente conetados a um SVM no cluster.

Sobre esta tarefa

Para simplificar a configuração dessas funções em sistemas de storage, você pode usar a ferramenta Criador de usuários do RBAC para Data ONTAP, publicada no Fórum de Comunidades do NetApp.

Esta ferramenta lida automaticamente com a configuração correta do ONTAP Privileges. Por exemplo, a ferramenta Criador de Usuário RBAC para Data ONTAP adiciona automaticamente o Privileges na ordem correta para que o Privileges de Acesso total apareça primeiro. Se você adicionar primeiro o Privileges somente leitura e depois adicionar o Privileges All-Access, o ONTAP marca o Privileges All-Access como duplicatas e os ignora.

Se você atualizar mais tarde o SnapCenter ou o ONTAP, execute novamente a ferramenta Criador de usuários do RBAC para Data ONTAP para atualizar as funções de usuário criadas anteriormente. As funções de usuário criadas para uma versão anterior do SnapCenter ou do ONTAP não funcionam corretamente com versões atualizadas. Quando você executa novamente a ferramenta, ela manipula automaticamente a atualização. Você não precisa recriar os papéis.

Para obter mais informações sobre como configurar funções RBAC do ONTAP, consulte "Guia de autenticação do administrador da ONTAP 9 e alimentação RBAC".

Para consistência, a documentação do SnapCenter refere-se às funções como usando o Privileges. A GUI do OnCommand System Manager usa o termo *attribute* em vez de *Privilege*. Ao configurar funções RBAC do ONTAP, esses dois termos significam a mesma coisa.

Passos

1. No sistema de armazenamento, crie uma nova função inserindo o seguinte comando:

   ```
   security login role create <role_name\> -cmddirname "command" -access all
   -vserver <svm_name\>
   ```

   - SVM_name é o nome do SVM. Se você deixar isso em branco, o padrão será administrador do cluster.
   - role_name é o nome que você especifica para a função.
   - Comando é a capacidade ONTAP.

     Você deve repetir este comando para cada permissão. Lembre-se de que os comandos All-Access devem ser listados antes dos comandos somente leitura.

   Para obter informações sobre a lista de permissões, "Comandos CLI do ONTAP para criar funções e atribuir permissões"consulte .

2. Crie um nome de usuário digitando o seguinte comando:

   ```
   security login create -username <user_name\> -application ontapi -authmethod
   <password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment
   "user_description"
   ```

   - user_name é o nome do usuário que você está criando.
   - <password> é a sua palavra-passe. Se você não especificar uma senha, o sistema solicitará uma.
   - SVM_name é o nome do SVM.

3. Atribua a função ao utilizador introduzindo o seguinte comando:

   ```
   security login modify username <user_name\> –vserver <svm_name\> -role
   <role_name\> -application ontapi -application console -authmethod <password\>
   ```

   - <user_name> é o nome do usuário que você criou na Etapa 2. Este comando permite modificar o usuário para associá-lo à função.
   - <svm_name> é o nome do SVM.
   - <role_name> é o nome da função que você criou na Etapa 1.
   - <password> é a sua palavra-passe. Se você não especificar uma senha, o sistema solicitará uma.

4. Verifique se o usuário foi criado corretamente digitando o seguinte comando:

   ```
   security login show –vserver <svm_name\> -user-or-group-name <user_name\>
   ```

   User_name é o nome do usuário que você criou na Etapa 3.

Criar funções do SVM com Privileges mínimo

Há vários comandos de CLI do ONTAP que você deve executar ao criar uma função para um novo usuário do SVM no ONTAP. Essa função é necessária se você configurar SVMs no ONTAP para usar com o SnapCenter e não quiser usar a função vsadmin.

Passos

1. No sistema de storage, crie uma função e atribua todas as permissões à função.

   ```
   security login role create –vserver <svm_name\>- role <SVM_Role_Name\>
   -cmddirname <permission\>
   ```

   Você deve repetir este comando para cada permissão.

2. Crie um usuário e atribua a função a esse usuário.

   ```
   security login create -user <user_name\> -vserver <svm_name\> -application
   ontapi -authmethod password -role <SVM_Role_Name\>
   ```

3. Desbloquear o utilizador.

   ```
   security login unlock -user <user_name\> -vserver <svm_name\>
   ```

Comandos CLI do ONTAP para criar funções SVM e atribuir permissões

Existem vários comandos de CLI do ONTAP que você deve executar para criar funções SVM e atribuir permissões.

A partir do 5,0, os usuários de administração do vserver só são suportados com APIS REST. Se você quiser criar funções usando um administrador que não seja vserver, use o ZAPI.

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname`

"snapmirror list-destinations" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"volume destroy" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname`

"nvme subsystem host" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all

Criar funções de cluster do ONTAP com Privileges mínimo

Você deve criar uma função de cluster do ONTAP com Privileges mínimo para que você não precise usar a função de administrador do ONTAP para executar operações no SnapCenter. Você pode executar vários comandos de CLI do ONTAP para criar a função de cluster do ONTAP e atribuir Privileges mínimo.

Passos

1. No sistema de storage, crie uma função e atribua todas as permissões à função.

   ```
   security login role create –vserver <cluster_name\>- role <role_name\>
   -cmddirname <permission\>
   ```

   Você deve repetir este comando para cada permissão.

2. Crie um usuário e atribua a função a esse usuário.

   ```
   security login create -user <user_name\> -vserver <cluster_name\> -application
   ontapi -authmethod password -role <role_name\>
   ```

3. Desbloquear o utilizador.

   ```
   security login unlock -user <user_name\> -vserver <cluster_name\>
   ```

Comandos de CLI do ONTAP para criar funções de cluster e atribuir permissões

Há vários comandos de CLI do ONTAP que você deve executar para criar funções de cluster e atribuir permissões.

A partir do SnapCenter 5,0, os usuários de administradores de cluster só são compatíveis com APIs REST. Se você quiser criar funções usando um administrador que não seja de cluster, use o ZAPI.

- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly
- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"lun mapping create" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"volume clone show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

```
"vserver export-policy rule delete" -access all
```

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all`

Configure pools de aplicativos do IIS para habilitar permissões de leitura do ative Directory

Você pode configurar os Serviços de informações da Internet (IIS) no servidor Windows para criar uma conta de pool de aplicativos personalizada quando precisar ativar as permissões de leitura do ative Directory para o SnapCenter.

Passos

1. Abra o Gerenciador do IIS no servidor Windows em que o SnapCenter está instalado.
2. No painel de navegação esquerdo, clique em **pools de aplicativos**.
3. Selecione SnapCenter na lista pools de aplicativos e clique em **Configurações avançadas** no painel ações.
4. Selecione identidade e, em seguida, clique em **…** para editar a identidade do conjunto de aplicações SnapCenter.
5. No campo conta personalizada, insira um nome de usuário de domínio ou conta de administrador de domínio com permissão de leitura do ative Directory.
6. Clique em OK.

   A conta personalizada substitui a conta ApplicationPoolIdentity incorporada para o pool de aplicativos do SnapCenter.

Informações sobre direitos autorais

Informações sobre marcas comerciais