



Gerenciar funções de controle de acesso

ONTAP 9

NetApp
January 17, 2025

Índice

- Gerenciar funções de controle de acesso 1
 - Gerencie a visão geral das funções de controle de acesso..... 1
 - Modifique a função atribuída a um administrador 1
 - Definir funções personalizadas 1
 - Funções predefinidas para administradores de cluster 3
 - Funções predefinidas para administradores de SVM 5
 - Controle o acesso do administrador 7

Gerenciar funções de controle de acesso

Gerencie a visão geral das funções de controle de acesso

A função atribuída a um administrador determina os comandos aos quais o administrador tem acesso. Você atribui a função ao criar a conta para o administrador. Você pode atribuir uma função diferente ou definir funções personalizadas conforme necessário.

Modifique a função atribuída a um administrador

Você pode usar o `security login modify` comando para alterar a função de uma conta de administrador de cluster ou SVM. Pode atribuir uma função predefinida ou personalizada.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Alterar a função de um administrador de cluster ou SVM:

```
security login modify -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

Para obter a sintaxe de comando completa, consulte ["folha de trabalho"](#).

"Criando ou modificando contas de login"

O comando a seguir altera a função da conta de administrador do cluster do AD `DOMAIN1\guest1` para a função predefinida `readonly`.

```
cluster1::>security login modify -vserver engCluster -user-or-group-name  
DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
```

O comando a seguir altera a função das contas de administrador do SVM na conta do grupo AD `DOMAIN1\adgroup` para a função personalizada `vol_role`.

```
cluster1::>security login modify -vserver engData -user-or-group-name  
DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
```

Definir funções personalizadas

Você pode usar o `security login role create` comando para definir uma função personalizada. Você pode executar o comando quantas vezes for necessário para obter

a combinação exata de recursos que deseja associar à função.

Sobre esta tarefa

- Uma função, predefinida ou personalizada, concede ou nega acesso a comandos ou diretórios de comandos do ONTAP.

Um diretório de comandos (`volume`, por exemplo) é um grupo de comandos e subdiretórios de comandos relacionados. Exceto conforme descrito neste procedimento, conceder ou negar acesso a um diretório de comando concede ou nega acesso a cada comando no diretório e seus subdiretórios.

- O acesso a comandos específicos ou o acesso a subdiretórios substitui o acesso ao diretório pai.

Se uma função for definida com um diretório de comando e, em seguida, for definida novamente com um nível de acesso diferente para um comando específico ou para um subdiretório do diretório pai, o nível de acesso especificado para o comando ou subdiretório substitui o do pai.



Não é possível atribuir a um administrador SVM uma função que dê acesso a um diretório de comando ou comando que esteja disponível apenas para o `admin` administrador de cluster - por exemplo, o `security` diretório de comando.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Definir uma função personalizada:

```
security login role create -vserver SVM_name -role role -cmddirname  
command_or_directory_name -access access_level -query query
```

Para obter a sintaxe de comando completa, consulte ["folha de trabalho"](#).

Os comandos a seguir concedem à `vol_role` função acesso total aos comandos no `volume` diretório de comandos e acesso somente leitura aos comandos `volume snapshot` no subdiretório.

```
cluster1::>security login role create -role vol_role -cmddirname  
"volume" -access all  
  
cluster1::>security login role create -role vol_role -cmddirname "volume  
snapshot" -access readonly
```

Os comandos a seguir concedem à `SVM_storage` função acesso somente leitura aos comandos no `storage` diretório de comandos, sem acesso aos comandos `storage encryption` no subdiretório e acesso total ao `storage aggregate plex offline` comando não intrínseco.

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly
```

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none
```

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

Funções predefinidas para administradores de cluster

As funções predefinidas para administradores de cluster devem atender à maioria das suas necessidades. Você pode criar funções personalizadas conforme necessário. Por padrão, um administrador de cluster recebe a função predefinida `admin`.

A tabela a seguir lista as funções predefinidas para administradores de cluster:

Esta função...	Tem este nível de acesso...	Para os seguintes comandos ou diretórios de comandos
administrador	tudo	Todos os diretórios de comando (DEFAULT)
admin-no-fsa (disponível a partir de ONTAP 9.12,1)	Leitura/escrita	<ul style="list-style-type: none">• Todos os diretórios de comando (DEFAULT)• <code>security login rest-role</code>• <code>security login role</code>

Somente leitura	<ul style="list-style-type: none"> • security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics 	Nenhum
volume file show-disk-usage	AutoSupport	tudo
<ul style="list-style-type: none"> • set • system node autosupport 	nenhum	Todos os outros diretórios de comando (DEFAULT)
backup	tudo	vserver services ndmp
readonly	volume	nenhum
Todos os outros diretórios de comando (DEFAULT)	readonly	tudo

<ul style="list-style-type: none"> • <code>security login password</code> <p>Apenas para gerir a palavra-passe local da conta de utilizador e as informações das chaves</p> <ul style="list-style-type: none"> • <code>set</code> 	nenhum	security
readonly	Todos os outros diretórios de comando (DEFAULT)	SnapLock
tudo	<ul style="list-style-type: none"> • <code>set</code> • <code>volume create</code> • <code>volume modify</code> • <code>volume move</code> • <code>volume show</code> 	nenhum
<ul style="list-style-type: none"> • <code>volume move governor</code> • <code>volume move recommend</code> 	nenhum	Todos os outros diretórios de comando (DEFAULT)
nenhum	nenhum	Todos os diretórios de comando (DEFAULT)



A `autosupport` função é atribuída à conta predefinida `autosupport`, que é usada pelo AutoSupport OnDemand. O ONTAP impede que você modifique ou exclua a `autosupport` conta. O ONTAP também impede que você atribua `autosupport` a função a outras contas de usuário.

Funções predefinidas para administradores de SVM

As funções predefinidas para administradores de SVM devem atender à maioria das suas necessidades. Você pode criar funções personalizadas conforme necessário. Por padrão, a função predefinida é atribuída a um administrador SVM `vsadmin`.

A tabela a seguir lista as funções predefinidas para administradores de SVM:

Nome da função	Recursos
----------------	----------

vsadmin	<ul style="list-style-type: none"> • Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Gerenciamento de volumes, exceto movimentos de volume • Gerenciamento de cotas, qtrees, cópias Snapshot e arquivos • Gerenciamento de LUNs • Executando operações SnapLock, exceto exclusão privilegiada • Configuração de protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurando serviços: DNS, LDAP e NIS • Tarefas de monitorização • Monitoramento de conexões de rede e interface de rede • Monitoramento da integridade do SVM
vsadmin-volume	<ul style="list-style-type: none"> • Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Gerenciamento de volumes, incluindo movimentos de volume • Gerenciamento de cotas, qtrees, cópias Snapshot e arquivos • Gerenciamento de LUNs • Configuração de protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurando serviços: DNS, LDAP e NIS • Monitorização da interface de rede • Monitoramento da integridade do SVM
protocolo vsadmin	<ul style="list-style-type: none"> • Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Configuração de protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurando serviços: DNS, LDAP e NIS • Gerenciamento de LUNs • Monitorização da interface de rede • Monitoramento da integridade do SVM

vsadmin-backup	<ul style="list-style-type: none"> • Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Gerenciamento de operações NDMP • Fazendo uma leitura/gravação de volume restaurada • Gerenciamento de relacionamentos do SnapMirror e cópias Snapshot • Visualização de volumes e informações de rede
vsadmin-SnapLock	<ul style="list-style-type: none"> • Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Gerenciamento de volumes, exceto movimentos de volume • Gerenciamento de cotas, qtrees, cópias Snapshot e arquivos • Executar operações SnapLock, incluindo exclusão privilegiada • Configurando protocolos: NFS e SMB • Configurando serviços: DNS, LDAP e NIS • Tarefas de monitorização • Monitoramento de conexões de rede e interface de rede
vsadmin-readonly	<ul style="list-style-type: none"> • Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Monitoramento da integridade do SVM • Monitorização da interface de rede • Visualização de volumes e LUNs • Visualização de serviços e protocolos

Controle o acesso do administrador

A função atribuída a um administrador determina quais funções o administrador pode executar com o System Manager. Funções predefinidas para administradores de cluster e administradores de VM de storage são fornecidas pelo System Manager. Você atribui a função ao criar a conta do administrador ou pode atribuir uma função diferente posteriormente.

Dependendo de como você ativou o acesso à conta, talvez seja necessário executar qualquer um dos seguintes procedimentos:

- Associar uma chave pública a uma conta local.
- Instale um certificado digital de servidor assinado pela CA.



- Configure o acesso AD, LDAP ou NIS.

Você pode executar essas tarefas antes ou depois de ativar o acesso à conta.

Atribuindo uma função a um administrador

Atribua uma função a um administrador, da seguinte forma:


Passos

1. Selecione **Cluster > Settings**.
2. Selecione  ao lado de **usuários e funções**.
3.  **Add** Selecione em **Users**.
4. Especifique um nome de usuário e selecione uma função no menu suspenso **role**.
5. Especifique um método de login e uma senha para o usuário.

Alterar a função de administrador

Altere a função de um administrador, da seguinte forma:

Passos

1. Clique em **Cluster > Settings**.
2. Selecione o nome do usuário cuja função deseja alterar e clique no  que aparece ao lado do nome de usuário.
3. Clique em **Editar**.
4. Selecione uma função no menu suspenso **Role**.

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 SOBRESSALIENTES; 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 SOFTWARES, 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.