Gerencie o acesso a arquivos usando SMB

ONTAP 9

NetApp
January 17, 2025

Índice

Gerencie o acesso a arquivos usando SMB

Use usuários e grupos locais para autenticação e autorização

Como o ONTAP usa usuários e grupos locais

Conceitos de usuários e grupos locais

Você deve saber o que são usuários e grupos locais e algumas informações básicas sobre eles, antes de determinar se deseja configurar e usar usuários e grupos locais em seu ambiente.

- **Usuário local**

  Uma conta de usuário com um identificador de segurança exclusivo (SID) que tem visibilidade somente na máquina virtual de armazenamento (SVM) na qual é criada. As contas de usuário locais têm um conjunto de atributos, incluindo nome de usuário e SID. Uma conta de usuário local autentica localmente no servidor CIFS usando autenticação NTLM.

  As contas de usuário têm vários usos:

  - Usado para conceder *Gerenciamento de Direitos de Usuário* Privileges a um usuário.
  - Usado para controlar o acesso em nível de compartilhamento e em nível de arquivo aos recursos de arquivo e pasta que o SVM possui.

- **Grupo local**

  Um grupo com um SID exclusivo tem visibilidade somente na SVM em que ele é criado. Grupos contêm um conjunto de membros. Os membros podem ser usuários locais, usuários de domínio, grupos de domínio e contas de máquinas de domínio. Os grupos podem ser criados, modificados ou excluídos.

  Os grupos têm vários usos:

  - Usado para conceder *Gerenciamento de Direitos de Usuário* Privileges aos seus membros.
  - Usado para controlar o acesso em nível de compartilhamento e em nível de arquivo aos recursos de arquivo e pasta que o SVM possui.

- **Domínio local**

  Um domínio que tem escopo local, limitado pelo SVM. O nome do domínio local é o nome do servidor CIFS. Os usuários e grupos locais estão contidos no domínio local.

- **Identificador de segurança (SID)**

  Um SID é um valor numérico de comprimento variável que identifica os princípios de segurança do estilo Windows. Por exemplo, um SID típico assume a seguinte forma: S-1-5-21-3139654847-1303905135-2517279418-123456.

- * Autenticação NTLM*

  Um método de segurança do Microsoft Windows usado para autenticar usuários em um servidor CIFS.

- **Banco de dados replicado em cluster (RDB)**

  Um banco de dados replicado com uma instância em cada nó em um cluster. Os objetos de usuário local e grupo são armazenados no RDB.

Razões para criar usuários locais e grupos locais

Há várias razões para criar usuários locais e grupos locais na sua máquina virtual de storage (SVM). Por exemplo, você pode acessar um servidor SMB usando uma conta de usuário local se os controladores de domínio (DCs) não estiverem disponíveis, talvez queira usar grupos locais para atribuir Privileges ou se o servidor SMB estiver em um grupo de trabalho.

Você pode criar uma ou mais contas de usuário locais pelos seguintes motivos:

- Seu servidor SMB está em um grupo de trabalho e os usuários de domínio não estão disponíveis.

  Os utilizadores locais são necessários nas configurações do grupo de trabalho.

- Você deseja a capacidade de autenticar e fazer login no servidor SMB se os controladores de domínio não estiverem disponíveis.

  Os usuários locais podem se autenticar com o servidor SMB usando a autenticação NTLM quando o controlador de domínio está inativo ou quando problemas de rede impedem que o servidor SMB entre em Contato com o controlador de domínio.

- Você deseja atribuir *User Rights Management* Privileges a um usuário local.

  User Rights Management é a capacidade de um administrador de servidor SMB controlar quais direitos os usuários e grupos têm no SVM. Você pode atribuir Privileges a um usuário atribuindo o Privileges à conta do usuário ou tornando o usuário membro de um grupo local que tenha esses Privileges.

Você pode criar um ou mais grupos locais pelos seguintes motivos:

- O servidor SMB está em um grupo de trabalho e os grupos de domínio não estão disponíveis.

  Os grupos locais não são necessários nas configurações do grupo de trabalho, mas podem ser úteis para gerenciar o Access Privileges para usuários locais do grupo de trabalho.

- Você deseja controlar o acesso aos recursos de arquivos e pastas usando grupos locais para controle de compartilhamento e acesso a arquivos.
- Você deseja criar grupos locais com *User Rights Management* Privileges personalizado.

  Alguns grupos de utilizadores incorporados têm Privileges predefinidos. Para atribuir um conjunto personalizado de Privileges, você pode criar um grupo local e atribuir o Privileges necessário a esse grupo. Em seguida, você pode adicionar usuários locais, usuários de domínio e grupos de domínio ao grupo local.

Informações relacionadas

Como funciona a autenticação de usuário local

Lista de Privileges suportados

Como funciona a autenticação de usuário local

Antes que um usuário local possa acessar dados em um servidor CIFS, o usuário deve criar uma sessão autenticada.

Como o SMB é baseado em sessão, a identidade do usuário pode ser determinada apenas uma vez, quando a sessão é configurada pela primeira vez. O servidor CIFS usa autenticação baseada em NTLM ao autenticar usuários locais. Tanto o NTLMv1 como o NTLMv2 são suportados.

O ONTAP usa autenticação local em três casos de uso. Cada caso de uso depende se a parte do domínio do nome de usuário (com o formato DOMÍNIO/usuário) corresponde ao nome de domínio local do servidor CIFS (o nome do servidor CIFS):

- A parte do domínio corresponde

  Os usuários que fornecem credenciais de usuário local ao solicitar acesso aos dados são autenticados localmente no servidor CIFS.

- A parte do domínio não corresponde

  O ONTAP tenta usar a autenticação NTLM com um controlador de domínio no domínio ao qual o servidor CIFS pertence. Se a autenticação for bem-sucedida, o login será concluído. Se não for bem-sucedido, o que acontece a seguir depende do motivo pelo qual a autenticação não foi bem-sucedida.

  Por exemplo, se o usuário existir no ative Directory mas a senha for inválida ou expirada, o ONTAP não tentará usar a conta de usuário local correspondente no servidor CIFS. Em vez disso, a autenticação falha. Existem outros casos em que o ONTAP usa a conta local correspondente no servidor CIFS, se existir, para autenticação - mesmo que os nomes de domínio NetBIOS não correspondam. Por exemplo, se existir uma conta de domínio correspondente mas estiver desativada, o ONTAP utiliza a conta local correspondente no servidor CIFS para autenticação.

- A parte do domínio não é especificada

  O ONTAP tenta pela primeira vez a autenticação como um usuário local. Se a autenticação como um usuário local falhar, o ONTAP autenticará o usuário com um controlador de domínio no domínio ao qual o servidor CIFS pertence.

Depois que a autenticação de usuário local ou de domínio for concluída com sucesso, o ONTAP constrói um token de acesso completo de usuário, que leva em conta a associação de grupo local e o Privileges.

Para obter mais informações sobre autenticação NTLM para usuários locais, consulte a documentação do Microsoft Windows.

Informações relacionadas

Ativar ou desativar a autenticação de utilizador local

Como os tokens de acesso do usuário são construídos

Quando um usuário mapeia um compartilhamento, uma sessão SMB autenticada é estabelecida e um token de acesso de usuário é construído que contém informações sobre o usuário, a associação de grupo do usuário e Privileges cumulativos e o usuário UNIX mapeado.

A menos que a funcionalidade esteja desativada, as informações de usuário local e grupo também são adicionadas ao token de acesso do usuário. A forma como os tokens de acesso são construídos depende se o login é para um usuário local ou um usuário de domínio do ative Directory:

- Início de sessão do utilizador local

  Embora os usuários locais possam ser membros de diferentes grupos locais, os grupos locais não podem ser membros de outros grupos locais. O token de acesso de usuário local é composto por uma união de todos os Privileges atribuídos a grupos aos quais um usuário local específico é membro.

- Login de usuário de domínio

  Quando um usuário de domínio faz login, o ONTAP obtém um token de acesso de usuário que contém o SID do usuário e os SIDs para todos os grupos de domínio aos quais o usuário é membro. O ONTAP usa a união do token de acesso do usuário de domínio com o token de acesso fornecido por associações locais dos grupos de domínio do usuário (se houver), bem como qualquer Privileges direto atribuído ao usuário do domínio ou qualquer uma de suas associações de grupo de domínio.

Para login de usuário local e de domínio, o RID de grupo principal também é definido para o token de acesso do usuário. O RID predefinido é `Domain Users` (RID 513). Não é possível alterar a predefinição.

O processo de mapeamento de nomes do Windows para UNIX e UNIX para Windows segue as mesmas regras para contas locais e de domínio.

> Não há mapeamento automático implícito de um usuário UNIX para uma conta local. Se isso for necessário, uma regra de mapeamento explícito deve ser especificada usando os comandos de mapeamento de nomes existentes.

Diretrizes para o uso do SnapMirror em SVMs que contêm grupos locais

Você deve estar ciente das diretrizes ao configurar o SnapMirror em volumes de propriedade de SVMs que contêm grupos locais.

Não é possível usar grupos locais em ACEs aplicados a arquivos, diretórios ou compartilhamentos replicados pelo SnapMirror para outro SVM. Se você usar o recurso SnapMirror para criar um espelhamento de DR para um volume em outro SVM e o volume tiver um ACE para um grupo local, o ACE não será válido no espelhamento. Se os dados forem replicados para uma SVM diferente, eles serão migrados para um domínio local diferente. As permissões concedidas a usuários e grupos locais são válidas somente dentro do escopo do SVM no qual foram criados originalmente.

O que acontece com usuários e grupos locais ao excluir servidores CIFS

O conjunto padrão de usuários e grupos locais é criado quando um servidor CIFS é criado e eles são associados à máquina virtual de armazenamento (SVM) que hospeda o servidor CIFS. Os administradores do SVM podem criar usuários e grupos locais a qualquer momento. Você precisa estar ciente do que acontece com usuários e grupos locais quando você exclui o servidor CIFS.

Usuários e grupos locais estão associados a SVMs; portanto, eles não são excluídos quando os servidores CIFS são excluídos devido a considerações de segurança. Embora os usuários e grupos locais não sejam excluídos quando o servidor CIFS é excluído, eles ficam ocultos. Não é possível exibir ou gerenciar usuários e grupos locais até que você crie novamente um servidor CIFS no SVM.

O status administrativo do servidor CIFS não afeta a visibilidade de usuários ou grupos locais.

Como você pode usar o Microsoft Management Console com usuários e grupos locais

Você pode exibir informações sobre usuários e grupos locais no Console de Gerenciamento da Microsoft. Com esta versão do ONTAP, não é possível executar outras tarefas de gerenciamento para usuários e grupos locais a partir do Console de Gerenciamento da Microsoft.

Diretrizes para reverter

Se você pretende reverter o cluster para uma versão do ONTAP que não ofereça suporte a usuários e grupos locais e usuários e grupos locais estejam sendo usados para gerenciar o acesso a arquivos ou direitos de usuário, você deve estar ciente de certas considerações.

- Devido a razões de segurança, as informações sobre usuários locais configurados, grupos e Privileges não são excluídas quando o ONTAP é revertido para uma versão que não suporta a funcionalidade de usuários locais e grupos.
- Após a reversão para uma versão principal anterior do ONTAP, o ONTAP não usa usuários e grupos locais durante a autenticação e criação de credenciais.
- Os utilizadores e grupos locais não são removidos das ACLs de ficheiros e pastas.
- Solicitações de acesso a arquivos que dependem do acesso concedido devido às permissões concedidas a usuários ou grupos locais são negadas.

  Para permitir o acesso, você deve reconfigurar as permissões de arquivo para permitir o acesso com base em objetos de domínio em vez de objetos de usuário local e grupo.

O que são os Privileges locais

Lista de Privileges suportados

O ONTAP tem um conjunto predefinido de Privileges suportados. Alguns grupos locais predefinidos têm alguns desses Privileges adicionados a eles por padrão. Você também pode adicionar ou remover Privileges dos grupos predefinidos ou criar novos usuários ou grupos locais e adicionar Privileges aos grupos criados ou aos usuários e grupos de domínio existentes.

A tabela a seguir lista os Privileges suportados na máquina virtual de armazenamento (SVM) e fornece uma lista de grupos BUILTIN com Privileges atribuídos:

Nome do privilégio	Configuração de segurança padrão	Descrição
`SeTcbPrivilege`	Nenhum	Agir como parte do sistema operacional

Nome do privilégio	Configuração de segurança padrão	Descrição
`SeBackupPrivilege`	`BUILTIN\Administrators, BUILTIN\Backup Operators`	Faça backup de arquivos e diretórios, substituindo quaisquer ACLs
`SeRestorePrivilege`	`BUILTIN\Administrators, BUILTIN\Backup Operators`	Restaure arquivos e diretórios, substituindo qualquer ACLs defina qualquer SID válido de usuário ou grupo como proprietário do arquivo
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	Assuma a propriedade de arquivos ou outros objetos
`SeSecurityPrivilege`	`BUILTIN\Administrators`	Gerenciar a auditoria Isso inclui a visualização, o dumping e a limpeza do log de segurança.
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators BUILTIN\Backup Operators,, BUILTIN\Power Users BUILTIN\Users,,,Everyone`	Verificação da travessa de derivação Os usuários com esse privilégio não são obrigados a ter permissões de avanço (x) para percorrer pastas, links simbólicos ou junções.

Informações relacionadas

- Atribuir Privileges local
- Configuração da verificação transversal de derivação

Atribuir Privileges

Você pode atribuir Privileges diretamente a usuários locais ou usuários de domínio. Como alternativa, você pode atribuir usuários a grupos locais cujos Privileges atribuídos correspondem aos recursos que você deseja que esses usuários tenham.

- Você pode atribuir um conjunto de Privileges a um grupo que você criar.

  Em seguida, adicione um utilizador ao grupo que tem o Privileges que pretende que esse utilizador tenha.

- Você também pode atribuir usuários locais e usuários de domínio a grupos predefinidos cujo Privileges padrão corresponde ao Privileges que você deseja conceder a esses usuários.

Informações relacionadas

- Adicionando Privileges a usuários ou grupos locais ou de domínio
- Removendo Privileges de usuários ou grupos locais ou de domínio

- Redefinir o Privileges para usuários e grupos locais ou de domínio
- Configuração da verificação transversal de derivação

Diretrizes para usar grupos BUILTIN e a conta de administrador local

Há certas diretrizes que você deve ter em mente quando você usa grupos BUILTIN e a conta de administrador local. Por exemplo, você pode renomear a conta de administrador local, mas não pode excluir essa conta.

- A conta de administrador pode ser renomeada, mas não pode ser excluída.
- A conta de administrador não pode ser removida do grupo BUILTIN/Administradores.
- Os grupos DE COMPILAÇÃO podem ser renomeados, mas não podem ser excluídos.

  Depois que o grupo BUILTIN é renomeado, outro objeto local pode ser criado com o nome conhecido; no entanto, o objeto recebe um novo RID.

- Não existe uma conta de convidado local.

Informações relacionadas

Grupos BUILTIN predefinidos e Privileges padrão

Requisitos para senhas de usuários locais

Por padrão, as senhas de usuário local devem atender aos requisitos de complexidade. Os requisitos de complexidade de senha são semelhantes aos requisitos definidos na política de segurança local do Microsoft Windows *diretiva de segurança*.

A senha deve atender aos seguintes critérios:

- Deve ter pelo menos seis carateres de comprimento
- Não deve conter o nome da conta de utilizador
- Deve conter carateres de pelo menos três das quatro categorias seguintes:
  - Carateres maiúsculos em inglês (A a Z)
  - Carateres minúsculos em inglês (a a z)
  - Base 10 dígitos (0 a 9)
  - Carateres especiais:

    i. ! ( ) [ ] : ; " ' > , . ? /

Informações relacionadas

Ativar ou desativar a complexidade de senha necessária para usuários SMB locais

Exibindo informações sobre as configurações de segurança do servidor CIFS

Alterando senhas de contas de usuário locais

Grupos BUILTIN predefinidos e Privileges padrão

Você pode atribuir a associação de um usuário local ou usuário de domínio a um conjunto predefinido de grupos BUILTIN fornecidos pelo ONTAP. Grupos predefinidos têm Privileges predefinidos atribuídos.

A tabela a seguir descreve os grupos predefinidos:

Grupo BUILTIN predefinido	Privileges padrão
`BUILTIN\Administrators`LIVRAR-SE 544 Quando criada pela primeira vez, a conta local `Administrator`, com um RID de 500, é automaticamente feita um membro deste grupo. Quando a máquina virtual de storage (SVM) é unida a um domínio, o `domain\Domain Admins` grupo é adicionado ao grupo. Se o SVM sair do domínio, o `domain\Domain Admins` grupo será removido do grupo.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`LIVRAR-SE 547 Quando criado pela primeira vez, este grupo não tem nenhum membro. Os membros deste grupo têm as seguintes caraterísticas: • Pode criar e gerenciar usuários e grupos locais. • Não é possível adicionar a si mesmos ou qualquer outro objeto ao `BUILTIN\Administrators` grupo.	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`LIVRAR-SE 551 Quando criado pela primeira vez, este grupo não tem nenhum membro. Os membros deste grupo podem substituir as permissões de leitura e gravação em arquivos ou pastas se forem abertos com intenção de backup.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`LIVRAR-SE 545 Quando criado pela primeira vez, este grupo não tem nenhum membro (além do grupo especial implícito `Authenticated Users`). Quando o SVM é associado a um domínio, o `domain\Domain Users` grupo é adicionado a esse grupo. Se o SVM sair do domínio, o `domain\Domain Users` grupo será removido desse grupo.	`SeChangeNotifyPrivilege`

Grupo BUILTIN predefinido	Privileges padrão
`Everyone`SID S-1-1-0 Este grupo inclui todos os utilizadores, incluindo convidados (mas não utilizadores anónimos). Este é um grupo implícito com uma associação implícita.	`SeChangeNotifyPrivilege`

Informações relacionadas

Diretrizes para usar grupos BUILTIN e a conta de administrador local

Lista de Privileges suportados

Configuração da verificação transversal de derivação

Ativar ou desativar a funcionalidade de utilizadores e grupos locais

Ative ou desative a visão geral da funcionalidade de usuários e grupos locais

Antes de poder utilizar utilizadores e grupos locais para o controlo de acesso de dados de estilo de segurança NTFS, a funcionalidade de grupo e utilizador local tem de estar ativada. Além disso, se você quiser usar usuários locais para autenticação SMB, a funcionalidade de autenticação de usuário local deve estar ativada.

A funcionalidade de utilizadores e grupos locais e a autenticação de utilizadores locais são ativadas por predefinição. Se eles não estiverem ativados, você deverá ativá-los antes de configurar e usar usuários e grupos locais. Você pode desativar a funcionalidade de usuários e grupos locais a qualquer momento.

Além de desabilitar explicitamente a funcionalidade de usuário local e grupo, o ONTAP desabilita a funcionalidade de usuário local e grupo se qualquer nó no cluster for revertido para uma versão do ONTAP que não ofereça suporte à funcionalidade. A funcionalidade de usuário e grupo local não é ativada até que todos os nós do cluster estejam executando uma versão do ONTAP que o suporte.

Informações relacionadas

Modificar contas de usuário locais

Modificar grupos locais

Adicione Privileges a usuários ou grupos locais ou de domínio

Ative ou desative usuários e grupos locais

Você pode ativar ou desativar usuários locais e grupos para acesso SMB em máquinas virtuais de armazenamento (SVMs). A funcionalidade de utilizadores e grupos locais está ativada por predefinição.

Sobre esta tarefa

Você pode usar usuários e grupos locais ao configurar permissões de compartilhamento SMB e arquivos NTFS e pode, opcionalmente, usar usuários locais para autenticação ao criar uma conexão SMB. Para utilizar utilizadores locais para autenticação, também tem de ativar a opção de autenticação utilizadores locais e grupos.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser que os usuários e grupos locais sejam…	Digite o comando…
Ativado	`vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled true`
Desativado	`vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled false`

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O exemplo a seguir habilita a funcionalidade de usuários e grupos locais no SVM VS1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

Informações relacionadas

Ativar ou desativar a autenticação de utilizador local

Ativar ou desativar contas de utilizador locais

Ativar ou desativar a autenticação de utilizador local

Você pode ativar ou desativar a autenticação de usuário local para acesso SMB em máquinas virtuais de armazenamento (SVMs). O padrão é permitir a autenticação de usuário local, o que é útil quando o SVM não pode entrar em Contato com um controlador de domínio ou se você optar por não usar controles de acesso em nível de domínio.

Antes de começar

A funcionalidade de usuários e grupos locais deve estar ativada no servidor CIFS.

Sobre esta tarefa

Você pode ativar ou desativar a autenticação de usuário local a qualquer momento. Se você quiser usar usuários locais para autenticação ao criar uma conexão SMB, também deverá ativar a opção usuários e grupos locais do servidor CIFS.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser que a autenticação local seja…	Digite o comando…
Ativado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
Desativado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O exemplo a seguir habilita a autenticação de usuário local no SVM VS1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Informações relacionadas

Como funciona a autenticação de usuário local

Ativar ou desativar utilizadores e grupos locais

Gerenciar contas de usuários locais

Modificar contas de usuário locais

Você pode modificar uma conta de usuário local se quiser alterar o nome completo ou a descrição de um usuário existente e se quiser ativar ou desativar a conta de usuário. Você também pode renomear uma conta de usuário local se o nome do usuário estiver comprometido ou se uma alteração de nome for necessária para fins administrativos.

Se você quiser…	Digite o comando…
Modifique o nome completo do usuário local	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-full-name text` Se o nome completo contiver um espaço, ele deve ser incluído entre aspas duplas.
Modifique a descrição do usuário local	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-description text` Se a descrição contém um espaço, então ele deve ser fechado dentro de aspas duplas.
Ative ou desative a conta de utilizador local	`vserver cifs users-and-groups local-user modify -vserver` *vserver_name* -user-name *user_name* -is -account-disabled {true
false}`	Renomeie a conta de usuário local

Exemplo

O exemplo a seguir renomeia o usuário local "'CIFS_SERVER'" para "'CIFS_Server' sue_new'" na máquina virtual de armazenamento (SVM, anteriormente conhecida como SVM) VS1:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Ativar ou desativar contas de utilizador locais

Você ativa uma conta de usuário local se quiser que o usuário possa acessar os dados contidos na máquina virtual de armazenamento (SVM) em uma conexão SMB. Você também pode desativar uma conta de usuário local se não quiser que esse usuário acesse dados do SVM em SMB.

Sobre esta tarefa

Você ativa um usuário local modificando a conta de usuário.

Passo

1. Execute a ação apropriada:

Se você quiser…	Digite o comando…
Ative a conta de utilizador	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled false`

Se você quiser…	Digite o comando…
Desative a conta de usuário	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled true`

Altere as senhas da conta de usuário local

Pode alterar a palavra-passe da conta de um utilizador local. Isso pode ser útil se a senha do usuário for comprometida ou se o usuário tiver esquecido a senha.

Passo

1. Altere a senha executando a ação apropriada: `vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name`

Exemplo

O exemplo a seguir define a senha do usuário local "'CIFS_Server'" associada à máquina virtual de armazenamento (SVM, anteriormente conhecida como SVM) VS1:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

Informações relacionadas

Ativar ou desativar a complexidade de senha necessária para usuários SMB locais

Exibindo informações sobre as configurações de segurança do servidor CIFS

Exibir informações sobre usuários locais

Você pode exibir uma lista de todos os usuários locais em um formulário de resumo. Se você quiser determinar quais configurações de conta estão configuradas para um usuário específico, você pode exibir informações detalhadas de conta para esse usuário, bem como as informações de conta para vários usuários. Essas informações podem ajudá-lo a determinar se você precisa modificar as configurações de um usuário e também solucionar problemas de autenticação ou acesso a arquivos.

Sobre esta tarefa

As informações sobre a palavra-passe de um utilizador nunca são apresentadas.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Exibir informações sobre todos os usuários na máquina virtual de storage (SVM)	`vserver cifs users-and-groups local-user show -vserver vserver_name`
Exibir informações detalhadas da conta para um usuário	`vserver cifs users-and-groups local-user show -instance -vserver vserver_name -user-name user_name`

Há outros parâmetros opcionais que você pode escolher quando você executa o comando. Consulte a página de manual para obter mais informações.

Exemplo

O exemplo a seguir exibe informações sobre todos os usuários locais no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- ---------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue   Jones
```

Exibir informações sobre associações de grupos para usuários locais

Você pode exibir informações sobre os grupos locais aos quais um usuário local pertence. Você pode usar essas informações para determinar qual acesso o usuário deve ter aos arquivos e pastas. Essas informações podem ser úteis para determinar quais direitos de acesso o usuário deve ter a arquivos e pastas ou ao solucionar problemas de acesso ao arquivo.

Sobre esta tarefa

Você pode personalizar o comando para exibir apenas as informações que deseja ver.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Exibir informações de associação de usuário local para um usuário local especificado	`vserver cifs users-and-groups local-user show-membership -user-name user_name`
Exibir informações de associação de usuários locais para o grupo local do qual esse usuário local é membro	`vserver cifs users-and-groups local-user show-membership -membership group_name`

Se você quiser…	Digite o comando…
Exibir informações de associação de usuários para usuários locais associados a uma máquina virtual de armazenamento (SVM) especificada	`vserver cifs users-and-groups local-user show-membership -vserver` *vserver_name*
Exibir informações detalhadas de todos os usuários locais em um SVM especificado	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *vserver_name*

Exemplo

O exemplo a seguir exibe as informações de associação para todos os usuários locais no SVM VS1; o usuário "CIFS_SERVER" é membro do grupo "BUILTIN" Administradores, e "'CIFS_Server'" é membro do grupo "'CIFS_Server' G1":

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                    Membership
---------- ---------------------------- ----------------------
vs1        CIFS_SERVER\Administrator    BUILTIN\Administrators
           CIFS_SERVER\sue              CIFS_SERVER\g1
```

Eliminar contas de utilizador locais

Você pode excluir contas de usuários locais da máquina virtual de storage (SVM) se elas não forem mais necessárias para a autenticação SMB local para o servidor CIFS ou para determinar os direitos de acesso aos dados contidos no SVM.

Sobre esta tarefa

Tenha em mente o seguinte ao excluir usuários locais:

- O sistema de ficheiros não foi alterado.

  Os descritores de segurança do Windows em arquivos e diretórios que se referem a esse usuário não são ajustados.

- Todas as referências a usuários locais são removidas dos bancos de dados de associação e Privileges.
- Usuários padrão e bem conhecidos, como Administrador, não podem ser excluídos.

Passos

1. Determine o nome da conta de usuário local que você deseja excluir: `vserver cifs users-and-groups local-user show -vserver` *vserver_name*
2. Eliminar o utilizador local: `vserver cifs users-and-groups local-user delete -vserver` *vserver_name* `-user-name` *username_name*
3. Verifique se a conta de usuário foi excluída: `vserver cifs users-and-groups local-user show -vserver` *vserver_name*

Exemplo

O exemplo a seguir exclui o usuário local "'CIFS_Server'" associado ao SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

Gerenciar grupos locais

Modificar grupos locais

Você pode modificar grupos locais existentes alterando a descrição de um grupo local existente ou renomeando o grupo.

Se você quiser…	Use o comando…
Modifique a descrição do grupo local	`vserver cifs users-and-groups local-group modify -vserver` *`vserver_name`* `-group-name` *`group_name`* `-description text` Se a descrição contém um espaço, então ele deve ser fechado dentro de aspas duplas.
Renomeie o grupo local	`vserver cifs users-and-groups local-group rename -vserver` *`vserver_name`* `-group-name` *`group_name`* `-new-group-name` *`new_group_name`*

Exemplos

O exemplo a seguir renomeia o grupo local "'CIFS_SERVER' Engineering" para "'CIFS_Server' Engineering_new'":

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

O exemplo a seguir modifica a descrição do grupo local "'CIFS_SERVER' Engineering":

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Exibir informações sobre grupos locais

É possível exibir uma lista de todos os grupos locais configurados no cluster ou em uma máquina virtual de armazenamento (SVM) especificada. Essas informações podem ser úteis ao solucionar problemas de acesso a arquivos para dados contidos no SVM ou problemas de direitos de usuário (privilégios) no SVM.

Passo

1. Execute uma das seguintes ações:

Se você quiser informações sobre…	Digite o comando…
Todos os grupos locais no cluster	`vserver cifs users-and-groups local-group show`
Todos os grupos locais no SVM	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

   Há outros parâmetros opcionais que você pode escolher quando você executar este comando. Consulte a página de manual para obter mais informações.

Exemplo

O exemplo a seguir exibe informações sobre todos os grupos locais no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                  Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative privileges
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Gerenciar a associação ao grupo local

Você pode gerenciar a associação de grupo local adicionando e removendo usuários locais ou de domínio ou adicionando e removendo grupos de domínio. Isso é útil se você quiser controlar o acesso a dados com base nos controles de acesso colocados no grupo ou se quiser que os usuários tenham o Privileges associado a esse grupo.

Sobre esta tarefa

Diretrizes para adicionar membros a um grupo local:

- Você não pode adicionar usuários ao grupo especial *todos*.
- O grupo local deve existir antes de poder adicionar um utilizador a ele.
- O utilizador tem de existir antes de poder adicionar o utilizador a um grupo local.
- Não é possível adicionar um grupo local a outro grupo local.
- Para adicionar um usuário ou grupo de domínio a um grupo local, o Data ONTAP deve ser capaz de resolver o nome para um SID.

Diretrizes para remover membros de um grupo local:

- Você não pode remover membros do grupo especial *todos*.
- O grupo do qual você deseja remover um membro deve existir.
- O ONTAP deve ser capaz de resolver os nomes dos membros que você deseja remover do grupo para um SID correspondente.

Passo

1. Adicione ou remova um membro em um grupo.

Se você quiser…	Em seguida, use o comando…
Adicione um membro a um grupo	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Você pode especificar uma lista delimitada por vírgulas de usuários locais, usuários de domínio ou grupos de domínio para adicionar ao grupo local especificado.
Remova um membro de um grupo	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Você pode especificar uma lista delimitada por vírgulas de usuários locais, usuários de domínio ou grupos de domínio a serem removidos do grupo local especificado.

O exemplo a seguir adiciona um usuário local "'SMB_SERVER'" e um grupo de domínio "'AD_Dom_eng'" ao grupo local "'SMB_SERVER' Engineering" no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

O exemplo a seguir remove os usuários locais "'SMB_SERVER'" e "'SMB_SERVER' james' do grupo local "'SMB_Server' Engineering" no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Informações relacionadas

Exibindo informações sobre membros de grupos locais

Exibir informações sobre membros de grupos locais

É possível exibir uma lista de todos os membros de grupos locais configurados no cluster ou em uma máquina virtual de armazenamento especificada (SVM). Essas informações podem ser úteis ao solucionar problemas de acesso a arquivos ou problemas de direitos de usuário (privilégios).

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite o comando…
Membros de todos os grupos locais no cluster	`vserver cifs users-and-groups local-group show-members`
Membros de todos os grupos locais no SVM	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir exibe informações sobre membros de todos os grupos locais no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- --------------------------- ----------------------
vs1       BUILTIN\Administrators       CIFS_SERVER\Administrator
                                       AD_DOMAIN\Domain Admins
                                       AD_DOMAIN\dom_grp1
          BUILTIN\Users                AD_DOMAIN\Domain Users
                                       AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering      CIFS_SERVER\james
```

Eliminar um grupo local

Você poderá excluir um grupo local da máquina virtual de storage (SVM) se não for mais necessário para determinar direitos de acesso a dados associados a esse SVM ou se não for mais necessário atribuir direitos de usuário (Privileges) a membros do grupo.

Sobre esta tarefa

Tenha em mente o seguinte ao excluir grupos locais:

- O sistema de ficheiros não foi alterado.

  Os descritores de segurança do Windows em arquivos e diretórios que se referem a esse grupo não são ajustados.

- Se o grupo não existir, um erro será retornado.
- O grupo especial *todos* não pode ser excluído.
- Grupos internos, como *BUILTIN__BUILTIN/Users*, não podem ser excluídos.

Passos

1. Determine o nome do grupo local que você deseja excluir exibindo a lista de grupos locais no SVM: `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Eliminar o grupo local: `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. Verifique se o grupo foi excluído: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir exclui o grupo local "CIFS_SERVER" associado ao SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
```

Atualizar nomes de usuários e grupos de domínio em bancos de dados locais

Você pode adicionar usuários e grupos de domínio aos grupos locais de um servidor CIFS. Esses objetos de domínio são registrados em bancos de dados locais no cluster. Se um objeto de domínio for renomeado, os bancos de dados locais devem ser atualizados manualmente.

Sobre esta tarefa

Você deve especificar o nome da máquina virtual de armazenamento (SVM) na qual deseja atualizar nomes de domínio.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute a ação apropriada:

Se você quiser atualizar usuários e grupos de domínio e…	Use este comando…
Exibir usuários e grupos de domínio que foram atualizados com êxito e que falharam na atualização	`vserver cifs users-and-groups update-names -vserver` *vserver_name*

Se você quiser atualizar usuários e grupos de domínio e…	Use este comando…
Exibir usuários e grupos de domínio que foram atualizados com êxito	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
Exiba apenas os usuários e grupos de domínio que não conseguem atualizar	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true`
Suprimir todas as informações de status sobre atualizações	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true`

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O exemplo a seguir atualiza os nomes de usuários e grupos de domínio associados à máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1. Para a última atualização, há uma cadeia de nomes dependente que precisa ser atualizada:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

Gerenciar Privileges local

Adicione Privileges a usuários ou grupos locais ou de domínio

Você pode gerenciar os direitos de usuário para usuários ou grupos locais ou de domínio adicionando o Privileges. O Privileges adicionado substitui o Privileges padrão atribuído a qualquer um desses objetos. Isso fornece segurança aprimorada, permitindo que você personalize o que o Privileges um usuário ou grupo tem.

Antes de começar

O usuário ou grupo local ou domínio ao qual o Privileges será adicionado já deve existir.

Sobre esta tarefa

Adicionar um privilégio a um objeto substitui o Privileges padrão para esse usuário ou grupo. Adicionar um privilégio não remove Privileges adicionados anteriormente.

Você deve ter em mente o seguinte ao adicionar o Privileges a usuários ou grupos locais ou de domínio:

- Você pode adicionar um ou mais Privileges.
- Ao adicionar Privileges a um usuário ou grupo de domínio, o ONTAP pode validar o usuário ou grupo de domínio contatando o controlador de domínio.

  O comando pode falhar se o ONTAP não conseguir entrar em Contato com o controlador de domínio.

Passos

1. Adicione um ou mais Privileges a um usuário ou grupo local ou de domínio: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Verifique se os Privileges desejados são aplicados ao objeto: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemplo

O exemplo a seguir adiciona o "SeTcbPrivilege" e o "SeTakeOwnershipPrivilege" do Privileges ao usuário ""SERVIDOR_Sue"" na máquina virtual de armazenamento (SVM, anteriormente conhecida como CIFS) VS1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege
```

Remova o Privileges de usuários ou grupos locais ou de domínio

Você pode gerenciar os direitos de usuário para usuários ou grupos locais ou de domínio removendo o Privileges. Isso fornece segurança aprimorada, permitindo que você

personalize o Privileges máximo que os usuários e grupos têm.

Antes de começar

O usuário ou grupo local ou domínio do qual o Privileges será removido já deve existir.

Sobre esta tarefa

Você deve ter em mente o seguinte ao remover o Privileges de usuários ou grupos locais ou de domínio:

- Você pode remover um ou mais Privileges.
- Ao remover o Privileges de um usuário ou grupo de domínio, o ONTAP pode validar o usuário ou grupo de domínio entrando em Contato com o controlador de domínio.

  O comando pode falhar se o ONTAP não conseguir entrar em Contato com o controlador de domínio.

Passos

1. Remova um ou mais Privileges de um usuário ou grupo local ou de domínio: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group -name _name_ -privileges _privilege_[,...]`
2. Verifique se os Privileges desejados foram removidos do objeto: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemplo

O exemplo a seguir remove o Privileges "SeTcbPrivilege" e o "SeTakeOwnershipPrivilege" do usuário ""SERVIDOR_Sue"" na máquina virtual de armazenamento (SVM, anteriormente conhecida como CIFS) VS1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

Redefinir o Privileges para usuários e grupos locais ou de domínio

Você pode redefinir o Privileges para usuários e grupos locais ou de domínio. Isso pode ser útil quando você fez modificações no Privileges para um usuário ou grupo local ou de domínio e essas modificações não são mais desejadas ou necessárias.

Sobre esta tarefa

A redefinição do Privileges para um usuário ou grupo local ou de domínio remove quaisquer entradas de privilégio para esse objeto.

Passos

1. Redefina o Privileges em um usuário ou grupo local ou de domínio: `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. Verifique se os Privileges são redefinidos no objeto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Exemplos

O exemplo a seguir redefine o Privileges no usuário "CIFS_SERVER" na máquina virtual de armazenamento (SVM, anteriormente conhecida como SVM) VS1. Por padrão, os usuários normais não têm o Privileges associado às suas contas:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

O exemplo a seguir redefine o Privileges para o grupo "Administradores", removendo efetivamente a entrada de privilégio:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ----------------------- ------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Exibir informações sobre substituições de privilégios

Você pode exibir informações sobre Privileges personalizados atribuídos a grupos ou

contas de usuário locais ou de domínio. Essas informações ajudam a determinar se os direitos de usuário desejados são aplicados.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite este comando…
Privileges personalizado para todos os usuários e grupos de domínio e locais na máquina virtual de storage (SVM)	`vserver cifs users-and-groups privilege show -vserver vserver_name`
Privileges personalizado para um domínio específico ou usuário local e grupo no SVM	`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

   Há outros parâmetros opcionais que você pode escolher quando você executar este comando. Consulte a página de manual para obter mais informações.

Exemplo

O comando a seguir exibe todos os Privileges explicitamente associados a usuários e grupos locais ou de domínio para o SVM VS1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
---------- ---------------------  ---------------
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1        CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

Configure a verificação de desvio transversal

Configure a visão geral da verificação da travessia de derivação

A verificação de desvio transversal é um direito de usuário (também conhecido como *privilégio*) que determina se um usuário pode percorrer todos os diretórios no caminho para um arquivo, mesmo que o usuário não tenha permissões no diretório atravessado. Você deve entender o que acontece ao permitir ou desativar a verificação de desvio transversal e como configurar a verificação de desvio transversal para usuários em máquinas virtuais de armazenamento (SVMs).

O que acontece ao permitir ou ao desativar a verificação transversal de desvio

- Se permitido, quando um usuário tenta acessar um arquivo, o ONTAP não verifica a permissão de avanço para os diretórios intermediários ao determinar se deve conceder ou negar acesso ao arquivo.

- Se não for permitido, o ONTAP verifica a permissão de avanço (execução) para todos os diretórios no caminho para o arquivo.

  Se qualquer um dos diretórios intermediários não tiver o "X" (permissão de avanço), o ONTAP nega o acesso ao arquivo.

Configure a verificação de desvio transversal

Você pode configurar a verificação de desvio transversal usando a CLI do ONTAP ou configurando políticas de grupo do ative Directory com esse direito de usuário.

O `SeChangeNotifyPrivilege` privilégio controla se os usuários têm permissão para ignorar a verificação transversal.

- Adicioná-lo a usuários ou grupos SMB locais na SVM ou a usuários ou grupos de domínio permite a verificação de desvio transversal.
- Removê-lo de usuários ou grupos SMB locais no SVM ou de usuários ou grupos de domínio não permite a verificação de desvio transversal.

Por padrão, os seguintes grupos BUILTIN no SVM têm o direito de ignorar a verificação transversal:

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

Se você não quiser permitir que membros de um desses grupos ignorem a verificação transversal, você deve remover esse privilégio do grupo.

Você deve ter em mente o seguinte ao configurar a verificação de desvio transversal para usuários e grupos SMB locais no SVM usando a CLI:

- Se você quiser permitir que membros de um grupo de domínio ou local personalizado ignorem a verificação transversal, você deve adicionar o `SeChangeNotifyPrivilege` privilégio a esse grupo.
- Se você quiser permitir que um usuário local ou de domínio individual ignore a verificação transversal e que o usuário não seja membro de um grupo com esse privilégio, você pode adicionar o `SeChangeNotifyPrivilege` privilégio a essa conta de usuário.
- Você pode desativar a verificação de desvio transversal para usuários ou grupos locais ou de domínio removendo o `SeChangeNotifyPrivilege` privilégio a qualquer momento.

> Para desativar a verificação de desvio de travers para usuários ou grupos locais ou de domínio especificados, você também deve remover o `SeChangeNotifyPrivilege` privilégio do `Everyone` grupo.

Informações relacionadas

Permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Não permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Configure o mapeamento de carateres para a tradução de nomes de arquivo SMB em volumes

Criar listas de controle de acesso de compartilhamento SMB

Proteja o acesso aos arquivos usando o Storage-Level Access Guard

Lista de Privileges suportados

Adicione Privileges a usuários ou grupos locais ou de domínio

Permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Se você quiser que um usuário possa percorrer todos os diretórios no caminho para um arquivo, mesmo que o usuário não tenha permissões em um diretório atravessado, você pode adicionar o `SeChangeNotifyPrivilege` privilégio a usuários ou grupos SMB locais em máquinas virtuais de armazenamento (SVMs). Por padrão, os usuários são capazes de ignorar a verificação de rotação do diretório.

Antes de começar

- Um servidor SMB deve estar presente na SVM.
- A opção local Users and Groups SMB Server (usuários locais e grupos) deve estar ativada.
- O usuário ou grupo local ou domínio ao qual o `SeChangeNotifyPrivilege` privilégio será adicionado já deve existir.

Sobre esta tarefa

Ao adicionar Privileges a um usuário ou grupo de domínio, o ONTAP pode validar o usuário ou grupo de domínio contatando o controlador de domínio. O comando pode falhar se o ONTAP não puder entrar em Contato com o controlador de domínio.

Passos

1. Ative a verificação de desvio transversal adicionando o `SeChangeNotifyPrivilege` privilégio a um usuário ou grupo local ou de domínio: `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   O valor para o `-user-or-group-name` parâmetro é um usuário ou grupo local, ou um usuário ou grupo de domínio.

2. Verifique se o usuário ou grupo especificado tem a verificação transversal de desvio ativada: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemplo

O comando a seguir permite que os usuários que pertencem ao grupo "'EXAMPLE'" ignorem a verificação da rotação do diretório adicionando o `SeChangeNotifyPrivilege` privilégio ao grupo:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege
```

Informações relacionadas

Não permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Não permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Se você não quiser que um usuário percorra todos os diretórios no caminho para um arquivo porque o usuário não tem permissões no diretório atravessado, você pode remover o `SeChangeNotifyPrivilege` privilégio de usuários SMB locais ou grupos em máquinas virtuais de armazenamento (SVMs).

Antes de começar

O usuário ou grupo local ou domínio do qual o Privileges será removido já deve existir.

Sobre esta tarefa

Ao remover o Privileges de um usuário ou grupo de domínio, o ONTAP pode validar o usuário ou grupo de domínio entrando em Contato com o controlador de domínio. O comando pode falhar se o ONTAP não puder entrar em Contato com o controlador de domínio.

Passos

1. Não permitir a verificação da travessa de derivação: `vserver cifs users-and-groups privilege remove-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   O comando remove o `SeChangeNotifyPrivilege` privilégio do usuário ou grupo local ou domínio que você especificar com o valor do `-user-or-group-name` *`name`* parâmetro.

2. Verifique se o usuário ou grupo especificado tem verificação de desvio de rotação desativada: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemplo

O comando a seguir despermite que os usuários que pertencem ao grupo "'EXAMPLE'" ignorem a verificação da rotação do diretório:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ----------------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ----------------------
vs1       EXAMPLE\eng           -
```

Informações relacionadas

Permitir que usuários ou grupos ignorem a verificação de rotação do diretório

Exibir informações sobre segurança de arquivos e diretivas de auditoria

Exibir informações sobre a visão geral das políticas de auditoria e segurança de arquivos

Você pode exibir informações sobre segurança de arquivos em arquivos e diretórios contidos em volumes em máquinas virtuais de armazenamento (SVMs). Você pode exibir informações sobre políticas de auditoria no FlexVol volumes. Se configurado, você pode exibir informações sobre as configurações de segurança do Guarda de Acesso em nível de armazenamento e Controle Dinâmico de Acesso no FlexVol volumes.

Exibindo informações sobre segurança de arquivos

Você pode exibir informações sobre a segurança de arquivos aplicada a dados contidos em volumes e qtrees (para volumes FlexVol) com os seguintes estilos de segurança:

- NTFS
- UNIX
- Misto

Exibindo informações sobre políticas de auditoria

Você pode exibir informações sobre políticas de auditoria para auditar eventos de acesso em volumes do FlexVol nos seguintes protocolos nas:

- SMB (todas as versões)
- NFSv4.x

Exibindo informações sobre a segurança do Storage-Level Access Guard (SLAG)

A segurança do Access Guard no nível de storage pode ser aplicada em volumes e objetos de qtree do FlexVol com os seguintes estilos de segurança:

- NTFS
- Misto
- UNIX (se um servidor CIFS estiver configurado na SVM que contém o volume)

Apresentar informações sobre a segurança do controlo de acesso dinâmico (DAC)

A segurança do controle de acesso dinâmico pode ser aplicada em um objeto dentro de um FlexVol volume com os seguintes estilos de segurança:

- NTFS
- Misto (se o objeto tiver segurança efetiva NTFS)

Informações relacionadas

Protegendo o acesso aos arquivos usando o Storage-Level Access Guard

Exibindo informações sobre o Storage-Level Access Guard

Exibir informações sobre segurança de arquivos em volumes de estilo de segurança NTFS

Você pode exibir informações sobre a segurança de arquivos e diretórios em volumes de estilo de segurança NTFS, incluindo o estilo de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre os atributos dos. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os dados cujas informações de segurança de arquivo ou pasta você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Como os volumes e qtrees de estilo de segurança NTFS usam apenas permissões de arquivo NTFS e usuários e grupos do Windows ao determinar direitos de acesso a arquivos, os campos de saída relacionados ao UNIX contêm informações de permissão de arquivo UNIX somente para exibição.
- A saída ACL é exibida para arquivos e pastas com segurança NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada na raiz de volume ou qtree, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard está configurado pode exibir ACLs de arquivo regulares e ACLs de Storage-Level Access Guard.
- A saída também exibe informações sobre os ACEs do Controle de Acesso Dinâmico se o Controle de Acesso Dinâmico estiver configurado para o caminho do arquivo ou diretório específico.

Passo

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver vserver_name -path path`
Com detalhes expandidos	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemplos

O exemplo a seguir exibe as informações de segurança sobre o caminho `/vol4` no SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         Security Style: ntfs
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                          Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

O exemplo a seguir exibe as informações de segurança com máscaras expandidas sobre o caminho `/data/engineering` no SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

               Vserver: vs1
             File Path: /data/engineering
     File Inode Number: 5544
```

```
          Security Style: ntfs
         Effective Style: ntfs
          DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
```

```
Generic All
                            .... ...0 .... .... .... .... .... .... =
System Security
                            .... .... ...1 .... .... .... .... .... =
Synchronize
                            .... .... .... 1... .... .... .... .... =
Write Owner
                            .... .... .... .1.. .... .... .... .... =
Write DAC
                            .... .... .... ..1. .... .... .... .... =
Read Control
                            .... .... .... ...1 .... .... .... .... =
Delete
                            .... .... .... .... .... ...1 .... .... =
Write Attributes
                            .... .... .... .... .... .... 1... .... =
Read Attributes
                            .... .... .... .... .... .... .1.. .... =
Delete Child
                            .... .... .... .... .... .... ..1. .... =
Execute
                            .... .... .... .... .... .... ...1 .... =
Write EA
                            .... .... .... .... .... .... .... 1... =
Read EA
                            .... .... .... .... .... .... .... .1.. =
Append
                            .... .... .... .... .... .... .... ..1. =
Write
                            .... .... .... .... .... .... .... ...1 =
Read

                          ALLOW-Everyone-0x10000000-OI|CI|IO
                            0... .... .... .... .... .... .... .... =
Generic Read
                            .0.. .... .... .... .... .... .... .... =
Generic Write
                            ..0. .... .... .... .... .... .... .... =
Generic Execute
                            ...1 .... .... .... .... .... .... .... =
Generic All
                            .... ...0 .... .... .... .... .... .... =
System Security
                            .... .... ...0 .... .... .... .... .... =
Synchronize
                            .... .... .... 0... .... .... .... .... =
```

```
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

O exemplo a seguir exibe informações de segurança, incluindo informações de segurança do Storage-Level Access Guard, para o volume com o caminho `/datavol1` no SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Informações relacionadas

Exibindo informações sobre segurança de arquivos em volumes mistos de estilo de segurança

Exibindo informações sobre segurança de arquivos em volumes estilo de segurança UNIX

Exibir informações sobre segurança de arquivos em volumes mistos de estilo de segurança

Você pode exibir informações sobre segurança de arquivos e diretórios em volumes mistos de estilo de segurança, incluindo o estilo de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre proprietários e grupos UNIX. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os dados cujas informações de segurança de arquivo ou pasta você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e pastas que usam permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 e alguns arquivos e diretórios que usam permissões de arquivo NTFS.
- O nível superior de um volume de estilo de segurança misto pode ter segurança eficaz UNIX ou NTFS.
- A saída ACL é exibida apenas para arquivos e pastas com segurança NTFS ou NFSv4.

  Este campo está vazio para arquivos e diretórios que usam segurança UNIX que têm somente permissões de bit de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída do proprietário e do grupo na saída da ACL aplicam-se apenas no caso de descritores de segurança NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada em um volume ou qtree misto de estilo de segurança, mesmo que o estilo de segurança efetivo da raiz de volume ou qtree seja UNIX, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard esteja configurado pode exibir tanto as permissões de arquivo UNIX quanto as ACLs Storage-Level Access Guard.
- Se o caminho inserido no comando for para dados com segurança efetiva NTFS, a saída também exibirá informações sobre ACEs de Controle de Acesso Dinâmico se o Controle de Acesso Dinâmico estiver configurado para o caminho de arquivo ou diretório dado.

Passo

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver vserver_name -path path`
Com detalhes expandidos	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemplos

O exemplo a seguir exibe as informações de segurança sobre o caminho `/projects` no SVM VS1 no formulário de máscara expandida. Este caminho de estilo de segurança misto tem segurança eficaz UNIX.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

               Vserver: vs1
             File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

O exemplo a seguir exibe as informações de segurança sobre o caminho `/data` no SVM VS1. Este caminho misto de estilo de segurança tem uma segurança eficaz NTFS.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

O exemplo a seguir exibe as informações de segurança sobre o volume no caminho `/datavol5` no SVM VS1. O nível superior deste volume misto de estilo de segurança tem segurança eficaz UNIX. O volume tem segurança Storage-Level Access Guard.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

Informações relacionadas

Exibindo informações sobre segurança de arquivos em volumes de estilo de segurança NTFS

Exibindo informações sobre segurança de arquivos em volumes estilo de segurança UNIX

Exibir informações sobre segurança de arquivos em volumes estilo de segurança UNIX

Você pode exibir informações sobre segurança de arquivos e diretórios em volumes estilo de segurança UNIX, incluindo quais são os estilos de segurança e estilos de

segurança eficazes, quais permissões são aplicadas e informações sobre proprietários e grupos UNIX. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os dados cujas informações de segurança de arquivo ou diretório você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Os volumes e qtrees de estilo de segurança UNIX usam apenas permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 ao determinar direitos de acesso a arquivos.
- A saída ACL é exibida apenas para arquivos e pastas com segurança NFSv4.

  Este campo está vazio para arquivos e diretórios que usam segurança UNIX que têm somente permissões de bit de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída de proprietário e grupo na saída ACL não se aplicam no caso de descritores de segurança NFSv4.

  Eles são apenas significativos para descritores de segurança NTFS.

- Como a segurança do Storage-Level Access Guard é suportada em um volume ou qtree UNIX se um servidor CIFS estiver configurado no SVM, a saída pode conter informações sobre a segurança do Storage-Level Access Guard aplicada ao volume ou qtree especificado no `-path` parâmetro.

Passo

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Com detalhes expandidos	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Exemplos

O exemplo a seguir exibe as informações de segurança sobre o caminho `/home` no SVM VS1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

O exemplo a seguir exibe as informações de segurança sobre o caminho `/home` no SVM VS1 no formulário de máscara expandida:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
                    .... .... ..0. .... = Archive
                    .... .... ...1 .... = Directory
                    .... .... .... .0.. = System
                    .... .... .... ..0. = Hidden
                    .... .... .... ...0 = Read Only
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

Informações relacionadas

Exibindo informações sobre segurança de arquivos em volumes de estilo de segurança NTFS

Exibindo informações sobre segurança de arquivos em volumes mistos de estilo de segurança

Exibir informações sobre políticas de auditoria NTFS em volumes FlexVol usando a CLI

Você pode exibir informações sobre políticas de auditoria NTFS no FlexVol volumes, incluindo quais são os estilos de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre listas de controle de acesso do sistema. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de auditoria.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os arquivos ou pastas cujas informações de auditoria você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Os volumes e qtrees de estilo de segurança NTFS usam apenas as listas de controle de acesso do sistema NTFS (SACLs) para políticas de auditoria.
- Arquivos e pastas em um volume misto de estilo de segurança com segurança efetiva NTFS podem ter políticas de auditoria NTFS aplicadas a eles.

  Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e diretórios que usam permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 e alguns arquivos e diretórios que usam permissões de arquivo NTFS.

- O nível superior de um volume de estilo de segurança misto pode ter segurança efetiva UNIX ou NTFS e pode ou não conter SACLs NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada em um volume ou qtree misto de estilo de segurança, mesmo que o estilo de segurança efetivo da raiz de volume ou qtree seja UNIX, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard está configurado pode exibir tanto o arquivo normal quanto a pasta NFSv4 SACLs e o Storage-Level Access Guard NTFS SACLs.
- Se o caminho inserido no comando for para dados com segurança efetiva NTFS, a saída também exibirá informações sobre ACEs de Controle de Acesso Dinâmico se o Controle de Acesso Dinâmico estiver configurado para o caminho do arquivo ou diretório fornecido.
- Ao exibir informações de segurança sobre arquivos e pastas com segurança efetiva NTFS, os campos de saída relacionados ao UNIX contêm informações de permissão de arquivo UNIX somente para exibição.

  Arquivos e pastas de estilo de segurança NTFS usam apenas permissões de arquivo NTFS e usuários e grupos do Windows ao determinar direitos de acesso a arquivos.

- A saída ACL é exibida apenas para arquivos e pastas com segurança NTFS ou NFSv4.

  Este campo está vazio para arquivos e pastas que usam segurança UNIX que têm apenas permissões de bits de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída do proprietário e do grupo na saída da ACL aplicam-se apenas no caso de descritores de segurança NTFS.

Passo

1. Exiba as configurações de diretiva de auditoria de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver vserver_name -path path`
Como uma lista detalhada	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemplos

O exemplo a seguir exibe as informações da política de auditoria do caminho `/corp` no SVM VS1. O caminho tem segurança eficaz NTFS. O descritor de segurança NTFS contém uma entrada SACL DE sucesso e uma entrada de sucesso/FALHA.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

O exemplo a seguir exibe as informações da política de auditoria do caminho `/datavol1` no SVM VS1. O caminho contém SACLs de arquivo e pasta regulares e SACLs de proteção de acesso em nível de armazenamento.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Exiba informações sobre as políticas de auditoria do NFSv4 em volumes do FlexVol usando a CLI

Você pode exibir informações sobre as políticas de auditoria do NFSv4 em volumes do

FlexVol usando a CLI do ONTAP, incluindo quais são os estilos de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre as listas de controle de acesso do sistema (SACLs). Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de auditoria.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os arquivos ou diretórios cujas informações de auditoria você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Os volumes e qtrees de estilo de segurança UNIX usam apenas SACLs NFSv4 para políticas de auditoria.
- Arquivos e diretórios em um volume misto de estilo de segurança que são de estilo de segurança UNIX podem ter políticas de auditoria NFSv4 aplicadas a eles.

  Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e diretórios que usam permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 e alguns arquivos e diretórios que usam permissões de arquivo NTFS.

- O nível superior de um volume de estilo de segurança misto pode ter segurança efetiva UNIX ou NTFS e pode ou não conter SACLs NFSv4.
- A saída ACL é exibida apenas para arquivos e pastas com segurança NTFS ou NFSv4.

  Este campo está vazio para arquivos e pastas que usam segurança UNIX que têm apenas permissões de bits de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída do proprietário e do grupo na saída da ACL aplicam-se apenas no caso de descritores de segurança NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada em um volume ou qtree misto de estilo de segurança, mesmo que o estilo de segurança efetivo da raiz de volume ou qtree seja UNIX, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard esteja configurado pode exibir tanto SACLs de arquivo NFSv4 regulares como de diretório e SACLs de acesso no nível de armazenamento NTFS SACLs.
- Como a segurança do Storage-Level Access Guard é suportada em um volume ou qtree UNIX se um servidor CIFS estiver configurado no SVM, a saída pode conter informações sobre a segurança do Storage-Level Access Guard aplicada ao volume ou qtree especificado no `-path` parâmetro.

Passos

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver vserver_name -path path`
Com detalhes expandidos	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemplos

O exemplo a seguir exibe as informações de segurança sobre o caminho `/lab` no SVM VS1. Este caminho de estilo de segurança UNIX tem um SACL NFSv4.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

Maneiras de exibir informações sobre segurança de arquivos e diretivas de auditoria

Você pode usar o caractere curinga (*) para exibir informações sobre segurança de arquivos e políticas de auditoria de todos os arquivos e diretórios em um determinado caminho ou volume raiz.

O caractere curinga (**) pode ser usado como o último subcomponente de um determinado caminho de diretório abaixo do qual você deseja exibir informações de todos os arquivos e diretórios. Se você quiser exibir informações de um arquivo ou diretório específico chamado "*"**, então você precisa fornecer o caminho completo dentro de aspas duplas ("*").

Exemplo

O comando a seguir com o caractere curinga exibe as informações sobre todos os arquivos e diretórios abaixo do caminho `/1/` do SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

O comando a seguir exibe as informações de um arquivo chamado "*" no caminho `/vol1/a` do SVM VS1. O caminho está entre aspas duplas (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: “/vol1/a/*”
      Security Style: mixed
     Effective Style: unix
      DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
         Unix User Id: 1002
        Unix Group Id: 65533
       Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                  ACLs: NFSV4 Security Descriptor
                        Control:0x8014
                        SACL - ACEs
                          AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                        DACL - ACEs
                          ALLOW-EVERYONE@-0x1f00a9-FI|DI
                          ALLOW-OWNER@-0x1f01ff-FI|DI
                          ALLOW-GROUP@-0x1200a9-IG
```

Gerencie a segurança de arquivos NTFS, as políticas de auditoria NTFS e o Storage-Level Access Guard em SVMs usando a CLI

Gerencie a segurança de arquivos NTFS, as políticas de auditoria NTFS e o Storage-Level Access Guard em SVMs usando a visão geral da CLI

Você pode gerenciar a segurança de arquivos NTFS, políticas de auditoria NTFS e o Storage-Level Access Guard em máquinas virtuais de armazenamento (SVMs) usando a CLI.

Você pode gerenciar políticas de segurança e auditoria de arquivos NTFS de clientes SMB ou usando a CLI. No entanto, usar a CLI para configurar políticas de segurança e auditoria de arquivos remove a necessidade de usar um cliente remoto para gerenciar a segurança de arquivos. Usar a CLI pode reduzir significativamente o tempo necessário para aplicar a segurança em muitos arquivos e pastas usando um único comando.

Você pode configurar o Storage-Level Access Guard, que é outra camada de segurança aplicada pelo ONTAP aos volumes SVM. O Storage-Level Access Guard aplica-se a acessos de todos os protocolos nas ao objeto de armazenamento ao qual o Storage-Level Access Guard é aplicado.

O protetor de acesso no nível de storage pode ser configurado e gerenciado somente a partir da CLI do ONTAP. Não é possível gerenciar as configurações do protetor de acesso em nível de armazenamento de clientes SMB. Além disso, se você exibir as configurações de segurança em um arquivo ou diretório de um

cliente NFS ou SMB, não verá a segurança Storage-Level Access Guard. A segurança do Access Guard no nível de armazenamento não pode ser revogada de um cliente, mesmo por um administrador do sistema (Windows ou UNIX). Portanto, o Storage-Level Access Guard fornece uma camada extra de segurança para o acesso aos dados que é definido e gerenciado de forma independente pelo administrador do armazenamento.

Embora apenas as permissões de acesso NTFS sejam suportadas pelo Guarda de Acesso em nível de armazenamento, o ONTAP pode executar verificações de segurança para acesso através de NFS a dados em volumes em que o Guarda de Acesso em nível de armazenamento é aplicado se o utilizador do UNIX mapear para um utilizador do Windows na SVM que possui o volume.

Volumes de estilo de segurança NTFS

Todos os arquivos e pastas contidos em volumes e qtrees de estilo de segurança NTFS têm segurança efetiva NTFS. Você pode usar a `vserver security file-directory` família de comandos para implementar os seguintes tipos de segurança em volumes de estilo de segurança NTFS:

- Permissões de arquivo e políticas de auditoria para arquivos e pastas contidos no volume
- Segurança no nível de armazenamento de acesso Guarda em volumes

Volumes mistos de estilo de segurança

Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e pastas que têm segurança efetiva UNIX e usam permissões de arquivos UNIX, bits de modo ou ACLs NFSv4.x e diretivas de auditoria NFSv4.x, e alguns arquivos e pastas que têm segurança efetiva NTFS e usam permissões de arquivos NTFS e políticas de auditoria. Você pode usar a `vserver security file-directory` família de comandos para aplicar os seguintes tipos de segurança a dados mistos de estilo de segurança:

- Permissões de arquivos e diretivas de auditoria para arquivos e pastas com o estilo de segurança eficaz NTFS no volume ou qtree misto
- Proteção de acesso no nível de armazenamento para volumes com o estilo de segurança eficaz NTFS e UNIX

Volumes de estilo de segurança UNIX

Os volumes e qtrees de estilo de segurança UNIX contêm arquivos e pastas que têm segurança efetiva UNIX (bits de modo ou ACLs NFSv4.x). Você deve ter em mente o seguinte se quiser usar a `vserver security file-directory` família de comandos para implementar a segurança em volumes estilo de segurança UNIX:

- A `vserver security file-directory` família de comandos não pode ser usada para gerenciar políticas de segurança e auditoria de arquivos UNIX em volumes e qtrees de estilo de segurança UNIX.
- Você pode usar a `vserver security file-directory` família de comandos para configurar o Storage-Level Access Guard em volumes de estilo de segurança UNIX, desde que o SVM com o volume de destino contenha um servidor CIFS.

Informações relacionadas

Exibir informações sobre segurança de arquivos e diretivas de auditoria

Configure e aplique segurança de arquivos em arquivos e pastas NTFS usando a CLI

Configure e aplique políticas de auditoria a arquivos e pastas NTFS usando a CLI

Use casos para usar a CLI para definir a segurança de arquivos e pastas

Como você pode aplicar e gerenciar a segurança de arquivos e pastas localmente sem envolvimento de um cliente remoto, você pode reduzir significativamente o tempo necessário para definir a segurança em massa em um grande número de arquivos ou pastas.

Você pode se beneficiar do uso da CLI para definir a segurança de arquivos e pastas nos seguintes casos de uso:

- Armazenamento de arquivos em grandes ambientes empresariais, como armazenamento de arquivos em diretórios base
- Migração de dados
- Mudança de domínio do Windows
- Padronização de políticas de segurança e auditoria de arquivos em sistemas de arquivos NTFS

Limites ao usar a CLI para definir a segurança de arquivos e pastas

Você precisa estar ciente de certos limites ao usar a CLI para definir a segurança de arquivos e pastas.

- A `vserver security file-directory` família de comandos não suporta a configuração de ACLs NFSv4.

  Você só pode aplicar descritores de segurança NTFS a arquivos e pastas NTFS.

Como os descritores de segurança são usados para aplicar a segurança de arquivos e pastas

Os descritores de segurança contêm as listas de controle de acesso que determinam quais ações um usuário pode executar em arquivos e pastas e o que é auditado quando um usuário acessa arquivos e pastas.

- **Permissões**

  As permissões são permitidas ou negadas pelo proprietário de um objeto e determinam quais ações um objeto (usuários, grupos ou objetos de computador) pode executar em arquivos ou pastas especificados.

- **Descritores de segurança**

  Descritores de segurança são estruturas de dados que contêm informações de segurança que definem permissões associadas a um arquivo ou pasta.

- **Listas de controle de acesso (ACLs)**

  Listas de controle de acesso são as listas contidas em um descritor de segurança que contêm informações sobre quais ações os usuários, grupos ou objetos de computador podem executar no arquivo ou pasta à qual o descritor de segurança é aplicado. O descritor de segurança pode conter os dois tipos

de ACLs a seguir:

  - Listas de controle de acesso discricionárias (DACLs)
  - Listas de controle de acesso do sistema (SACLs)

- **Listas de controle de acesso discricionárias (DACLs)**

  As DACLs contêm a lista de SIDS para os usuários, grupos e objetos de computador que têm acesso permitido ou negado para executar ações em arquivos ou pastas. As DACLs contêm zero ou mais entradas de controle de acesso (ACEs).

- **Listas de controle de acesso do sistema (SACLs)**

  Os SACLs contêm a lista de SIDS para os usuários, grupos e objetos de computador para os quais eventos de auditoria bem-sucedidos ou com falha são registrados. SACLs contêm zero ou mais entradas de controle de acesso (ACEs).

- **Entradas de Controle de Acesso (ACEs)**

  Os ases são entradas individuais em DACLs ou SACLs:

  - Uma entrada de controle de acesso DACL especifica os direitos de acesso que são permitidos ou negados para usuários, grupos ou objetos de computador específicos.
  - Uma entrada de controle de acesso SACL especifica os eventos de sucesso ou falha a serem registrados ao auditar ações especificadas executadas por determinados usuários, grupos ou objetos de computador.

- * Herança de permissão*

  A herança de permissões descreve como as permissões definidas em descritores de segurança são propagadas para um objeto de um objeto pai. Somente permissões herdáveis são herdadas por objetos filho. Ao definir permissões no objeto pai, você pode decidir se pastas, subpastas e arquivos podem herdá-los com ""aplicar a `this-folder`, `sub-folders` e 'arquivos"".

Informações relacionadas

"Auditoria de SMB e NFS e rastreamento de segurança"

Configurando e aplicando políticas de auditoria a arquivos e pastas NTFS usando a CLI

Diretrizes para a aplicação de políticas de diretório de arquivos que usam usuários locais ou grupos no destino da recuperação de desastres do SVM

Há certas diretrizes que você deve ter em mente antes de aplicar políticas de diretório de arquivos no destino de recuperação de desastres de máquina virtual de armazenamento (SVM) em uma configuração de descarte de ID se a configuração de diretiva de diretório de arquivos usar usuários locais ou grupos no descritor de segurança ou nas entradas DACL ou SACL.

Você pode configurar uma configuração de recuperação de desastre para um SVM em que o SVM de origem no cluster de origem replique os dados e a configuração da SVM de origem a um SVM de destino em um cluster de destino.

É possível configurar um dos dois tipos de recuperação de desastres da SVM:

- Identidade preservada

  Com essa configuração, a identidade do SVM e do servidor CIFS é preservada.

- Identidade descartada

  Com essa configuração, a identidade do SVM e do servidor CIFS não é preservada. Nesse cenário, o nome do SVM e do servidor CIFS no SVM de destino são diferentes do SVM e do nome do servidor CIFS na SVM de origem.

Diretrizes para configurações de identidade descartadas

Em uma configuração de identidade descartada, para uma origem SVM que contenha configurações de usuário, grupo e privilégio locais, o nome do domínio local (nome do servidor CIFS local) deve ser alterado para corresponder ao nome do servidor CIFS no destino SVM. Por exemplo, se o nome do SVM de origem for "'VS1'" e o nome do servidor CIFS for "'CIFS1 user1'", e o nome do SVM de destino for "'VS1 user1_dst'" e o nome do servidor CIFS for "'CIFS1_DST'", então o nome de domínio local para um usuário local chamado "'CIFS1'" é alterado automaticamente para "'CIFS1_DST'" no destino:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Mesmo que os nomes de usuários e grupos locais sejam alterados automaticamente nos bancos de dados de usuários e grupos locais, usuários locais ou nomes de grupos não são alterados automaticamente nas configurações de diretiva de diretório de arquivos (políticas configuradas na CLI usando a `vserver security file-directory` família de comandos).

Por exemplo, para "'VS1'", se você configurou uma entrada DACL onde o `-account` parâmetro é definido como "'CIFS1 " user1'", a configuração não será alterada automaticamente no SVM de destino para refletir o nome do servidor CIFS de destino.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

Você deve usar os `vserver security file-directory modify` comandos para alterar manualmente o nome do servidor CIFS para o nome do servidor CIFS de destino.

Componentes de configuração de diretiva de diretório de arquivos que contêm parâmetros de conta

Há três componentes de configuração de diretiva de diretório de arquivos que podem usar configurações de parâmetros que podem conter usuários ou grupos locais:

- Descritor de segurança

  Opcionalmente, você pode especificar o proprietário do descritor de segurança e o grupo principal do proprietário do descritor de segurança. Se o descritor de segurança usar um usuário ou grupo local para as entradas do proprietário e do grupo primário, você deverá modificar o descritor de segurança para usar o SVM de destino no nome da conta. Você pode usar o `vserver security file-directory ntfs modify` comando para fazer quaisquer alterações necessárias nos nomes de conta.

- Entradas DACL

  Cada entrada DACL deve ser associada a uma conta. Você deve modificar quaisquer DACLs que usem contas de usuário ou grupo locais para usar o nome do SVM de destino. Como você não pode modificar o nome da conta para entradas DACL existentes, você deve remover quaisquer entradas DACL com usuários locais ou grupos dos descritores de segurança, criar novas entradas DACL com os nomes de conta de destino corrigidos e associar essas novas entradas DACL aos descritores de segurança apropriados.

- Entradas SACL

  Cada entrada SACL deve ser associada a uma conta. Você deve modificar quaisquer SACLs que usem contas de usuário ou grupo locais para usar o nome do SVM de destino. Como você não pode modificar o

nome da conta para entradas SACL existentes, você deve remover quaisquer entradas SACL com usuários locais ou grupos dos descritores de segurança, criar novas entradas SACL com os nomes de conta de destino corrigidos e associar essas novas entradas SACL aos descritores de segurança apropriados.

Você deve fazer as alterações necessárias aos usuários locais ou grupos usados na configuração da diretiva de diretório de arquivos antes de aplicar a diretiva; caso contrário, a tarefa aplicar falha.

Configure e aplique segurança de arquivos em arquivos e pastas NTFS usando a CLI

Crie um descritor de segurança NTFS

Criar um descritor de segurança NTFS (política de segurança de arquivos) é a primeira etapa na configuração e aplicação de listas de controle de acesso (ACLs) NTFS a arquivos e pastas residentes em máquinas virtuais de armazenamento (SVMs). Você pode associar o descritor de segurança ao caminho do arquivo ou da pasta em uma tarefa de diretiva.

Sobre esta tarefa

Você pode criar descritores de segurança NTFS para arquivos e pastas que residem em volumes de estilo de segurança NTFS ou para arquivos e pastas que residem em volumes de estilo de segurança misto.

Por padrão, quando um descritor de segurança é criado, quatro entradas de controle de acesso (ACEs) da lista de controle de acesso discricionária (DACL) são adicionadas a esse descritor de segurança. Os quatro ACEs predefinidos são os seguintes:

Objeto	Tipo de acesso	Direitos de acesso	Onde aplicar as permissões
CRIAR/Administradores	Permitir	Controlo total	esta pasta, subpastas, ficheiros
CONSTRUIR/usuários	Permitir	Controlo total	esta pasta, subpastas, ficheiros
PROPRIETÁRIO DO CRIADOR	Permitir	Controlo total	esta pasta, subpastas, ficheiros
AUTORIDADE NT/SISTEMA	Permitir	Controlo total	esta pasta, subpastas, ficheiros

Você pode personalizar a configuração do descritor de segurança usando os seguintes parâmetros opcionais:

- Proprietário do descritor de segurança
- Grupo primário do proprietário
- Flags de controle bruto

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas de manual para obter mais informações.

Adicione entradas de controle de acesso NTFS DACL ao descritor de segurança NTFS

Adicionar entradas de controle de acesso (ACEs) DACL (lista de controle de acesso discricionária) ao descritor de segurança NTFS é a segunda etapa na configuração e aplicação de ACLs NTFS a um arquivo ou pasta. Cada entrada identifica qual objeto é permitido ou negado acesso e define o que o objeto pode ou não pode fazer aos arquivos ou pastas definidos no ACE.

Sobre esta tarefa

Você pode adicionar um ou mais ACEs à DACL do descritor de segurança.

Se o descritor de segurança contiver uma DACL que tenha ACEs existentes, o comando adicionará o novo ACE à DACL. Se o descritor de segurança não contiver uma DACL, o comando criará a DACL e adicionará a nova ACE a ele.

Opcionalmente, você pode personalizar entradas DACL especificando quais direitos deseja permitir ou negar para a conta especificada no `-account` parâmetro. Existem três métodos mutuamente exclusivos para especificar direitos:

- Direitos
- Direitos avançados
- Direitos brutos (privilégio avançado)

Se você não especificar direitos para a entrada DACL, o padrão será definir os direitos como `Full Control`.

Opcionalmente, você pode personalizar entradas DACL especificando como aplicar herança.

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas de manual para obter mais informações.

Passos

1. Adicione uma entrada DACL a um descritor de segurança: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
   ```

2. Verifique se a entrada DACL está correta: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                Vserver: vs1
      Security Descriptor Name: sd1
                Allow or Deny: deny
           Account Name or SID: DOMAIN\joe
                Access Rights: full-control
        Advanced Access Rights: -
                     Apply To: this-folder
                Access Rights: full-control
```

Crie políticas de segurança

Criar uma política de segurança de arquivos para SVMs é a terceira etapa na configuração e aplicação de ACLs a um arquivo ou pasta. Uma política atua como um contentor para várias tarefas, onde cada tarefa é uma única entrada que pode ser aplicada a arquivos ou pastas. Pode adicionar tarefas à política de segurança mais tarde.

Sobre esta tarefa

As tarefas que você adiciona a uma diretiva de segurança contêm associações entre o descritor de segurança NTFS e os caminhos de arquivo ou pasta. Portanto, você deve associar a política de segurança a cada SVM (contendo volumes de estilo de segurança NTFS ou volumes de estilo de segurança misto).

Passos

1. Criar uma política de segurança: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Verifique a política de segurança: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
  ------------     --------------
      vs1              policy1
```

Adicione uma tarefa à política de segurança

Criar e adicionar uma tarefa de diretiva a uma diretiva de segurança é a quarta etapa na configuração e aplicação de ACLs a arquivos ou pastas em SVMs. Ao criar a tarefa de política, associe a tarefa a uma política de segurança. Você pode adicionar uma ou mais entradas de tarefa a uma diretiva de segurança.

Sobre esta tarefa

A política de segurança é um contentor para uma tarefa. Uma tarefa refere-se a uma única operação que pode ser feita por uma política de segurança para arquivos ou pastas com NTFS ou segurança mista (ou para

um objeto de volume se configurar o Storage-Level Access Guard).

Existem dois tipos de tarefas:

- Tarefas de arquivo e diretório

  Usado para especificar tarefas que aplicam descritores de segurança a arquivos e pastas especificados. As ACLs aplicadas através de tarefas de arquivo e diretório podem ser gerenciadas com clientes SMB ou com a CLI do ONTAP.

- Tarefas do Access Guard no nível de storage

  Usado para especificar tarefas que aplicam descritores de segurança do Storage-Level Access Guard a um volume especificado. As ACLs aplicadas por meio de tarefas de proteção de acesso no nível do storage podem ser gerenciadas somente por meio da CLI do ONTAP.

Uma tarefa contém definições para a configuração de segurança de um ficheiro (ou pasta) ou conjunto de ficheiros (ou pastas). Cada tarefa em uma política é identificada exclusivamente pelo caminho. Só pode haver uma tarefa por caminho dentro de uma única política. Uma política não pode ter entradas de tarefa duplicadas.

Diretrizes para adicionar uma tarefa a uma política:

- Pode haver um máximo de 10.000 entradas de tarefas por política.
- Uma política pode conter uma ou mais tarefas.

  Mesmo que uma diretiva possa conter mais de uma tarefa, você não pode configurar uma diretiva para conter tarefas de diretório de arquivos e Guarda de Acesso em nível de armazenamento. Uma diretiva deve conter todas as tarefas do Guarda de Acesso no nível de armazenamento ou todas as tarefas do diretório de arquivos.

- O Access Guard no nível de storage é usado para restringir permissões.

  Ele nunca dará permissões de acesso extra.

Ao adicionar tarefas a políticas de segurança, você deve especificar os quatro parâmetros necessários a seguir:

- Nome do SVM
- Nome da política
- Caminho
- Descritor de segurança para associar ao caminho

Você pode personalizar a configuração do descritor de segurança usando os seguintes parâmetros opcionais:

- Tipo de segurança
- Modo de propagação
- Posição do índice
- Tipo de controle de acesso

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas

de manual para obter mais informações.

Passos

1. Adicione uma tarefa com um descritor de segurança associado à diretiva de segurança: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` é o valor padrão para o `-access-control` parâmetro. Especificar o tipo de controle de acesso ao configurar tarefas de acesso a arquivos e diretórios é opcional.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. Verifique a configuração da tarefa de política: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   `vserver security file-directory policy task show`

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Aplicar políticas de segurança

Aplicar uma política de segurança de arquivos a SVMs é a última etapa na criação e aplicação de ACLs NTFS a arquivos ou pastas.

Sobre esta tarefa

Você pode aplicar as configurações de segurança definidas na diretiva de segurança a arquivos e pastas NTFS residentes em volumes FlexVol (NTFS ou estilo de segurança misto).

> Quando uma política de auditoria e SACLs associados são aplicados, todas as DACLs existentes são substituídas. Quando uma diretiva de segurança e suas DACLs associadas são aplicadas, todas as DACLs existentes são substituídas. Você deve revisar as políticas de segurança existentes antes de criar e aplicar novas.

Passo

1. Aplicar uma política de segurança: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

O trabalho de aplicação de política está agendado e o Código trabalho é devolvido.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
53322" command to view the status of the operation
```

Monitorize o trabalho de política de segurança

Ao aplicar a diretiva de segurança a máquinas virtuais de armazenamento (SVMs), você pode monitorar o progresso da tarefa monitorando a tarefa de diretiva de segurança. Isso é útil se você quiser verificar se a aplicação da diretiva de segurança foi bem-sucedida. Isso também é útil se você tiver um trabalho de longa duração onde você estiver aplicando segurança em massa a um grande número de arquivos e pastas.

Sobre esta tarefa

Para exibir informações detalhadas sobre um trabalho de política de segurança, use o `-instance` parâmetro.

Passo

1. Monitorar o trabalho de política de segurança: `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verifique a segurança do arquivo aplicado

Você pode verificar as configurações de segurança do arquivo para confirmar se os arquivos ou pastas na máquina virtual de armazenamento (SVM) à qual você aplicou a diretiva de segurança têm as configurações desejadas.

Sobre esta tarefa

Você deve fornecer o nome do SVM que contém os dados e o caminho para o arquivo e pastas em que deseja verificar as configurações de segurança. Você pode usar o parâmetro opcional `-expand-mask` para exibir informações detalhadas sobre as configurações de segurança.

Passo

1. Exibir configurações de segurança de arquivos e pastas: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   ```
   vserver security file-directory show -vserver vs1 -path /data/engineering
   -expand-mask true
   ```

```
         Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
```

```
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
```

```
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

Configure e aplique políticas de auditoria a arquivos e pastas NTFS usando a CLI

Configure e aplique políticas de auditoria a arquivos e pastas NTFS usando a visão geral da CLI

Existem várias etapas que você deve executar para aplicar políticas de auditoria a arquivos e pastas NTFS ao usar a CLI do ONTAP. Primeiro, você cria um descritor de segurança NTFS e adiciona SACLs ao descritor de segurança. Em seguida, você cria uma política de segurança e adiciona tarefas de política. Em seguida, você aplica a política de segurança a uma máquina virtual de storage (SVM).

Sobre esta tarefa

Depois de aplicar a política de segurança, pode monitorizar o trabalho de política de segurança e, em seguida, verificar as definições da política de auditoria aplicada.

Quando uma política de auditoria e SACLs associados são aplicados, todas as DACLs existentes são substituídas. Você deve revisar as políticas de segurança existentes antes de criar e aplicar novas.

Informações relacionadas

Protegendo o acesso aos arquivos usando o Storage-Level Access Guard

Limites ao usar a CLI para definir a segurança de arquivos e pastas

Como os descritores de segurança são usados para aplicar a segurança de arquivos e pastas

"Auditoria de SMB e NFS e rastreamento de segurança"

Configure e aplique segurança de arquivos em arquivos e pastas NTFS usando a CLI

Crie um descritor de segurança NTFS

Criar uma política de auditoria do descritor de segurança NTFS é a primeira etapa na configuração e aplicação de listas de controle de acesso (ACLs) NTFS a arquivos e pastas residentes em SVMs. Você associará o descritor de segurança ao caminho do arquivo ou da pasta em uma tarefa de diretiva.

Sobre esta tarefa

Você pode criar descritores de segurança NTFS para arquivos e pastas que residem em volumes de estilo de segurança NTFS ou para arquivos e pastas que residem em volumes de estilo de segurança misto.

Por padrão, quando um descritor de segurança é criado, quatro entradas de controle de acesso (ACEs) da lista de controle de acesso discricionária (DACL) são adicionadas a esse descritor de segurança. Os quatro ACEs predefinidos são os seguintes:

Objeto	Tipo de acesso	Direitos de acesso	Onde aplicar as permissões
CRIAR/Administradores	Permitir	Controlo total	esta pasta, subpastas, ficheiros
CONSTRUIR/usuários	Permitir	Controlo total	esta pasta, subpastas, ficheiros
PROPRIETÁRIO DO CRIADOR	Permitir	Controlo total	esta pasta, subpastas, ficheiros
AUTORIDADE NT/SISTEMA	Permitir	Controlo total	esta pasta, subpastas, ficheiros

Você pode personalizar a configuração do descritor de segurança usando os seguintes parâmetros opcionais:

- Proprietário do descritor de segurança
- Grupo primário do proprietário
- Flags de controle bruto

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas de manual para obter mais informações.

Passos

1. Se pretender utilizar os parâmetros avançados, defina o nível de privilégio para avançado: `set -privilege advanced`
2. Criar um descritor de segurança: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   `vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`

3. Verifique se a configuração do descritor de segurança está correta: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                   Vserver: vs1
                         Security Descriptor Name: sd1
                   Owner of the Security Descriptor: DOMAIN\joe
   ```

4. Se estiver no nível de privilégio avançado, regresse ao nível de privilégio admin: `set -privilege admin`

Adicione entradas de controle de acesso NTFS SACL ao descritor de segurança NTFS

Adicionar entradas de controle de acesso (ACEs) SACL (lista de controle de acesso do sistema) ao descritor de segurança NTFS é a segunda etapa na criação de políticas de auditoria NTFS para arquivos ou pastas em SVMs. Cada entrada identifica o usuário ou grupo que você deseja auditar. A entrada SACL define se você deseja auditar tentativas de acesso bem-sucedidas ou com falha.

Sobre esta tarefa

Você pode adicionar um ou mais ACEs ao SACL do descritor de segurança.

Se o descritor de segurança contiver um SACL que tenha ACEs existentes, o comando adicionará o novo ACE ao SACL. Se o descritor de segurança não contiver um SACL, o comando criará o SACL e adicionará o novo ACE a ele.

Você pode configurar entradas SACL especificando quais direitos deseja auditar para eventos de sucesso ou falha para a conta especificada no `-account` parâmetro. Existem três métodos mutuamente exclusivos para especificar direitos:

- Direitos
- Direitos avançados
- Direitos brutos (privilégio avançado)

Se não especificar direitos para a entrada SACL, a predefinição é `Full Control`.

Opcionalmente, você pode personalizar entradas SACL especificando como aplicar herança com o `apply to` parâmetro. Se você não especificar esse parâmetro, o padrão é aplicar essa entrada SACL a essa pasta, subpastas e arquivos.

Passos

1. Adicione uma entrada SACL a um descritor de segurança: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. Verifique se a entrada SACL está correta: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                                Vserver: vs1
                  Security Descriptor Name: sd1
   Access type for Specified Access Rights: failure
                       Account Name or SID: DOMAIN\joe
                             Access Rights: full-control
                    Advanced Access Rights: -
                                  Apply To: this-folder
                             Access Rights: full-control
   ```

Crie políticas de segurança

Criar uma política de auditoria para máquinas virtuais de armazenamento (SVMs) é a terceira etapa na configuração e aplicação de ACLs a um arquivo ou pasta. Uma política atua como um contentor para várias tarefas, onde cada tarefa é uma única entrada que pode ser aplicada a arquivos ou pastas. Pode adicionar tarefas à política de segurança mais tarde.

Sobre esta tarefa

As tarefas que você adiciona a uma diretiva de segurança contêm associações entre o descritor de segurança NTFS e os caminhos de arquivo ou pasta. Portanto, você deve associar a política de segurança a cada máquina virtual de armazenamento (SVM) (contendo volumes de estilo de segurança NTFS ou volumes mistos de estilo de segurança).

Passos

1. Criar uma política de segurança: `vserver security file-directory policy create -vserver`

```
vserver_name -policy-name policy_name

vserver security file-directory policy create -policy-name policy1 -vserver
vs1
```

2. Verifique a política de segurança: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Adicione uma tarefa à política de segurança

Criar e adicionar uma tarefa de diretiva a uma diretiva de segurança é a quarta etapa na configuração e aplicação de ACLs a arquivos ou pastas em SVMs. Ao criar a tarefa de política, associe a tarefa a uma política de segurança. Você pode adicionar uma ou mais entradas de tarefa a uma diretiva de segurança.

Sobre esta tarefa

A política de segurança é um contentor para uma tarefa. Uma tarefa refere-se a uma única operação que pode ser feita por uma política de segurança para arquivos ou pastas com NTFS ou segurança mista (ou para um objeto de volume se configurar o Storage-Level Access Guard).

Existem dois tipos de tarefas:

- Tarefas de arquivo e diretório

  Usado para especificar tarefas que aplicam descritores de segurança a arquivos e pastas especificados. As ACLs aplicadas através de tarefas de arquivo e diretório podem ser gerenciadas com clientes SMB ou com a CLI do ONTAP.

- Tarefas do Access Guard no nível de storage

  Usado para especificar tarefas que aplicam descritores de segurança do Storage-Level Access Guard a um volume especificado. As ACLs aplicadas por meio de tarefas de proteção de acesso no nível do storage podem ser gerenciadas somente por meio da CLI do ONTAP.

Uma tarefa contém definições para a configuração de segurança de um ficheiro (ou pasta) ou conjunto de ficheiros (ou pastas). Cada tarefa em uma política é identificada exclusivamente pelo caminho. Só pode haver uma tarefa por caminho dentro de uma única política. Uma política não pode ter entradas de tarefa duplicadas.

Diretrizes para adicionar uma tarefa a uma política:

- Pode haver um máximo de 10.000 entradas de tarefas por política.
- Uma política pode conter uma ou mais tarefas.

  Mesmo que uma diretiva possa conter mais de uma tarefa, você não pode configurar uma diretiva para conter tarefas de diretório de arquivos e Guarda de Acesso em nível de armazenamento. Uma diretiva

deve conter todas as tarefas do Guarda de Acesso no nível de armazenamento ou todas as tarefas do diretório de arquivos.

- O Access Guard no nível de storage é usado para restringir permissões.

  Ele nunca dará permissões de acesso extra.

Você pode personalizar a configuração do descritor de segurança usando os seguintes parâmetros opcionais:

- Tipo de segurança
- Modo de propagação
- Posição do índice
- Tipo de controle de acesso

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas de manual para obter mais informações.

Passos

1. Adicione uma tarefa com um descritor de segurança associado à diretiva de segurança: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` é o valor padrão para o `-access-control` parâmetro. Especificar o tipo de controle de acesso ao configurar tarefas de acesso a arquivos e diretórios é opcional.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. Verifique a configuração da tarefa de política: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Aplicar políticas de segurança

Aplicar uma política de auditoria a SVMs é a última etapa na criação e aplicação de

ACLs NTFS a arquivos ou pastas.

Sobre esta tarefa

Você pode aplicar as configurações de segurança definidas na diretiva de segurança a arquivos e pastas NTFS residentes em volumes FlexVol (NTFS ou estilo de segurança misto).

> Quando uma política de auditoria e SACLs associados são aplicados, todas as DACLs existentes são substituídas. Quando uma diretiva de segurança e suas DACLs associadas são aplicadas, todas as DACLs existentes são substituídas. Você deve revisar as políticas de segurança existentes antes de criar e aplicar novas.

Passo

1. Aplicar uma política de segurança: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   O trabalho de aplicação de política está agendado e o Código trabalho é devolvido.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

Monitorize o trabalho de política de segurança

Ao aplicar a diretiva de segurança a máquinas virtuais de armazenamento (SVMs), você pode monitorar o progresso da tarefa monitorando a tarefa de diretiva de segurança. Isso é útil se você quiser verificar se a aplicação da diretiva de segurança foi bem-sucedida. Isso também é útil se você tiver um trabalho de longa duração onde você estiver aplicando segurança em massa a um grande número de arquivos e pastas.

Sobre esta tarefa

Para exibir informações detalhadas sobre um trabalho de política de segurança, use o `-instance` parâmetro.

Passo

1. Monitorar o trabalho de política de segurança: `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verifique a política de auditoria aplicada

Você pode verificar a política de auditoria para confirmar se os arquivos ou pastas na máquina virtual de armazenamento (SVM) à qual você aplicou a diretiva de segurança têm as configurações de segurança de auditoria desejadas.

Sobre esta tarefa

Você usa o `vserver security file-directory show` comando para exibir informações da política de auditoria. Você deve fornecer o nome do SVM que contém os dados e o caminho para os dados cujas informações de política de auditoria de arquivo ou pasta você deseja exibir.

Passo

1. Exibir configurações da política de auditoria: `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Exemplo

O comando a seguir exibe as informações da política de auditoria aplicadas ao caminho "'/corp" no SVM VS1. O caminho tem um SUCESSO e uma entrada SACL DE SUCESSO/FALHA aplicada a ele:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
      Security Style: ntfs
     Effective Style: ntfs
      DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
       Unix Group Id: 0
      Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                  ACLs: NTFS Security Descriptor
                        Control:0x8014
                        Owner:DOMAIN\Administrator
                        Group:BUILTIN\Administrators
                        SACL - ACEs
                          ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                          SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                        DACL - ACEs
                          ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                          ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                          ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Considerações ao gerenciar trabalhos de diretiva de segurança

Se existir um trabalho de política de segurança, em determinadas circunstâncias, não é possível modificar essa política de segurança ou as tarefas atribuídas a essa diretiva. Você deve entender em que condições você pode ou não pode modificar políticas de segurança para que quaisquer tentativas que você fizer para modificar a diretiva sejam bem-sucedidas. As modificações à política incluem adicionar, remover ou modificar tarefas atribuídas à política e excluir ou modificar a política.

Não é possível modificar uma política de segurança ou uma tarefa atribuída a essa política se existir um trabalho para essa política e essa tarefa estiver nos seguintes estados:

- O trabalho está em execução ou em curso.
- O trabalho está em pausa.
- O trabalho é retomado e está no estado em execução.
- Se a tarefa estiver aguardando o failover para outro nó.

Nas seguintes circunstâncias, se existir um trabalho para uma política de segurança, pode modificar com êxito essa política de segurança ou uma tarefa atribuída a essa política:

- O trabalho de política é interrompido.
- O trabalho de política foi concluído com êxito.

Comandos para gerenciar descritores de segurança NTFS

Existem comandos ONTAP específicos para gerenciar descritores de segurança. Você pode criar, modificar, excluir e exibir informações sobre descritores de segurança.

Se você quiser…	Use este comando…
Crie descritores de segurança NTFS	`vserver security file-directory ntfs create`
Modificar descritores de segurança NTFS existentes	`vserver security file-directory ntfs modify`
Exibir informações sobre descritores de segurança NTFS existentes	`vserver security file-directory ntfs show`
Excluir descritores de segurança NTFS	`vserver security file-directory ntfs delete`

Consulte as páginas de manual para `vserver security file-directory ntfs` obter mais informações.

Comandos para gerenciar entradas de controle de acesso NTFS DACL

Existem comandos ONTAP específicos para gerenciar entradas de controle de acesso DACL (ACEs). Você pode adicionar ACEs a DACLs NTFS a qualquer momento. Você também pode gerenciar DACLs NTFS existentes modificando, excluindo e exibindo informações sobre ACEs em DACLs.

Se você quiser…	Use este comando…
Crie ACEs e adicione-os a DACLs NTFS	`vserver security file-directory ntfs dacl add`
Modificar ACEs existentes em DACLs NTFS	`vserver security file-directory ntfs dacl modify`
Exibir informações sobre ACEs existentes em DACLs NTFS	`vserver security file-directory ntfs dacl show`
Remover ACEs existentes de DACLs NTFS	`vserver security file-directory ntfs dacl remove`

Consulte as páginas de manual para `vserver security file-directory ntfs dacl` obter mais informações.

Comandos para gerenciar entradas de controle de acesso NTFS SACL

Existem comandos ONTAP específicos para gerenciar entradas de controle de acesso SACL (ACEs). Você pode adicionar ACEs a SACLs NTFS a qualquer momento. Você também pode gerenciar SACLs NTFS existentes modificando, excluindo e exibindo informações sobre ACEs em SACLs.

Se você quiser…	Use este comando…
Crie ACEs e adicione-os a SACLs NTFS	`vserver security file-directory ntfs sacl add`
Modificar ACEs existentes em SACLs NTFS	`vserver security file-directory ntfs sacl modify`
Exibir informações sobre ACEs existentes em SACLs NTFS	`vserver security file-directory ntfs sacl show`
Remover ACEs existentes de SACLs NTFS	`vserver security file-directory ntfs sacl remove`

Consulte as páginas de manual para `vserver security file-directory ntfs sacl` obter mais informações.

Comandos para gerenciar políticas de segurança

Existem comandos ONTAP específicos para gerenciar políticas de segurança. Você pode exibir informações sobre políticas e excluir políticas. Não é possível modificar uma política de segurança.

Se você quiser…	Use este comando…
Crie políticas de segurança	`vserver security file-directory policy create`
Exibir informações sobre políticas de segurança	`vserver security file-directory policy show`
Eliminar políticas de segurança	`vserver security file-directory policy delete`

Consulte as páginas de manual para `vserver security file-directory policy` obter mais informações.

Comandos para gerenciar tarefas de diretiva de segurança

Existem comandos ONTAP para adicionar, modificar, remover e exibir informações sobre tarefas de diretiva de segurança.

Se você quiser…	Use este comando…
Adicione tarefas de política de segurança	`vserver security file-directory policy task add`
Modificar tarefas de política de segurança	`vserver security file-directory policy task modify`
Exibir informações sobre as tarefas da diretiva de segurança	`vserver security file-directory policy task show`
Remover tarefas de política de segurança	`vserver security file-directory policy task remove`

Consulte as páginas de manual para `vserver security file-directory policy task` obter mais informações.

Comandos para gerenciar trabalhos de diretiva de segurança

Existem comandos ONTAP para pausar, retomar, parar e exibir informações sobre tarefas de diretiva de segurança.

Se você quiser…	Use este comando…
Pausar trabalhos de diretiva de segurança	`vserver security file-directory job pause -vserver vserver_name -id integer`
Retomar os trabalhos de política de segurança	`vserver security file-directory job resume -vserver vserver_name -id integer`
Exibir informações sobre os trabalhos de diretiva de segurança	`vserver security file-directory job show -vserver vserver_name` Pode determinar a ID da tarefa de uma tarefa utilizando este comando.
Interromper trabalhos de política de segurança	`vserver security file-directory job stop -vserver vserver_name -id integer`

Consulte as páginas de manual para `vserver security file-directory job` obter mais informações.

Configure o cache de metadados para compartilhamentos SMB

Como o armazenamento em cache de metadados SMB funciona

O armazenamento em cache de metadados permite o armazenamento em cache de atributos de arquivo em clientes SMB 1,0 para fornecer acesso mais rápido aos atributos de arquivo e pasta. Você pode ativar ou desativar o cache de atributos por compartilhamento. Você também pode configurar o tempo de permanência para entradas em cache se o armazenamento em cache de metadados estiver habilitado. A configuração do cache de metadados não é necessária se os clientes estiverem se conetando a compartilhamentos por SMB 2.x ou SMB 3,0.

Quando ativado, o cache de metadados SMB armazena dados de caminho e atributo de arquivo por um período limitado de tempo. Isso pode melhorar a performance do SMB para clientes SMB 1,0 com workloads comuns.

Para certas tarefas, o SMB cria uma quantidade significativa de tráfego que pode incluir várias consultas idênticas para metadados de caminho e arquivo. Você pode reduzir o número de consultas redundantes e melhorar o desempenho para clientes SMB 1,0 usando o cache de metadados SMB para buscar informações do cache.

> Embora improvável, é possível que o cache de metadados possa servir informações obsoletas para clientes SMB 1,0. Se o seu ambiente não puder suportar esse risco, você não deve habilitar esse recurso.

Ative o cache de metadados SMB

Você pode melhorar o desempenho do SMB para clientes SMB 1,0 ativando o cache de metadados SMB. Por padrão, o armazenamento em cache de metadados SMB está

desativado.

Passo

1. Execute a ação desejada:

Se você quiser…	Digite o comando…
Ative o armazenamento em cache de metadados SMB ao criar um compartilhamento	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties attributecache`
Habilite o armazenamento em cache de metadados SMB em um compartilhamento existente	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache`

Informações relacionadas

Configurando o tempo de vida das entradas de cache de metadados SMB

Adicionar ou remover propriedades de compartilhamento em um compartilhamento SMB existente

Configure o tempo de vida das entradas de cache de metadados SMB

Você pode configurar o tempo de vida das entradas de cache de metadados SMB para otimizar o desempenho do cache de metadados SMB em seu ambiente. O padrão é 10 segundos.

Antes de começar

Você deve ter habilitado o recurso de cache de metadados SMB. Se o armazenamento em cache de metadados SMB não estiver ativado, a configuração TTL de cache SMB não será usada.

Passo

1. Execute a ação desejada:

Se você quiser configurar o tempo de vida das entradas de cache de metadados SMB quando…	Digite o comando…
Crie um compartilhamento	`vserver cifs share -create -vserver vserver_name -share-name share_name -path path -attribute-cache-ttl [integerh][integerm][integers]`
Modificar um compartilhamento existente	`vserver cifs share -modify -vserver vserver_name -share-name share_name -attribute-cache-ttl [integerh][integerm][integers]`

Você pode especificar opções e propriedades de configuração de compartilhamento adicionais ao criar ou

modificar compartilhamentos. Consulte as páginas de manual para obter mais informações.

Gerenciar bloqueios de arquivos

Acerca do bloqueio de ficheiros entre protocolos

Bloqueio de arquivos é um método usado por aplicativos cliente para impedir que um usuário acesse um arquivo aberto anteriormente por outro usuário. A forma como o ONTAP bloqueia ficheiros depende do protocolo do cliente.

Se o cliente for um cliente NFS, os bloqueios são consultivos; se o cliente for um cliente SMB, os bloqueios são obrigatórios.

Devido às diferenças entre os bloqueios de arquivos NFS e SMB, um cliente NFS pode não conseguir acessar um arquivo aberto anteriormente por um aplicativo SMB.

O seguinte ocorre quando um cliente NFS tenta aceder a um ficheiro bloqueado por uma aplicação SMB:

- Em volumes mistos ou NTFS, operações de manipulação de arquivos como `rm` , `rmdir` e `mv` podem causar falha no aplicativo NFS.
- As operações de leitura e gravação NFS são negadas pelos modos abertos SMB deny-read e deny-write, respetivamente.
- As operações de gravação NFS falham quando o intervalo escrito do arquivo é bloqueado com um bytelock SMB exclusivo.
- Desvincular
  - Para sistemas de arquivos NTFS, as operações de exclusão SMB e CIFS são suportadas.

    O arquivo será removido após o último fechamento.
  - As operações de desvinculação NFS não são suportadas.

    Ele não é suportado porque as semânticas NTFS e SMB são necessárias e a última operação Excluir-em-close não é suportada para NFS.
  - Para sistemas de arquivos UNIX, a operação de desvinculação é suportada.

    Ele é compatível porque a semântica NFS e UNIX são necessárias.
- Mudar o nome
  - Para sistemas de arquivos NTFS, se o arquivo de destino for aberto a partir de SMB ou CIFS, o arquivo de destino pode ser renomeado.
  - O nome de NFS não é suportado.

    Não é suportado porque as semânticas NTFS e SMB são necessárias.

Em volumes de estilo de segurança UNIX, as operações NFS desvincular e renomear ignoram o estado de bloqueio SMB e permitem o acesso ao arquivo. Todas as outras operações NFS em volumes estilo segurança UNIX honram o estado de bloqueio SMB.

Como o ONTAP trata bits somente de leitura

O bit somente leitura é definido em uma base arquivo por arquivo para refletir se um arquivo é gravável (desativado) ou somente leitura (habilitado).

Os clientes SMB que usam o Windows podem definir um bit somente leitura por arquivo. Os clientes NFS não definem um bit somente leitura por arquivo porque os clientes NFS não têm operações de protocolo que usam um bit somente leitura por arquivo.

O ONTAP pode definir um bit somente leitura em um arquivo quando um cliente SMB que usa o Windows cria esse arquivo. O ONTAP também pode definir um bit somente leitura quando um arquivo é compartilhado entre clientes NFS e clientes SMB. Alguns softwares, quando usados por clientes NFS e clientes SMB, exigem que o bit somente leitura seja ativado.

Para que o ONTAP mantenha as permissões de leitura e gravação apropriadas em um arquivo compartilhado entre clientes NFS e clientes SMB, ele trata o bit somente leitura de acordo com as seguintes regras:

- O NFS trata qualquer arquivo com o bit somente leitura ativado como se ele não tivesse bits de permissão de gravação ativados.
- Se um cliente NFS desativar todos os bits de permissão de gravação e pelo menos um desses bits tiver sido ativado anteriormente, o ONTAP ativa o bit somente leitura para esse arquivo.
- Se um cliente NFS ativar qualquer bit de permissão de gravação, o ONTAP desativa o bit somente leitura para esse arquivo.
- Se o bit somente leitura de um arquivo estiver ativado e um cliente NFS tentar descobrir permissões para o arquivo, os bits de permissão para o arquivo não serão enviados para o cliente NFS; em vez disso, o ONTAP enviará os bits de permissão para o cliente NFS com os bits de permissão de gravação mascarados.
- Se o bit somente leitura de um arquivo estiver ativado e um cliente SMB desabilitar o bit somente leitura, o ONTAP ativa o bit de permissão de gravação do proprietário para o arquivo.
- Os arquivos com o bit somente leitura habilitado são graváveis somente pelo root.

> As alterações às permissões de arquivo entram em vigor imediatamente em clientes SMB, mas podem não ter efeito imediatamente em clientes NFS se o cliente NFS ativar o armazenamento em cache de atributos.

Como o ONTAP difere do Windows ao lidar com bloqueios em componentes de caminho de compartilhamento

Ao contrário do Windows, o ONTAP não bloqueia cada componente do caminho para um arquivo aberto enquanto o arquivo está aberto. Esse comportamento também afeta os caminhos de compartilhamento SMB.

Como o ONTAP não bloqueia cada componente do caminho, é possível renomear um componente do caminho acima do arquivo aberto ou do compartilhamento, o que pode causar problemas para determinados aplicativos ou fazer com que o caminho de compartilhamento na configuração do SMB seja inválido. Isso pode fazer com que o compartilhamento seja inacessível.

Para evitar problemas causados pela renomeação de componentes de caminho, você pode aplicar configurações de segurança que impedem que usuários ou aplicativos renomeem diretórios críticos.

Apresentar informações sobre bloqueios

Você pode exibir informações sobre os bloqueios de arquivo atuais, incluindo quais tipos de bloqueios são mantidos e qual é o estado de bloqueio, detalhes sobre bloqueios de intervalo de bytes, modos de sharelock, bloqueios de delegação e bloqueios oportunistas, e se os bloqueios são abertos com alças duráveis ou persistentes.

Sobre esta tarefa

O endereço IP do cliente não pode ser exibido para bloqueios estabelecidos através de NFSv4 ou NFSv4,1.

Por padrão, o comando exibe informações sobre todos os bloqueios. Você pode usar parâmetros de comando para exibir informações sobre bloqueios de uma máquina virtual de armazenamento específica (SVM) ou para filtrar a saída do comando por outros critérios.

O `vserver locks show` comando exibe informações sobre quatro tipos de bloqueios:

- Bloqueios de intervalo de bytes, que bloqueiam apenas uma parte de um arquivo.
- Bloqueios de compartilhamento, que bloqueiam arquivos abertos.
- Bloqueios oportunistas, que controlam o cache do lado do cliente sobre SMB.
- Delegações, que controlam o cache do lado do cliente sobre NFSv4.x.

Ao especificar parâmetros opcionais, você pode determinar informações importantes sobre cada tipo de bloqueio. Consulte a página de manual para obter mais informações.

Passo

1. Exiba informações sobre bloqueios usando o `vserver locks show` comando.

Exemplos

O exemplo a seguir exibe informações de resumo de um bloqueio NFSv4 em um arquivo com o `/vol1/file1` caminho . O modo de acesso sharelock é write-deny_none, e o bloqueio foi concedido com delegação de gravação:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

O exemplo a seguir exibe informações detalhadas de oplock e sharelock sobre o bloqueio SMB em um arquivo com o `/data2/data2_2/intro.pptx` caminho . Um manipulador durável é concedido no arquivo com um modo de acesso de bloqueio de compartilhamento de write-deny_none para um cliente com um endereço IP de 10,3.1,3. Uma locação de oplock é concedida com um nível de lote de oplock:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                  Vserver: vs1
                   Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
              Lock Protocol: cifs
                  Lock Type: share-level
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                  Vserver: vs1
                   Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
```

```
            Delegation Type: -
             Client Address: 10.3.1.3
              SMB Open Type: -
          SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Bloqueios de rutura

Quando os bloqueios de arquivos estão impedindo o acesso do cliente aos arquivos, você pode exibir informações sobre os bloqueios atualmente mantidos e, em seguida, quebrar bloqueios específicos. Exemplos de cenários em que você pode precisar quebrar bloqueios incluem depuração de aplicativos.

Sobre esta tarefa

O `vserver locks break` comando está disponível apenas no nível de privilégio avançado e superior. A página de manual do comando contém informações detalhadas.

Passos

1. Para encontrar as informações que você precisa para quebrar um bloqueio, use o `vserver locks show` comando.

   A página de manual do comando contém informações detalhadas.

2. Defina o nível de privilégio como avançado: `set -privilege advanced`
3. Execute uma das seguintes ações:

Se você quiser quebrar um bloqueio especificando…	Digite o comando…
O nome do SVM, o nome do volume, o nome LIF e o caminho do arquivo	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
A ID de bloqueio	`vserver locks break -lockid UUID`

4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Monitorar a atividade de SMB

Exibir informações de sessão SMB

Você pode exibir informações sobre sessões SMB estabelecidas, incluindo a conexão SMB e Session ID e o endereço IP da estação de trabalho usando a sessão. Você pode exibir informações sobre a versão do protocolo SMB da sessão e o nível de proteção

continuamente disponível, o que ajuda a identificar se a sessão é compatível com operações ininterruptas.

Sobre esta tarefa

É possível exibir informações de todas as sessões no SVM no formulário de resumo. No entanto, em muitos casos, a quantidade de saída que é retornada é grande. Você pode personalizar quais informações são exibidas na saída especificando parâmetros opcionais:

- Você pode usar o parâmetro opcional `-fields` para exibir a saída sobre os campos que você escolher.

  Você pode inserir `-fields ?` para determinar quais campos você pode usar.

- Você pode usar o `-instance` parâmetro para exibir informações detalhadas sobre sessões SMB estabelecidas.
- Você pode usar o `-fields` parâmetro ou o `-instance` parâmetro sozinho ou em combinação com outros parâmetros opcionais.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações de sessão SMB…	Digite o seguinte comando…
Para todas as sessões no SVM de forma resumida	`vserver cifs session show -vserver vserver_name`
Em um ID de conexão especificado	`vserver cifs session show -vserver vserver_name -connection-id integer`
A partir de um endereço IP de estação de trabalho especificado	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
Em um endereço IP de LIF especificado	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
Em um nó especificado	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	De um usuário do Windows especificado
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	Com um mecanismo de autenticação especificado
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2

Se você quiser exibir informações de sessão SMB…	Digite o seguinte comando…
Kerberos	Anonymous}`
Com uma versão de protocolo especificada	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== A proteção continuamente disponível e o SMB multicanal estão disponíveis apenas nas sessões SMB 3,0 e posteriores. Para ver o seu estado em todas as sessões de qualificação, deve especificar este parâmetro com o valor definido para `SMB3` ou posterior. ====
Com um nível especificado de proteção continuamente disponível	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== Se o status continuamente disponível for `Partial`, isso significa que a sessão contém pelo menos um arquivo aberto continuamente disponível, mas a sessão tem alguns arquivos que não estão abertos com proteção continuamente disponível. Você pode usar o `vserver cifs sessions file show` comando para determinar quais arquivos na sessão estabelecida não estão abertos com proteção continuamente disponível. ====
Com um status de sessão de assinatura SMB especificado	`vserver cifs session show -vserver vserver_name -is-session-signed {true

Exemplos

O comando a seguir exibe informações de sessão para as sessões no SVM VS1 estabelecidas a partir de uma estação de trabalho com endereço IP 10,1.1,1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2         23s
```

O comando a seguir exibe informações detalhadas da sessão para sessões com proteção continuamente disponível no SVM VS1. A conexão foi feita usando a conta de domínio.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

O comando a seguir exibe informações de sessão em uma sessão usando SMB 3,0 e SMB Multichannel no SVM VS1. No exemplo, o usuário conetado a esse compartilhamento a partir de um cliente compatível com SMB 3,0 usando o endereço IP LIF; portanto, o mecanismo de autenticação padrão é NTLMv2. A conexão deve ser feita usando a autenticação Kerberos para se conetar com a proteção continuamente disponível.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Informações relacionadas

Exibindo informações sobre arquivos SMB abertos

Exibir informações sobre arquivos SMB abertos

Você pode exibir informações sobre arquivos SMB abertos, incluindo a conexão SMB e Session ID, o volume de hospedagem, o nome do compartilhamento e o caminho do compartilhamento. Você pode exibir informações sobre o nível de proteção continuamente disponível de um arquivo, o que é útil para determinar se um arquivo aberto está em um estado compatível com operações ininterruptas.

Sobre esta tarefa

Você pode exibir informações sobre arquivos abertos em uma sessão SMB estabelecida. As informações exibidas são úteis quando você precisa determinar informações de sessão SMB para arquivos específicos em uma sessão SMB.

Por exemplo, se você tiver uma sessão SMB em que alguns dos arquivos abertos estão abertos com proteção continuamente disponível e alguns não estão abertos com proteção continuamente disponível (o valor para o `-continuously-available` campo na `vserver cifs session show` saída de comando é `Partial`), você pode determinar quais arquivos não estão disponíveis continuamente usando este comando.

Você pode exibir informações de todos os arquivos abertos em sessões SMB estabelecidas em máquinas virtuais de armazenamento (SVMs) em forma de resumo usando o `vserver cifs session file show`

comando sem quaisquer parâmetros opcionais.

No entanto, em muitos casos, a quantidade de saída retornada é grande. Você pode personalizar quais informações são exibidas na saída especificando parâmetros opcionais. Isso pode ser útil quando você deseja exibir informações para apenas um pequeno subconjunto de arquivos abertos.

- Você pode usar o parâmetro opcional `-fields` para exibir a saída nos campos que você escolher.

  Você pode usar este parâmetro sozinho ou em combinação com outros parâmetros opcionais.

- Você pode usar o `-instance` parâmetro para exibir informações detalhadas sobre arquivos SMB abertos.

  Você pode usar este parâmetro sozinho ou em combinação com outros parâmetros opcionais.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir arquivos SMB abertos…	Digite o seguinte comando…
No SVM no formulário de resumo	`vserver cifs session file show -vserver vserver_name`
Em um nó especificado	`vserver cifs session file show -vserver vserver_name -node {node_name`
local}`	Em um ID de arquivo especificado
`vserver cifs session file show -vserver vserver_name -file-id integer`	Em uma ID de conexão SMB especificada
`vserver cifs session file show -vserver vserver_name -connection-id integer`	Em um SMB Session ID especificado
`vserver cifs session file show -vserver vserver_name -session-id integer`	No agregado de hospedagem especificado
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	No volume especificado
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	No compartilhamento SMB especificado

Se você quiser exibir arquivos SMB abertos…	Digite o seguinte comando…
`vserver cifs session file show -vserver vserver_name -share share_name`	No caminho SMB especificado
`vserver cifs session file show -vserver vserver_name -path path`	Com o nível especificado de proteção continuamente disponível
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== Se o status continuamente disponível for `No`, isso significa que esses arquivos abertos não serão capazes de se recuperar sem interrupções da aquisição e da giveback. Eles também não podem se recuperar da realocação geral agregada entre parceiros em um relacionamento de alta disponibilidade. ====
Com o estado de reconexão especificado	`vserver cifs session file show -vserver vserver_name -reconnected {No

Existem parâmetros opcionais adicionais que você pode usar para refinar os resultados de saída. Consulte a página de manual para obter mais informações.

Exemplos

O exemplo a seguir exibe informações sobre arquivos abertos no SVM VS1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

O exemplo a seguir exibe informações detalhadas sobre arquivos SMB abertos com ID de arquivo 82 no SVM VS1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
             CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Informações relacionadas

Exibindo informações de sessão SMB

Determine quais objetos e contadores de estatísticas estão disponíveis

Antes de obter informações sobre as estatísticas de hash CIFS, SMB, auditoria e BranchCache e monitorar o desempenho, você deve saber quais objetos e contadores estão disponíveis a partir dos quais você pode obter dados.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser determinar…	Digite…
Quais objetos estão disponíveis	`statistics catalog object show`
Objetos específicos que estão disponíveis	`statistics catalog object show object object_name`
Quais contadores estão disponíveis	`statistics catalog counter show object object_name`

Consulte as páginas man para obter mais informações sobre quais objetos e contadores estão disponíveis.

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplos

O comando a seguir exibe descrições de objetos estatísticos selecionados relacionados ao acesso CIFS e SMB no cluster, como visto no nível avançado de privilégio:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

O comando a seguir exibe informações sobre alguns dos contadores para o `cifs` objeto, como visto no nível

de privilégio avançado:

Este exemplo não exibe todos os contadores disponíveis para o `cifs` objeto; a saída é truncada.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Informações relacionadas

Exibindo estatísticas

Apresentar estatísticas

É possível exibir várias estatísticas, incluindo estatísticas sobre CIFS e SMB, auditoria e hashes BranchCache, para monitorar a performance e diagnosticar problemas.

Antes de começar

Você deve ter coletado amostras de dados usando os `statistics start` comandos e `statistics stop` antes de exibir informações sobre objetos.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser exibir estatísticas para…	Digite…
Todas as versões do SMB	`statistics show -object cifs`
SMB 1,0	`statistics show -object smb1`
SMB 2.x e SMB 3,0	`statistics show -object smb2`
Subsistema CIFS do nó	`statistics show -object nblade_cifs`
Auditoria multiprotocolo	`statistics show -object audit_ng`
Serviço de hash BranchCache	`statistics show -object hashd`
DNS dinâmico	`statistics show -object ddns_update`

   Consulte a página de manual de cada comando para obter mais informações.

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

Determinando quais objetos e contadores de estatísticas estão disponíveis

Monitoramento de estatísticas de sessão assinadas pelo SMB

Exibindo estatísticas do BranchCache

Uso de estatísticas para monitorar a atividade automática de referência de nós

"Configuração SMB para Microsoft Hyper-V e SQL Server"

"Configuração do monitoramento de desempenho"

Informações sobre direitos autorais

Informações sobre marcas comerciais