Gerenciar servidores SMB

ONTAP 9

NetApp
February 12, 2026

Índice

Gerenciar servidores SMB

Modificar servidores SMB do ONTAP

Pode mover um servidor SMB de um grupo de trabalho para um domínio do ative Directory, de um grupo de trabalho para outro grupo de trabalho ou de um domínio do ative Directory para um grupo de trabalho utilizando o `vserver cifs modify` comando.

Sobre esta tarefa

Você também pode modificar outros atributos do servidor SMB, como o nome do servidor SMB e o status administrativo. Saiba mais sobre `vserver cifs modify` o "Referência do comando ONTAP"na .

Opções

- Mova o servidor SMB de um grupo de trabalho para um domínio do ative Directory:

  a. Defina o status administrativo do servidor SMB como `down`.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. Mova o servidor SMB do grupo de trabalho para um domínio do ative Directory: `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
  ```

  Para criar uma conta de máquina do ative Directory para o servidor SMB, você deve fornecer o nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores ao `ou=`*`example`* `ou` contentor dentro do *`example`* domínio .com.

  A partir do ONTAP 9.7, o administrador do AD pode fornecer um URI para um arquivo keytab como alternativa para fornecer um nome e uma senha para uma conta privilegiada do Windows. Quando receber o URI, inclua-o `-keytab-uri` no parâmetro com os `vserver cifs` comandos.

- Mover o servidor SMB de um grupo de trabalho para outro grupo de trabalho:

  a. Defina o status administrativo do servidor SMB como `down`.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. Modifique o grupo de trabalho para o servidor SMB: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`new_workgroup_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
  ```

- Mova o servidor SMB de um domínio do ative Directory para um grupo de trabalho:
  a. Defina o status administrativo do servidor SMB como `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. Mova o servidor SMB do domínio do ative Directory para um grupo de trabalho: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`workgroup_name`*

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```

> Para entrar no modo de grupo de trabalho, todos os recursos baseados em domínio devem ser desativados e suas configurações removidas automaticamente pelo sistema, incluindo compartilhamentos continuamente disponíveis, cópias de sombra e AES. No entanto, as ACLs de compartilhamento configuradas por domínio, como "EXAMPLE.COM\userName", não funcionarão corretamente, mas não poderão ser removidas pelo ONTAP. Remova essas ACLs de compartilhamento o mais rápido possível usando ferramentas externas após a conclusão do comando. Se o AES estiver ativado, você poderá ser solicitado a fornecer o nome e a senha de uma conta do Windows com Privileges suficiente para desativá-lo no domínio "example.com".

  - Modifique outros atributos usando o parâmetro apropriado do `vserver cifs modify` comando.

Use as opções para personalizar servidores SMB

Opções de servidor ONTAP SMB disponíveis

É útil saber quais opções estão disponíveis ao considerar como personalizar o servidor SMB. Embora algumas opções sejam para uso geral no servidor SMB, várias são usadas para ativar e configurar a funcionalidade SMB específica. As opções de servidor SMB são controladas com a `vserver cifs options modify` opção.

A lista a seguir especifica as opções do servidor SMB que estão disponíveis no nível de privilégio de administrador:

- **Configurando o valor de tempo limite da sessão SMB**

  Configurar esta opção permite especificar o número de segundos de tempo ocioso antes de uma sessão SMB ser desconetada. Uma sessão ociosa é uma sessão na qual um usuário não tem arquivos ou diretórios abertos no cliente. O valor padrão é de 900 segundos.

- **Configurando o usuário UNIX padrão**

  Configurar esta opção permite especificar o utilizador UNIX predefinido que o servidor SMB utiliza. O ONTAP cria automaticamente um usuário padrão chamado "'pcuser'" (com um UID de 65534), cria um grupo chamado "'pcuser'" (com um GID de 65534) e adiciona o usuário padrão ao grupo "'pcuser'". Quando você cria um servidor SMB, o ONTAP configura automaticamente "'pcuser'" como o usuário UNIX padrão.

- **Configurando o usuário UNIX convidado**

  A configuração desta opção permite especificar o nome de um usuário UNIX ao qual os usuários que fazem login de domínios não confiáveis são mapeados, o que permite que um usuário de um domínio não confiável se conete ao servidor SMB. Por padrão, essa opção não está configurada (não há valor padrão); portanto, o padrão é não permitir que usuários de domínios não confiáveis se conetem ao servidor SMB.

- * Ativar ou desativar a execução de concessão de leitura para bits de modo*

  Ativar ou desativar esta opção permite que você especifique se deseja permitir que clientes SMB executem arquivos executáveis com bits de modo UNIX aos quais eles têm acesso de leitura, mesmo quando o bit executável UNIX não está definido. Esta opção está desativada por predefinição.

- **Ativar ou desativar a capacidade de eliminar ficheiros só de leitura de clientes NFS**

  Ativar ou desativar esta opção determina se os clientes NFS devem excluir arquivos ou pastas com o conjunto de atributos somente leitura. A semântica de exclusão NTFS não permite a exclusão de um arquivo ou pasta quando o atributo somente leitura é definido. A semântica de exclusão do UNIX ignora o bit somente leitura, usando as permissões do diretório pai para determinar se um arquivo ou pasta pode ser excluído. A configuração padrão é `disabled`, o que resulta em semântica de exclusão NTFS.

- **Configurando endereços de servidor do Windows Internet Name Service**

  Configurar esta opção permite especificar uma lista de endereços de servidor WINS (Serviço de nomes de Internet do Windows) como uma lista delimitada por vírgulas. Você deve especificar endereços IPv4. Os endereços IPv6 não são suportados. Não há valor padrão.

A lista a seguir especifica as opções do servidor SMB que estão disponíveis no nível avançado de privilégio:

- **Concessão de permissões de grupo UNIX para usuários CIFS**

  Configurar esta opção determina se o usuário CIFS de entrada que não é o proprietário do arquivo pode receber a permissão de grupo. Se o usuário CIFS não for o proprietário do arquivo de estilo de segurança UNIX e esse parâmetro estiver definido como `true`, a permissão de grupo será concedida para o arquivo. Se o usuário CIFS não for o proprietário do arquivo de estilo de segurança UNIX e esse parâmetro estiver definido como `false`, as regras UNIX normais serão aplicáveis para conceder a permissão de arquivo. Este parâmetro é aplicável a arquivos de estilo de segurança UNIX que têm permissão definida como `mode bits` e não é aplicável a arquivos com o modo de segurança NTFS ou NFSv4. A predefinição é `false`.

- **Ativar ou desativar o SMB 1,0**

  O SMB 1,0 é desativado por padrão em uma SVM para a qual um servidor SMB é criado no ONTAP 9.3.

  > A partir do ONTAP 9.3, o SMB 1,0 é desativado por padrão para novos servidores SMB criados no ONTAP 9.3. Você deve migrar para uma versão SMB mais recente o mais rápido possível para se preparar para melhorias de segurança e conformidade. Contacte o seu representante da NetApp para obter mais informações.

- **Ativar ou desativar o SMB 2.x**

  SMB 2,0 é a versão mínima de SMB que suporta failover de LIF. Se desativar o SMB 2.x, o ONTAP também desativa automaticamente o SMB 3.X.

O SMB 2,0 é compatível apenas com SVMs. A opção é ativada por padrão em SVMs

- **Ativar ou desativar o SMB 3,0**

  O SMB 3,0 é a versão mínima para SMB compatível com compartilhamentos disponíveis continuamente. O Windows Server 2012 e o Windows 8 são as versões mínimas do Windows que suportam SMB 3,0.

  O SMB 3,0 é compatível apenas com SVMs. A opção é ativada por padrão em SVMs

- **Ativar ou desativar o SMB 3,1**

  O Windows 10 é a única versão do Windows que suporta SMB 3,1.

  O SMB 3,1 é compatível apenas com SVMs. A opção é ativada por padrão em SVMs

- * Ativar ou desativar a descarga de cópia ODX*

  O descarregamento de cópia ODX é usado automaticamente por clientes Windows que o suportam. Esta opção está ativada por predefinição.

- * Ativar ou desativar o mecanismo de cópia direta para descarga de cópia ODX*

  O mecanismo de cópia direta aumenta o desempenho da operação de descarga de cópia quando os clientes do Windows tentam abrir o arquivo de origem de uma cópia em um modo que impede que o arquivo seja alterado enquanto a cópia está em andamento. Por padrão, o mecanismo de cópia direta está ativado.

- * Ativar ou desativar referências automáticas de nós*

  Com referências automáticas de nós, o servidor SMB refere automaticamente os clientes a um data LIF local para o nó que hospeda os dados acessados através do compartilhamento solicitado.

- **Ativar ou desativar políticas de exportação para SMB**

  Esta opção está desativada por predefinição.

- * Ativar ou desativar usando pontos de junção como pontos de reparação*

  Se esta opção estiver ativada, o servidor SMB expõe pontos de junção para clientes SMB como pontos de reparação. Esta opção é válida apenas para ligações SMB 2.x ou SMB 3,0. Esta opção está ativada por predefinição.

  Esta opção é suportada apenas em SVMs. A opção é ativada por padrão em SVMs

- **Configurando o número máximo de operações simultâneas por conexão TCP**

  O valor padrão é 255.

- **Ativar ou desativar a funcionalidade de grupos e utilizadores locais do Windows**

  Esta opção está ativada por predefinição.

- **Ativar ou desativar a autenticação de utilizadores locais do Windows**

  Esta opção está ativada por predefinição.

- * Ativar ou desativar a funcionalidade de cópia de sombra VSS*

  O ONTAP usa a funcionalidade de cópia de sombra para executar backups remotos de dados armazenados usando a solução Hyper-V sobre SMB.

  Esta opção é suportada apenas em SVMs e apenas para configurações Hyper-V em SMB. A opção é ativada por padrão em SVMs

- **Configurando a profundidade do diretório de cópia de sombra**

  A configuração desta opção permite definir a profundidade máxima dos diretórios para criar cópias de sombra ao usar a funcionalidade de cópia de sombra.

  Esta opção é suportada apenas em SVMs e apenas para configurações Hyper-V em SMB. A opção é ativada por padrão em SVMs

- * Ativar ou desativar recursos de pesquisa de vários domínios para mapeamento de nomes*

  Se ativado, quando um usuário UNIX é mapeado para um usuário de domínio do Windows usando um curinga (*) na parte de domínio do nome de usuário do Windows (por exemplo, * / joe), o ONTAP procura o usuário especificado em todos os domínios com confiança bidirecional para o domínio doméstico. O domínio inicial é o domínio que contém a conta de computador do servidor SMB.

  Como alternativa à pesquisa de todos os domínios bidirecionalmente confiáveis, você pode configurar uma lista de domínios confiáveis preferenciais. Se esta opção estiver ativada e uma lista de preferências estiver configurada, a lista de preferências será utilizada para efetuar pesquisas de mapeamento de nomes de vários domínios.

  O padrão é habilitar pesquisas de mapeamento de nomes de vários domínios.

- **Configurando o tamanho do setor do sistema de arquivos**

  A configuração desta opção permite configurar o tamanho do setor do sistema de arquivos em bytes que o ONTAP reporta para clientes SMB. Existem dois valores válidos para esta opção: `4096` E `512`. O valor padrão é `4096`. Talvez seja necessário definir esse valor `512` se o aplicativo Windows suportar apenas um tamanho de setor de 512 bytes.

- **Ativar ou desativar o controlo de Acesso Dinâmico**

  Ativar esta opção permite proteger objetos no servidor SMB utilizando o controlo de Acesso Dinâmico (DAC), incluindo a utilização de auditoria para encenar políticas de acesso centrais e utilizar objetos de Diretiva de Grupo para implementar políticas de acesso centrais. A opção está desativada por predefinição.

  Esta opção é suportada apenas em SVMs.

- * Definir as restrições de acesso para sessões não autenticadas (restringir anônimo)*

  Definir esta opção determina quais são as restrições de acesso para sessões não autenticadas. As restrições são aplicadas a usuários anônimos. Por padrão, não há restrições de acesso para usuários anônimos.

- * Ativar ou desativar a apresentação de ACLs NTFS em volumes com segurança eficaz UNIX (volumes estilo de segurança UNIX ou volumes mistos estilo de segurança com segurança eficaz UNIX)*

  Ativar ou desativar esta opção determina como a segurança de arquivos em arquivos e pastas com

segurança UNIX é apresentada aos clientes SMB. Se ativado, o ONTAP apresenta arquivos e pastas em volumes com segurança UNIX para clientes SMB como tendo segurança de arquivos NTFS com ACLs NTFS. Se desativado, o ONTAP apresenta volumes com segurança UNIX como volumes FAT, sem segurança de arquivos. Por padrão, os volumes são apresentados como tendo segurança de arquivos NTFS com ACLs NTFS.

- * Habilitando ou desativando a funcionalidade de abertura falsa do SMB*

  A ativação dessa funcionalidade melhora o desempenho do SMB 2.x e do SMB 3,0, otimizando como o ONTAP faz solicitações abertas e fechadas ao consultar informações de atributos em arquivos e diretórios. Por padrão, a funcionalidade de abertura falsa do SMB está ativada. Essa opção é útil somente para conexões feitas com SMB 2.x ou posterior.

- * Ativar ou desativar as extensões UNIX*

  Ativar esta opção ativa extensões UNIX num servidor SMB. As extensões UNIX permitem que a segurança de estilo POSIX/UNIX seja exibida através do protocolo SMB. Por predefinição, esta opção está desativada.

  Se você tiver clientes SMB baseados em UNIX, como clientes Mac OSX, em seu ambiente, você deve habilitar extensões UNIX. A habilitação de extensões UNIX permite que o servidor SMB transmita informações de segurança POSIX/UNIX sobre SMB para o cliente baseado em UNIX, o que converte as informações de segurança em segurança POSIX/UNIX.

- * Ativar ou desativar o suporte para pesquisas de nomes curtos*

  Ativar esta opção permite que o servidor SMB realize pesquisas em nomes curtos. Uma consulta de pesquisa com esta opção ativada tenta corresponder a nomes de arquivo 8,3 juntamente com nomes de arquivo longos. O valor padrão para este parâmetro é `false`.

- * Ativar ou desativar o suporte para publicidade automática de capacidades DFS*

  Ativar ou desativar esta opção determina se os servidores SMB anunciam automaticamente os recursos DFS para clientes SMB 2.x e SMB 3,0 que se conetam a compartilhamentos. O ONTAP usa referências DFS na implementação de links simbólicos para acesso SMB. Se ativado, o servidor SMB sempre anuncia recursos DFS, independentemente de o acesso a links simbólicos estar habilitado. Se estiver desativado, o servidor SMB anunciará os recursos DFS somente quando os clientes se conetarem a compartilhamentos onde o acesso ao link simbólico está habilitado.

- **Configurando o número máximo de créditos SMB**

  A partir do ONTAP 9.4, a configuração da `-max-credits` opção permite limitar o número de créditos a serem concedidos em uma conexão SMB quando clientes e servidor estão executando o SMB versão 2 ou posterior. O valor padrão é 128.

- * Ativar ou desativar o suporte para SMB Multichannel*

  Ativar a `-is-multichannel-enabled` opção no ONTAP 9.4 e versões posteriores permite que o servidor SMB estabeleça várias conexões para uma única sessão SMB quando as NICs apropriadas são implantadas no cluster e em seus clientes. Isso melhora a taxa de transferência e a tolerância a falhas. O valor padrão para este parâmetro é `false`.

  Quando o Multichannel SMB está ativado, você também pode especificar os seguintes parâmetros:

  - O número máximo de conexões permitido por sessão multicanal. O valor padrão para este parâmetro

é 32.

- O número máximo de interfaces de rede anunciadas por sessão multicanal. O valor padrão para este parâmetro é 256.

Configure as opções do servidor SMB do ONTAP

Você pode configurar as opções de servidor SMB a qualquer momento depois de criar um servidor SMB em uma máquina virtual de storage (SVM).

Passo

1. Execute a ação desejada:

Se pretender configurar as opções do servidor SMB…	Digite o comando…
No nível de privilégios de administrador	`vserver cifs options modify -vserver` *`vserver_name options`*
Em nível avançado de privilégios	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

Saiba mais sobre `vserver cifs options modify` e configurar as opções de servidor SMB no "Referência do comando ONTAP".

Configure a permissão Grant UNIX group para usuários SMB do ONTAP

Você pode configurar essa opção para conceder permissões de grupo para acessar arquivos ou diretórios, mesmo que o usuário SMB de entrada não seja o proprietário do arquivo.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Configure a permissão Grant UNIX group conforme apropriado:

Se você quiser	Introduza o comando
Ative o acesso aos arquivos ou diretórios para obter permissões de grupo, mesmo que o usuário não seja o proprietário do arquivo	`vserver cifs options modify -grant-unix-group-perms-to-others true`
Desative o acesso aos arquivos ou diretórios para obter permissões de grupo, mesmo que o usuário não seja o proprietário do arquivo	`vserver cifs options modify -grant-unix-group-perms-to-others false`

3. Verifique se a opção está definida para o valor desejado: `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Configurar restrições de acesso SMB do ONTAP para usuários anônimos

Por padrão, um usuário anônimo e não autenticado (também conhecido como *null user*) pode acessar certas informações na rede. Você pode usar uma opção de servidor SMB para configurar restrições de acesso para o usuário anônimo.

Sobre esta tarefa

A `-restrict-anonymous` opção servidor SMB corresponde à `RestrictAnonymous` entrada do Registro no Windows.

Os usuários anônimos podem listar ou enumerar certos tipos de informações de sistema de hosts do Windows na rede, incluindo nomes e detalhes de usuários, políticas de conta e nomes de compartilhamento. Você pode controlar o acesso para o usuário anônimo especificando uma das três configurações de restrição de acesso:

Valor	Descrição
`no-restriction` (predefinição)	Não especifica restrições de acesso para usuários anônimos.
`no-enumeration`	Especifica que somente a enumeração é restrita para usuários anônimos.
`no-access`	Especifica que o acesso é restrito para usuários anônimos.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Configure a configuração restringir anônimo: `vserver cifs options modify -vserver vserver_name -restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Verifique se a opção está definida para o valor desejado: `vserver cifs options show -vserver vserver_name`
4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

Opções de servidor disponíveis

Gerencie como a segurança de arquivos é apresentada aos clientes SMB para dados de estilo de segurança UNIX

Saiba mais sobre como apresentar a segurança de arquivos ONTAP a clientes SMB para dados de estilo de segurança UNIX

Você pode escolher como deseja apresentar a segurança de arquivos a clientes SMB

para dados de estilo de segurança UNIX ativando ou desativando a apresentação de ACLs NTFS para clientes SMB. Há vantagens em cada configuração, que você deve entender para escolher a configuração mais adequada para seus requisitos de negócios.

Por padrão, o ONTAP apresenta permissões UNIX em volumes estilo de segurança UNIX para clientes SMB como ACLs NTFS. Existem cenários em que isso é desejável, incluindo o seguinte:

- Você deseja exibir e editar permissões UNIX usando a guia **Segurança** na caixa Propriedades do Windows.

  Não é possível modificar permissões de um cliente Windows se a operação não for permitida pelo sistema UNIX. Por exemplo, você não pode alterar a propriedade de um arquivo que você não possui, porque o sistema UNIX não permite essa operação. Essa restrição impede que clientes SMB ignorem permissões UNIX definidas nos arquivos e pastas.

- Os usuários estão editando e salvando arquivos no volume estilo de segurança UNIX usando certos aplicativos do Windows, por exemplo, Microsoft Office, onde o ONTAP deve preservar permissões UNIX durante operações de salvamento.
- Existem certos aplicativos do Windows no seu ambiente que esperam ler ACLs NTFS em arquivos que usam.

Em certas circunstâncias, você pode querer desativar a apresentação de permissões UNIX como ACLs NTFS. Se esta funcionalidade estiver desativada, o ONTAP apresenta volumes de estilo de segurança UNIX como volumes FAT para clientes SMB. Existem razões específicas pelas quais você pode querer apresentar volumes de estilo de segurança UNIX como volumes FAT para clientes SMB:

- Você só altera permissões UNIX usando montagens em clientes UNIX.

  A guia Segurança não está disponível quando um volume de estilo de segurança UNIX é mapeado em um cliente SMB. A unidade mapeada parece ser formatada com o sistema de arquivos FAT, que não tem permissões de arquivo.

- Você está usando aplicativos sobre SMB que definem ACLs NTFS em arquivos e pastas acessados, o que pode falhar se os dados residirem em volumes de estilo de segurança UNIX.

  Se o ONTAP relatar o volume como FAT, o aplicativo não tenta alterar uma ACL.

Informações relacionadas

- Configurar estilos de segurança no FlexVol volumes
- Configurar estilos de segurança no qtrees

Configure a apresentação de ACLs NTFS para clientes SMB do ONTAP para dados de estilo de segurança UNIX

Você pode ativar ou desativar a apresentação de ACLs NTFS para clientes SMB para dados de estilo de segurança UNIX (volumes de estilo de segurança UNIX e volumes mistos de estilo de segurança com segurança efetiva UNIX).

Sobre esta tarefa

Se você ativar essa opção, o ONTAP apresenta arquivos e pastas em volumes com estilo de segurança UNIX eficaz para clientes SMB como tendo ACLs NTFS. Se desativar esta opção, os volumes são apresentados como volumes FAT para clientes SMB. O padrão é apresentar ACLs NTFS a clientes SMB.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Configure a configuração da opção ACL NTFS UNIX: `vserver cifs options modify -vserver` *`vserver_name`* `-is-unix-nt-acl-enabled {true|false}`
3. Verifique se a opção está definida para o valor desejado: `vserver cifs options show -vserver` *`vserver_name`*
4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Saiba mais sobre como preservar permissões UNIX para volumes FlexVol SMB do ONTAP

Quando os arquivos em um FlexVol volume que atualmente têm permissões UNIX são editados e salvos por aplicativos do Windows, o ONTAP pode preservar as permissões UNIX.

Quando os aplicativos em clientes do Windows editam e salvam arquivos, eles leem as propriedades de segurança do arquivo, criam um novo arquivo temporário, aplicam essas propriedades ao arquivo temporário e dão ao arquivo temporário o nome do arquivo original.

Quando os clientes Windows executam uma consulta para as propriedades de segurança, eles recebem uma ACL construída que representa exatamente as permissões UNIX. O único propósito desta ACL construída é preservar as permissões UNIX do arquivo, pois os arquivos são atualizados por aplicativos do Windows para garantir que os arquivos resultantes tenham as mesmas permissões UNIX. O ONTAP não define nenhuma ACLs NTFS usando a ACL construída.

Saiba mais sobre como gerenciar permissões UNIX usando a guia Segurança do Windows para servidores SMB do ONTAP

Se você quiser manipular permissões UNIX de arquivos ou pastas em volumes mistos de estilo de segurança ou qtrees em SVMs, você pode usar a guia Segurança em clientes Windows. Como alternativa, você pode usar aplicativos que podem consultar e definir ACLs do Windows.

- Modificação de permissões UNIX

  Você pode usar a guia Segurança do Windows para exibir e alterar permissões UNIX para um volume ou qtree misto de estilo de segurança. Se você usar a guia principal de Segurança do Windows para alterar permissões UNIX, primeiro remova o ACE existente que deseja editar (isso define os bits de modo como 0) antes de fazer as alterações. Como alternativa, você pode usar o editor avançado para alterar permissões.

  Se as permissões de modo forem usadas, você pode alterar diretamente as permissões de modo para o UID listado, GID e outros (todos os outros com uma conta no computador). Por exemplo, se o UID exibido tiver permissões r-x, você pode alterar as permissões UID para rwx.

- Alterando permissões UNIX para permissões NTFS

  Você pode usar a guia Segurança do Windows para substituir objetos de segurança UNIX por objetos de segurança do Windows em um volume de estilo de segurança misto ou qtree onde os arquivos e pastas têm um estilo de segurança eficaz UNIX.

  Você deve primeiro remover todas as entradas de permissão UNIX listadas antes de poder substituí-las

pelos objetos de Usuário e Grupo do Windows desejados. Em seguida, você pode configurar ACLs baseadas em NTFS nos objetos Usuário e Grupo do Windows. Removendo todos os objetos de segurança UNIX e adicionando apenas usuários e grupos do Windows a um arquivo ou pasta em um volume ou qtree misto de estilo de segurança, você altera o estilo de segurança efetivo no arquivo ou pasta de UNIX para NTFS.

Ao alterar permissões em uma pasta, o comportamento padrão do Windows é propagar essas alterações para todas as subpastas e arquivos. Portanto, você deve alterar a opção de propagação para a configuração desejada se não quiser propagar uma alteração no estilo de segurança para todas as pastas, subpastas e arquivos filhos.

Gerenciar configurações de segurança do servidor SMB

Saiba mais sobre como lidar com a autenticação de cliente SMB do ONTAP

Antes que os usuários possam criar conexões SMB para acessar dados contidos no SVM, elas devem ser autenticadas pelo domínio ao qual o servidor SMB pertence. O servidor SMB suporta dois métodos de autenticação, Kerberos e NTLM (NTLMv1 ou NTLMv2). Kerberos é o método padrão usado para autenticar usuários de domínio.

Autenticação Kerberos

O ONTAP oferece suporte à autenticação Kerberos ao criar sessões SMB autenticadas.

Kerberos é o serviço de autenticação principal do ative Directory. O servidor Kerberos, ou serviço KDC (Centro de distribuição de chaves Kerberos), armazena e recupera informações sobre princípios de segurança no ative Directory. Ao contrário do modelo NTLM, os clientes do ative Directory que desejam estabelecer uma sessão com outro computador, como o servidor SMB, contatam diretamente um KDC para obter suas credenciais de sessão.

Autenticação NTLM

A autenticação de cliente NTLM é feita usando um protocolo de resposta de desafio baseado no conhecimento compartilhado de um segredo específico do usuário com base em uma senha.

Se um usuário criar uma conexão SMB usando uma conta de usuário local do Windows, a autenticação é feita localmente pelo servidor SMB usando NTLMv2.

Saiba mais sobre as configurações de segurança do servidor SMB para a configuração de recuperação de desastres do ONTAP SVM

Antes de criar um SVM configurado como um destino de recuperação de desastres em que a identidade não seja preservada (a `-identity-preserve` opção está definida como `false` na configuração do SnapMirror), você deve saber como as configurações de segurança do servidor SMB são gerenciadas no SVM de destino.

- As configurações de segurança de servidor SMB não padrão não são replicadas para o destino.

  Quando você cria um servidor SMB no SVM de destino, todas as configurações de segurança do servidor SMB são definidas como valores padrão. Quando o destino de recuperação de desastres da SVM é inicializado, atualizado ou ressincido, as configurações de segurança do servidor SMB na origem não são

replicadas para o destino.

- Você deve configurar manualmente configurações de segurança de servidor SMB não padrão.

  Se você tiver configurações de segurança de servidor SMB não padrão configuradas no SVM de origem, será necessário configurar manualmente essas mesmas configurações no SVM de destino depois que o destino se tornar leitura-gravação (depois que a relação SnapMirror for interrompida).

Exibir informações sobre as configurações de segurança do servidor SMB do ONTAP

Você pode exibir informações sobre as configurações de segurança do servidor SMB em suas máquinas virtuais de armazenamento (SVMs). Pode utilizar estas informações para verificar se as definições de segurança estão corretas.

Sobre esta tarefa

Uma configuração de segurança exibida pode ser o valor padrão para esse objeto ou um valor não padrão configurado usando a CLI do ONTAP ou usando objetos de diretiva de grupo (GPOs) do ative Directory.

Não use o `vserver cifs security show` comando para servidores SMB no modo de grupo de trabalho, porque algumas das opções não são válidas.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite o comando…
Todas as configurações de segurança em uma SVM especificada	`vserver cifs security show -vserver` *`vserver_name`*
Configurações ou configurações de segurança específicas no SVM	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` Você pode inserir `-fields ?` para determinar quais campos você pode usar.

Exemplo

O exemplo a seguir mostra todas as configurações de segurança do SVM VS1:

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                          Kerberos Clock Skew:        5 minutes
                          Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:        7 days
                         Kerberos KDC Timeout:        3 seconds
                          Is Signing Required:        false
               Is Password Complexity Required:        true
          Use start_tls For AD LDAP connection:        false
                     Is AES Encryption Enabled:        false
                        LM Compatibility Level:        lm-ntlm-ntlmv2-krb
                    Is SMB Encryption Required:        false
                       Client Session Security:        none
              SMB1 Enabled for DC Connections:        false
              SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:        false
             Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:        false
 AES session key enabled for NetLogon channel:        false
  Try Channel Binding For AD LDAP Connections:        false
```

Observe que as configurações exibidas dependem da versão do ONTAP em execução.

O exemplo a seguir mostra a inclinação do relógio Kerberos para SVM VS1:

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

Informações relacionadas

Apresentar informações sobre as configurações do GPO

Configurar a complexidade da senha do ONTAP para usuários locais de SMB

A complexidade de senha necessária fornece segurança aprimorada para usuários locais de SMB em suas máquinas virtuais de armazenamento (SVMs). A funcionalidade de complexidade de palavra-passe necessária está ativada por predefinição. Você pode desativá-lo e reativá-lo a qualquer momento.

Antes de começar

Usuários locais, grupos locais e autenticação de usuário local devem estar habilitados no servidor CIFS.

Sobre esta tarefa

Não use o `vserver cifs security modify` comando para um servidor CIFS no modo de grupo de trabalho porque algumas das opções não são válidas.

Passos

1. Execute uma das seguintes ações:

Se você quiser que a complexidade de senha necessária para usuários SMB locais seja…	Digite o comando…
Ativado	`vserver cifs security modify -vserver vserver_name -is-password-complexity -required true`
Desativado	`vserver cifs security modify -vserver vserver_name -is-password-complexity -required false`

2. Verifique a configuração de segurança para a complexidade necessária da senha: `vserver cifs security show -vserver vserver_name`

Exemplo

O exemplo a seguir mostra que a complexidade de senha necessária está habilitada para usuários SMB locais para SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- ------------------------------
vs1     true
```

Informações relacionadas

- Exibir informações sobre as configurações de segurança do servidor
- Aprenda sobre usuários e grupos locais
- Requisitos para senhas de usuários locais
- Altere as senhas da conta de usuário local

Modifique as configurações de segurança Kerberos do servidor SMB do ONTAP

Você pode modificar certas configurações de segurança Kerberos do servidor CIFS, incluindo o tempo máximo permitido de distorção do relógio Kerberos, a vida útil do ticket

Kerberos e o número máximo de dias de renovação de ticket.

Sobre esta tarefa

Modificar as configurações do Kerberos do servidor CIFS usando o `vserver cifs security modify` comando modifica as configurações somente na máquina virtual de armazenamento (SVM) única que você especificar com o `-vserver` parâmetro. Você pode gerenciar centralmente as configurações de segurança Kerberos para todos os SVMs no cluster que pertencem ao mesmo domínio do ative Directory usando os GPOs (objetos de diretiva de grupo) do ative Directory.

Passos

1. Execute uma ou mais das seguintes ações:

Se você quiser…	Digite…
Especifique o tempo máximo permitido de distorção do relógio Kerberos em minutos (9.13.1 e posterior) ou segundos (9.12.1 ou anterior).	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* A predefinição é 5 minutos.
Especifique a vida útil do ticket Kerberos em horas.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` A predefinição é 10 horas.
Especifique o número máximo de dias de renovação do ticket.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`* A configuração padrão é de 7 dias.
Especifique o tempo limite para sockets em KDCs após o qual todos os KDCs são marcados como inalcançáveis.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* A predefinição é 3 segundos.

2. Verifique as configurações de segurança do Kerberos:

   `vserver cifs security show -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir faz as seguintes alterações na segurança Kerberos: "'Kerberos Clock Skew'" está definido como 3 minutos e "'Kerberos Ticket Age'" está definido como 8 horas para o SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                    Kerberos Clock Skew:                    3 minutes
                    Kerberos Ticket Age:                    8 hours
                  Kerberos Renewal Age:                     7 days
                  Kerberos KDC Timeout:                     3 seconds
                    Is Signing Required:                false
         Is Password Complexity Required:                 true
   Use start_tls For AD LDAP connection:                 false
              Is AES Encryption Enabled:                 false
                 LM Compatibility Level:  lm-ntlm-ntlmv2-krb
             Is SMB Encryption Required:                 false
```

Informações relacionadas

"Exibir informações sobre as configurações de segurança do servidor"

"GPOs compatíveis"

"Aplicando objetos de Diretiva de Grupo a servidores CIFS"

Defina o nível mínimo de segurança de autenticação do servidor SMB do ONTAP

Você pode definir o nível mínimo de segurança do servidor SMB, também conhecido como *LMCompatibilityLevel*, em seu servidor SMB para atender aos requisitos de segurança da sua empresa para acesso ao cliente SMB. O nível mínimo de segurança é o nível mínimo dos tokens de segurança que o servidor SMB aceita de clientes SMB.

Sobre esta tarefa

- Os servidores SMB no modo de grupo de trabalho suportam apenas a autenticação NTLM. A autenticação Kerberos não é suportada.
- LMCompatibilityLevel aplica-se apenas à autenticação de cliente SMB, não à autenticação de administrador.

Você pode definir o nível mínimo de segurança de autenticação para um dos quatro níveis de segurança suportados.

Valor	Descrição
`lm-ntlm-ntlmv2-krb` (predefinição)	A máquina virtual de armazenamento (SVM) aceita segurança de autenticação LM, NTLM, NTLMv2 e Kerberos.

Valor	Descrição
`ntlm-ntlmv2-krb`	O SVM aceita segurança de autenticação NTLM, NTLMv2 e Kerberos. O SVM nega a autenticação LM.
`ntlmv2-krb`	O SVM aceita a segurança de autenticação NTLMv2 e Kerberos. O SVM nega a autenticação LM e NTLM.
`krb`	O SVM aceita apenas a segurança de autenticação Kerberos. O SVM nega a autenticação LM, NTLM e NTLMv2.

Passos

1. Defina o nível mínimo de segurança de autenticação: `vserver cifs security modify -vserver` *`vserver_name`* `-lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Verifique se o nível de segurança de autenticação está definido para o nível desejado: `vserver cifs security show -vserver` *`vserver_name`*

Informações relacionadas

Configurar criptografia AES para comunicação baseada em Kerberos

Configure a segurança forte do SMB do ONTAP para comunicação baseada no Kerberos usando criptografia AES

Para uma segurança mais forte com comunicação baseada no Kerberos, é possível ativar a criptografia AES-256 e AES-128 no servidor SMB. Por padrão, quando você cria um servidor SMB no SVM, a criptografia AES (Advanced Encryption Standard) é desativada. Você deve habilitá-lo para aproveitar a segurança forte fornecida pela criptografia AES.

A comunicação relacionada ao Kerberos para SMB é usada durante a criação do servidor SMB na SVM, bem como durante a fase de configuração da sessão SMB. O servidor SMB suporta os seguintes tipos de criptografia para comunicação Kerberos:

- AES 256
- AES 128
- DES
- RC4-HMAC

Se você quiser usar o tipo de criptografia de segurança mais alto para comunicação Kerberos, ative a criptografia AES para comunicação Kerberos no SVM.

Quando o servidor SMB é criado, o controlador de domínio cria uma conta de máquina de computador no ative Directory. Neste momento, o KDC se torna ciente dos recursos de criptografia da conta de máquina específica. Posteriormente, um tipo de criptografia específico é selecionado para criptografar o ticket de serviço que o cliente apresenta ao servidor durante a autenticação.

A partir do ONTAP 9.12,1, você pode especificar quais tipos de criptografia anunciar no KDC do ative

Directory (AD). Pode utilizar a `-advertised-enc-types` opção para ativar os tipos de encriptação recomendados e pode utilizá-la para desativar os tipos de encriptação mais fracos. Aprenda a "Configurar criptografia AES para comunicação baseada em Kerberos".

> As novas instruções Intel AES (Intel AES NI) estão disponíveis no SMB 3,0, melhorando o algoritmo AES e acelerando a criptografia de dados com famílias de processadores suportadas.começando com SMB 3,1.1, AES-128-GCM substitui AES-128-CCM como o algoritmo hash usado pela criptografia SMB.

Informações relacionadas

Modifique as configurações de segurança do servidor

Configurar a criptografia AES para comunicação baseada em Kerberos ONTAP SMB

Para aproveitar a segurança mais forte com a comunicação baseada no Kerberos, você deve usar a criptografia AES-256 e AES-128 no servidor SMB. A partir do ONTAP 9.13,1, a encriptação AES é ativada por predefinição. Se você não quiser que o servidor SMB selecione os tipos de criptografia AES para comunicação baseada em Kerberos com o KDC do ative Directory (AD), você pode desativar a criptografia AES.

Se a encriptação AES está ativada por predefinição e se tem a opção de especificar tipos de encriptação depende da versão do ONTAP.

Versão de ONTAP	A encriptação AES está ativada …	Você pode especificar tipos de criptografia?
9.13.1 e mais tarde	Por padrão	Sim
9.12.1	Manualmente	Sim
9.11.1 e anteriores	Manualmente	Não

A partir do ONTAP 9.12,1, a criptografia AES é ativada e desativada usando a `-advertised-enc-types` opção, que permite especificar os tipos de criptografia anunciados para o AD KDC. A configuração padrão é `rc4` e `des`, mas quando um tipo AES é especificado, a criptografia AES é ativada. Você também pode usar a opção para desativar explicitamente os tipos de criptografia RC4 e DES mais fracos. No ONTAP 9.11,1 e anterior, você deve usar a `-is-aes-encryption-enabled` opção para ativar e desativar a criptografia AES e os tipos de criptografia não podem ser especificados.

Para melhorar a segurança, a máquina virtual de armazenamento (SVM) altera a senha da conta de máquina no AD sempre que a opção de segurança AES é modificada. A alteração da senha pode exigir credenciais administrativas do AD para a unidade organizacional (ou) que contém a conta da máquina.

Se um SVM for configurado como um destino de recuperação de desastres em que a identidade não seja preservada (a `-identity-preserve` opção está definida como `false` na configuração do SnapMirror), as configurações de segurança do servidor SMB não padrão não serão replicadas para o destino. Se você ativou a criptografia AES no SVM de origem, será necessário habilitá-la manualmente.

Exemplo 1. Passos

ONTAP 9.12,1 e posterior

1. Execute uma das seguintes ações:

Se você quiser que os tipos de criptografia AES para comunicação Kerberos sejam…	Digite o comando…
Ativado	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
Desativado	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

   Nota: a `-is-aes-encryption-enabled` opção está obsoleta no ONTAP 9.12,1 e pode ser removida em uma versão posterior.

2. Verifique se a criptografia AES está ativada ou desativada conforme desejado: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Exemplos

O exemplo a seguir habilita os tipos de criptografia AES para o servidor SMB no SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

O exemplo a seguir habilita os tipos de criptografia AES para o servidor SMB no SVM VS2. O administrador é solicitado a inserir as credenciais administrativas do AD para a UO que contém o servidor SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11,1 e anteriores

1. Execute uma das seguintes ações:

Se você quiser que os tipos de criptografia AES para comunicação Kerberos sejam…	Digite o comando…
Ativado	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
Desativado	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. Verifique se a criptografia AES está ativada ou desativada conforme desejado: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   O `is-aes-encryption-enabled` campo é exibido `true` se a criptografia AES estiver ativada e `false` se estiver desativada.

Exemplos

O exemplo a seguir habilita os tipos de criptografia AES para o servidor SMB no SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

O exemplo a seguir habilita os tipos de criptografia AES para o servidor SMB no SVM VS2. O administrador é solicitado a inserir as credenciais administrativas do AD para a UO que contém o servidor SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

Informações relacionadas

"O usuário de domínio não consegue fazer login no cluster com Domain-Tunnel"

Utilize a assinatura SMB para melhorar a segurança da rede

Saiba mais sobre como usar a assinatura SMB do ONTAP para melhorar a segurança da rede

A assinatura SMB ajuda a garantir que o tráfego de rede entre o servidor SMB e o cliente não seja comprometido; isso evita ataques de repetição. Por padrão, o ONTAP oferece suporte à assinatura SMB quando solicitado pelo cliente. Opcionalmente, o administrador de armazenamento pode configurar o servidor SMB para exigir assinatura SMB.

Saiba como as políticas de assinatura afetam a comunicação com servidores SMB da ONTAP

Além das configurações de segurança de assinatura SMB do servidor CIFS, duas diretivas de assinatura SMB em clientes Windows controlam a assinatura digital de comunicações entre clientes e o servidor CIFS. Você pode configurar a configuração que atende aos requisitos da sua empresa.

As diretivas SMB do cliente são controladas por meio das configurações de diretiva de segurança local do Windows, que são configuradas usando o MMC (Console de Gerenciamento da Microsoft) ou GPOs do ative Directory. Para obter mais informações sobre a assinatura SMB do cliente e problemas de segurança, consulte a documentação do Microsoft Windows.

Aqui estão descrições das duas políticas de assinatura SMB em clientes Microsoft:

- `Microsoft network client: Digitally sign communications (if server agrees)`

  Esta configuração controla se a capacidade de assinatura SMB do cliente está ativada. Ele é habilitado por padrão. Quando essa configuração é desativada no cliente, as comunicações do cliente com o servidor CIFS dependem da configuração de assinatura SMB no servidor CIFS.

- `Microsoft network client: Digitally sign communications (always)`

  Esta configuração controla se o cliente requer assinatura SMB para se comunicar com um servidor. Ele está desativado por padrão. Quando essa configuração é desativada no cliente, o comportamento de assinatura SMB é baseado na configuração de diretiva `Microsoft network client: Digitally sign communications (if server agrees)` e na configuração no servidor CIFS.

> Se o seu ambiente incluir clientes Windows configurados para exigir assinatura SMB, você deverá ativar a assinatura SMB no servidor CIFS. Se você não fizer isso, o servidor CIFS não poderá fornecer dados a esses sistemas.

Os resultados efetivos das configurações de assinatura SMB do cliente e do servidor CIFS dependem se as sessões SMB usam SMB 1,0 ou SMB 2.x e posterior.

A tabela a seguir resume o comportamento eficaz de assinatura SMB se a sessão usar SMB 1,0:

Cliente	ONTAP—assinatura não necessária	ONTAP - assinatura necessária
Assinatura desativada e não necessária	Não assinado	Assinado
Assinatura ativada e não necessária	Não assinado	Assinado
Assinatura desativada e necessária	Assinado	Assinado
Assinatura ativada e necessária	Assinado	Assinado

Clientes Windows SMB 1 mais antigos e alguns clientes SMB 1 não Windows podem não conseguir se conetar se a assinatura estiver desativada no cliente, mas necessária no servidor CIFS.

A tabela a seguir resume o comportamento eficaz de assinatura SMB se a sessão usar SMB 2.x ou SMB 3,0:

Para clientes SMB 2.x e SMB 3,0, a assinatura SMB está sempre ativada. Não pode ser desativado.

Cliente	ONTAP—assinatura não necessária	ONTAP - assinatura necessária
Assinatura não necessária	Não assinado	Assinado
Assinatura necessária	Assinado	Assinado

A tabela a seguir resume o comportamento padrão de assinatura SMB de cliente e servidor da Microsoft:

Protocolo	Algoritmo hash	Pode ativar/desativar	Pode exigir/não exigir	Padrão do cliente	Padrão do servidor	DC predefinido
SMB 1,0	MD5	Sim	Sim	Ativado (não necessário)	Desativado (não necessário)	Obrigatório
SMB 2.x	HMAC SHA-256	Não	Sim	Não é necessário	Não é necessário	Obrigatório
SMB 3,0	AES-CMAC.	Não	Sim	Não é necessário	Não é necessário	Obrigatório

A Microsoft não recomenda mais o uso `Digitally sign communications (if client agrees)` das configurações de Diretiva de Grupo ou `Digitally sign communications (if server agrees)` . A Microsoft também não recomenda mais o uso das `EnableSecuritySignature` configurações do Registro. Essas opções afetam apenas o comportamento do SMB 1 e podem ser substituídas pela `Digitally sign communications (always)` configuração de Diretiva de Grupo ou pela `RequireSecuritySignature` configuração do Registro. Você também pode obter mais informações do blog da Microsoft.http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[The Fundamentos de assinatura SMB (abrangendo SMB1 e SMB2)]

Saiba mais sobre o impactos no desempenho da assinatura SMB do ONTAP

Quando as sessões SMB usam a assinatura SMB, todas as comunicações SMB de e para clientes Windows têm um impactos na performance, o que afeta tanto os clientes quanto o servidor (ou seja, os nós no cluster que executa o SVM que contém o servidor SMB).

O impactos no desempenho mostra como aumento do uso da CPU tanto nos clientes quanto no servidor, embora a quantidade de tráfego de rede não mude.

A extensão do impactos no desempenho depende da versão do ONTAP 9 que você está executando. A partir do ONTAP 9.7, um novo algoritmo de criptografia off-load pode permitir melhor desempenho no tráfego SMB assinado. A descarga de assinatura SMB é ativada por padrão quando a assinatura SMB está ativada.

O desempenho aprimorado de assinatura SMB requer a capacidade de descarga AES-NI. Consulte o Hardware Universe (HWU) para verificar se a descarga AES-NI é suportada para sua plataforma.

Melhorias adicionais de desempenho também são possíveis se você for capaz de usar SMB versão 3,11, que suporta o algoritmo GCM muito mais rápido.

Dependendo da sua rede, versão do ONTAP 9, versão do SMB e implementação do SVM, o impactos na performance da assinatura SMB pode variar muito. Você pode verificá-lo somente por meio de testes em seu ambiente de rede.

A maioria dos clientes do Windows negocia a assinatura SMB por padrão se estiver habilitada no servidor. Se você precisar de proteção SMB para alguns de seus clientes Windows e se a assinatura SMB estiver causando problemas de desempenho, você poderá desativar a assinatura SMB em qualquer um de seus clientes Windows que não precisem de proteção contra ataques de repetição. Para obter informações sobre como desativar a assinatura SMB em clientes Windows, consulte a documentação do Microsoft Windows.

Recomendações de configuração de assinatura SMB do ONTAP

Você pode configurar o comportamento de assinatura SMB entre clientes SMB e o servidor CIFS para atender aos seus requisitos de segurança. As configurações escolhidas ao configurar a assinatura SMB no servidor CIFS dependem de quais são os requisitos de segurança.

Você pode configurar a assinatura SMB no cliente ou no servidor CIFS. Considere as seguintes recomendações ao configurar a assinatura SMB:

Se…	Recomendação…
Você deseja aumentar a segurança da comunicação entre o cliente e o servidor	Torne a assinatura SMB necessária no cliente ativando a `Require Option (Sign always)` configuração de segurança no cliente.
Você deseja que todo o tráfego SMB para uma determinada máquina virtual de storage (SVM) seja assinado	Torne necessária a assinatura SMB no servidor CIFS configurando as configurações de segurança para exigir assinatura SMB.

Consulte a documentação da Microsoft para obter mais informações sobre como configurar as configurações de segurança do cliente Windows.

Saiba mais sobre a configuração de assinatura SMB do ONTAP para vários LIFS de dados

Se você ativar ou desativar a assinatura SMB necessária no servidor SMB, você deve estar ciente das diretrizes para várias configurações LIFS de dados para um SVM.

Quando você configura um servidor SMB, pode haver várias LIFs de dados configuradas. Nesse caso, o

servidor DNS contém várias `A` entradas de Registro para o servidor CIFS, todas usando o mesmo nome de host do servidor SMB, mas cada uma com um endereço IP exclusivo. Por exemplo, um servidor SMB que tem duas LIFs de dados configuradas pode ter as seguintes entradas de Registro DNS `A`:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

O comportamento normal é que, ao alterar a configuração de assinatura SMB necessária, apenas novas conexões de clientes são afetadas pela alteração na configuração de assinatura SMB. No entanto, há uma exceção a esse comportamento. Há um caso em que um cliente tem uma conexão existente com um compartilhamento, e o cliente cria uma nova conexão com o mesmo compartilhamento após a configuração ser alterada, mantendo a conexão original. Nesse caso, tanto a conexão SMB nova quanto a existente adotam os novos requisitos de assinatura SMB.

Considere o seguinte exemplo:

1. Client1 coneta-se a um compartilhamento sem a assinatura SMB necessária usando o caminho `O:\`.
2. O administrador de armazenamento modifica a configuração do servidor SMB para exigir assinatura SMB.
3. O Client1 coneta-se ao mesmo compartilhamento com a assinatura SMB necessária usando o caminho `S:\` (mantendo a conexão usando o caminho `O:\`).
4. O resultado é que a assinatura SMB é usada ao acessar dados `O:\` nas unidades e `S:\` .

Configurar a assinatura ONTAP para o tráfego SMB de entrada

Você pode impor o requisito para que os clientes assinem mensagens SMB habilitando a assinatura SMB necessária. Se ativado, o ONTAP aceita mensagens SMB somente se elas tiverem assinaturas válidas. Se você quiser permitir a assinatura SMB, mas não a exigir, você pode desativar a assinatura SMB necessária.

Sobre esta tarefa

Por padrão, a assinatura SMB necessária está desativada. Você pode ativar ou desativar a assinatura SMB necessária a qualquer momento.

> A assinatura SMB não está desativada por padrão nas seguintes circunstâncias:
>
> 1. A assinatura SMB necessária está ativada e o cluster é revertido para uma versão do ONTAP que não suporta assinatura SMB.
> 2. O cluster é posteriormente atualizado para uma versão do ONTAP que suporte a assinatura SMB.
>
>   Nestas circunstâncias, a configuração de assinatura SMB que foi originalmente configurada em uma versão suportada do ONTAP é mantida por meio de reversão e atualização subsequente.

Quando você configura uma relação de recuperação de desastres de máquina virtual de storage (SVM), o valor selecionado para a `-identity-preserve` opção `snapmirror create` do comando determina os detalhes de configuração replicados no SVM de destino.

Se você definir `-identity-preserve` a opção como `true` (ID-Preserve), a configuração de segurança de assinatura SMB será replicada para o destino.

Se você definir `-identity-preserve` a opção como `false` (non-ID-Preserve), a configuração de segurança de assinatura SMB não será replicada para o destino. Nesse caso, as configurações de segurança do servidor CIFS no destino são definidas com os valores padrão. Se você ativou a assinatura SMB necessária na SVM de origem, habilite manualmente a assinatura SMB necessária no SVM de destino.

Passos

1. Execute uma das seguintes ações:

Se você quiser que a assinatura SMB seja necessária…	Digite o comando…
Ativado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
Desativado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. Verifique se a assinatura SMB necessária está ativada ou desativada determinando se o valor no `Is Signing Required` campo na saída do comando a seguir está definido para o valor desejado: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

Exemplo

O exemplo a seguir habilita a assinatura SMB necessária para o SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- --------------------
vs1      true
```

As alterações nas definições de encriptação entram em vigor para novas ligações. As ligações existentes não são afetadas.

Informações relacionadas

- "SnapMirror create"

Determine se as sessões SMB do ONTAP são assinadas

Você pode exibir informações sobre sessões SMB conetadas no servidor CIFS. Você pode usar essas informações para determinar se as sessões SMB são assinadas. Isso pode ser útil para determinar se as sessões de cliente SMB estão se conetando com as

configurações de segurança desejadas.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite o comando…
Todas as sessões assinadas em uma máquina virtual de storage (SVM) especificada	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
Detalhes de uma sessão assinada com um Session ID específico no SVM	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

Exemplos

O comando a seguir exibe informações de sessão sobre sessões assinadas no SVM VS1. A saída de resumo padrão não exibe o campo de saída "'is Session signed'":

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

O comando a seguir exibe informações detalhadas da sessão, incluindo se a sessão está assinada, em uma sessão SMB com um Session ID de 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   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: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Informações relacionadas

Monitoramento de estatísticas de sessão assinadas pelo SMB

Monitorar estatísticas de sessão assinadas pelo ONTAP SMB

Você pode monitorar estatísticas de sessões SMB e determinar quais sessões estabelecidas são assinadas e quais não são.

Sobre esta tarefa

O `statistics` comando no nível de privilégio avançado fornece o `signed_sessions` contador que você pode usar para monitorar o número de sessões SMB assinadas. O `signed_sessions` contador está disponível com os seguintes objetos estatísticos:

- `cifs` Permite monitorar a assinatura SMB para todas as sessões SMB.
- `smb1` Permite monitorar a assinatura SMB para sessões SMB 1,0.
- `smb2` Permite monitorar a assinatura SMB para sessões SMB 2.x e SMB 3,0.

  As estatísticas SMB 3,0 são incluídas na saída para o `smb2` objeto.

Se você quiser comparar o número de sessão assinada com o número total de sessões, você pode comparar a saída para o contador com a saída `established_sessions` para `signed_sessions` o contador.

Você deve iniciar uma coleta de amostras de estatísticas antes de poder visualizar os dados resultantes. Você pode exibir dados da amostra se não parar a coleta de dados. Parar a coleta de dados dá-lhe uma amostra

fixa. Não interromper a coleta de dados dá a você a capacidade de obter dados atualizados que você pode usar para comparar com consultas anteriores. A comparação pode ajudá-lo a identificar tendências.

Passos

1. Defina o nível de privilégio como avançado `set -privilege advanced`
2. Iniciar uma coleta de dados `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Se você não especificar o `-sample-id` parâmetro, o comando gera um identificador de amostra para você e define esse exemplo como a amostra padrão para a sessão CLI. O valor para `-sample-id` é uma cadeia de texto. Se você executar esse comando durante a mesma sessão CLI e não especificar o `-sample-id` parâmetro, o comando sobrescreverá a amostra padrão anterior.

   Opcionalmente, você pode especificar o nó no qual deseja coletar estatísticas. Se você não especificar o nó, a amostra coletará estatísticas para todos os nós no cluster.

   Saiba mais sobre `statistics start` o "Referência do comando ONTAP"na .

3. Use o `statistics stop` comando para parar de coletar dados para a amostra.

   Saiba mais sobre `statistics stop` no "Referência do comando ONTAP" .

4. Exibir estatísticas de assinatura SMB:

Se você quiser ver informações para…	**Digite…**
Sessões assinadas	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	Sessões assinadas e sessões estabelecidas
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   Se você quiser exibir informações apenas para um único nó, especifique o parâmetro opcional `-node`.

   Saiba mais sobre `statistics show` o "Referência do comando ONTAP"na .

5. Voltar para o nível de privilégio de administrador `set -privilege admin`

Exemplos

O exemplo a seguir mostra como você pode monitorar as estatísticas de assinatura SMB 2.x e SMB 3,0 na máquina virtual de armazenamento (SVM) VS1.

O seguinte comando move-se para o nível de privilégio avançado:

```
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
```

O comando a seguir inicia a coleta de dados para uma nova amostra:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

O comando a seguir interrompe a coleta de dados para a amostra:

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

O comando a seguir mostra sessões SMB assinadas e sessões SMB estabelecidas por nó da amostra:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    established_sessions                                         0
    node_name                                                node1
    signed_sessions                                              0
    established_sessions                                         1
    node_name                                                node2
    signed_sessions                                              1
    established_sessions                                         0
    node_name                                                node3
    signed_sessions                                              0
    established_sessions                                         0
    node_name                                                node4
    signed_sessions                                              0
```

O comando a seguir mostra sessões SMB assinadas para node2 da amostra:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    node_name                                                node2
    signed_sessions                                              1
```

O seguinte comando volta para o nível de privilégio admin:

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

Informações relacionadas

- Determine se as sessões SMB são assinadas
- "Visão geral do gerenciamento e monitoramento de desempenho"

Configurar a criptografia SMB necessária em servidores SMB para transferências de dados por SMB

Saiba mais sobre a criptografia SMB do ONTAP

A encriptação SMB para transferências de dados através de SMB é um melhoramento de segurança que pode ativar ou desativar em servidores SMB. Você também pode configurar a configuração de criptografia SMB desejada em uma base de compartilhamento por compartilhamento por meio de uma configuração de propriedade de compartilhamento.

Por padrão, quando você cria um servidor SMB na máquina virtual de storage (SVM), a criptografia SMB é desativada. Você deve habilitá-lo para aproveitar a segurança aprimorada fornecida pela criptografia SMB.

Para criar uma sessão SMB encriptada, o cliente SMB tem de suportar a encriptação SMB. Os clientes Windows que começam com o Windows Server 2012 e o Windows 8 suportam a encriptação SMB.

A criptografia SMB no SVM é controlada por meio de duas configurações:

- Uma opção de segurança de servidor SMB que habilita a funcionalidade no SVM
- Uma propriedade de compartilhamento SMB que configura a configuração de criptografia SMB em uma base de compartilhamento por compartilhamento

Você pode decidir se deseja exigir criptografia para acesso a todos os dados no SVM ou se exige que a criptografia SMB acesse dados somente em compartilhamentos selecionados. As configurações de nível SVM substituem as configurações de nível de compartilhamento.

A configuração eficaz de criptografia SMB depende da combinação das duas configurações e é descrita na tabela a seguir:

Encriptação SMB do servidor SMB ativada	Compartilhar criptografar a configuração de dados ativada	Comportamento de criptografia do lado do servidor
Verdadeiro	Falso	A criptografia no nível do servidor está habilitada para todos os compartilhamentos na SVM. Com essa configuração, a criptografia acontece para toda a sessão SMB.
Verdadeiro	Verdadeiro	A criptografia no nível do servidor é ativada para todos os compartilhamentos no SVM, independentemente da criptografia no nível de compartilhamento. Com essa configuração, a criptografia acontece para toda a sessão SMB.

Encriptação SMB do servidor SMB ativada	Compartilhar criptografar a configuração de dados ativada	Comportamento de criptografia do lado do servidor
Falso	Verdadeiro	A criptografia no nível de compartilhamento está ativada para compartilhamentos específicos. Com essa configuração, a criptografia acontece a partir da conexão em árvore.
Falso	Falso	Nenhuma criptografia está ativada.

Os clientes SMB que não suportam encriptação não podem estabelecer ligação a um servidor SMB ou partilha que requeira encriptação.

As alterações nas definições de encriptação entram em vigor para novas ligações. As ligações existentes não são afetadas.

Saiba mais sobre o impactos do desempenho da criptografia SMB do ONTAP

Quando as sessões SMB usam criptografia SMB, todas as comunicações SMB de e para clientes Windows têm um impactos na performance, o que afeta tanto os clientes quanto o servidor (ou seja, os nós no cluster que executa o SVM que contém o servidor SMB).

O impactos no desempenho mostra como aumento do uso da CPU tanto nos clientes quanto no servidor, embora a quantidade de tráfego de rede não mude.

A extensão do impactos no desempenho depende da versão do ONTAP 9 que você está executando. A partir do ONTAP 9.7, um novo algoritmo de criptografia off-load pode permitir melhor desempenho no tráfego SMB criptografado. A descarga de criptografia SMB é ativada por padrão quando a criptografia SMB está ativada.

O desempenho aprimorado da criptografia SMB requer a capacidade de descarga AES-NI. Consulte o Hardware Universe (HWU) para verificar se a descarga AES-NI é suportada para sua plataforma.

Melhorias adicionais de desempenho também são possíveis se você for capaz de usar SMB versão 3,11, que suporta o algoritmo GCM muito mais rápido.

Dependendo da sua rede, versão do ONTAP 9, versão do SMB e implementação do SVM, o impacto na performance da criptografia SMB pode variar muito. Você pode verificá-lo somente por meio de testes em seu ambiente de rede.

A encriptação SMB está desativada por predefinição no servidor SMB. Você deve habilitar a criptografia SMB somente nos compartilhamentos SMB ou servidores SMB que exigem criptografia. Com a criptografia SMB, o ONTAP realiza processamento adicional de descriptografar as solicitações e criptografar as respostas para cada solicitação. A criptografia SMB deve, portanto, ser ativada somente quando necessário.

Ative ou desative a encriptação SMB do ONTAP para o tráfego de entrada

Se pretender exigir encriptação SMB para o tráfego SMB de entrada, pode ativá-la no servidor CIFS ou no nível de partilha. Por padrão, a criptografia SMB não é necessária.

Sobre esta tarefa

Você pode ativar a criptografia SMB no servidor CIFS, que se aplica a todos os compartilhamentos no servidor CIFS. Se não pretender a encriptação SMB necessária para todos os partilhas no servidor CIFS ou se pretender ativar a encriptação SMB necessária para o tráfego SMB de entrada numa base de partilha por partilha, pode desativar a encriptação SMB necessária no servidor CIFS.

Quando você configura uma relação de recuperação de desastres de máquina virtual de storage (SVM), o valor selecionado para a `-identity-preserve` opção `snapmirror create` do comando determina os detalhes de configuração replicados no SVM de destino.

Se você definir `-identity-preserve` a opção como `true` (ID-Preserve), a configuração de segurança de criptografia SMB será replicada para o destino.

Se você definir `-identity-preserve` a opção como `false` (não-ID-Preserve), a configuração de segurança de criptografia SMB não será replicada para o destino. Nesse caso, as configurações de segurança do servidor CIFS no destino são definidas com os valores padrão. Se tiver ativado a encriptação SMB na SVM de origem, tem de ativar manualmente a encriptação SMB do servidor CIFS no destino.

Passos

1. Execute uma das seguintes ações:

Se pretender que a encriptação SMB necessária para o tráfego SMB de entrada no servidor CIFS seja…	**Digite o comando…**
Ativado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`
Desativado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required false`

2. Verifique se a criptografia SMB necessária no servidor CIFS está ativada ou desativada conforme desejado: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   O `is-smb-encryption-required` campo é exibido `true` se a criptografia SMB necessária estiver ativada no servidor CIFS e `false` se estiver desativada.

Exemplo

O exemplo a seguir habilita a criptografia SMB necessária para o tráfego SMB de entrada para o servidor CIFS no SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

Informações relacionadas

- "SnapMirror create"

Determine se os clientes estão conetados usando sessões criptografadas do ONTAP SMB

Você pode exibir informações sobre sessões SMB conetadas para determinar se os clientes estão usando conexões SMB criptografadas. Isso pode ser útil para determinar se as sessões de cliente SMB estão se conetando com as configurações de segurança desejadas.

Sobre esta tarefa

As sessões de clientes SMB podem ter um dos três níveis de criptografia:

- `unencrypted`

  A sessão SMB não está encriptada. Nem a criptografia no nível de máquina virtual de storage (SVM) nem no nível de compartilhamento são configuradas.

- `partially-encrypted`

  A criptografia é iniciada quando ocorre a conexão em árvore. A criptografia no nível de compartilhamento está configurada. A criptografia no nível da SVM não está ativada.

- `encrypted`

  A sessão SMB está totalmente encriptada. A criptografia no nível da SVM está ativada. A encriptação do nível de partilha pode ou não estar ativada. A configuração de criptografia no nível da SVM substitui a configuração de criptografia no nível de compartilhamento.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite o comando…
Sessões com uma configuração de criptografia especificada para sessões em um SVM especificado	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`

Se você quiser exibir informações sobre…	Digite o comando…
A configuração de criptografia para um Session ID específico em um SVM especificado	`vserver cifs session show -vserver` *`vserver_name`* `-session-id` *`integer`* `-instance`

Exemplos

O comando a seguir exibe informações detalhadas da sessão, incluindo a configuração de criptografia, em uma sessão SMB com um Session ID de 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
                Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   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: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Monitore as estatísticas de criptografia SMB do ONTAP

Você pode monitorar estatísticas de criptografia SMB e determinar quais sessões estabelecidas e conexões de compartilhamento são criptografadas e quais não são.

Sobre esta tarefa

O `statistics` comando no nível avançado de privilégios fornece os seguintes contadores, que podem ser utilizados para monitorizar o número de sessões SMB encriptadas e partilhar ligações:

Nome do contador	Descrições
`encrypted_sessions`	Fornece o número de sessões criptografadas do SMB 3,0

Nome do contador	Descrições
`encrypted_share_connections`	Fornece o número de compartilhamentos criptografados nos quais uma conexão em árvore aconteceu
`rejected_unencrypted_sessions`	Fornece o número de configurações de sessão rejeitadas devido à falta de capacidade de criptografia do cliente
`rejected_unencrypted_shares`	Fornece o número de mapeamentos de compartilhamento rejeitados devido à falta de capacidade de criptografia do cliente

Esses contadores estão disponíveis com os seguintes objetos estatísticos:

- `cifs` Permite monitorizar a encriptação SMB para todas as sessões SMB 3,0.

  As estatísticas SMB 3,0 são incluídas na saída para o `cifs` objeto. Se você quiser comparar o número de sessões criptografadas com o número total de sessões, você pode comparar a saída para o contador com a saída `established_sessions` para `encrypted_sessions` o contador.

  Se você quiser comparar o número de conexões de compartilhamento criptografadas com o número total de conexões de compartilhamento, você pode comparar a saída para o contador com a saída `connected_shares` para `encrypted_share_connections` o contador.

- `rejected_unencrypted_sessions` Fornece o número de vezes que uma tentativa foi feita para estabelecer uma sessão SMB que requer criptografia de um cliente que não suporta criptografia SMB.
- `rejected_unencrypted_shares` Fornece o número de vezes que uma tentativa foi feita para se conetar a um compartilhamento SMB que requer criptografia de um cliente que não suporta criptografia SMB.

Você deve iniciar uma coleta de amostras de estatísticas antes de poder visualizar os dados resultantes. Você pode exibir dados da amostra se não parar a coleta de dados. Parar a coleta de dados dá-lhe uma amostra fixa. Não interromper a coleta de dados dá a você a capacidade de obter dados atualizados que você pode usar para comparar com consultas anteriores. A comparação pode ajudá-lo a identificar tendências.

Passos

1. Defina o nível de privilégio como avançado `set -privilege advanced`
2. Iniciar uma coleta de dados `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Se você não especificar o `-sample-id` parâmetro, o comando gera um identificador de amostra para você e define esse exemplo como a amostra padrão para a sessão CLI. O valor para `-sample-id` é uma cadeia de texto. Se você executar esse comando durante a mesma sessão CLI e não especificar o `-sample-id` parâmetro, o comando sobrescreverá a amostra padrão anterior.

   Opcionalmente, você pode especificar o nó no qual deseja coletar estatísticas. Se você não especificar o nó, a amostra coletará estatísticas para todos os nós no cluster.

   Saiba mais sobre `statistics start` o "Referência do comando ONTAP"na .

3. Use o `statistics stop` comando para parar de coletar dados para a amostra.

   Saiba mais sobre `statistics stop` no "Referência do comando ONTAP" .

4. Exibir estatísticas de criptografia SMB:

Se você quiser ver informações para…	**Digite…**
Sessões criptografadas	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	Sessões criptografadas e sessões estabelecidas
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	Conexões de compartilhamento criptografadas
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
Conexões de compartilhamento criptografadas e compartilhamentos conetados	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
Sessões não criptografadas rejeitadas	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	Conexões de compartilhamento não criptografadas rejeitadas
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

   Se você quiser exibir informações apenas para um único nó, especifique o parâmetro opcional `-node`.

   Saiba mais sobre `statistics show` o "Referência do comando ONTAP"na .

5. Voltar para o nível de privilégio de administrador `set -privilege admin`

Exemplos

O exemplo a seguir mostra como você pode monitorar as estatísticas de criptografia SMB 3,0 na máquina virtual de armazenamento (SVM) VS1.

O seguinte comando move-se para o nível de privilégio avançado:

```
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
```

O comando a seguir inicia a coleta de dados para uma nova amostra:

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

O comando a seguir interrompe a coleta de dados para essa amostra:

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

O comando a seguir mostra sessões criptografadas SMB e sessões estabelecidas SMB pelo nó da amostra:

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                 Value
    --------------------------  ----------------------
    established_sessions                       1
    encrypted_sessions                         1

2 entries were displayed
```

O comando a seguir mostra o número de sessões SMB não criptografadas rejeitadas pelo nó da amostra:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    --------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

O comando a seguir mostra o número de compartilhamentos SMB conetados e compartilhamentos SMB criptografados pelo nó da amostra:

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    --------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

O comando a seguir mostra o número de conexões de compartilhamento SMB não criptografadas rejeitadas pelo nó da amostra:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

Informações relacionadas

- Determinar quais estatísticas, objetos e contadores estão disponíveis nos servidores
- "Visão geral do gerenciamento e monitoramento de desempenho"

Comunicação de sessão LDAP segura

Saiba mais sobre a assinatura e a vedação do LDAP do ONTAP SMB

A partir do ONTAP 9, você pode configurar a assinatura e a vedação para habilitar a segurança da sessão LDAP em consultas para um servidor AD (ative Directory). Você

deve configurar as configurações de segurança do servidor CIFS na máquina virtual de armazenamento (SVM) para corresponder às do servidor LDAP.

A assinatura confirma a integridade dos dados de carga útil LDAP usando tecnologia de chave secreta. A vedação criptografa os dados de carga útil LDAP para evitar a transmissão de informações confidenciais em texto não criptografado. Uma opção *LDAP Security Level* indica se o tráfego LDAP precisa ser assinado, assinado e selado, ou não. A predefinição é `none`.

A assinatura LDAP e a vedação no tráfego CIFS são ativadas no SVM com a `-session-security-for-ad-ldap` opção de `vserver cifs security modify` comando.

Ative a assinatura LDAP e a vedação em servidores SMB do ONTAP

Antes que o servidor CIFS possa usar assinatura e vedação para comunicação segura com um servidor LDAP do ative Directory, você deve modificar as configurações de segurança do servidor CIFS para habilitar a assinatura e a vedação LDAP.

Antes de começar

Você deve consultar o administrador do servidor AD para determinar os valores de configuração de segurança apropriados.

Passos

1. Configure a configuração de segurança do servidor CIFS que permite o tráfego assinado e selado com servidores LDAP do ative Directory: `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap {none|sign|seal}`

   Você pode ativar assinatura (`sign`, integridade de dados), assinatura e vedação (`seal`, integridade e criptografia de dados) ou nenhum `none`, sem assinatura ou vedação). O valor padrão é `none`.

2. Verifique se a configuração de segurança de assinatura e vedação LDAP está definida corretamente: `vserver cifs security show -vserver` *`vserver_name`*

> Se o SVM usar o mesmo servidor LDAP para consultar o mapeamento de nomes ou outras informações do UNIX, como usuários, grupos e netgroups, você deverá ativar a configuração correspondente com `-session-security` a opção do `vserver services name-service ldap client modify` comando.

Configurar LDAP em TLS

Exporte certificados de CA raiz autoassinados para SVMs SMB do ONTAP

Para usar LDAP em SSL/TLS para proteger a comunicação do ative Directory, primeiro você deve exportar uma cópia do certificado CA raiz autoassinado do ative Directory Service para um arquivo de certificado e convertê-lo em um arquivo de texto ASCII. Esse arquivo de texto é usado pelo ONTAP para instalar o certificado na máquina virtual de storage (SVM).

Antes de começar

O Serviço de certificados do ative Directory já deve estar instalado e configurado para o domínio ao qual o servidor CIFS pertence. Você pode encontrar informações sobre a instalação e configuração dos Serviços de

certificados do ative diretor consultando a Biblioteca Microsoft TechNet.

"Microsoft TechNet Library: technet.microsoft.com"

Passo

1. Obtenha um certificado de CA raiz do controlador de domínio que está no `.pem` formato de texto.

   "Microsoft TechNet Library: technet.microsoft.com"

Depois de terminar

Instale o certificado no SVM.

Informações relacionadas

"Microsoft TechNet Library"

Instalar certificados de CA raiz autoassinados no ONTAP SMB

Se a autenticação LDAP com TLS for necessária ao vincular a servidores LDAP, primeiro você deverá instalar o certificado de CA raiz autoassinado no SVM.

Sobre esta tarefa

Todos os aplicativos do ONTAP que usam comunicações TLS podem verificar o status do certificado digital usando o protocolo OCSP (Online Certificate Status Protocol). Se o OCSP estiver ativado para LDAP através de TLS, os certificados revogados serão rejeitados e a conexão falhará.

Passos

1. Instale o certificado CA raiz autoassinado:
   a. Inicie a instalação do certificado: `security certificate install -vserver vserver_name -type server-ca`

      A saída do console exibe a seguinte mensagem: `Please enter Certificate: Press <Enter> when done`

   b. Abra o arquivo de certificado `.pem` com um editor de texto, copie o certificado, incluindo as linhas que começam com `-----BEGIN CERTIFICATE-----` e terminam com `-----END CERTIFICATE-----`, e cole o certificado após o prompt de comando.
   c. Verifique se o certificado é exibido corretamente.
   d. Conclua a instalação pressionando Enter.
2. Verifique se o certificado está instalado: `security certificate show -vserver *vserver_name*`

Informações relacionadas

- "instalação do certificado de segurança"
- "certificado de segurança mostrar"

Ative o LDAP através de TLS no servidor SMB do ONTAP

Antes que o servidor SMB possa usar TLS para comunicação segura com um servidor LDAP do ative Directory, você deve modificar as configurações de segurança do servidor SMB para ativar o LDAP sobre TLS.

A partir do ONTAP 9.10,1, a vinculação de canal LDAP é suportada por padrão para conexões LDAP do ative Directory (AD) e serviços de nome. O ONTAP tentará a vinculação de canais com conexões LDAP somente se o Start-TLS ou LDAPS estiver ativado junto com a segurança da sessão definida para assinar ou selar. Para desativar ou reativar a vinculação de canais LDAP com servidores AD, use o `-try-channel-binding-for-ad-ldap` parâmetro com o `vserver cifs security modify` comando.

Para saber mais, consulte:

- "Saiba mais sobre LDAP para SVMs ONTAP NFS"
- "2020 requisitos de vinculação de canal LDAP e assinatura LDAP para Windows".

Passos

1. Configure a configuração de segurança do servidor SMB que permite a comunicação LDAP segura com servidores LDAP do ative Directory: `vserver cifs security modify -vserver` *`vserver_name`* `-use-start-tls-for-ad-ldap true`
2. Verifique se a configuração de segurança LDAP sobre TLS está definida como `true`: `vserver cifs security show -vserver` *`vserver_name`*

> Se o SVM usar o mesmo servidor LDAP para consultar o mapeamento de nomes ou outras informações do UNIX (como usuários, grupos e netgroups), você também deve modificar a `-use-start-tls` opção usando o `vserver services name-service ldap client modify` comando.

Configure o multicanais SMB do ONTAP para desempenho e redundância

A partir do ONTAP 9.4, você pode configurar o multicanais SMB para fornecer várias conexões entre o ONTAP e os clientes em uma única sessão SMB. Isso melhora a taxa de transferência e a tolerância a falhas.

Antes de começar

Você pode usar a funcionalidade de multicanal SMB somente quando os clientes negociam em versões SMB 3,0 ou posteriores. Por padrão, o SMB 3,0 e posterior está habilitado no servidor SMB do ONTAP.

Sobre esta tarefa

Os clientes SMB detetam e usam automaticamente várias conexões de rede se uma configuração adequada for identificada no cluster ONTAP.

O número de conexões simultâneas em uma sessão SMB depende das NICs que você implantou:

- **1G NICs em cliente e cluster ONTAP**

  O cliente estabelece uma conexão por NIC e liga a sessão a todas as conexões.

- **10G e placas de rede de maior capacidade no cluster cliente e ONTAP**

  O cliente estabelece até quatro conexões por NIC e liga a sessão a todas as conexões. O cliente pode estabelecer conexões em várias NICs de 10G GB e maior capacidade.

Você também pode modificar os seguintes parâmetros (privilégio avançado):

- `-max-connections-per-session`

  O número máximo de conexões permitido por sessão multicanal. O padrão é 32 conexões.

  Se você quiser habilitar mais conexões do que o padrão, você deve fazer ajustes comparáveis à configuração do cliente, que também tem um padrão de 32 conexões.

- `-max-lifs-per-session`

  O número máximo de interfaces de rede anunciadas por sessão multicanal. O padrão é 256 interfaces de rede.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Ative SMB Multichannel no servidor SMB:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. Verifique se o ONTAP está relatando sessões multicanais SMB:

```
vserver cifs session show
```

4. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Exemplo

O exemplo a seguir exibe informações sobre todas as sessões SMB, mostrando várias conexões para uma única sessão:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

O exemplo a seguir exibe informações detalhadas sobre uma sessão SMB com session-id 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                  Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                  Connected Time: 5s
                       Idle Time: 5s
               Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

Configure o usuário padrão do Windows para mapeamentos de usuários UNIX no servidor SMB

Configure o usuário padrão do ONTAP SMB UNIX

Você pode configurar o usuário UNIX padrão para usar se todas as outras tentativas de mapeamento falharem para um usuário ou se não quiser mapear usuários individuais entre UNIX e Windows. Alternativamente, se você quiser que a autenticação de usuários não mapeados falhe, você não deve configurar o usuário UNIX padrão.

Sobre esta tarefa

Por padrão, o nome do usuário UNIX padrão é "'pcuser'", o que significa que, por padrão, o mapeamento de usuário para o usuário UNIX padrão está habilitado. Você pode especificar outro nome para usar como usuário UNIX padrão. O nome especificado deve existir nos bancos de dados do serviço de nomes configurados para a máquina virtual de storage (SVM). Se essa opção for definida como uma cadeia de carateres nula, ninguém poderá acessar o servidor CIFS como um usuário padrão UNIX. Ou seja, cada usuário deve ter uma conta no banco de dados de senhas antes de poder acessar o servidor CIFS.

Para que um usuário se conete ao servidor CIFS usando a conta de usuário UNIX padrão, o usuário deve atender aos seguintes pré-requisitos:

- O utilizador está autenticado.
- O usuário está no banco de dados de usuários do Windows local do servidor CIFS, no domínio doméstico do servidor CIFS ou em um domínio confiável (se pesquisas de mapeamento de nomes de vários domínios estiverem ativadas no servidor CIFS).
- O nome de usuário não é explicitamente mapeado para uma cadeia de carateres nula.

Passos

1. Configure o usuário UNIX padrão:

Se você quiser …	Introduza …
Use o usuário padrão do UNIX "'pcuser'"	`vserver cifs options modify -default -unix-user pcuser`
Use outra conta de usuário UNIX como usuário padrão	`vserver cifs options modify -default -unix-user` *`user_name`*
Desative o usuário UNIX padrão	`vserver cifs options modify -default -unix-user ""`

```
vserver cifs options modify -default-unix-user pcuser
```

2. Verifique se o usuário UNIX padrão está configurado corretamente: `vserver cifs options show -vserver` *`vserver_name`*

   No exemplo a seguir, tanto o usuário UNIX padrão quanto o usuário UNIX convidado no SVM VS1 são configurados para usar o usuário UNIX "'pcuser'":

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Configure o usuário UNIX SMB do ONTAP convidado

Configurar a opção de usuário UNIX convidado significa que os usuários que fazem login de domínios não confiáveis são mapeados para o usuário UNIX convidado e podem se conetar ao servidor CIFS. Alternativamente, se você quiser que a autenticação de usuários de domínios não confiáveis falhe, você não deve configurar o usuário UNIX convidado. O padrão é não permitir que usuários de domínios não confiáveis se conetem ao servidor CIFS (a conta UNIX convidada não está configurada).

Sobre esta tarefa

Você deve ter em mente o seguinte ao configurar a conta UNIX Guest:

- Se o servidor CIFS não puder autenticar o usuário em um controlador de domínio para o domínio doméstico ou um domínio confiável ou o banco de dados local e essa opção estiver ativada, o servidor CIFS considera o usuário como um usuário convidado e mapeia o usuário para o usuário UNIX especificado.
- Se essa opção for definida como uma cadeia de carateres nula, o usuário UNIX convidado será desativado.
- Você deve criar um usuário UNIX para usar como usuário UNIX convidado em um dos bancos de dados do serviço de nomes de máquina virtual de armazenamento (SVM).
- Um usuário conetado como um usuário convidado é automaticamente membro do grupo BUILTIN/convidados no servidor CIFS.
- A opção 'homedirs-public' aplica-se apenas a utilizadores autenticados. Um usuário conetado como um usuário convidado não tem um diretório home e não pode acessar os diretórios home de outros usuários.

Passos

1. Execute uma das seguintes ações:

Se você quiser…	Digite…
Configure o usuário UNIX convidado	`vserver cifs options modify -guest -unix-user` *`unix_name`*

Se você quiser…	Digite…
Desative o usuário UNIX convidado	`vserver cifs options modify -guest -unix-user ""`

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Verifique se o usuário UNIX convidado está configurado corretamente: `vserver cifs options show -vserver` *vserver_name*

   No exemplo a seguir, tanto o usuário UNIX padrão quanto o usuário UNIX convidado no SVM VS1 são configurados para usar o usuário UNIX "'pcuser'":

   ```
   vserver cifs options show -vserver vs1
   ```

   ```
   Vserver: vs1

     Client Session Timeout : 900
     Default Unix Group     : -
     Default Unix User      : pcuser
     Guest Unix User        : pcuser
     Read Grants Exec       : disabled
     Read Only Delete       : disabled
     WINS Servers           : -
   ```

Mapeie grupos de administradores para a raiz SMB do ONTAP

Se você tiver apenas clientes CIFS em seu ambiente e sua máquina virtual de storage (SVM) tiver sido configurada como um sistema de storage multiprotocolo, você deverá ter pelo menos uma conta do Windows que tenha privilégios de raiz para acessar arquivos no SVM; caso contrário, não será possível gerenciar o SVM porque não tem direitos de usuário suficientes.

Sobre esta tarefa

Se o seu sistema de armazenamento foi configurado apenas como NTFS, o `/etc` diretório tem uma ACL no nível do ficheiro que permite ao grupo de administradores aceder aos ficheiros de configuração do ONTAP.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Configure a opção de servidor CIFS que mapeia o grupo de administradores para fazer root conforme apropriado:

Se você quiser…	Então…
Mapeie os membros do grupo de administradores para fazer root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled true` Todas as contas do grupo administrators são consideradas root, mesmo que você não tenha uma `/etc/usermap.cfg` entrada mapeando as contas para root. Se você criar um arquivo usando uma conta que pertence ao grupo administrators, o arquivo será de propriedade do root quando você exibir o arquivo de um cliente UNIX.
Desative o mapeamento dos membros do grupo de administradores para fazer root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled false` As contas no grupo administrators não são mais mapeadas para o root. Você só pode mapear explicitamente um único usuário para o root.

3. Verifique se a opção está definida para o valor desejado: `vserver cifs options show -vserver` *`vserver_name`*
4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exiba informações sobre quais tipos de usuários estão conetados por sessões do ONTAP SMB

Você pode exibir informações sobre que tipo de usuários estão conetados em sessões SMB. Isso pode ajudar você a garantir que apenas o tipo apropriado de usuário esteja se conetando por sessões SMB na máquina virtual de storage (SVM).

Sobre esta tarefa

Os seguintes tipos de usuários podem se conetar através de sessões SMB:

- `local-user`

  Autenticado como um usuário CIFS local

- `domain-user`

  Autenticado como um usuário de domínio (do domínio doméstico do servidor CIFS ou de um domínio confiável)

- `guest-user`

  Autenticado como usuário convidado

- `anonymous-user`

  Autenticado como um usuário anônimo ou nulo

Passos

1. Determine que tipo de usuário está conetado em uma sessão SMB: `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

Se você quiser exibir informações de tipo de usuário para sessões estabelecidas…	Digite o seguinte comando…
Para todas as sessões com um tipo de usuário especificado	`vserver cifs session show -vserver *vserver_name* -user-type {local-user
domain-user	guest-user
anonymous-user}`	Para um usuário específico

Exemplos

O comando a seguir exibe informações de sessão sobre o tipo de usuário para sessões no SVM VS1 estabelecido pelo usuário "" iebubs user1":

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

Opções de comando ONTAP para limitar o consumo excessivo de recursos do cliente Windows

As opções para o `vserver cifs options modify` comando permitem controlar o consumo de recursos para clientes Windows. Isso pode ser útil se algum cliente estiver fora dos limites normais de consumo de recursos, por exemplo, se houver um número excepcionalmente alto de arquivos abertos, sessões abertas ou solicitações Change Notify.

As seguintes opções para o `vserver cifs options modify` comando foram adicionadas para controlar o consumo de recursos do cliente Windows. Se o valor máximo de qualquer uma dessas opções for excedido, a solicitação será negada e uma mensagem EMS será enviada. Uma mensagem de aviso EMS também é enviada quando 80% do limite configurado para essas opções é atingido.

- `-max-opens-same-file-per-tree`

  Número máximo de aberturas no mesmo arquivo por árvore CIFS

- `-max-same-user-sessions-per-connection`

Número máximo de sessões abertas pelo mesmo usuário por conexão

- `-max-same-tree-connect-per-session`

  O número máximo de árvores se coneta no mesmo compartilhamento por sessão

- `-max-watches-set-per-tree`

  Número máximo de relógios (também conhecido como *change notifica*) estabelecido por árvore

Saiba mais sobre `vserver cifs options modify` o "Referência do comando ONTAP"na .

A partir do ONTAP 9.4, os servidores que executam o SMB versão 2 ou posterior podem limitar o número de solicitações pendentes (*créditos SMB*) que o cliente pode enviar para o servidor em uma conexão SMB. O gerenciamento de créditos SMB é iniciado pelo cliente e controlado pelo servidor.

O número máximo de solicitações pendentes que podem ser concedidas em uma conexão SMB é controlado pela `-max-credits` opção. O valor padrão para essa opção é 128.

Melhore o desempenho do cliente com os oplocks tradicionais e de leasing

Saiba mais sobre como melhorar o desempenho do cliente ONTAP SMB com os princípios tradicionais e de leasing

Os oplocks tradicionais (bloqueios oportunistas) e os oplocks de leasing permitem que um cliente SMB em determinados cenários de compartilhamento de arquivos execute o armazenamento em cache do lado do cliente de informações de leitura antecipada, gravação e bloqueio. Um cliente pode então ler ou gravar em um arquivo sem lembrar regularmente o servidor de que precisa de acesso ao arquivo em questão. Isso melhora o desempenho reduzindo o tráfego de rede.

Os calços de leasing são uma forma melhorada de oplocks disponíveis com o protocolo SMB 2,1 e posterior. Os locks permitem que um cliente obtenha e preserve o estado de cache do cliente em várias aberturas SMB originadas de si mesmo.

Os calços podem ser controlados de duas maneiras:

- Por uma propriedade share, usando o `vserver cifs share create` comando quando o compartilhamento é criado, ou o `vserver share properties` comando após a criação.
- Por uma propriedade de qtree, usando o `volume qtree create` comando quando a qtree é criada, ou os `volume qtree oplock` comandos após a criação.

Saiba mais sobre como escrever considerações sobre perda de dados de cache SMB do ONTAP ao usar os oplocks

Em algumas circunstâncias, se um processo tem um oplock exclusivo em um arquivo e um segundo processo tenta abrir o arquivo, o primeiro processo deve invalidar dados em cache e flush escreve e bloqueia. O cliente deve então abandonar o oplock e o acesso

ao arquivo. Se houver uma falha de rede durante esse flush, os dados de gravação em cache podem ser perdidos.

- Possibilidades de perda de dados

  Qualquer aplicativo que tenha dados gravados em cache pode perder esses dados sob o seguinte conjunto de circunstâncias:

  - A conexão é feita usando SMB 1,0.
  - Tem um oplock exclusivo no arquivo.
  - É dito para interromper esse oplock ou fechar o arquivo.
  - Durante o processo de limpeza do cache de gravação, a rede ou o sistema de destino gera um erro.
- Erro de manipulação e conclusão de gravação

  O cache em si não tem nenhum tratamento de erros - os aplicativos fazem.quando o aplicativo faz uma gravação no cache, a gravação é sempre concluída. Se o cache, por sua vez, faz uma gravação no sistema de destino em uma rede, ele deve assumir que a gravação é concluída porque, se não fizer, os dados são perdidos.

Ative ou desative os oplocks ao criar compartilhamentos SMB do ONTAP

Oplocks permitem que os clientes bloqueiem arquivos e armazenem conteúdo de cache localmente, o que pode aumentar o desempenho para operações de arquivos. Os Oplocks são ativados em compartilhamentos SMB residentes em máquinas virtuais de armazenamento (SVMs). Em algumas circunstâncias, você pode querer desativar os oplocks. Você pode ativar ou desativar os oplocks em uma base de compartilhamento por compartilhamento.

Sobre esta tarefa

Se os oplocks estiverem ativados no volume que contém uma partilha, mas a propriedade de partilha de oplock para essa partilha estiver desativada, os oplocks serão desativados para essa partilha. A desativação de oplocks em um compartilhamento tem precedência sobre a configuração de volume de oplock A desativação de oplocks na partilha desativa os oplocks oportunistas e de leasing.

Você pode especificar outras propriedades de compartilhamento além de especificar a propriedade de compartilhamento de oplock usando uma lista delimitada por vírgulas. Você também pode especificar outros parâmetros de compartilhamento.

Passos

1. Execute a ação aplicável:

Se você quiser…	Então…
Ative os oplocks em um compartilhamento durante a criação de compartilhamento	Introduza o seguinte comando: `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]` Se desejar que o compartilhamento tenha apenas as propriedades padrão de compartilhamento, que são `oplocks`, `browsable` e `changenotify` ativadas, não será necessário especificar o `-share -properties` parâmetro ao criar um compartilhamento SMB. Se você quiser qualquer combinação de propriedades de compartilhamento diferente do padrão, especifique o `-share-properties` parâmetro com a lista de propriedades de compartilhamento a ser usada para esse compartilhamento.
Desative os oplocks em um compartilhamento durante a criação de compartilhamento	Introduza o seguinte comando: `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` Ao desativar os oplocks, você deve especificar uma lista de propriedades de compartilhamento ao criar o compartilhamento, mas não deve especificar a `oplocks` propriedade.

Informações relacionadas

Ative ou desative os oplocks em compartilhamentos SMB existentes

Monitorar o status de oplock

Comandos ONTAP para ativar ou desativar os oplocks em volumes SMB e qtrees

Oplocks permitem que os clientes bloqueiem arquivos e armazenem conteúdo de cache localmente, o que pode aumentar o desempenho para operações de arquivos. Você precisa saber os comandos para ativar ou desativar os oplocks em volumes ou qtrees. Você também deve saber quando você pode ativar ou desativar os oplocks em volumes e qtrees.

- Os calços são ativados em volumes por predefinição.
- Não é possível desativar os oplocks ao criar um volume.
- Você pode ativar ou desativar os oplocks em volumes existentes para SVMs a qualquer momento.
- Você pode ativar os oplocks em qtrees para SVMs.

  A configuração do modo de oplock é uma propriedade da ID de qtree 0, a qtree padrão que todos os volumes têm. Se você não especificar uma configuração de oplock ao criar uma qtree, a qtree herdará a configuração de oplock do volume pai, que é habilitada por padrão. No entanto, se você especificar uma configuração de oplock na nova qtree, ela terá precedência sobre a configuração de oplock no volume.

Se você quiser…	Use este comando…
Ative os oplocks em volumes ou qtrees	`volume qtree oplocks` com o `-oplock-mode` parâmetro definido como `enable`
Desative os oplocks em volumes ou qtrees	`volume qtree oplocks` com o `-oplock-mode` parâmetro definido como `disable`

Informações relacionadas

Monitorar o status de oplock

Ative ou desative os oplocks em compartilhamentos SMB do ONTAP existentes

Os Oplocks são ativados em compartilhamentos SMB em máquinas virtuais de armazenamento (SVMs) por padrão. Em algumas circunstâncias, você pode querer desativar os oplocks; alternativamente, se você tiver desabilitado previamente os oplocks em uma ação, você pode querer reativar os oplocks.

Sobre esta tarefa

Se os oplocks estiverem ativados no volume que contém uma partilha, mas a propriedade de partilha de oplock para essa partilha estiver desativada, os oplocks serão desativados para essa partilha. A desativação de oplocks em um compartilhamento tem precedência sobre a ativação de oplocks no volume. Desativar os oplocks na partilha, desativa os oplocks oportunistas e de leasing. Você pode ativar ou desativar os oplocks em compartilhamentos existentes a qualquer momento.

Passo

1. Execute a ação aplicável:

Se você quiser…	Então…
Ative os oplocks em um compartilhamento modificando um compartilhamento existente	Introduza o seguinte comando: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties oplocks` Você pode especificar propriedades de compartilhamento adicionais a serem adicionadas usando uma lista delimitada por vírgulas. As propriedades recém-adicionadas são anexadas à lista existente de propriedades de compartilhamento. Quaisquer propriedades de compartilhamento que você especificou anteriormente permanecem em vigor.
Desative os oplocks em um compartilhamento modificando um compartilhamento existente	Introduza o seguinte comando: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks` Você pode especificar propriedades de compartilhamento adicionais para remover usando uma lista delimitada por vírgulas. As propriedades de compartilhamento que você remover são excluídas da lista existente de propriedades de compartilhamento; no entanto, as propriedades de compartilhamento configuradas anteriormente que você não remove permanecem em vigor.

Exemplos

O comando a seguir habilita os oplocks para o compartilhamento chamado "Engenharia" na máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

O comando a seguir desativa os oplocks para a ação chamada "Engenharia" no SVM VS1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

Informações relacionadas

- Ative ou desative os oplocks ao criar compartilhamentos SMB
- Monitorar o status de oplock
- Adicionar ou remover propriedades de compartilhamento em compartilhamentos existentes

Monitorar o status de oplock do ONTAP SMB

Você pode monitorar e exibir informações sobre o status de oplock Você pode usar essas informações para determinar quais arquivos têm oplocks, quais são o nível de oplock e o nível de estado de oplock e se o leasing de oplock é usado. Você também pode determinar informações sobre bloqueios que você pode precisar quebrar manualmente.

Sobre esta tarefa

Você pode exibir informações sobre todos os oplocks em forma de resumo ou em um formulário de lista detalhado. Você também pode usar parâmetros opcionais para exibir informações sobre um subconjunto menor de bloqueios existentes. Por exemplo, você pode especificar que a saída retorna apenas bloqueia com o endereço IP do cliente especificado ou com o caminho especificado.

Você pode exibir as seguintes informações sobre os oplocks tradicionais e de leasing:

- SVM, nó, volume e LIF em que o oplock

- Bloquear UUID
- Endereço IP do cliente com o oplock
- Caminho no qual o oplock é estabelecido
- Protocolo de bloqueio (SMB) e tipo (oplock)
- Estado de bloqueio
- Nível do calço
- Estado da conexão e tempo de expiração do SMB
- Abra o ID do grupo se for concedida uma locação de oplock

Saiba mais sobre `vserver oplocks show` o "Referência do comando ONTAP"na .

Passos

1. Apresentar o estado de oplock utilizando o `vserver locks show` comando.

Exemplos

O comando a seguir exibe informações padrão sobre todos os bloqueios. O oplock no ficheiro apresentado é concedido com um `read-batch` nível de oplock:

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

O exemplo a seguir exibe informações mais detalhadas sobre o bloqueio em um arquivo com o `/data2/data2_2/intro.pptx` caminho . Um leasing de oplock é concedido no arquivo com um `batch` nível de oplock a um cliente com um endereço IP de `10.3.1.3`:

> Ao exibir informações detalhadas, o comando fornece saída separada para informações de oplock e sharelock. Este exemplo mostra apenas a saída da secção de oplock

```
cluster1::> vserver lock 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: ff1cbf29-bfef-4d91-ae06-062bf69212c3
              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
```

Informações relacionadas

Ative ou desative os oplocks ao criar compartilhamentos SMB

Ative ou desative os oplocks em compartilhamentos SMB existentes

Comandos para habilitar ou desabilitar oplocks em volumes SMB e qtrees

Aplique objetos de Diretiva de Grupo a servidores SMB

Saiba mais sobre como aplicar objetos de Diretiva de Grupo a servidores SMB do ONTAP

Seu servidor SMB oferece suporte a objetos de Diretiva de Grupo (GPOs), um conjunto de regras conhecidas como *atributos de diretiva de grupo* que se aplicam a computadores em um ambiente do ative Directory. Você pode usar GPOs para gerenciar centralmente as configurações de todas as máquinas virtuais de storage (SVMs) no cluster que pertence ao mesmo domínio do ative Directory.

Quando os GPOs estão ativados no servidor SMB, o ONTAP envia consultas LDAP ao servidor do ative Directory solicitando informações de GPO. Se houver definições de GPO aplicáveis ao servidor SMB, o servidor do ative Directory retornará as seguintes informações de GPO:

- Nome GPO
- Versão GPO atual
- Localização da definição GPO
- Listas de UUIDs (identificadores universalmente exclusivos) para conjuntos de políticas GPO

Informações relacionadas

- Saiba mais sobre segurança de acesso a arquivos para servidores
- "Auditoria de SMB e NFS e rastreamento de segurança"

Saiba mais sobre os GPOs SMB compatíveis do ONTAP

Embora nem todos os objetos de Diretiva de Grupo (GPOs) sejam aplicáveis às máquinas virtuais de storage (SVMs) habilitadas para CIFS, os SVMs podem reconhecer e processar o conjunto relevante de GPOs.

Os GPOs a seguir são compatíveis atualmente com SVMs:

- Definições avançadas de configuração da política de auditoria:

  Acesso a objetos: Preparação da Política de Acesso Central

  Especifica o tipo de eventos a serem auditados para o estadiamento da política de acesso central (CAP), incluindo as seguintes configurações:

  - Não faça auditoria
  - Audite apenas eventos de sucesso
  - Auditar apenas eventos de falha
  - Audite eventos de sucesso e falha

  > Se qualquer uma das três opções de auditoria estiver definida (auditar apenas eventos de sucesso, auditar apenas eventos de falha, auditar eventos de sucesso e falha), o ONTAP fará a auditoria de eventos de sucesso e falha.

  Defina utilizando a `Audit Central Access Policy Staging` definição no `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.

  > Para usar configurações avançadas de GPO de diretiva de auditoria, a auditoria deve ser configurada no SVM habilitado para CIFS ao qual você deseja aplicar essas configurações. Se a auditoria não estiver configurada no SVM, as configurações do GPO não serão aplicadas e serão descartadas.

- Definições do registo:

  - Intervalo de atualização da política de grupo para SVM habilitado para CIFS

Defina utilizando o `Registry` GPO.

- Atualizar desvio aleatório da política de grupo

  Defina utilizando o `Registry` GPO.

- Publicação hash para BranchCache

  A publicação Hash para o GPO BranchCache corresponde ao modo de operação BranchCache. Os três modos de operação suportados a seguir são suportados:

  - Por compartilhamento
  - Todos os compartilhamentos
  - Desativado definido utilizando o `Registry` GPO.

- Suporte à versão hash para BranchCache

  As seguintes três configurações de versão hash são suportadas:

  - BranchCache versão 1
  - BranchCache versão 2
  - BranchCache versões 1 e 2 definidas usando o `Registry` GPO.

> Para usar as configurações de GPO do BranchCache, o BranchCache deve ser configurado no SVM habilitado para CIFS ao qual você deseja aplicar essas configurações. Se o BranchCache não estiver configurado no SVM, as configurações do GPO não serão aplicadas e serão descartadas.

- Definições de segurança
  - Política de auditoria e log de eventos
    - Audite eventos de logon

      Especifica o tipo de eventos de logon a serem auditados, incluindo as seguintes configurações:

      - Não faça auditoria
      - Audite apenas eventos de sucesso
      - Auditoria em eventos de falha
      - Audite eventos de sucesso e falha definidos usando a `Audit logon events` configuração no `Local Policies/Audit Policy` GPO.

> Se qualquer uma das três opções de auditoria estiver definida (auditar apenas eventos de sucesso, auditar apenas eventos de falha, auditar eventos de sucesso e falha), o ONTAP fará a auditoria de eventos de sucesso e falha.

    - Auditar o acesso a objeto

      Especifica o tipo de acesso a objeto a ser auditado, incluindo as seguintes configurações:

      - Não faça auditoria

- Audite apenas eventos de sucesso
- Auditoria em eventos de falha
- Audite eventos de sucesso e falha definidos usando a `Audit object access` configuração no `Local Policies/Audit Policy` GPO.

> Se qualquer uma das três opções de auditoria estiver definida (auditar apenas eventos de sucesso, auditar apenas eventos de falha, auditar eventos de sucesso e falha), o ONTAP fará a auditoria de eventos de sucesso e falha.

- Método de retenção de log

  Especifica o método de retenção do log de auditoria, incluindo as seguintes configurações:

  - Substituir o registo de eventos quando o tamanho do ficheiro de registo exceder o tamanho máximo do registo
  - Não substituir o registo de eventos (limpar registo manualmente) definido utilizando a `Retention method for security log` definição no `Event Log` GPO.

- Tamanho máximo do registo

  Especifica o tamanho máximo do log de auditoria.

  Defina utilizando a `Maximum security log size` definição no `Event Log` GPO.

> Para usar a diretiva de auditoria e as configurações de GPO de log de eventos, a auditoria deve ser configurada no SVM habilitado para CIFS ao qual você deseja aplicar essas configurações. Se a auditoria não estiver configurada no SVM, as configurações do GPO não serão aplicadas e serão descartadas.

◦ Segurança do sistema de arquivos

Especifica uma lista de arquivos ou diretórios nos quais a segurança de arquivos é aplicada por meio de um GPO.

Defina utilizando o `File System` GPO.

> O caminho do volume para o qual o GPO de segurança do sistema de arquivos está configurado deve existir na SVM.

◦ Política Kerberos

- Inclinação máxima do relógio

  Especifica a tolerância máxima em minutos para a sincronização do relógio do computador.

  Defina utilizando a `Maximum tolerance for computer clock synchronization` definição no `Account Policies/Kerberos Policy` GPO.

- Idade máxima do bilhete

  Especifica a vida útil máxima em horas para o ticket de usuário.

Defina utilizando a `Maximum lifetime for user ticket` definição no `Account Policies/Kerberos Policy` GPO.

- Idade máxima de renovação do bilhete

  Especifica o tempo de vida máximo em dias para a renovação do ticket do usuário.

Defina utilizando a `Maximum lifetime for user ticket renewal` definição no `Account Policies/Kerberos Policy` GPO.

◦ Atribuição de direitos de utilizador (direitos de privilégio)

- Assuma a propriedade

  Especifica a lista de usuários e grupos que têm o direito de assumir a propriedade de qualquer objeto que possa ser protegido.

  Defina utilizando a `Take ownership of files or other objects` definição no `Local Policies/User Rights Assignment` GPO.

- Privilégio de segurança

  Especifica a lista de usuários e grupos que podem especificar opções de auditoria para acesso a objetos de recursos individuais, como arquivos, pastas e objetos do ative Directory.

  Defina utilizando a `Manage auditing and security log` definição no `Local Policies/User Rights Assignment` GPO.

- Privilégio Change Notify (verificação de desvio transversal)

  Especifica a lista de usuários e grupos que podem atravessar árvores de diretório, mesmo que os usuários e grupos possam não ter permissões no diretório atravessado.

O mesmo privilégio é necessário para que os usuários recebam notificações de alterações em arquivos e diretórios. Defina utilizando a `Bypass traverse checking` definição no `Local Policies/User Rights Assignment` GPO.

◦ Valores do registo

- Definição de assinatura necessária

  Especifica se a assinatura SMB necessária está ativada ou desativada.

Defina utilizando a `Microsoft network server: Digitally sign communications (always)` definição no `Security Options` GPO.

◦ Restringir o anonimato

Especifica quais são as restrições para usuários anônimos e inclui as seguintes três configurações de GPO:

- Sem enumeração de contas SAM (Security Account Manager):

  Esta configuração de segurança determina quais permissões adicionais são concedidas para conexões anônimas ao computador. Esta opção é apresentada como `no-enumeration` no

ONTAP se estiver ativada.

Defina utilizando a `Network access: Do not allow anonymous enumeration of SAM accounts` definição no `Local Policies/Security Options` GPO.

- Nenhuma enumeração de contas e compartilhamentos SAM

  Esta configuração de segurança determina se a enumeração anônima de contas e compartilhamentos SAM é permitida. Esta opção é apresentada como `no-enumeration` no ONTAP se estiver ativada.

  Defina utilizando a `Network access: Do not allow anonymous enumeration of SAM accounts and shares` definição no `Local Policies/Security Options` GPO.

- Restringir o acesso anônimo a compartilhamentos e pipes nomeados

  Essa configuração de segurança restringe o acesso anônimo a compartilhamentos e pipes. Esta opção é apresentada como `no-access` no ONTAP se estiver ativada.

  Defina utilizando a `Network access: Restrict anonymous access to Named Pipes and Shares` definição no `Local Policies/Security Options` GPO.

  Ao exibir informações sobre políticas de grupo definidas e aplicadas, o `Resultant restriction for anonymous user` campo de saída fornece informações sobre a restrição resultante das três configurações de GPO anônimo restrito. As possíveis restrições resultantes são as seguintes:

° `no-access`

O usuário anônimo tem acesso negado aos compartilhamentos especificados e pipes nomeados e não pode usar enumeração de contas e compartilhamentos SAM. Esta restrição resultante é vista se o `Network access: Restrict anonymous access to Named Pipes and Shares` GPO estiver ativado.

° `no-enumeration`

O usuário anônimo tem acesso aos compartilhamentos especificados e pipes nomeados, mas não pode usar enumeração de contas e compartilhamentos SAM. Esta restrição resultante é vista se ambas as seguintes condições forem cumpridas:

- O `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está desativado.
- `Network access: Do not allow anonymous enumeration of SAM accounts`O ou os `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPOs estão ativados.

° `no-restriction`

O usuário anônimo tem acesso total e pode usar enumeração. Esta restrição resultante é vista se ambas as seguintes condições forem cumpridas:

- O `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está desativado.

        - `Network access: Do not allow anonymous enumeration of SAM accounts`Os GPOs e `Network access: Do not allow anonymous enumeration of SAM accounts and shares` os GPOs estão desativados.
        - Grupos restritos

          Você pode configurar grupos restritos para gerenciar centralmente a associação de grupos internos ou definidos pelo usuário. Quando você aplica um grupo restrito por meio de uma política de grupo, a associação de um grupo local de servidor CIFS é definida automaticamente para corresponder às configurações da lista de membros definidas na política de grupo aplicada.

      Defina utilizando o `Restricted Groups` GPO.

- Definições da política de acesso central

  Especifica uma lista de políticas de acesso central. As políticas de acesso central e as regras de política de acesso central associadas determinam permissões de acesso para vários arquivos no SVM.

Informações relacionadas

- Habilitar ou desabilitar o suporte a GPO em servidores
- Saiba mais sobre segurança de acesso a arquivos para servidores
- "Auditoria de SMB e NFS e rastreamento de segurança"
- Modifique as configurações de segurança do servidor
- Saiba mais sobre como usar o BranchCache para armazenar em cache o conteúdo compartilhado em uma filial
- Aprenda a usar a assinatura ONTAP para aumentar a segurança da rede
- Aprenda sobre a configuração da verificação de desvio transversal
- Configurar restrições de acesso para usuários anônimos

Requisitos de servidor SMB do ONTAP para GPOs

Para usar objetos de diretiva de grupo (GPOs) com seu servidor SMB, o sistema deve atender a vários requisitos.

- O SMB deve ser licenciado no cluster. A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.
- Um servidor SMB deve ser configurado e Unido a um domínio do ative Directory do Windows.
- O status de administrador do servidor SMB deve estar ativado.
- Os GPOs devem ser configurados e aplicados à Unidade organizacional do ative Directory (ou) do Windows que contém o objeto de computador servidor SMB.
- O suporte ao GPO deve estar ativado no servidor SMB.

Ative ou desative o suporte GPO em servidores SMB do ONTAP

Você pode ativar ou desativar o suporte de GPO (Group Policy Object) em um servidor CIFS. Se você habilitar o suporte a GPO em um servidor CIFS, os GPOs aplicáveis

definidos na diretiva de grupo - a diretiva aplicada à unidade organizacional (ou) que contém o objeto computador servidor CIFS - serão aplicados ao servidor CIFS.

Sobre esta tarefa

Os GPOs não podem ser ativados em servidores CIFS no modo de grupo de trabalho.

Passos

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Ativar GPOs	`vserver cifs group-policy modify -vserver` *`vserver_name`* `-status enabled`
Desativar GPOs	`vserver cifs group-policy modify -vserver` *`vserver_name`* `-status disabled`

2. Verifique se o suporte GPO está no estado desejado: `vserver cifs group-policy show -vserver +vserver_name_`

   O status da Diretiva de Grupo para servidores CIFS no modo de grupo de trabalho é exibido como "habilitado".

Exemplo

O exemplo a seguir habilita o suporte a GPO na máquina virtual de storage (SVM) VS1:

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

Informações relacionadas

Saiba mais sobre GPOs suportados

Requisitos de servidor para GPOs

Saiba mais sobre como atualizar GPOs em servidores SMB

Atualizar manualmente as configurações de GPO em servidores SMB

Apresentar informações sobre as configurações do GPO

Como os GPOs são atualizados no servidor SMB

Saiba mais sobre como atualizar GPOs em servidores SMB do ONTAP

Por padrão, o ONTAP recupera e aplica alterações de Objeto de Diretiva de Grupo (GPO) a cada 90 minutos. As configurações de segurança são atualizadas a cada 16 horas. Se você quiser atualizar os GPOs para aplicar novas configurações de política de GPO antes que o ONTAP as atualize automaticamente, você pode acionar uma atualização manual em um servidor CIFS com um comando ONTAP.

- Por padrão, todos os GPOs são verificados e atualizados conforme necessário a cada 90 minutos.

  Este intervalo é configurável e pode ser definido utilizando as `Refresh interval` definições e `Random offset` GPO.

  O ONTAP consulta o ative Directory quanto a alterações nos GPOs. Se os números de versão do GPO registrados no ative Directory forem maiores do que os do servidor CIFS, o ONTAP recuperará e aplicará os novos GPOs. Se os números de versão forem os mesmos, os GPOs no servidor CIFS não serão atualizados.

- Os GPOs são atualizados a cada 16 horas.

  O ONTAP recupera e aplica GPOs de configurações de segurança a cada 16 horas, independentemente de estes GPOs terem sido alterados ou não.

  > O valor padrão de 16 horas não pode ser alterado na versão atual do ONTAP. É uma configuração padrão do cliente Windows.

- Todos os GPOs podem ser atualizados manualmente com um comando ONTAP.

  Este comando simula o comando Windows `gpupdate.exe`/force.

Informações relacionadas

Atualizar manualmente as configurações de GPO em servidores SMB

Atualizar manualmente as configurações do GPO em servidores SMB do ONTAP

Se pretender atualizar imediatamente as definições do GPO (Group Policy Object) no servidor CIFS, pode atualizar manualmente as definições. Você pode atualizar apenas as configurações alteradas ou forçar uma atualização para todas as configurações, incluindo as configurações que foram aplicadas anteriormente, mas não foram alteradas.

Passo

1. Execute a ação apropriada:

Se você quiser atualizar…	Digite o comando…
Definições GPO alteradas	`vserver cifs group-policy update -vserver` *`vserver_name`*

Se você quiser atualizar…	Digite o comando…
Todas as definições do GPO	`vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true`

Informações relacionadas

Saiba mais sobre como atualizar GPOs em servidores SMB

Exibir informações sobre as configurações de GPO SMB do ONTAP

Você pode exibir informações sobre configurações de GPO (Group Policy Object) definidas no ative Directory e sobre configurações GPO aplicadas ao servidor CIFS.

Sobre esta tarefa

Você pode exibir informações sobre todas as configurações de GPO definidas no ative Directory do domínio ao qual o servidor CIFS pertence, ou você pode exibir informações apenas sobre as configurações de GPO aplicadas a um servidor CIFS.

Passos

1. Exiba informações sobre as configurações do GPO executando uma das seguintes ações:

Se você quiser exibir informações sobre todas as configurações de Diretiva de Grupo…	Digite o comando…
Definido no ative Directory	`vserver cifs group-policy show-defined -vserver vserver_name`
Aplicado a uma máquina virtual de storage habilitada por CIFS (SVM)	`vserver cifs group-policy show-applied -vserver vserver_name`

Exemplo

O exemplo a seguir exibe as configurações de GPO definidas no ative Directory ao qual pertence o SVM habilitado para CIFS chamado VS1:

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
```

```
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache : version1
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for Mode BranchCache: per-share
    Hash Version Support for BranchCache: version1
Security Settings:
```

```
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

O exemplo a seguir exibe as configurações de GPO aplicadas ao SVM VS1 habilitado para CIFS:

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
-----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
```

```
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

Informações relacionadas

Habilitar ou desabilitar o suporte a GPO em servidores

Exibir informações sobre GPOs de grupo restrito ONTAP SMB

Você pode exibir informações detalhadas sobre grupos restritos definidos como objetos de Diretiva de Grupo (GPOs) no ative Directory e aplicados ao servidor CIFS.

Sobre esta tarefa

Por padrão, as seguintes informações são exibidas:

- Nome da política de grupo
- Versão da política de grupo
- Link

  Especifica o nível no qual a diretiva de grupo está configurada. Os possíveis valores de saída incluem o seguinte:

  - `Local` Quando a política de grupo é configurada no ONTAP

- `Site` quando a política de grupo é configurada no nível do site no controlador de domínio
- `Domain` quando a política de grupo é configurada no nível do domínio no controlador de domínio
- `OrganizationalUnit` Quando a política de grupo é configurada no nível de unidade organizacional (ou) no controlador de domínio
- `RSOP` para o conjunto resultante de políticas derivadas de todas as políticas de grupo definidas em vários níveis

- Nome do grupo restrito
- Os usuários e grupos que pertencem e que não pertencem ao grupo restrito
- A lista de grupos aos quais o grupo restrito é adicionado

  Um grupo pode ser membro de grupos que não sejam os listados aqui.

Passo

1. Exiba informações sobre todos os GPOs de grupo restrito executando uma das seguintes ações:

Se você quiser exibir informações sobre todos os GPOs de grupo restrito…	Digite o comando…
Definido no ative Directory	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
Aplicado a um servidor CIFS	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

Exemplo

O exemplo a seguir exibe informações sobre GPOs de grupo restrito definidos no domínio do ative Directory ao qual pertence o SVM habilitado para CIFS chamado VS1:

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9
```

O exemplo a seguir exibe informações sobre GPOs de grupos restritos aplicados ao SVM VS1 habilitado para CIFS:

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9
```

Informações relacionadas

Exibir informações sobre as políticas de acesso central do ONTAP SMB

Você pode exibir informações detalhadas sobre as políticas de acesso central definidas no ative Directory. Você também pode exibir informações sobre as políticas de acesso central aplicadas ao servidor CIFS por meio de objetos de diretiva de grupo (GPOs).

Sobre esta tarefa

Por padrão, as seguintes informações são exibidas:

- Nome do SVM
- Nome da política de acesso central
- SID
- Descrição
- Tempo de criação
- Tempo de modificação
- Regras dos membros

Os servidores CIFS no modo de grupo de trabalho não são exibidos porque não suportam GPOs.

Passo

1. Exiba informações sobre políticas de acesso central executando uma das seguintes ações:

Se você quiser exibir informações sobre todas as políticas de acesso central…	Digite o comando…
Definido no ative Directory	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
Aplicado a um servidor CIFS	`vserver cifs group-policy central-access-policy show-applied -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir exibe informações de todas as políticas de acesso central definidas no ative Directory:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

O exemplo a seguir exibe informações de todas as políticas de acesso central aplicadas às máquinas virtuais de armazenamento (SVMs) no cluster:

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                  SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

Informações relacionadas

- Saiba mais sobre segurança de acesso a arquivos para servidores
- Apresentar informações sobre as configurações do GPO
- Exibir informações sobre as regras da política de acesso central

Exibir informações sobre as regras da política de acesso central do ONTAP SMB

Você pode exibir informações detalhadas sobre regras de política de acesso central associadas a políticas de acesso centrais definidas no ative Directory. Você também pode exibir informações sobre regras de políticas de acesso centrais aplicadas ao servidor CIFS por meio de GPOs de diretiva de acesso central (objetos de diretiva de grupo).

Sobre esta tarefa

Você pode exibir informações detalhadas sobre regras de política de acesso central definidas e aplicadas. Por padrão, as seguintes informações são exibidas:

- Nome do SVM
- Nome da regra de acesso central
- Descrição
- Tempo de criação
- Tempo de modificação
- Permissões atuais
- Permissões propostas
- Direcionar recursos

Se você quiser exibir informações sobre todas as regras de política de acesso central associadas às políticas de acesso central…	Digite o comando…
Definido no ative Directory	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
Aplicado a um servidor CIFS	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

Exemplo

O exemplo a seguir exibe informações de todas as regras de política de acesso central associadas às políticas de acesso central definidas no ative Directory:

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

O exemplo a seguir exibe informações de todas as regras de política de acesso central associadas às políticas de acesso central aplicadas a máquinas virtuais de armazenamento (SVMs) no cluster:

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Informações relacionadas

- Saiba mais sobre segurança de acesso a arquivos para servidores
- Apresentar informações sobre as configurações do GPO
- Exibir informações sobre políticas de acesso centrais

Comandos ONTAP para gerenciar senhas de contas de computador de servidor SMB

Você precisa saber os comandos para alterar, redefinir e desativar senhas e para configurar agendas de atualização automática. Você também pode configurar um agendamento no servidor SMB para atualizá-lo automaticamente.

Se você quiser…	Use este comando…
Altere a senha da conta de domínio quando o ONTAP estiver sincronizado com os serviços do AD	`vserver cifs domain password change`
Redefina a senha da conta de domínio quando o ONTAP não estiver sincronizado com os serviços do AD	`vserver cifs domain password reset`
Configurar servidores SMB para alterações automáticas de senha de conta de computador	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`
Desativar alterações automáticas de senha de conta de computador em servidores SMB	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

Saiba mais sobre `vserver cifs domain password` o "Referência do comando ONTAP"na .

Gerenciar conexões do controlador de domínio

Exibir informações sobre os servidores descobertos por SMB do ONTAP

Você pode exibir informações relacionadas a servidores LDAP e controladores de domínio descobertos em seu servidor CIFS.

Passo

1. Para exibir informações relacionadas aos servidores descobertos, digite o seguinte comando: `vserver cifs domain discovered-servers show`

Exemplo

O exemplo a seguir mostra os servidores descobertos para o SVM VS1:

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Informações relacionadas

- Redefinir e redescobrir servidores
- Parar ou iniciar servidores

Redefina e redescubra os servidores SMB do ONTAP

Redefinir e redescobrir servidores no servidor CIFS permite que o servidor CIFS descarte informações armazenadas sobre servidores LDAP e controladores de domínio. Depois de descartar as informações do servidor, o servidor CIFS readquire as informações atuais sobre esses servidores externos. Isso pode ser útil quando os servidores conetados não estão respondendo adequadamente.

Passos

1. Introduza o seguinte comando: `vserver cifs domain discovered-servers reset-servers -vserver` *`vserver_name`*
2. Exibir informações sobre os servidores recém-redescobertos: `vserver cifs domain discovered-servers show -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir redefine e redescobre servidores para máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1:

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Informações relacionadas

- Exibir informações sobre servidores descobertos
- Parar ou iniciar servidores

Gerenciar a descoberta do controlador de domínio SMB do ONTAP

A partir do ONTAP 9.3, você pode modificar o processo padrão pelo qual controladores de domínio (DCs) são descobertos. Isso permite limitar a descoberta ao seu site ou a um pool de DCs preferenciais, o que pode levar a melhorias de desempenho, dependendo do ambiente.

Sobre esta tarefa

Por padrão, o processo de descoberta dinâmica descobre todos os DCs disponíveis, incluindo todos os DCs preferenciais, todos os DCs no local e todos os DCs remotos. Essa configuração pode levar à latência na autenticação e ao acesso a compartilhamentos em determinados ambientes. Se você já determinou o pool de DCs que deseja usar, ou se os DCs remotos são inadequados ou inacessíveis, você pode alterar o método de descoberta.

No ONTAP 9.3 e versões posteriores, o `discovery-mode` parâmetro `cifs domain discovered-servers` do comando permite selecionar uma das seguintes opções de descoberta:

- Todos os DCs no domínio são descobertos.
- Apenas DCs no local são descobertos.

  O `default-site` parâmetro para o servidor SMB pode ser definido para usar esse modo com LIFs que não são atribuídos a um site em sites e serviços.

- A deteção de servidor não é realizada, a configuração do servidor SMB depende apenas de DCs preferenciais.

  Para utilizar este modo, tem de definir primeiro os DCs preferidos para o servidor SMB.

Antes de começar

Você deve estar no nível de privilégio avançado.

Passo

1. Especifique a opção de descoberta desejada: `vserver cifs domain discovered-servers discovery-mode modify -vserver vserver_name -mode {all|site|none}`

   Opções para o `mode` parâmetro:

   - `all`

     Descubra todos os DCs disponíveis (padrão).

   - `site`

     Limite a descoberta DC ao seu site.

   - `none`

     Use apenas DCs preferenciais e não execute a descoberta.

Adicione controladores de domínio SMB ONTAP preferenciais

O ONTAP descobre automaticamente controladores de domínio através do DNS. Opcionalmente, você pode adicionar um ou mais controladores de domínio à lista de controladores de domínio preferenciais para um domínio específico.

Sobre esta tarefa

Se já existir uma lista de controlador de domínio preferencial para o domínio especificado, a nova lista será mesclada com a lista existente.

Passo

1. Para adicionar à lista de controladores de domínio preferenciais, digite o seguinte comando `vserver cifs domain preferred-dc add -vserver vserver_name -domain domain_name -preferred-dc IP_address, …+`

   `-vserver vserver_name` Especifica o nome da máquina virtual de storage (SVM).

   `-domain domain_name` Especifica o nome totalmente qualificado do ative Directory do domínio ao qual pertencem os controladores de domínio especificados.

   `-preferred-dc IP_address`,… especifica um ou mais endereços IP dos controladores de domínio preferidos, como uma lista delimitada por vírgulas, por ordem de preferência.

Exemplo

O comando a seguir adiciona controladores de domínio 172.17.102.25 e 172.17.102.24 à lista de controladores de domínio preferenciais que o servidor SMB no SVM VS1 usa para gerenciar o acesso externo ao domínio cifs.lab.example.com.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

Informações relacionadas

Comandos para gerenciar controladores de domínio preferenciais

Comandos ONTAP para gerenciar controladores de domínio SMB preferenciais

Você precisa saber os comandos para adicionar, exibir e remover controladores de domínio preferenciais.

Se você quiser…	Use este comando…
Adicione um controlador de domínio preferido	`vserver cifs domain preferred-dc add`
Exibir controladores de domínio preferenciais	`vserver cifs domain preferred-dc show`
Remova um controlador de domínio preferido	`vserver cifs domain preferred-dc remove`

Saiba mais sobre `vserver cifs domain preferred-dc` o "Referência do comando ONTAP"na .

Informações relacionadas

Adicione controladores de domínio preferenciais

Ative conexões criptografadas com controladores de domínio SMB do ONTAP

A partir do ONTAP 9.8, você pode especificar que as conexões aos controladores de domínio sejam criptografadas.

Sobre esta tarefa

O ONTAP requer criptografia para comunicações de controlador de domínio (DC) quando a `-encryption -required-for-dc-connection` opção está definida como `true`; o padrão é `false`. Quando a opção está definida, apenas o protocolo SMB3 será utilizado para ligações ONTAP-DC, uma vez que a encriptação é suportada apenas pelo SMB3.

Quando as comunicações CC criptografadas são necessárias, a `-smb2-enabled-for-dc-connections` opção é ignorada, porque o ONTAP negocia somente conexões SMB3. Se um DC não suportar SMB3 e criptografia, o ONTAP não se conetará a ele.

Passo

1. Ative a comunicação encriptada com o DC: `vserver cifs security modify -vserver` *`svm_name`* `-encryption-required-for-dc-connection true`

Use sessões nulas para acessar o armazenamento em ambientes não Kerberos

Use sessões nulas ONTAP SMB para acessar o armazenamento em ambientes que não sejam Kerberos

O acesso de sessão nula fornece permissões para recursos de rede, como dados do sistema de armazenamento de dados, e para serviços baseados em cliente executados no sistema local. Uma sessão nula ocorre quando um processo de cliente usa a conta "system" para acessar um recurso de rede. A configuração de sessão nula é específica para autenticação não Kerberos.

Saiba como os sistemas de armazenamento ONTAP SMB fornecem acesso a sessão nula

Como compartilhamentos de sessão nulos não exigem autenticação, os clientes que exigem acesso de sessão null devem ter seus endereços IP mapeados no sistema de armazenamento.

Por padrão, os clientes de sessão nula não mapeados podem acessar determinados serviços do sistema ONTAP, como enumeração de compartilhamento, mas eles são restritos a acessar quaisquer dados do sistema de storage.

> O ONTAP suporta os valores de configuração do Registro anônimo do Windows com a `-restrict-anonymous` opção. Isso permite controlar até que ponto os usuários nulos não mapeados podem exibir ou acessar recursos do sistema. Por exemplo, você pode desativar a enumeração de compartilhamento e o acesso ao compartilhamento IPC (o compartilhamento de pipe nomeado oculto). Saiba mais sobre `vserver cifs options modify` e `vserver cifs options show` e a `-restrict-anonymous` opção no "Referência do comando ONTAP".

A menos que configurado de outra forma, um cliente executando um processo local que solicita acesso ao sistema de armazenamento por meio de uma sessão nula é membro apenas de grupos não restritivos, como "'todos'". Para limitar o acesso de sessão nula a recursos selecionados do sistema de armazenamento, você pode querer criar um grupo ao qual todos os clientes de sessão nula pertencem; a criação deste grupo permite restringir o acesso ao sistema de armazenamento e definir permissões de recursos do sistema de armazenamento que se aplicam especificamente a clientes de sessão nula.

O ONTAP fornece uma sintaxe de mapeamento no `vserver name-mapping` conjunto de comandos para especificar o endereço IP dos clientes que têm acesso permitido aos recursos do sistema de armazenamento usando uma sessão de usuário nula. Depois de criar um grupo para usuários nulos, você pode especificar restrições de acesso para recursos do sistema de armazenamento e permissões de recursos que se aplicam somente a sessões nulas. O usuário nulo é identificado como logon anônimo. Os usuários nulos não têm acesso a nenhum diretório home.

Qualquer usuário nulo que acesse o sistema de armazenamento a partir de um endereço IP mapeado recebe permissões de usuário mapeadas. Considere as precauções apropriadas para evitar o acesso não autorizado aos sistemas de armazenamento mapeados com usuários nulos. Para máxima proteção, coloque o sistema de armazenamento e todos os clientes que necessitem de acesso nulo ao sistema de armazenamento de utilizadores numa rede separada, para eliminar a possibilidade de "spoofing" de endereço IP.

Informações relacionadas

Configurar restrições de acesso para usuários anônimos

Conceder acesso a usuários nulos aos compartilhamentos do sistema de arquivos SMB do ONTAP

Você pode permitir o acesso aos recursos do seu sistema de armazenamento por clientes de sessão nulos, atribuindo um grupo a ser usado por clientes de sessão nulos e registrando os endereços IP de clientes de sessão nulos para adicionar à lista de clientes com permissão para acessar dados usando sessões nulas.

Passos

1. Use o `vserver name-mapping create` comando para mapear o usuário nulo para qualquer usuário válido do Windows, com um qualificador IP.

   O comando a seguir mapeia o usuário nulo para user1 com um nome de host válido google.com:

   ```
   vserver name-mapping create -direction win-unix  -position 1 -pattern
   "ANONYMOUS LOGON" -replacement user1 - hostname google.com
   ```

   O comando a seguir mapeia o usuário nulo para user1 com um endereço IP válido 10.238.2.54/32:

   ```
   vserver name-mapping create -direction win-unix  -position 2 -pattern
   "ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
   ```

2. Use o `vserver name-mapping show` comando para confirmar o mapeamento de nomes.

   ```
   vserver name-mapping show

   Vserver:   vs1
   Direction: win-unix
   Position Hostname         IP Address/Mask
   -------- --------         ----------------
   1        -                10.72.40.83/32      Pattern: anonymous logon
                                              Replacement: user1
   ```

3. Use o `vserver cifs options modify –win-name-for-null-user` comando para atribuir a associação do Windows ao usuário nulo.

   Essa opção é aplicável somente quando há um mapeamento de nome válido para o usuário nulo.

   ```
   vserver cifs options modify -win-name-for-null-user user1
   ```

4. Use o `vserver cifs options show` comando para confirmar o mapeamento do usuário nulo para o

usuário ou grupo do Windows.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

Gerencie aliases NetBIOS para servidores SMB

Saiba mais sobre como gerenciar aliases NetBIOS para servidores SMB ONTAP

Os aliases NetBIOS são nomes alternativos para o servidor SMB que os clientes SMB podem usar ao se conetar ao servidor SMB. A configuração de aliases NetBIOS para um servidor SMB pode ser útil quando você está consolidando dados de outros servidores de arquivos para o servidor SMB e deseja que o servidor SMB responda aos nomes dos servidores de arquivos originais.

Você pode especificar uma lista de aliases NetBIOS ao criar o servidor SMB ou a qualquer momento depois de criar o servidor SMB. Você pode adicionar ou remover aliases NetBIOS da lista a qualquer momento. Você pode se conetar ao servidor SMB usando qualquer um dos nomes na lista de alias do NetBIOS.

Informações relacionadas

Exibir informações sobre NetBIOS sobre conexões TCP

Adicione listas de alias NetBIOS aos servidores SMB do ONTAP

Se você quiser que os clientes SMB se conetem ao servidor SMB usando um alias, você pode criar uma lista de aliases NetBIOS ou adicionar aliases NetBIOS a uma lista existente de aliases NetBIOS.

Sobre esta tarefa

- O nome de alias NetBIOS pode ter 15 até carateres de comprimento.
- Você pode configurar até 200 aliases NetBIOS no servidor SMB.
- Não são permitidos os seguintes carateres:
- ( ) [ ] | ; : " , > / ?

Passos

1. Adicione os aliases NetBIOS `vserver cifs add-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases` *`NetBIOS_alias`*`,…`

   ```
   vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
   alias_1,alias_2,alias_3
   ```

   - Você pode especificar um ou mais aliases NetBIOS usando uma lista delimitada por vírgulas.
   - Os aliases NetBIOS especificados são adicionados à lista existente.

◦ Uma nova lista de aliases NetBIOS é criada se a lista estiver vazia no momento.

2. Verifique se os aliases NetBIOS foram adicionados corretamente: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

Informações relacionadas

- Remover aliases NetBIOS da lista de servidores SMB
- Exibir a lista de aliases NetBIOS para servidores SMB

Remova os aliases NetBIOS da lista para servidores SMB do ONTAP

Se você não precisar de aliases NetBIOS específicos para um servidor CIFS, você poderá remover esses aliases NetBIOS da lista. Você também pode remover todos os aliases NetBIOS da lista.

Sobre esta tarefa

Você pode remover mais de um alias NetBIOS usando uma lista delimitada por vírgulas. Você pode remover todos os aliases NetBIOS em um servidor CIFS especificando - como o valor para o `-netbios-aliases` parâmetro.

Passos

1. Execute uma das seguintes ações:

Se você quiser remover…	Digite…
Aliases NetBIOS específicos da lista	`vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...`
Todos os aliases NetBIOS da lista	`vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -`

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. Verifique se os aliases NetBIOS especificados foram removidos: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_2, ALIAS_3
```

Exiba a lista de aliases NetBIOS para servidores SMB do ONTAP

Você pode exibir a lista de aliases NetBIOS. Isso pode ser útil quando você deseja determinar a lista de nomes sobre os quais clientes SMB podem fazer conexões com o servidor CIFS.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite…
Os aliases NetBIOS de um servidor CIFS	`vserver cifs show -display-netbios -aliases`
A lista de aliases NetBIOS como parte das informações detalhadas do servidor CIFS	`vserver cifs show -instance`

O exemplo a seguir exibe informações sobre os aliases NetBIOS de um servidor CIFS:

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

O exemplo a seguir exibe a lista de aliases NetBIOS como parte das informações detalhadas do servidor CIFS:

```
vserver cifs show -instance
```

```
                                        Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_SERVER
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                           Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

Saiba mais sobre `vserver cifs show` o "Referência do comando ONTAP"na .

Informações relacionadas

- Adicionar listas de alias NetBIOS aos servidores
- Comandos para gerenciamento de servidores

Determine se os clientes SMB do ONTAP estão conetados usando aliases NetBIOS

Você pode determinar se os clientes SMB estão conetados usando aliases NetBIOS e, em caso afirmativo, qual alias NetBIOS é usado para fazer a conexão. Isso pode ser útil ao solucionar problemas de conexão.

Sobre esta tarefa

Você deve usar o `-instance` parâmetro para exibir o alias NetBIOS (se houver) associado a uma conexão SMB. Se o nome do servidor CIFS ou um endereço IP for usado para fazer a conexão SMB, a saída para o `NetBIOS Name` campo é - (hífen).

Passo

1. Execute a ação desejada:

Se você quiser exibir informações do NetBIOS para…	Digite…
Conexões SMB	`vserver cifs session show -instance`
Conexões usando um alias NetBIOS especificado:	`vserver cifs session show -instance -netbios-name` *`netbios_name`*

O exemplo a seguir exibe informações sobre o alias NetBIOS usado para fazer a conexão SMB com o Session ID 1:

```
vserver cifs session show -session-id 1 -instance
```

```
                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
                 Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                Windows User: EXAMPLE\user1
                   UNIX User: user1
                 Open Shares: 2
                  Open Files: 2
                  Open Other: 0
              Connected Time: 1d 1h 10m 5s
                   Idle Time: 22s
           Protocol Version: SMB3
      Continuously Available: No
          Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

Gerenciar diversas tarefas de servidor SMB

Pare ou inicie servidores SMB do ONTAP

Você pode parar o servidor CIFS em uma SVM, que pode ser útil na execução de tarefas enquanto os usuários não acessam dados por compartilhamentos SMB. Você pode reiniciar o acesso SMB iniciando o servidor CIFS. Ao parar o servidor CIFS, você também pode modificar os protocolos permitidos na máquina virtual de storage (SVM).

Passos

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Pare o servidor CIFS	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	Inicie o servidor CIFS
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

`-foreground` especifica se o comando deve ser executado em primeiro plano ou em segundo plano. Se você não inserir esse parâmetro, ele será definido como `true`, e o comando será executado em primeiro

plano.

2. Verifique se o status administrativo do servidor CIFS está correto usando o `vserver cifs show` comando.

Exemplo

Os comandos a seguir iniciam o servidor CIFS no SVM VS1:

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

Informações relacionadas

- Exibir informações sobre servidores descobertos
- Redefinir e redescobrir servidores

Mova os servidores SMB do ONTAP para OUs diferentes

O processo de criação do servidor CIFS usa a unidade organizacional padrão (ou) CN de computadores durante a configuração, a menos que você especifique uma ou diferente. Você pode mover servidores CIFS para diferentes OUs após a configuração.

Passos

1. No servidor Windows, abra a árvore **usuários e computadores do ative Directory**.
2. Localize o objeto do ative Directory da máquina virtual de storage (SVM).
3. Clique com o botão direito do rato no objeto e selecione **mover**.
4. Selecione a UO que você deseja associar ao SVM

Resultados

O objeto SVM é colocado na UO selecionada.

Modifique o domínio DNS dinâmico antes de mover os servidores SMB do ONTAP

Se desejar que o servidor DNS integrado ao ative Directory Registre dinamicamente os Registros DNS do servidor SMB no DNS ao mover o servidor SMB para outro domínio, você deve modificar DNS dinâmico (DDNS) na máquina virtual de armazenamento (SVM) antes de mover o servidor SMB.

Antes de começar

Os serviços de nomes DNS devem ser modificados no SVM para usar o domínio DNS que contém os Registros de localização do serviço para o novo domínio que conterá a conta de computador do servidor SMB. Se você estiver usando DDNS seguro, você deve usar servidores de nomes DNS integrados ao ative Directory.

Sobre esta tarefa

Embora o DDNS (se configurado no SVM) adicione automaticamente os Registros DNS para LIFs de dados ao novo domínio, os Registros DNS para o domínio original não são excluídos automaticamente do servidor DNS original. Você deve excluí-los manualmente.

Para concluir as modificações do DDNS antes de mover o servidor SMB, consulte o seguinte tópico:

"Configurar serviços DNS dinâmicos"

Junte-se a SVMs SMB do ONTAP aos domínios do ative Directory

É possível associar uma máquina virtual de armazenamento (SVM) a um domínio do ative Directory sem excluir o servidor SMB existente, modificando o domínio usando o `vserver cifs modify` comando. Você pode ingressar novamente no domínio atual ou ingressar em um novo.

Antes de começar

- O SVM já deve ter uma configuração de DNS.
- A configuração DNS do SVM deve ser capaz de servir o domínio de destino.

  Os servidores DNS têm de conter os registos de localização de serviço (SRV) para os servidores LDAP de domínio e controlador de domínio.

Sobre esta tarefa

- O status administrativo do servidor CIFS deve ser definido como `down` para prosseguir com a modificação de domínio do ative Directory.
- Se o comando for concluído com êxito, o status administrativo será automaticamente definido como `up`. Saiba mais sobre `up` o "Referência do comando ONTAP"na .
- Ao ingressar em um domínio, esse comando pode levar vários minutos para ser concluído.

Passos

1. Junte-se ao SVM ao domínio do servidor CIFS: `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

   Saiba mais sobre `vserver cifs modify` o "Referência do comando ONTAP"na . Se precisar reconfigurar o DNS para o novo domínio, saiba mais sobre o `vserver dns modify` "Referência do comando ONTAP".

   Para criar uma conta de máquina do ative Directory para o servidor SMB, você deve fornecer o nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores ao `ou=` *`example`* `ou` contentor dentro do *`example`* domínio .com.

   A partir do ONTAP 9.7, o administrador do AD pode fornecer um URI para um arquivo keytab como alternativa para fornecer um nome e uma senha para uma conta privilegiada do Windows. Quando

receber o URI, inclua-o `-keytab-uri` no parâmetro com os `vserver cifs` comandos.

2. Verifique se o servidor CIFS está no domínio desejado do ative Directory: `vserver cifs show`

Exemplo

No exemplo a seguir, o servidor SMB "'CIFSSERVER1"" no SVM VS1 junta o domínio example.com usando autenticação keytab:

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE           domain
```

Exibir informações sobre o NetBIOS SMB do ONTAP em conexões TCP

Você pode exibir informações sobre conexões NetBIOS sobre TCP (NBT). Isso pode ser útil ao solucionar problemas relacionados ao NetBIOS.

Passo

1. Use o `vserver cifs nbtstat` comando para exibir informações sobre NetBIOS sobre conexões TCP.

   O serviço de nomes NetBIOS (NBNS) em IPv6 não é suportado.

Exemplo

O exemplo a seguir mostra as informações do serviço de nomes NetBIOS exibidas para "'cluster1":

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1          00               wins          58
         CLUSTER_1          20               wins          58
         4 entries were displayed.
```

Comandos ONTAP para gerenciar servidores SMB

Você precisa saber os comandos para criar, exibir, modificar, parar, iniciar e excluir servidores SMB. Há também comandos para redefinir e redescobrir servidores, alterar ou redefinir senhas de conta de máquina, agendar alterações para senhas de conta de máquina e adicionar ou remover aliases NetBIOS.

Se você quiser…	Use este comando…
Crie um servidor SMB	`vserver cifs create`
Exibir informações sobre um servidor SMB	`vserver cifs show`
Modifique um servidor SMB	`vserver cifs modify`
Mova um servidor SMB para outro domínio	`vserver cifs modify`

Parar um servidor SMB	`vserver cifs stop`
Inicie um servidor SMB	`vserver cifs start`
Excluir um servidor SMB	`vserver cifs delete`
Redefinir e redescobrir servidores para o servidor SMB	`vserver cifs domain discovered-servers reset-servers`
Altere a senha da conta de máquina do servidor SMB	`vserver cifs domain password change`
Redefina a senha da conta da máquina do servidor SMB	`vserver cifs domain password change`
Agendar alterações automáticas de senha para a conta de máquina do servidor SMB	`vserver cifs domain password schedule modify`
Adicione aliases NetBIOS para o servidor SMB	`vserver cifs add-netbios-aliases`
Remova os aliases NetBIOS para o servidor SMB	`vserver cifs remove-netbios-aliases`

Saiba mais sobre `vserver cifs` o "Referência do comando ONTAP"na .

Informações relacionadas

"O que acontece com usuários e grupos locais ao excluir servidores SMB"

Ative o serviço de nomes NetBIOS SMB do ONTAP

Começando com ONTAP 9, o serviço de nomes NetBIOS (NBNS, às vezes chamado de Serviço de nomes de Internet do Windows ou WINS) é desativado por padrão. Anteriormente, as máquinas virtuais de armazenamento (SVMs) habilitadas por CIFS enviavam transmissões de Registro de nomes, independentemente de o WINS estar habilitado em uma rede. Para limitar tais transmissões a configurações em que o NBNS é necessário, você deve habilitar o NBNS explicitamente para novos servidores CIFS.

Antes de começar

- Se você já estiver usando NBNS e atualizar para o ONTAP 9, não é necessário concluir esta tarefa. NBNS continuará a funcionar como antes.
- O NBNS é ativado por UDP (porta 137).
- NBNS sobre IPv6 não é suportado.

Passos

1. Defina o nível de privilégio como avançado.

```
set -privilege advanced
```

2. Ative NBNS em um servidor CIFS.

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. Retorne ao nível de privilégio de administrador.

```
set -privilege admin
```

Use o IPv6 para acesso SMB e serviços SMB

Saiba mais sobre os requisitos de SMB do ONTAP para IPv6

Antes de poder usar o IPv6 no servidor SMB, você precisa saber quais versões do ONTAP e SMB o suportam e quais são os requisitos de licença.

Requisitos de licença do ONTAP

Nenhuma licença especial é necessária para o IPv6 quando o SMB é licenciado. A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.

Requisitos de versão do protocolo SMB

- Para SVMs, o ONTAP oferece suporte a IPv6 em todas as versões do protocolo SMB.

O serviço de nomes NetBIOS (NBNS) em IPv6 não é suportado.

Saiba mais sobre o suporte para IPv6 com acesso ONTAP SMB e serviços CIFS

Se você quiser usar o IPv6 em seu servidor CIFS, você precisa estar ciente de como o ONTAP suporta o IPv6 para acesso SMB e comunicação de rede para serviços CIFS.

Suporte ao cliente e servidor Windows

O ONTAP fornece suporte para servidores e clientes Windows que suportam IPv6. A seguir descreve o suporte ao cliente e servidor Microsoft Windows IPv6:

- O Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 e posterior suportam o IPv6 para serviços de partilha de ficheiros SMB e ative Directory, incluindo DNS, LDAP, CLDAP e Kerberos.

  Se os endereços IPv6 estiverem configurados, o Windows 7 e o Windows Server 2008 e versões posteriores usam o IPv6 por padrão para serviços do ative Directory. Tanto a autenticação NTLM como Kerberos através de conexões IPv6 são suportadas.

Todos os clientes Windows suportados pelo ONTAP podem se conetar a compartilhamentos SMB usando endereços IPv6.

Para obter as informações mais recentes sobre quais clientes Windows ONTAP suportam, consulte "Matriz de interoperabilidade".

Os domínios NT não são suportados para IPv6.

Suporte adicional a serviços CIFS

Além do suporte IPv6 para compartilhamentos de arquivos SMB e serviços do ative Directory, o ONTAP oferece suporte IPv6 para o seguinte:

- Serviços do lado do cliente, incluindo pastas offline, perfis de roaming, redirecionamento de pastas e versões anteriores
- Serviços do lado do servidor, incluindo diretórios base dinâmicos (recurso Home Directory), links simbólicos e Widelinks, BranchCache, descarga de cópia ODX, referências automáticas de nós e versões anteriores
- Serviços de gerenciamento de acesso a arquivos, incluindo o uso de usuários e grupos locais do Windows para controle de acesso e gerenciamento de direitos, configuração de permissões de arquivos e políticas de auditoria usando a CLI, rastreamento de segurança, gerenciamento de bloqueios de arquivos e monitoramento de atividades SMB
- Auditoria multiprotocolo nas
- FPolicy
- Compartilhamentos continuamente disponíveis, protocolo de testemunha e VSS remoto (usado com configurações Hyper-V em SMB)

Serviço de nomes e suporte de serviços de autenticação

A comunicação com os seguintes serviços de nome é suportada com o IPv6:

- Controladores de domínio
- Servidores DNS
- Servidores LDAP
- Servidores KDC
- Servidores NIS

Saiba como os servidores SMB da ONTAP usam o IPv6 para se conetar a servidores externos

Para criar uma configuração que atenda aos seus requisitos, você deve estar ciente de como os servidores CIFS usam o IPv6 ao fazer conexões com servidores externos.

- Seleção do endereço de origem

  Se for feita uma tentativa de ligação a um servidor externo, o endereço de origem selecionado tem de ser do mesmo tipo que o endereço de destino. Por exemplo, se estiver conetando a um endereço IPv6, a máquina virtual de armazenamento (SVM) que hospeda o servidor CIFS deve ter um LIF de dados ou LIF de gerenciamento que tenha um endereço IPv6 para usar como endereço de origem. Da mesma forma, se

estiver conetando a um endereço IPv4, o SVM precisa ter um LIF de dados ou um LIF de gerenciamento que tenha um endereço IPv4 para usar como endereço de origem.

- Para servidores dinamicamente descobertos usando DNS, a descoberta do servidor é executada da seguinte forma:
  - Se o IPv6 estiver desativado no cluster, apenas serão detetados IPv4 endereços de servidores.
  - Se IPv6 estiver ativado no cluster, os endereços de servidor IPv4 e IPv6 serão descobertos. Qualquer tipo pode ser usado dependendo da adequação do servidor ao qual o endereço pertence e da disponibilidade de dados IPv6 ou IPv4 ou LIFs de gerenciamento. A descoberta dinâmica de servidor é usada para descobrir controladores de domínio e seus serviços associados, como LSA, NETLOGON, Kerberos e LDAP.
- Conetividade do servidor DNS

  Se o SVM usa IPv6 ao se conetar a um servidor DNS depende da configuração dos serviços de nome DNS. Se os serviços DNS estiverem configurados para usar endereços IPv6, as conexões serão feitas usando IPv6. Se desejar, a configuração dos serviços de nomes DNS pode usar endereços IPv4 para que as conexões com servidores DNS continuem a usar endereços IPv4. Combinações de endereços IPv4 e IPv6 podem ser especificadas ao configurar serviços de nomes DNS.

- Conetividade do servidor LDAP

  Se o SVM usa IPv6 ao se conetar a um servidor LDAP depende da configuração do cliente LDAP. Se o cliente LDAP estiver configurado para usar endereços IPv6, as conexões serão feitas usando IPv6. Se desejar, a configuração do cliente LDAP pode usar endereços IPv4 para que as conexões com servidores LDAP continuem a usar endereços IPv4. Combinações de endereços IPv4 e IPv6 podem ser especificadas ao configurar a configuração do cliente LDAP.

  > A configuração do cliente LDAP é usada ao configurar o LDAP para serviços de nome de usuário, grupo e netgroup UNIX.

- Conetividade do servidor NIS

  Se o SVM usa IPv6 ao conetar-se a um servidor NIS depende da configuração dos serviços de nome NIS. Se os serviços NIS estiverem configurados para usar endereços IPv6, as conexões serão feitas usando IPv6. Se desejar, a configuração dos serviços de nomes NIS pode usar endereços IPv4 para que as conexões com servidores NIS continuem a usar endereços IPv4. Combinações de endereços IPv4 e IPv6 podem ser especificadas ao configurar serviços de nomes NIS.

  > Os serviços de nomes NIS são usados para armazenar e gerenciar objetos de nome de usuário, grupo, netgroup e host UNIX.

Informações relacionadas

- Habilitar IPv6 para servidores
- Monitorar e exibir informações sobre sessões IPv6

Ative o IPv6 para servidores SMB do ONTAP

As redes IPv6 não estão ativadas durante a configuração do cluster. Um administrador de cluster deve habilitar o IPv6 após a conclusão da configuração do cluster para usar o IPv6 para SMB. Quando o administrador do cluster ativa o IPv6, ele é ativado para todo

o cluster.

Passo

1. Ativar IPv6: `network options ipv6 modify -enabled true`

   IPv6 está ativado. LIFs de dados IPv6 para acesso SMB podem ser configurados.

Informações relacionadas

- Monitorar e exibir informações sobre sessões IPv6
- "Visualize a rede usando o System Manager"
- "Habilitando IPv6 no cluster"
- "opções de rede ipv6 modificar"

Saiba mais sobre como desativar o IPv6 para servidores SMB do ONTAP

Mesmo que IPv6 esteja habilitado no cluster usando uma opção de rede, você não pode desabilitar IPv6 para SMB usando o mesmo comando. Em vez disso, o ONTAP desativa o IPv6 quando o administrador do cluster desativa a última interface habilitada para IPv6 no cluster. Você deve se comunicar com o administrador do cluster sobre o gerenciamento de suas interfaces IPv6 habilitadas.

Informações relacionadas

- "Visualize a rede ONTAP usando o Gerenciador do sistema"

Monitore e exiba informações sobre sessões IPv6 ONTAP SMB

Você pode monitorar e exibir informações sobre sessões SMB conetadas usando redes IPv6G. Essas informações são úteis para determinar quais clientes estão se conetando usando o IPv6, bem como outras informações úteis sobre sessões SMB do IPv6.

Passo

1. Execute a ação desejada:

Se você quiser determinar se…	Digite o comando…
As sessões de SMB a uma máquina virtual de storage (SVM) são conetadas usando o IPv6	`vserver cifs session show -vserver` *`vserver_name`* `-instance`
IPv6 é usado para sessões SMB através de um endereço LIF especificado	`vserver cifs session show -vserver` *`vserver_name`* `-lif-address` *`LIF_IP_address`* `-instance` *`LIF_IP_address`* É o endereço IPv6 do LIF de dados.

Informações sobre direitos autorais

Informações sobre marcas comerciais