Use as opções para personalizar servidores SMB

ONTAP 9

NetApp
January 17, 2025

Índice

Use as opções para personalizar servidores SMB

Opções de servidor 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.

Configurando opções de servidor SMB

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`

   Para obter mais informações sobre como configurar as opções do servidor SMB, consulte a página de manual do `vserver cifs options modify` comando.

Configure a permissão Grant UNIX group para usuários SMB

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 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.

Valor	Descrição
`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 SMB disponíveis

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

Gerencie como a segurança de arquivos é apresentada aos clientes SMB para visão geral de dados em 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

Configurando estilos de segurança no FlexVol volumes

Configurando estilos de segurança no qtrees

Ative ou desative a apresentação de ACLs NTFS 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`

Como o ONTAP preserva as permissões UNIX

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.

Gerenciar permissões UNIX usando a guia Segurança do Windows

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.

Informações sobre direitos autorais

Informações sobre marcas comerciais