



Como o ONTAP usa usuários e grupos locais

ONTAP 9

NetApp
January 17, 2025

Índice

- Como o ONTAP usa usuários e grupos locais 1
 - Conceitos de usuários e grupos locais 1
 - Razões para criar usuários locais e grupos locais 2
 - Como funciona a autenticação de usuário local 2
 - Como os tokens de acesso do usuário são construídos 3
 - Diretrizes para o uso do SnapMirror em SVMs que contêm grupos locais 4
 - O que acontece com usuários e grupos locais ao excluir servidores CIFS 4
 - Como você pode usar o Microsoft Management Console com usuários e grupos locais 5
 - Diretrizes para reverter 5

Como o ONTAP usa usuários e grupos locais

Conceitos de usuários e grupos locais

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

- **Usuário local**

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

As contas de usuário têm vários usos:

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

- **Grupo local**

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

Os grupos têm vários usos:

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

- **Domínio local**

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

- **Identificador de segurança (SID)**

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

- *** Autenticação NTLM***

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

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

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

Razões para criar usuários locais e grupos locais

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

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

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

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

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

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

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

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

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

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

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

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

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

Informações relacionadas

[Como funciona a autenticação de usuário local](#)

[Lista de Privileges suportados](#)

Como funciona a autenticação de usuário local

Antes que um usuário local possa acessar dados em um servidor CIFS, o usuário deve

criar uma sessão autenticada.

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

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

- A parte do domínio corresponde

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

- A parte do domínio não corresponde

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

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

- A parte do domínio não é especificada

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

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

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

Informações relacionadas

[Ativar ou desativar a autenticação de utilizador local](#)

Como os tokens de acesso do usuário são construídos

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

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

- Início de sessão do utilizador local

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

- Login de usuário de domínio

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

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

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



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

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

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

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

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

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

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



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

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

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

Diretrizes para reverter

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

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

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

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.