



Configurar mapeamentos de nomes

ONTAP 9

NetApp
January 17, 2025

Índice

Configurar mapeamentos de nomes	1
Configure a visão geral dos mapeamentos de nomes	1
Como o mapeamento de nomes funciona	1
Procura multidomínio para mapeamentos de nome de usuário do UNIX para o Windows	2
Regras de conversão de mapeamento de nomes	4
Crie um mapeamento de nomes	4
Configure o usuário padrão	5
Comandos para gerenciar mapeamentos de nomes	5

Configurar mapeamentos de nomes

Configure a visão geral dos mapeamentos de nomes

O ONTAP usa mapeamento de nomes para mapear identidades CIFS para identidades UNIX, identidades Kerberos para identidades UNIX e identidades UNIX para identidades CIFS. Ele precisa dessas informações para obter credenciais de usuário e fornecer acesso adequado aos arquivos, independentemente de estarem se conectando a partir de um cliente NFS ou de um cliente CIFS.

Há duas exceções em que você não precisa usar o mapeamento de nomes:

- Você configura um ambiente UNIX puro e não planeja usar o acesso CIFS ou o estilo de segurança NTFS em volumes.
- Em vez disso, você configura o usuário padrão a ser usado.

Nesse cenário, o mapeamento de nomes não é necessário porque, em vez de mapear cada credencial de cliente individual, todas as credenciais de cliente são mapeadas para o mesmo usuário padrão.

Observe que você pode usar o mapeamento de nomes somente para usuários, não para grupos.

No entanto, você pode mapear um grupo de usuários individuais para um usuário específico. Por exemplo, você pode mapear todos os usuários do AD que começam ou terminam com a palavra VENDAS para um usuário UNIX específico e para o UID do usuário.

Como o mapeamento de nomes funciona

Quando o ONTAP tem que mapear credenciais para um usuário, ele primeiro verifica o banco de dados de mapeamento de nomes local e o servidor LDAP para um mapeamento existente. Verifique uma ou ambas e em que ordem é determinada pela configuração do serviço de nomes do SVM.

- Para mapeamento do Windows para UNIX

Se nenhum mapeamento for encontrado, o ONTAP verifica se o nome de usuário do Windows em minúsculas é um nome de usuário válido no domínio UNIX. Se isso não funcionar, ele usará o usuário UNIX padrão desde que esteja configurado. Se o usuário UNIX padrão não estiver configurado e o ONTAP também não puder obter um mapeamento dessa maneira, o mapeamento falhará e um erro será retornado.

- Para mapeamento UNIX para Windows

Se nenhum mapeamento for encontrado, o ONTAP tentará encontrar uma conta do Windows que corresponda ao nome UNIX no domínio SMB. Se isso não funcionar, ele usará o usuário SMB padrão, desde que esteja configurado. Se o usuário CIFS padrão não estiver configurado e o ONTAP também não puder obter um mapeamento dessa maneira, o mapeamento falhará e um erro será retornado.

As contas de máquina são mapeadas para o usuário UNIX padrão especificado por padrão. Se nenhum usuário UNIX padrão for especificado, mapeamentos de contas de máquina falharão.

- A partir do ONTAP 9.5, você pode mapear contas de máquina para usuários que não sejam o usuário UNIX padrão.
- No ONTAP 9.4 e anteriores, você não pode mapear contas de máquina para outros usuários.

Mesmo que os mapeamentos de nomes para contas de máquinas sejam definidos, os mapeamentos serão ignorados.

Procura multidomínio para mapeamentos de nome de usuário do UNIX para o Windows

O ONTAP oferece suporte a pesquisas de vários domínios ao mapear usuários UNIX para usuários do Windows. Todos os domínios confiáveis descobertos são pesquisados por correspondências ao padrão de substituição até que um resultado correspondente seja retornado. Como alternativa, você pode configurar uma lista de domínios confiáveis preferenciais, que é usada em vez da lista de domínios confiáveis descobertos e é pesquisada em ordem até que um resultado correspondente seja retornado.

Como as relações de confiança de domínio afetam as pesquisas de mapeamento de nomes de usuário do Windows

Para entender como o mapeamento de nomes de usuário de vários domínios funciona, você deve entender como as relações de confiança de domínio funcionam com o ONTAP. As relações de confiança do ativo Directory com o domínio home do servidor CIFS podem ser uma confiança bidirecional ou podem ser um dos dois tipos de confiança unidirecionais, uma confiança de entrada ou uma confiança de saída. O domínio inicial é o domínio ao qual pertence o servidor CIFS na SVM.

- *Confiança bidirecional*

Com trusts bidirecionais, ambos os domínios confiam uns nos outros. Se o domínio home do servidor CIFS tiver uma confiança bidirecional com outro domínio, o domínio home pode autenticar e autorizar um usuário pertencente ao domínio confiável e vice-versa.

As pesquisas de mapeamento de nome de usuário do UNIX para o Windows podem ser realizadas apenas em domínios com confiança bidirecional entre o domínio inicial e o outro domínio.

- *Outbound Trust*

Com uma confiança de saída, o domínio home confia no outro domínio. Nesse caso, o domínio home pode autenticar e autorizar um usuário pertencente ao domínio confiável de saída.

Um domínio com uma confiança de saída com o domínio inicial é *not* pesquisado ao executar pesquisas de mapeamento de nomes de usuário do UNIX para o Windows.


- *Confiança inbound*

Com uma confiança de entrada, o outro domínio confia no domínio home do servidor CIFS. Neste caso, o domínio inicial não pode autenticar ou autorizar um usuário pertencente ao domínio confiável de entrada.

Um domínio com uma confiança de entrada com o domínio inicial é *not* pesquisado ao executar pesquisas de mapeamento de nomes de usuário do UNIX para o Windows.

Como os curingas (*) são usados para configurar pesquisas de vários domínios para mapeamento de nomes

As pesquisas de mapeamento de nomes de vários domínios são facilitadas pelo uso de curingas na seção domínio do nome de usuário do Windows. A tabela a seguir ilustra como usar curingas na parte de domínio de uma entrada de mapeamento de nomes para habilitar pesquisas de vários domínios:

Padrão	Substituição	Resultado
raiz	<ul style="list-style-type: none">• administrador	O usuário UNIX "root" é mapeado para o usuário chamado "administrador". Todos os domínios confiáveis são pesquisados em ordem até que o primeiro usuário correspondente chamado "administrador" seja encontrado.
*	<ul style="list-style-type: none">• *	Os usuários UNIX válidos são mapeados para os usuários do Windows correspondentes. Todos os domínios confiáveis são pesquisados em ordem até que o primeiro usuário correspondente com esse nome seja encontrado.  O padrão* é válido apenas para mapeamento de nomes do UNIX para o Windows, e não para o contrário.

Como as pesquisas de nomes de vários domínios são realizadas

Você pode escolher um dos dois métodos para determinar a lista de domínios confiáveis usados para pesquisas de nomes de vários domínios:

- Use a lista de confiança bidirecional descoberta automaticamente compilada pelo ONTAP
- Use a lista de domínio confiável preferida que você compila

Se um usuário UNIX for mapeado para um usuário do Windows com um curinga usado para a seção de domínio do nome de usuário, o usuário do Windows será pesquisado em todos os domínios confiáveis da seguinte forma:

- Se uma lista de domínio confiável preferencial estiver configurada, o usuário mapeado do Windows será pesquisado somente nesta lista de pesquisa, em ordem.
- Se uma lista preferencial de domínios confiáveis não estiver configurada, o usuário do Windows será pesquisado em todos os domínios confiáveis bidirecionais do domínio doméstico.
- Se não houver domínios bidirecionalmente confiáveis para o domínio home, o usuário será pesquisado no domínio home.

Se um usuário UNIX for mapeado para um usuário do Windows sem uma seção de domínio no nome de usuário, o usuário do Windows será pesquisado no domínio inicial.

Regras de conversão de mapeamento de nomes

Um sistema ONTAP mantém um conjunto de regras de conversão para cada SVM. Cada regra consiste em duas partes: Um *pattern* e um *replacement*. As conversões começam no início da lista apropriada e executam uma substituição com base na primeira regra de correspondência. O padrão é uma expressão regular estilo UNIX. A substituição é uma cadeia de caracteres contendo sequências de escape que representam subexpressões do padrão, como no programa UNIX `sed`.

Crie um mapeamento de nomes

Você pode usar o `vserver name-mapping create` comando para criar um mapeamento de nomes. Use mapeamentos de nomes para permitir que os usuários do Windows acessem volumes de estilo de segurança UNIX e o inverso.

Sobre esta tarefa

Para cada SVM, o ONTAP oferece suporte a até 12.500 mapeamentos de nomes para cada direção.

Passo

1. Criar um mapeamento de nomes: `vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text`



As `-pattern` declarações e `-replacement` podem ser formuladas como expressões regulares. Você também pode usar a `-replacement` instrução para negar explicitamente um mapeamento para o usuário usando a cadeia de substituição nula " " (o caractere de espaço). Consulte a `vserver name-mapping create` página de manual para obter detalhes.

Quando os mapeamentos do Windows para UNIX são criados, todos os clientes SMB que tenham conexões abertas ao sistema ONTAP no momento em que os novos mapeamentos são criados devem fazer logout e fazer login novamente para ver os novos mapeamentos.

Exemplos

O comando a seguir cria um mapeamento de nomes no SVM chamado VS1. O mapeamento é um mapeamento do UNIX para o Windows na posição 1 na lista de prioridades. O mapeamento mapeia o usuário UNIX johnd para o usuário do Windows Eng.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

O comando a seguir cria outro mapeamento de nomes no SVM chamado VS1. O mapeamento é um mapeamento do Windows para o UNIX na posição 1 na lista de prioridades. Aqui o padrão e a substituição

incluem expressões regulares. O mapeamento mapeia cada usuário CIFS no domínio ENG para usuários no domínio LDAP associado ao SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\\1"
```

O comando a seguir cria outro mapeamento de nomes no SVM chamado VS1. Aqui, o padrão inclui "" como um elemento no nome de usuário do Windows que deve ser escapado. O mapeamento mapeia as operações do usuário do Windows para o usuário do UNIX John_OPS.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configure o usuário padrão

Você pode configurar um usuário 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 um usuário padrão.

Sobre esta tarefa

Para autenticação CIFS, se você não quiser mapear cada usuário do Windows para um usuário UNIX individual, você pode especificar um usuário UNIX padrão.

Para autenticação NFS, se você não quiser mapear cada usuário UNIX para um usuário individual do Windows, você pode especificar um usuário padrão do Windows.


Passos

1. Execute uma das seguintes ações:

Se você quiser...	Digite o seguinte comando...
Configure o usuário UNIX padrão	<pre>vserver cifs options modify -default -unix-user <i>user_name</i></pre>
Configure o usuário padrão do Windows	<pre>vserver nfs modify -default-win-user <i>user_name</i></pre>

Comandos para gerenciar mapeamentos de nomes

Existem comandos ONTAP específicos para gerenciar mapeamentos de nomes.

Se você quiser...	Use este comando...
Crie um mapeamento de nomes	<code>vserver name-mapping create</code>
Insira um mapeamento de nomes em uma posição específica	<code>vserver name-mapping insert</code>
Exibir mapeamentos de nomes	<code>vserver name-mapping show</code>
Troque a posição de dois mapeamentos de nomes <div data-bbox="167 548 224 604" style="display: inline-block; vertical-align: middle; margin-right: 10px;">  </div> <div data-bbox="280 527 756 625" style="display: inline-block; vertical-align: middle;"> <p>Uma troca não é permitida quando o mapeamento de nomes é configurado com uma entrada de qualificador ip.</p> </div>	<code>vserver name-mapping swap</code>
Modificar um mapeamento de nomes	<code>vserver name-mapping modify</code>
Eliminar um mapeamento de nomes	<code>vserver name-mapping delete</code>
Valide o mapeamento de nomes correto	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win -user-name user1 -path / -share-name sh1</code>

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

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 INTERRUPTÃO 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.