



# Usando Kerberos com NFS para segurança forte

ONTAP 9

NetApp  
January 17, 2025

# Índice

- Usando Kerberos com NFS para segurança forte ..... 1
- Suporte ONTAP para Kerberos ..... 1
- Requisitos para configurar Kerberos com NFS ..... 1
- Especifique o domínio de ID de usuário para NFSv4 ..... 5

# Usando Kerberos com NFS para segurança forte

## Suporte ONTAP para Kerberos

O Kerberos fornece autenticação segura forte para aplicativos cliente/servidor. A autenticação fornece a verificação de identidades de usuário e processo para um servidor. No ambiente ONTAP, o Kerberos fornece autenticação entre máquinas virtuais de armazenamento (SVMs) e clientes NFS.

No ONTAP 9, a seguinte funcionalidade Kerberos é suportada:

- Autenticação Kerberos 5 com verificação de integridade (krb5i)

O Krb5i usa checksums para verificar a integridade de cada mensagem NFS transferida entre cliente e servidor. Isso é útil tanto por motivos de segurança (por exemplo, para garantir que os dados não foram adulterados) quanto por motivos de integridade de dados (por exemplo, para evitar a corrupção de dados ao usar NFS em redes não confiáveis).

- Autenticação Kerberos 5 com verificação de privacidade (krb5p)

Krb5p usa checksums para criptografar todo o tráfego entre o cliente e o servidor. Isto é mais seguro e também incorre mais carga.

- Criptografia AES de 128 bits e 256 bits

O Advanced Encryption Standard (AES) é um algoritmo de encriptação para proteger dados eletrônicos. O ONTAP suporta AES com chaves de 128 bits (AES-128) e AES com criptografia de chaves de 256 bits (AES-256) para Kerberos para maior segurança.

- Configurações de realm Kerberos no nível da SVM

Os administradores do SVM agora podem criar configurações do Kerberos Realm no nível SVM. Isso significa que os administradores do SVM não precisam mais confiar no administrador do cluster para a configuração do Kerberos Realm e podem criar configurações individuais do Kerberos Realm em um ambiente de alocação a vários clientes.

## Requisitos para configurar Kerberos com NFS

Antes de configurar o Kerberos com NFS no sistema, você deve verificar se determinados itens no ambiente de rede e armazenamento estão configurados corretamente.



As etapas para configurar seu ambiente dependem de qual versão e tipo de sistema operacional cliente, controlador de domínio, Kerberos, DNS, etc. que você está usando. Documentar todas essas variáveis está além do escopo deste documento. Para obter mais informações, consulte a respectiva documentação para cada componente.

Para um exemplo detalhado de como configurar o ONTAP e o Kerberos 5 com NFSv3 e NFSv4 em um ambiente usando o Active Directory do Windows Server 2008 R2 e hosts Linux, consulte o relatório técnico 4073.

Os seguintes itens devem ser configurados primeiro:

## Requisitos de ambiente de rede

- Kerberos

Você deve ter uma configuração Kerberos funcionando com um centro de distribuição de chaves (KDC), como Kerberos baseados no ativo Directory do Windows ou MIT Kerberos.

Os servidores NFS devem usar `nfs` como o componente principal de sua máquina principal.

- Serviço de diretório

Você deve usar um serviço de diretório seguro em seu ambiente, como ativo Directory ou OpenLDAP, que esteja configurado para usar LDAP em SSL/TLS.

- NTP

Você deve ter um servidor de tempo de trabalho executando NTP. Isso é necessário para evitar a falha de autenticação Kerberos devido ao desvio de tempo.

- Resolução de nome de domínio (DNS)

Cada cliente UNIX e cada SVM LIF devem ter um Registro de serviço (SRV) adequado registrado no KDC em zonas de pesquisa direta e inversa. Todos os participantes devem ser solucionáveis corretamente via DNS.

- Contas de utilizador

Cada cliente deve ter uma conta de usuário no Reino Kerberos. Os servidores NFS devem usar "nfs" como o componente principal de sua máquina principal.

## Requisitos do cliente NFS

- NFS

Cada cliente deve ser configurado corretamente para se comunicar através da rede usando NFSv3 ou NFSv4.

Os clientes devem suportar RFC1964 e RFC2203.

- Kerberos

Cada cliente deve ser configurado corretamente para usar a autenticação Kerberos, incluindo os seguintes detalhes:

- A encriptação para comunicação TGS está ativada.  
AES-256 para maior segurança.
- O tipo de encriptação mais seguro para comunicação TGT está ativado.
- O domínio e o domínio Kerberos estão configurados corretamente.
- O GSS está ativado.

Ao usar credenciais de máquina:

- Não execute `gssd` com o `-n` parâmetro.
- Não execute `kinit` como usuário raiz.

- Cada cliente deve usar a versão mais recente e atualizada do sistema operacional.

Isso fornece a melhor compatibilidade e confiabilidade para criptografia AES com Kerberos.

- DNS

Cada cliente deve ser configurado corretamente para usar o DNS para a resolução correta do nome.

- NTP

Cada cliente deve estar sincronizando com o servidor NTP.

- Informações de host e domínio

Cada cliente `/etc/hosts` e `/etc/resolv.conf` arquivos devem conter o nome de host correto e as informações de DNS, respetivamente.

- Ficheiros keytab

Cada cliente deve ter um arquivo keytab do KDC. O Reino deve estar em letras maiúsculas. O tipo de criptografia deve ser AES-256 para maior segurança.

- Opcional: Para obter o melhor desempenho, os clientes se beneficiam de ter pelo menos duas interfaces de rede: Uma para comunicação com a rede local e outra para comunicação com a rede de armazenamento.

## Requisitos do sistema de storage

- Licença NFS

O sistema de storage deve ter uma licença NFS válida instalada.

- Licença CIFS

A licença CIFS é opcional. Só é necessário para verificar credenciais do Windows ao usar mapeamento de nomes multiprotocolo. Não é necessário em um ambiente restrito somente para UNIX.

- SVM

Você precisa ter pelo menos um SVM configurado no sistema.

- DNS na SVM

Você deve ter DNS configurado em cada SVM.

- Servidor NFS

Você precisa ter o NFS configurado na SVM.

- Criptografia AES

Para uma segurança mais forte, você deve configurar o servidor NFS para permitir apenas criptografia AES-256 para Kerberos.

- Servidor SMB

Se você estiver executando um ambiente multiprotocolo, deverá ter o SMB configurado na SVM. O servidor SMB é necessário para o mapeamento de nomes multiprotocolo.

- Volumes

Você precisa ter um volume raiz e pelo menos um volume de dados configurados para uso pelo SVM.

- Volume raiz

O volume raiz do SVM precisa ter a seguinte configuração:

Nome	Definição
Estilo de segurança	UNIX
UID	Raiz ou ID 0
GID	Raiz ou ID 0
Permissões da UNIX	777

Em contraste com o volume raiz, os volumes de dados podem ter um estilo de segurança.

- Grupos UNIX

O SVM deve ter os seguintes grupos UNIX configurados:

Nome do grupo	ID do grupo
daemon	1
raiz	0
pcuser	65534 (criado automaticamente pelo ONTAP ao criar o SVM)

- Utilizadores UNIX

O SVM deve ter os seguintes usuários UNIX configurados:

Nome de utilizador	ID de utilizador	ID do grupo principal	Comentário
nfs	500	0	Necessário para a fase INIT do GSS  O primeiro componente do usuário cliente NFS SPN é usado como usuário.
pcuser	65534	65534	Necessário para uso multiprotocolo NFS e CIFS  Criado e adicionado ao grupo pcuser automaticamente pelo ONTAP ao criar o SVM.
raiz	0	0	Necessário para a montagem

O usuário nfs não é necessário se existir um mapeamento de nomes Kerberos-UNIX para o SPN do usuário cliente NFS.

- Políticas e regras de exportação

Você deve ter configurado políticas de exportação com as regras de exportação necessárias para os volumes raiz e de dados e qtrees. Se todos os volumes da SVM forem acessados por Kerberos, você poderá definir as opções de regra de exportação `-rorule`, `-rwrule` e `-superuser` para o volume raiz como `krb5`, `krb5i` ou `krb5p`.

- Mapeamento de nomes Kerberos-UNIX

Se você quiser que o usuário identificado pelo usuário cliente NFS SPN tenha permissões de raiz, você deve criar um mapeamento de nome para root.

### Informações relacionadas

["Relatório técnico da NetApp 4073: Autenticação unificada segura"](#)

["Ferramenta de Matriz de interoperabilidade do NetApp"](#)

["Administração do sistema"](#)

["Gerenciamento de storage lógico"](#)

## Especifique o domínio de ID de usuário para NFSv4

Para especificar o domínio de ID de usuário, você pode definir a `-v4-id-domain` opção.

**Sobre esta tarefa**

Por padrão, o ONTAP usa o domínio NIS para o mapeamento de ID de usuário NFSv4, se um estiver definido. Se um domínio NIS não estiver definido, o domínio DNS será usado. Talvez seja necessário definir o domínio de ID de usuário se, por exemplo, você tiver vários domínios de ID de usuário. O nome de domínio deve corresponder à configuração de domínio no controlador de domínio. Não é necessário para NFSv3.

**Passo**

1. Introduza o seguinte comando:

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```



## **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.