Use Kerberos com NFS para segurança forte

ONTAP 9

NetApp
January 17, 2025

Índice

Use Kerberos com NFS para segurança forte

Visão geral do uso do Kerberos com NFS para segurança forte

Se o Kerberos for usado em seu ambiente para autenticação forte, você precisará trabalhar com o administrador do Kerberos para determinar os requisitos e as configurações apropriadas do sistema de armazenamento e, em seguida, ativar o SVM como um cliente Kerberos.

Seu ambiente deve atender às seguintes diretrizes:

- A implantação do seu site deve seguir as práticas recomendadas para a configuração do servidor Kerberos e do cliente antes de configurar o Kerberos para ONTAP.
- Se possível, use NFSv4 ou posterior se a autenticação Kerberos for necessária.

  NFSv3 pode ser usado com Kerberos. No entanto, os benefícios completos de segurança do Kerberos só são realizados em implantações ONTAP de NFSv4 ou posterior.

- Para promover o acesso redundante ao servidor, o Kerberos deve ser habilitado em várias LIFs de dados em vários nós no cluster usando o mesmo SPN.
- Quando o Kerberos está habilitado no SVM, um dos seguintes métodos de segurança deve ser especificado em regras de exportação para volumes ou qtrees, dependendo da configuração do cliente NFS.
  - `krb5` (Protocolo Kerberos v5)
  - `krb5i` (Protocolo Kerberos v5 com verificação de integridade usando checksums)
  - `krb5p` (Protocolo Kerberos v5 com serviço de privacidade)

Além do servidor Kerberos e clientes, os seguintes serviços externos devem ser configurados para que o ONTAP suporte Kerberos:

- Serviço de diretório

  Você deve usar um serviço de diretório seguro em seu ambiente, como o ative Directory ou o OpenLDAP, configurado para usar LDAP em SSL/TLS. Não use NIS, cujos pedidos são enviados em texto não criptografado e, portanto, não são seguros.

- 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.

Verifique as permissões para a configuração Kerberos

O Kerberos requer que certas permissões UNIX sejam definidas para o volume raiz do SVM e para usuários e grupos locais.

Passos

1. Exiba as permissões relevantes no volume raiz da SVM:

   `volume show -volume root_vol_name-fields user,group,unix-permissions`

   O volume raiz do SVM precisa ter a seguinte configuração:

Nome…	A definir…
UID	Raiz ou ID 0
GID	Raiz ou ID 0
Permissões da UNIX	755

   Se esses valores não forem exibidos, use o `volume modify` comando para atualizá-los.

2. Exibir os usuários locais do UNIX:

   `vserver services name-service unix-user show -vserver vserver_name`

   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. O usuário nfs não é necessário se existir um mapeamento de nomes Kerberos-UNIX para o SPN do usuário cliente NFS.
raiz	0	0	Necessário para a montagem.

   Se esses valores não forem exibidos, você pode usar o `vserver services name-service unix-user modify` comando para atualizá-los.

3. Exibir os grupos UNIX locais:

   `vserver services name-service unix-group show -vserver` *vserver* `_name`

   O SVM deve ter os seguintes grupos UNIX configurados:

Nome do grupo	ID do grupo
daemon	1
raiz	0

   Se esses valores não forem exibidos, você pode usar o `vserver services name-service unix-group modify` comando para atualizá-los.

Crie uma configuração NFS Kerberos realm

Se você quiser que o ONTAP acesse servidores Kerberos externos em seu ambiente, primeiro configure o SVM para usar um realm Kerberos existente. Para fazer isso, você precisa reunir valores de configuração para o servidor KDC Kerberos e, em seguida, usar o `vserver nfs kerberos realm create` comando para criar a configuração de realm Kerberos em um SVM.

O que você vai precisar

O administrador do cluster deve ter configurado o NTP no sistema de armazenamento, cliente e servidor KDC para evitar problemas de autenticação. As diferenças de tempo entre um cliente e um servidor (desvio de relógio) são uma causa comum de falhas de autenticação.

Passos

1. Consulte o administrador do Kerberos para determinar os valores de configuração apropriados para fornecer com o `vserver nfs kerberos realm create` comando.
2. Crie uma configuração de realm Kerberos no SVM:

   `vserver nfs kerberos realm create -vserver` *vserver_name* `-realm` *realm_name* *{AD_KDC_server_values |AD_KDC_server_values}* `-comment "`*text*`"`

3. Verifique se a configuração do realm Kerberos foi criada com sucesso:

   `vserver nfs kerberos realm show`

Exemplos

O comando a seguir cria uma configuração NFS Kerberos Realm para o SVM VS1 que usa um servidor Microsoft ative Directory como servidor KDC. O Reino Kerberos é AUTH.EXAMPLE.COM. O servidor do ative Directory tem o nome ad-1 e seu endereço IP é 10.10.8.14. O desvio de relógio permitido é de 300 segundos (o padrão). O endereço IP do servidor KDC é 10.10.8.14, e seu número de porta é 88 (o padrão). "Configuração do Microsoft Kerberos" é o comentário.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

O comando a seguir cria uma configuração NFS Kerberos realm para o SVM VS1 que usa um MIT KDC. O Reino Kerberos é SECURITY.EXAMPLE.COM. A inclinação permitida do relógio é de 300 segundos. O endereço IP do servidor KDC é 10.10.9.1, e seu número de porta é 88. O fornecedor KDC é outro para indicar um fornecedor UNIX. O endereço IP do servidor administrativo é 10.10.9.1, e seu número de porta é 749 (o padrão). O endereço IP do servidor de senhas é 10.10.9.1, e seu número de porta é 464 (o padrão). "UNIX Kerberos config" é o comentário.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

Configurar os tipos de criptografia permitidos do NFS Kerberos

Por padrão, o ONTAP oferece suporte aos seguintes tipos de criptografia para o Kerberos NFS: DES, 3DES, AES-128 e AES-256. Você pode configurar os tipos de criptografia permitidos para cada SVM de acordo com os requisitos de segurança do seu ambiente específico usando o `vserver nfs modify` comando com o `-permitted -enc-types` parâmetro.

Sobre esta tarefa

Para maior compatibilidade com clientes, o ONTAP suporta criptografia DES fraca e AES forte por padrão. Isso significa, por exemplo, que se você quiser aumentar a segurança e seu ambiente a suportar, você pode usar este procedimento para desativar DES e 3DES e exigir que os clientes usem apenas criptografia AES.

Você deve usar a criptografia mais forte disponível. Para ONTAP, isso é AES-256. Deve confirmar com o administrador do KDC que este nível de encriptação é suportado no seu ambiente.

- Ativar ou desativar totalmente AES (AES-128 e AES-256) em SVMs é disruptivo porque destrói o arquivo DES principal/keytab original, exigindo assim que a configuração Kerberos seja desativada em todos os LIFs para o SVM.

  Antes de fazer essa alteração, você deve verificar se os clientes NFS não dependem da criptografia AES no SVM.

- Ativar ou desativar DES ou 3DES não requer alterações na configuração Kerberos em LIFs.

Passo

1. Ative ou desative o tipo de encriptação permitido que pretende:

Se quiser ativar ou desativar…	Siga estes passos…
DES ou 3DES	a. Configure os tipos de criptografia permitidos do NFS Kerberos da SVM `vserver nfs modify -vserver vserver_name -permitted -enc-types encryption_types` Separe vários tipos de criptografia com uma vírgula. b. Verifique se a alteração foi bem-sucedida `vserver nfs show -vserver vserver_name -fields permitted-enc-types`
AES-128 ou AES-256	a. Identifique em que SVM e LIF Kerberos estão ativados `vserver nfs kerberos interface show` b. Desative o Kerberos em todos os LIFs no SVM cujo tipo de criptografia NFS Kerberos permitido você deseja modificar `vserver nfs kerberos interface disable -lif lif_name` c. Configure os tipos de criptografia permitidos do NFS Kerberos da SVM `vserver nfs modify -vserver vserver_name -permitted -enc-types encryption_types` Separe vários tipos de criptografia com uma vírgula. d. Verifique se a alteração foi bem-sucedida `vserver nfs show -vserver vserver_name -fields permitted-enc-types` e. Reative o Kerberos em todos os LIFs na SVM `vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name` f. Verifique se o Kerberos está ativado em todos os LIFs `vserver nfs kerberos interface show`

Ative o Kerberos em um LIF de dados

Você pode usar o `vserver nfs kerberos interface enable` comando para

habilitar o Kerberos em um LIF de dados. Isso permite que o SVM use os serviços de segurança Kerberos para NFS.

Sobre esta tarefa

Se você estiver usando um KDC do ative Directory, os primeiros 15 carateres de qualquer SPNs usados devem ser exclusivos em SVMs dentro de um Reino ou domínio.

Passos

1. Crie a configuração NFS Kerberos:

   `vserver nfs kerberos interface enable -vserver` *`vserver_name`* `-lif` *`logical_interface`* `-spn` *`service_principal_name`*

   O ONTAP requer a chave secreta para o SPN do KDC para habilitar a interface Kerberos.

   Para os KDCs da Microsoft, o KDC é contatado e um prompt de nome de usuário e senha são emitidos na CLI para obter a chave secreta. Se você precisar criar o SPN em uma ou diferente do realm Kerberos, você poderá especificar o parâmetro opcional `-ou`.

   Para KDCs não Microsoft, a chave secreta pode ser obtida usando um de dois métodos:

Se você…	**Você também deve incluir o seguinte parâmetro com o comando…**
Peça às credenciais do administrador do KDC para recuperar a chave diretamente do KDC	`-admin-username` *`kdc_admin_username`*
Não tem as credenciais de administrador do KDC, mas tem um arquivo keytab do KDC que contém a chave	`-keytab-uri` digite seu comentário aqui://*`uri`*

2. Verifique se o Kerberos foi ativado no LIF:

   `vserver nfs kerberos-config show`

3. Repita as etapas 1 e 2 para ativar o Kerberos em várias LIFs.

Exemplo

O comando a seguir cria e verifica uma configuração NFS Kerberos para o SVM chamado VS1 na interface lógica ves03-D1, com o SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM na ou lab2ou:

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- --------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

Informações sobre direitos autorais

Informações sobre marcas comerciais