将 Kerberos 与 NFS 结合使用可增强安全性

ONTAP 9

NetApp
April 24, 2024

目录

将 Kerberos 与 NFS 结合使用可增强安全性

将 Kerberos 与 NFS 结合使用以增强安全性的概述

如果在您的环境中使用 Kerberos 进行强身份验证，则需要与 Kerberos 管理员一起确定要求和适当的存储系统配置，然后将 SVM 作为 Kerberos 客户端启用。

您的环境应符合以下准则：

- 在为 ONTAP 配置 Kerberos 之前，您的站点部署应遵循 Kerberos 服务器和客户端配置的最佳实践。
- 如果需要 Kerberos 身份验证，请尽可能使用 NFSv4 或更高版本。

  NFSv3 可与 Kerberos 结合使用。但是，只有在 NFSv4 或更高版本的 ONTAP 部署中，才会充分发挥 Kerberos 的全部安全优势。

- 要提高冗余服务器访问能力，应在使用同一 SPN 的集群中多个节点上的多个数据 LIF 上启用 Kerberos 。
- 在 SVM 上启用 Kerberos 时，必须根据 NFS 客户端配置在卷或 qtree 的导出规则中指定以下安全方法之一。
  - `krb5` (Kerberos v5协议)
  - `krb5i` (使用校验和进行完整性检查的Kerberos v5协议)
  - `krb5p` (具有隐私服务的Kerberos v5协议)

除了 Kerberos 服务器和客户端之外，还必须为 ONTAP 配置以下外部服务以支持 Kerberos：

- 目录服务

  您应在环境中使用安全目录服务，例如 Active Directory 或 OpenLDAP ，该服务配置为使用基于 SSL/TLS 的 LDAP 。请勿使用 NIS ，因为其请求会以明文形式发送，因此不安全。

- NTP

  您必须有一个运行 NTP 的工作时间服务器。为了防止因时间偏差而导致 Kerberos 身份验证失败，必须执行此操作。

- 域名解析（ DNS ）

  每个 UNIX 客户端和每个 SVM LIF 都必须在正向和反向查找区域下向 KDC 注册正确的服务记录（ SRV ）。所有参与者都必须可通过 DNS 正确解析。

验证 Kerberos 配置的权限

Kerberos 要求为 SVM 根卷以及本地用户和组设置某些 UNIX 权限。

步骤

1. 显示 SVM 根卷上的相关权限：

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

SVM 的根卷必须具有以下配置：

名称	正在设置 ...
UID	root 或 ID 0
GID	root 或 ID 0
UNIX 权限	755

如果未显示这些值、请使用 `volume modify` 命令进行更新。

2. 显示本地 UNIX 用户：

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

SVM 必须配置以下 UNIX 用户：

用户名	用户 **ID**	主组 **ID**	**comment**
NFS	500	0	GSS 初始化阶段需要此项。 NFS 客户端用户 SPN 的第一个组件用作用户。 如果 NFS 客户端用户的 SPN 存在 Kerberos-UNIX 名称映射，则不需要 NFS 用户。
root	0	0	挂载时需要。

如果未显示这些值、则可以使用 `vserver services name-service unix-user modify` 命令进行更新。

3. 显示本地 UNIX 组：

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

SVM 必须配置以下 UNIX 组：

组名称	组 **ID**
守护进程	1.
root	0

如果未显示这些值、则可以使用 `vserver services name-service unix-group modify` 命令进行更新。

创建 NFS Kerberos 域配置

如果您希望 ONTAP 访问环境中的外部 Kerberos 服务器，则必须先将 SVM 配置为使用现有 Kerberos 域。为此、您需要收集Kerberos KDC服务器的配置值、然后使用 `vserver nfs kerberos realm create` 命令以在SVM上创建Kerberos域配置。

您需要的内容

集群管理员应已在存储系统，客户端和 KDC 服务器上配置 NTP ，以避免出现身份验证问题。客户端和服务器之间的时间差异（时钟偏差）是常见的身份验证失败发生原因。

步骤

1. 请咨询Kerberos管理员以确定要为提供的适当配置值 `vserver nfs kerberos realm create` 命令：
2. 在 SVM 上创建 Kerberos 域配置：

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

3. 验证是否已成功创建 Kerberos 域配置：

   ```
   vserver nfs kerberos realm show
   ```

示例

以下命令将为 SVM vs1 创建一个 NFS Kerberos 域配置，该配置使用 Microsoft Active Directory 服务器作为 KDC 服务器。Kerberos 域为 AUTH.EXAMPLE.COM 。Active Directory 服务器名为 AD-1 ，其 IP 地址为 10.10.8.14 。允许的时钟偏差为 300 秒（默认值）。KDC 服务器的 IP 地址为 10.10.8.14 ，其端口号为 88 （默认值）。"Microsoft Kerberos config" 是注释。

```
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"
```

以下命令将为使用 MIT KDC 的 SVM vs1 创建 NFS Kerberos 域配置。Kerberos 域为 SECURITY.EXAMPLE.COM 。允许的时钟偏差为 300 秒。KDC 服务器的 IP 地址为 10.10.9.1 ，端口号为 88 。KDC 供应商为 "Other" ，表示 UNIX 供应商。管理服务器的 IP 地址为 10.10.9.1 ，端口号为 749 （默认值）。密码服务器的 IP 地址为 10.10.9.1 ，端口号为 464 （默认值）。"UNIX Kerberos config" 是注释。

```
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"
```

配置 NFS Kerberos 允许的加密类型

默认情况下， ONTAP 支持以下 NFS Kerberos 加密类型： DES ， 3DES ， AES-128 和 AES-256 。您可以使用为每个SVM配置允许的加密类型、以满足特定环境的安全要求 `vserver nfs modify` 命令 `-permitted-enc-types` 参数。

关于此任务

为了最大程度地实现客户端兼容性， ONTAP 默认同时支持弱 DES 和强 AES 加密。例如，这意味着，如果您要提高安全性，并且您的环境支持此安全性，则可以使用此操作步骤禁用 DES 和 3DES ，并要求客户端仅使用 AES 加密。

您应使用可用的最强加密。对于 ONTAP ，即 AES-256 。您应向 KDC 管理员确认您的环境支持此加密级别。

- 在 SVM 上完全启用或禁用 AES （ AES-128 和 AES-256 ）会造成中断，因为它会销毁原始 DES 主体 /keytab 文件，从而要求在 SVM 的所有 LIF 上禁用 Kerberos 配置。

  在进行此更改之前，您应验证 NFS 客户端是否不依赖于 SVM 上的 AES 加密。

- 启用或禁用 DES 或 3DES 不需要对 LIF 上的 Kerberos 配置进行任何更改。

步骤

1. 启用或禁用所需的允许加密类型：

要启用或禁用的项	请按照以下步骤操作 ...
DES 或 3DES	a. 配置SVM的NFS Kerberos允许的加密类型： `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* 使用逗号分隔多种加密类型。 b. 验证更改是否成功： `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

要启用或禁用的项	请按照以下步骤操作 ...

AES-128或AES-256	a. 确定启用了Kerberos的SVM和LIF：
	`vserver nfs kerberos interface show`
	b. 在要修改NFS Kerberos允许的加密类型的SVM上的所有SVM上禁用Kerberos：
	`vserver nfs kerberos interface disable -lif lif_name`
	c. 配置SVM的NFS Kerberos允许的加密类型：
	`vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types`
	使用逗号分隔多种加密类型。
	d. 验证更改是否成功：
	`vserver nfs show -vserver vserver_name -fields permitted-enc-types`
	e. 在SVM上的所有SVM上重新启用Kerberos：
	`vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name`
	f. 验证是否已在所有生命周期管理器上启用Kerberos：
	`vserver nfs kerberos interface show`

在数据 LIF 上启用 Kerberos

您可以使用 `vserver nfs kerberos interface enable` 命令以对数据LIF启用Kerberos。这样， SVM 就可以对 NFS 使用 Kerberos 安全服务。

关于此任务

如果您使用的是 Active Directory KDC ，则所使用的任何 SPN 的前 15 个字符必须在域或域中的 SVM 之间是唯一的。

步骤

1. 创建 NFS Kerberos 配置：

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

   ONTAP 需要 KDC 中 SPN 的机密密钥才能启用 Kerberos 接口。

   对于 Microsoft KDC ，将联系 KDC ，并在命令行界面上发出用户名和密码提示以获取机密密钥。如果需要在Kerberos域的其他OU中创建SPN、则可以指定可选 `-ou` 参数。

对于非 Microsoft KDC ，可以使用以下两种方法之一获取机密密钥：

如果您 ...	您还必须在命令中包含以下参数 ...
拥有 KDC 管理员凭据，以便直接从 KDC 检索密钥	`-admin-username` *`kdc_admin_username`*
没有 KDC 管理员凭据，但具有包含此密钥的 KDC 中的 keytab 文件	`-keytab-uri` {ftp-http} ： *//uri*

2. 验证是否已在 LIF 上启用 Kerberos：

   ```
   vserver nfs kerberos-config show
   ```

3. 重复步骤 1 和 2 ，在多个 LIF 上启用 Kerberos 。

示例

以下命令将在逻辑接口 ves03-d1 上为名为 vs1 的 SVM 创建并验证 NFS Kerberos 配置，并在 OU lab2ou 中使用 SPN NFS/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM：

```
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.
```