将 Kerberos 与 NFS 结合使用以增强安全性

ONTAP 9

NetApp
April 24, 2024

目录

将 Kerberos 与 NFS 结合使用以增强安全性

ONTAP 支持 Kerberos

Kerberos 可为客户端 / 服务器应用程序提供强大的安全身份验证。身份验证用于向服务器验证用户和进程身份。在 ONTAP 环境中， Kerberos 在 Storage Virtual Machine （ SVM ）和 NFS 客户端之间提供身份验证。

在 ONTAP 9 中，支持以下 Kerberos 功能：

- Kerberos 5 身份验证与完整性检查（ krb5i ）

  Krb5i 使用校验和验证在客户端和服务器之间传输的每个 NFS 消息的完整性。出于安全原因（例如，确保数据未被篡改）和数据完整性原因（例如，在不可靠的网络上使用 NFS 时，防止数据损坏），这一点非常有用。

- Kerberos 5 身份验证与隐私检查（ krb5p ）

  Krb5p 使用校验和对客户端和服务器之间的所有流量进行加密。这种方法更安全，并且会产生更多负载。

- 128 位和 256 位 AES 加密

  高级加密标准（ Advanced Encryption Standard ， AES ）是一种用于保护电子数据安全的加密算法。ONTAP支持使用128位密钥的AES (AES-128)和使用256位密钥的AES (AES-256)对Kerberos进行加密、以增强安全性。

- SVM 级别的 Kerberos 域配置

  现在， SVM 管理员可以在 SVM 级别创建 Kerberos 域配置。这意味着 SVM 管理员无需再依赖集群管理员来配置 Kerberos 域，并且可以在多租户环境中创建单独的 Kerberos 域配置。

使用 NFS 配置 Kerberos 的要求

在系统上使用 NFS 配置 Kerberos 之前，您必须验证网络和存储环境中的某些项是否已正确配置。

> 配置环境的步骤取决于您使用的客户端操作系统，域控制器， Kerberos ， DNS 等的版本和类型。本文档不会介绍如何记录所有这些变量。有关详细信息，请参见每个组件的相应文档。
>
> 有关如何在使用 Windows Server 2008 R2 Active Directory 和 Linux 主机的环境中为 NFSv3 和 NFSv4 设置 ONTAP 和 Kerberos 5 的详细示例，请参见技术报告 4073 。

应首先配置以下项：

网络环境要求

- Kerberos

您必须使用密钥分发中心（KDC）设置有效的 Kerberos，例如基于 Windows Active Directory 的 Kerberos 或 MIT Kerberos。

NFS服务器必须使用 `nfs` 作为其机器主体的主要组件。

- 目录服务

  您必须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。

- 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。

- 用户帐户

  每个客户端在 Kerberos 域中都必须有一个用户帐户。NFS 服务器必须使用 "`NFS`" 作为其计算机主体的主要组件。

NFS客户端要求

- NFS

  必须正确配置每个客户端，以便使用 NFSv3 或 NFSv4 通过网络进行通信。

  客户端必须支持 RFC1964 和 RFC2203。

- Kerberos

  必须正确配置每个客户端以使用 Kerberos 身份验证，其中包括以下详细信息：

  - 已启用 TGS 通信加密。

    AES-256 可提供最强大的安全性。

  - 启用 TGT 通信最安全的加密类型。
  - 已正确配置 Kerberos 域。
  - 已启用GSS。

    使用计算机凭据时：

  - 请勿运行 `gssd` 使用 `-n` 参数。
  - 请勿运行 `kinit` 以root用户身份。

- 每个客户端都必须使用最新且更新的操作系统版本。

这样可以为使用 Kerberos 进行 AES 加密提供最佳兼容性和可靠性。

- DNS

  必须正确配置每个客户端，以使用 DNS 进行正确的名称解析。

- NTP

  每个客户端都必须与 NTP 服务器同步。

- 主机和域信息

  每个客户端的 `/etc/hosts` 和 `/etc/resolv.conf` 文件必须分别包含正确的主机名和DNS信息。

- keytab 文件

  每个客户端都必须具有 KDC 中的 keytab 文件。域必须为大写字母。加密类型必须为 AES-256 ，以获得最高安全性。

- 可选：为了获得最佳性能，客户端至少可以使用两个网络接口：一个用于与局域网通信，一个用于与存储网络通信。

存储系统要求

- NFS 许可证

  存储系统必须安装有效的 NFS 许可证。

- CIFS许可证

  CIFS 许可证是可选的。只有在使用多协议名称映射时检查 Windows 凭据才需要此功能。在严格的纯 UNIX 环境中不需要此功能。

- SVM

  您必须在系统上至少配置一个 SVM 。

- SVM 上的 DNS

  您必须已在每个 SVM 上配置 DNS 。

- NFS 服务器

  您必须已在 SVM 上配置 NFS 。

- AES 加密

  为了获得最强的安全性，您必须将 NFS 服务器配置为仅允许对 Kerberos 进行 AES-256 加密。

- SMB服务器

  如果您运行的是多协议环境、则必须事先在SVM上配置SMB。多协议名称映射需要SMB服务器。

- Volumes

  您必须具有一个根卷和至少一个数据卷，以供 SVM 使用。

- 根卷

  SVM 的根卷必须具有以下配置：

Name	正在设置 **...**
安全风格	"unix"
UID	root 或 ID 0
GID	root 或 ID 0
UNIX 权限	777

  与根卷不同，数据卷可以采用任一安全模式。

- UNIX 组

  SVM 必须配置以下 UNIX 组：

组名称	组 **ID**
守护进程	1.
root	0
pcuser	65534 （在创建 SVM 时由 ONTAP 自动创建）

- UNIX用户

  SVM 必须配置以下 UNIX 用户：

用户名	用户 **ID**	主组 **ID**	**comment**
NFS	500	0	GSS INIT阶段需要此参数 NFS 客户端用户 SPN 的第一个组件用作用户。

用户名	用户 ID	主组 ID	comment
pcuser	6554	6554	使用NFS和CIFS多协议时需要此参数 在创建SVM时、ONTAP会自动创建并添加到pcuser组中。
root	0	0	挂载时需要

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。

- 导出策略和规则

  您必须已为导出策略配置根卷和数据卷以及 qtree 所需的导出规则。如果通过Kerberos访问SVM的所有卷、则可以设置导出规则选项 `-rorule`， `-rwrule`，和 `-superuser` 根卷的 `krb5` ， `krb5i`或 `krb5p`。

- Kerberos-UNIX 名称映射

  如果您希望 NFS 客户端用户 SPN 标识的用户具有 root 权限，则必须创建一个映射到 root 的名称。

相关信息

"NetApp 技术报告 4073：《安全统一身份验证》"

"NetApp 互操作性表工具"

"系统管理"

"逻辑存储管理"

指定 NFSv4 的用户 ID 域

要指定用户ID域、您可以设置 `-v4-id-domain` 选项

关于此任务

默认情况下，如果设置了 NIS 域，则 ONTAP 将使用 NIS 域进行 NFSv4 用户 ID 映射。如果未设置 NIS 域，则使用 DNS 域。例如，如果您有多个用户 ID 域，则可能需要设置用户 ID 域。域名必须与域控制器上的域配置匹配。NFSv3 不需要此功能。

步骤

1. 输入以下命令：

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