NSD ENGINEER DAY04

1 案例1：配置SMB文件夹共享

1.1 问题

本例要求在虚拟机 server0 上发布两个共享文件夹，具体要求如下：

1. 此服务器必须是 STAFF 工作组的一个成员
2. 发布目录 /common，共享名为 common
3. 发布目录 /devops，共享名为 devops
4. 这两个共享必须是可浏览的，只有 example.com 域内的客户端可以访问
5. 用户 harry 对共享 common 只读，密码是 migwhisk
6. 用户 kenji 对共享 devops 只读，密码是 atenorth
7. 用户 chihiro 对共享 devops 可读写，密码是atenorth

1.2 方案

Samba的用途：为多个客户机提供共享使用的文件夹。

Samba服务端：软件包samba、系统服务smb

Samba客户端：软件包samba-client和cifs-utils、客户端工具smbclient

传输协议及端口：TCP 139、TCP 445

Samba服务端配置文件：/etc/samba/smb.conf

Samba共享账号：存在独立的账号数据文件里，必须有同名系统账号（方便给权限）

Samba账号管理工具：

Top

- pdbedit -a 用户名
- pdbedit -L [用户名]
- pdbedit -x 用户名

测试Samba共享资源：

- smbclient -L 服务器地址 【密码为空（直接回车）】
- smbclient -U 用户名 //服务器地址/共享名 【需要密码】

1.3 步骤

实现此案例需要按照如下步骤进行。

步骤一：在服务器server0发布Samba共享文件夹

1）安装软件包samba

```
[root@server0 ~]# yum -y install samba
.. ..
```

2）创建共享账号

添加共享账号harry，密码为migwhisk：

```
[root@server0 ~]# useradd harry
[root@server0 ~]# pdbedit -a harry                    //根据提示设好密码migwhisk
new password:
retype new password:
```

Top

添加共享账号kenji，密码为atenorth：

```
[root@server0 ~]# useradd kenji
[root@server0 ~]# pdbedit -a kenji              //根据提示设好密码atenorth
new password:
retype new password:
```

添加共享账号chihiro，密码为atenorth：

```
[root@server0 ~]# useradd chihiro
[root@server0 ~]# pdbedit -a chihiro            //根据提示设好密码atenorth
new password:
retype new password:
```

确认共享账号：

```
[root@server0 ~]# pdbedit -L
harry:1003:
chihiro:1005:
kenji:1004:
```

3）准备共享文件夹

```
[root@server0 ~]# mkdir /common
[root@server0 ~]# mkdir /devops
[root@server0 ~]# setfacl -m u:chihiro:rwx /devops        //配置写入权限
```

Top

4）调整SELinux开关策略，允许发布可写的Samba共享资源

```
[root@server0 ~]# getsebool -a | grep ^samba_exp        //默认配置
samba_export_all_ro --> off
samba_export_all_rw --> off

[root@server0 ~]# setsebool -P samba_export_all_rw=on       //永久打开设置

[root@server0 ~]# getsebool -a | grep ^samba_exp        //查看结果
samba_export_all_ro --> off
samba_export_all_rw --> on
```

5）配置共享目录

```
[root@server0 ~]# vim /etc/samba/smb.conf
[global]
    workgroup = STAFF
    ...
[common]
    path = /common
    hosts allow = 172.25.0.0/24
[devops]
    path = /devops
    hosts allow = 172.25.0.0/24
    write list = chihiro
```

Top

6）启动系统服务smb，并设置开机自启

```
[root@server0 ~]# systemctl restart smb
[root@server0 ~]# systemctl enable smb
ln -s '/usr/lib/systemd/system/smb.service' '/etc/systemd/system/multi-user.target.wants/smb.service'
[root@server0 ~]# netstat -antpu | grep smb
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      4709/smbd
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      4709/smbd
```

步骤二：在客户机desktop0测试Samba共享资源

1）安装软件包samba-client

```
[root@server0 ~]# yum -y install samba-client
... ...
```

2）浏览目标主机提供了哪些共享资源

```
[root@desktop0 ~]# smbclient -L server0.example.com
Enter root's password:                    //此处无需输入密码，直接回车
Anonymous login successful
Domain=[MYGROUP] OS=[Unix] Server=[Samba 4.1.1]

        Sharename       Type      Comment
        ---------       ----      -------
```

Top

```
        common          Disk
        devops          Disk
        IPC$            IPC       IPC Service (Samba Server Version 4.1.1)
    Anonymous login successful
    Domain=[MYGROUP] OS=[Unix] Server=[Samba 4.1.1]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

3）连接到目标主机的共享目录

```
[root@desktop0 ~]# smbclient -U harry //server0.example.com/common
Enter harry's password:                          //输入harry的密码
Domain=[STAFF] OS=[Unix] Server=[Samba 4.1.1]
smb: \> ls                                       //检查是否可列出目录内容
  .                                   D        0  Sun Nov 27 03:07:29 2016
  ..                                  D        0  Sun Nov 27 03:07:32 2016

        40913 blocks of size 262144. 27826 blocks available
smb: \> quit                                     //退出smb: \>交互环境
[root@desktop0 ~]#
```

Top

2 案例2：多用户Samba挂载

2.1 问题

本例要求在虚拟机 desktop0 上访问 server0 提供的共享 devops，特性如下：

1. 将此共享永久挂载在 /mnt/dev 目录
2. 挂载时以用户 kenji 作为认证
3. 必要的时候，任何普通用户都可以通过用户 chihiro 来临时获取写的权限

2.2 方案

Samba客户端的multiuser挂载：支持切换访问Samba共享的用户身份，但不需要重新挂载共享资源。挂载参数需要添加“multiuser,sec=ntlmssp”，客户机上的普通用户可以通过cifscreds命令提交新的身份凭据。

在客户端挂载Samba共享目录，需要软件包cifs-utils的支持。

为访问网络资源配置开机挂载时，注意添加参数“_netdev”，表示等客户机网络配置可用以后才挂载对应资源。

2.3 步骤

实现此案例需要按照如下步骤进行。

步骤一：挂载Samba共享目录

1）创建挂载点

```
[root@desktop0 ~]# mkdir /mnt/dev
```

2）安装cifs-utils软件包

```
[root@desktop0 ~]# yum -y install cifs-utils
....
```

Top

3）配置开机挂载

```
[root@desktop0 ~]# vim /etc/fstab
...
//server0.example.com/devops /mnt/dev cifs username=kenji,password=atenorth,_netdev 0 0
```

4）测试挂载配置

```
[root@desktop0 ~]# mount -a
[root@desktop0 ~]# df -hT /mnt/dev
Filesystem Type Size Used Avail Use% Mounted on
//server0.example.com/devops cifs 10G 3.2G 6.8G 32% /mnt/dev
```

步骤二：启用multiuser多用户支持

1）修改挂载配置，添加多用户支持

```
[root@desktop0 ~]# vim /etc/fstab
...
//server0.example.com/devops /mnt/dev cifs username=kenji,password=atenorth,multiuser,sec=ntlmssp,_netdev 0 0
[root@desktop0 ~]# umount /mnt/dev //卸载此共享
[root@desktop0 ~]# mount /mnt/dev //重新挂载此共享
```

2）验证多用户访问

切换到普通用户student验证，无权访问挂载点/mnt/dev：

Top

```
[root@desktop0 ~]# su - student
Last login: Sun Nov 27 03:51:32 CST 2016 on pts/0
[student@desktop0 ~]$ ls /mnt/dev
ls: cannot access /mnt/dev: Permission denied
```

以共享用户chihiro身份提交新的访问凭据，再次验证，对挂载点/mnt/dev可读写：

```
[student@desktop0 ~]$ cifscreds -u chihiro add server0.example.com
Password:                                   //输入共享账号chihiro的密码
[student@desktop0 ~]$ touch /mnt/dev/a.txt
[student@desktop0 ~]$ ls /mnt/dev/a.txt
/mnt/dev/a.txt
```

3 案例3：普通NFS共享的实现

3.1 问题

本例要求在虚拟机 server0 上配置NFS服务，完成以下任务：

1. 只读的方式共享目录 /public，只能被 example.com 域中的系统访问
2. 可读写共享目录/protected，能被 example.com 域中的系统访问

然后在虚拟机 desktop0 上访问NFS共享目录

1. 将 server0 的 /public 挂到本地 /mnt/nfsmount
2. 这些文件系统在系统启动时自动挂载

Top

3.2 方案

对于普通NFS共享来说：

- 服务端需要运行系统服务 nfs-server.service
- 客户端不需要运行特定的系统服务

配置NFS共享目录的记录格式：

```
文件夹绝对路径    客户地址1(ro或rw等控制参数)  客户地址2(ro或rw等控制参数) ...
```

3.3 步骤

实现此案例需要按照如下步骤进行。

步骤一：在server0上发布NFS共享目录

1）准备需要共享的文件夹

```
[root@server0 ~]# mkdir /public
[root@server0 ~]# mkdir /protected
```

2）建立NFS共享配置

```
[root@server0 ~]# vim /etc/exports
/public          172.25.0.0/24(ro)
/protected       172.25.0.0/24(rw)
```

Top

3）启动系统服务nfs-server，并设置开机自启

```
[root@server0 ~]# systemctl restart nfs-server
[root@server0 ~]# systemctl enable nfs-server
ln -s '/usr/lib/systemd/system/nfs-server.service' '/etc/systemd/system/nfs.target.wants/nfs-server.service'
```

步骤二：在desktop0上挂载NFS共享目录/public

1）创建挂载点

```
[root@desktop0 ~]# mkdir /mnt/nfsmount
```

2）列出server0上提供的NFS共享资源

```
[root@desktop0 ~]# showmount -e server0.example.com
Export list for server0.example.com:
/protected 172.25.0.0/24
/public    172.25.0.0/24
```

3）配置开机挂载server0的NFS共享目录/public

```
[root@desktop0 ~]# vim /etc/fstab
. . .
server0.example.com:/public     /mnt/nfsmount   nfs     _netdev   0 0
```

Top

4）测试挂载配置

```
[root@desktop0 ~]# mount -a
[root@desktop0 ~]# df -hT /mnt/nfsmount/
Filesystem                 Type  Size  Used Avail Use% Mounted on
server0.example.com:/public nfs4   10G  3.2G  6.8G  32% /mnt/nfsmount
```

4 案例4：安全NFS共享的实现

4.1 问题

本例要求在虚拟机 server0 上配置安全NFS服务，完成以下任务：

1. 访问 /protected 需 kerberos 加密，密钥地址：http://classroom/pub/keytabs/server0.keytab
2. 目录 /protected 下包含名为 project 的子目录

然后在虚拟机 desktop0 上访问NFS共享目录

1. 挂载 /mnt/nfssecure 需 kerberos加密，密钥地址：http://classroom/pub/keytabs/desktop0.keytab
2. 用户 ldapuser0 能够在 /mnt/nfssecure/project 目录下创建文件，其密码为 kerberos

4.2 方案

对于安全NFS共享来说：

- 服务端需要运行系统服务 nfs-server.service、nfs-secure-server.service
- 客户端需要运行系统服务 nfs-secure.service

kerberos认证/加密：一次认证（获取通行证），多次免密码登录。

客户机密钥部署位置：/etc/krb5.keytab 。

参与kerberos认证/加密的客户机需要加入同一个kerberos领域，在教学环境虚拟机中可通过执行lab nfskrb5 setup操作来实现。

4.3 步骤

Top

实现此案例需要按照如下步骤进行。

步骤一：将server0、desktop0加入kerberos认证领域

教学环境虚拟机按以下操作处理。

1）初始化server0

```
[root@server0 ~]# lab nfskrb5 setup
Installing packages ...
Updating authconfig for ldap & krb5 ...
SUCCESS
```

2）初始化desktop0

```
[root@desktop0 ~]# lab nfskrb5 setup
Installing packages ...
Updating authconfig for ldap & krb5 ...
SUCCESS
```

3）验证初始化结果

可以使用网络账号ldapuser0登入到server0或desktop0，其密码是kerberos：

```
[root@server0 ~]# ssh ldapuser0@desktop0.example.com
The authenticity of host 'desktop0.example.com (172.25.0.10)' can't be established.
ECDSA key fingerprint is eb:24:0e:07:96:26:b1:04:c2:37:0c:78:2d:bc:b0:08.
Are you sure you want to continue connecting (yes/no)? yes        //接受密钥
Warning: Permanently added 'desktop0.example.com,172.25.0.10' (ECDSA) to the list of known hosts.
```

Top

```
ldapuser0@desktop0.example.com's password:              //输入密码kerberos
Creating home directory for ldapuser0.
[ldapuser0@desktop0 ~]$                                 //成功登入
[ldapuser0@desktop0 ~]$ exit                            //返回原环境
logout
Connection to desktop0.example.com closed.
[root@server0 ~]#
```

步骤二：为server0、desktop0部署kerberos密钥

1）为server0下载及部署密钥

```
[root@server0 ~]# wget  http://classroom/pub/keytabs/server0.keytab  -O /etc/krb5.keytab
..  ..
2016-11-27 04:26:38 (83.7 MB/s) -‘ /etc/krb5.keytab’ saved [1242/1242]

[root@server0 ~]# file  /etc/krb5.keytab                //检查部署结果
/etc/krb5.keytab:  data
```

2）为desktop0下载及部署密钥

```
[root@desktop0 ~]# wget  http://classroom/pub/keytabs/desktop0.keytab  -O /etc/krb5.keytab
..  ..
2016-11-27 04:27:25 (68.4 MB/s) -‘ /etc/krb5.keytab’ saved [1242/1242]

[root@desktop0 ~]# file  /etc/krb5.keytab               //检查部署结果
```

Top

```
06.     /etc/krb5.keytab: data
```

步骤三：在server0上调整/protected共享配置

1）创建指定的子目录

```
01.     [root@server0 ~]# mkdir  /protected/project
02.     [root@server0 ~]# chown  ldapuser0  /protected/project        //赋予可写权限
```

2）调整共享目录的安全控制类型

```
01.     [root@server0 ~]# vim  /etc/exports
02.     /public         172.25.0.0/24(ro)
03.     /protected      172.25.0.0/24(rw,sec=krb5p)                  //指定安全类型
```

3）重启系统服务nfs-server、nfs-secure-server，设置开机自启

```
01.     [root@server0 ~]# systemctl  restart  nfs-server  nfs-secure-server
02.     [root@server0 ~]# systemctl  enable  nfs-server  nfs-secure-server
03.     ln -s '/usr/lib/systemd/system/nfs-secure-server.service' '/etc/systemd/system/nfs.target.wants/nfs-secure-server.service'
```

步骤四：在desktop0上挂载安全NFS共享/protected

Top

1）创建挂载点

```
[root@desktop0 ~]# mkdir /mnt/nfssecure
```

2）启动系统服务nfs-secure，并配置开机自启

```
[root@desktop0 ~]# systemctl restart nfs-secure
[root@desktop0 ~]# systemctl enable nfs-secure
ln -s '/usr/lib/systemd/system/nfs-secure.service' '/etc/systemd/system/nfs.target.wants/nfs-secure.service'
```

3）配置开机挂载安全NFS共享

```
[root@desktop0 ~]# vim /etc/fstab
. . .
server0.example.com:/public     /mnt/nfsmount   nfs     _netdev  0 0
server0.example.com:/protected  /mnt/nfssecure  nfs     sec=krb5p,_netdev  0 0
```

4）验证挂载配置

```
[root@desktop0 ~]# mount -a
[root@desktop0 ~]# df -hT /mnt/nfs*
Filesystem                    Type  Size  Used Avail Use% Mounted on
server0.example.com:/public   nfs4   10G  3.3G  6.8G  33% /mnt/nfsmount
server0.example.com:/protected nfs4  10G  3.3G  6.8G  33% /mnt/nfssecure
```

Top

5）测试对挂载点的写入权限

以用户ldapuser0通过SSH的方式登入desktop0，验证密码（kerberos）以获取通行证：

```
[root@desktop0 ~]# ssh ldapuser0@desktop0.example.com
ldapuser0@desktop0.example.com's password:              //输入密码kerberos
Last login: Sun Nov 27 04:39:52 2016 from desktop0.example.com
[ldapuser0@desktop0 ~]$                                 //成功登入
```

访问desktop0的挂载点/mnt/nfssecure/的子目录project，测试可写入：

```
[ldapuser0@desktop0 ~]$ touch /mnt/nfssecure/project/a.txt
[ldapuser0@desktop0 ~]$ ls -lh /mnt/nfssecure/project/a.txt
-rw-rw-r--. 1 ldapuser0 ldapuser0 0 Nov 27 04:43 /mnt/nfssecure/project/a.txt
```

Top