FTP-сервер ProFTPd на CentOS 7

Подготовка системы

Прежде чем начать настройку нашего сервера, выполним следующие действия:

- Настроим правильное время на сервере. Это позволит нам видеть корректное значение в соответствующем атрибуте файлов и папок.
- Настроим брандмауэр. Откроем порты, которые нужны для работы ftp.
- Отключим или настроим SELinux. На выбор.

Рассмотрим эти действия подробнее.

1. Настройка времени

Зададим правильный часовой пояс:

```
timedatectl set-timezone Asia/Yekaterinburg
```

> * в данном примере будет задана зона по времени Екатеринбурга. Список всех доступных зон можно посмотреть командой `timedatectl list-timezones.`

Теперь установим утилиту для синхронизации времени и запустим ее в качестве сервиса:

```
yum install chrony -y
systemctl enable chronyd --now
```

2. Настройка брандмауэра

Нам нужно открыть порты 20, 21 для работы ftp и динамический диапазон — мы будем использовать 60000-65535.

В CentOS, как правило, используется утилита управления брандмауэром на базе firewalld, но мы также рассмотрим и iptables.

а) При использовании Firewalld:

```
firewall-cmd --permanent --add-port=20-21/tcp
firewall-cmd --permanent --add-port=60000-65535/tcp
firewall-cmd --reload
```

б) При использовании iptables:

```
iptables -I INPUT -p tcp --match multiport --dports 20,21,60000:65535 -j ACCEPT
service iptables save
```

3. Настройка SELinux

Для отключения SELinux вводим две команды:

```
sed -i 's/^SELINUX=.*/SELINUX=disabled/g' /etc/selinux/config
setenforce 0
```

Установка и базовая настройка ProFTPd

Устанавливаем EPEL репозиторий:

```
yum install epel-release -y
```

Устанавливаем ProFTPd:

```
yum install proftpd -y
```

Внесем небольшие правки в начальный конфигурационный файл:

```
nano /etc/proftpd.conf
```

Добавим строки:

```
    UseIPv6 off
IdentLookups off
PassivePorts 60000 65535
```

Разрешаем сервис и запускаем его:

```
    systemctl enable proftpd --now
```

Можно пробовать подключаться под любой системной учетной записью.

Если необходимо добавить отдельного пользователя, вводим команду:

```
    useradd ftpuser -m
passwd ftpuser
```

> * в данном примере мы создали пользователя ftpuser. Второй командой мы задали пароль.

ProFTPd через TLS

Откроем файл:

```
    nano /etc/sysconfig/proftpd
```

Зададим значение для опции **PROFTPD_OPTIONS**:

```
    PROFTPD_OPTIONS="-DTLS"
```

> * опция DTLS включает TLS.

Генерируем сертификат:

```
    openssl req -x509 -days 1461 -nodes -newkey rsa:2048 -sha256 -keyout /etc/pki/tls/certs/proftpd.pem -out
/etc/pki/tls/certs/proftpd.pem -subj "/C=RU/ST=SPb/L=SPb/O=Global Security/OU=IT
Department/CN=cdn.mylbt.ru/CN=mylbt"
```

Перезапускаем сервис:

```
systemctl restart proftpd
```

Виртуальные пользователи

Хранить пользователей можно в файле и базе данных. Рассмотрим настройку и того, и другого.

В файле

Устанавливаем proftpd-utils:

```
yum install proftpd-utils -y
```

Создаем каталог для хранения конфигурационных файлов froftpd:

```
mkdir /etc/proftpd.d
```

Создаем файл с паролями:

```
ftpasswd --passwd --file=/etc/proftpd.d/ftpd.passwd --name=vuser1 --uid=48 --gid=48 --home=/var/www --shell=/sbin/nologin
```

> * где **/etc/proftpd/ftpd.passwd** — полный путь до файла, в котором хранятся пользователи; **vuser1** — имя пользователя (логин); **uid** и **gid** — идентификаторы пользователя и группы системной учетной записи, от которой будет выступать сервер; **/var/www** — домашний каталог пользователя; **/sbin/nologin** — оболочка, запрещающая локальный вход пользователя в систему.

Редактируем proftpd.conf:

```
nano /etc/proftpd.conf
```

Комментируем следующую строку:

```
#AuthOrder       ...
```

Добавляем следующее:

```
RequireValidShell off
AuthUserFile /etc/proftpd.d/ftpd.passwd
AuthPAM off
```

```
LoadModule mod_auth_file.c
AuthOrder mod_auth_file.c
```

Перезапускаем сервис:

```
systemctl restart proftpd
```

Можно пробовать подключиться под созданным пользователем (в нашем примере, **vuser1**).

В базе данных MySQL (MariaDB)

Устанавливаем компонент proftpd-mysql:

```
yum install proftpd-mysql -y
```

Если не установлена, ставим MariaDB:

```
yum install mariadb mariadb-server -y
```

Разрешаем и запускаем сервис:

```
systemctl enable mariadb
systemctl start mariadb
```

Задаем пароль для суперпользователя базы данных:

```
mysqladmin -u root password
```

Подключаемся к базе данных:

```
mysql -uroot -p
```

Создаем базу данных, таблицу и пользователя:

```
> CREATE DATABASE proftpd DEFAULT CHARACTER SET utf8 DEFAULT COLLATE utf8_general_ci;
```

```
> CREATE TABLE `proftpd`.`users` (
`username` VARCHAR( 32 ) NOT NULL ,
`password` CHAR( 41 ) NOT NULL ,
`uid` INT NOT NULL ,
`gid` INT NOT NULL ,
```

```
`homedir` VARCHAR( 255 ) NOT NULL ,
`shell` VARCHAR( 255 ) NOT NULL DEFAULT '/sbin/nologin',
UNIQUE (`username`)
) ENGINE = MYISAM CHARACTER SET utf8 COLLATE utf8_general_ci;
```

```
> GRANT SELECT ON proftpd.* TO proftpu@localhost IDENTIFIED BY 'proftpdpass';
```

* данными командами мы создали базу данных **proftpd**. В ней таблицу **users** и пользователя **proftpu** с паролем **proftpdpass**, которому дали право подключаться только с локального сервера.

Добавляем пользователя в таблицу и отключаемся от базы:

```
> INSERT INTO `proftpd`.`users` VALUES ('sqluser1', ENCRYPT('sqlpassword'), '48', '48', '/var/www',
'/sbin/nologin');
> \q
```

* в данном примере мы создаем пользователя **sqluser1** с паролем **sqlpassword**.

Создаем файл с конфигурацией для SQL:

```
mkdir /etc/proftpd.d
```

```
nano /etc/proftpd.d/sql.conf
```

```
SQLBackend mysql
SQLEngine on
SQLAuthTypes Crypt
SQLConnectInfo proftpd@localhost proftpu proftpdpass
SQLUserInfo users username password uid gid homedir shell
SQLAuthenticate users*
SQLMinUserUID 33
SQLMinUserGID 33
SQLLogFile /var/log/proftpd/sql.log
```

Настраиваем proftpd (добавляем строки):

```
nano /etc/proftpd.conf
```

```
    LoadModule mod_sql.c
LoadModule mod_sql_mysql.c
Include /etc/proftpd.d/sql.conf
AuthOrder mod_sql.c
```

Перезапускаем сервис:

```
    systemctl restart proftpd
```

Возможные ошибки

1. A certificate in the chain was signed using an insecure algorithm

Ошибку можно увидеть в некоторых FTP-клиентах при попытке подключиться к серверу, который использует SSL.

Причина: как и следует из сообщения, клиенту не нравится алгоритм шифрования, так как он устарел и не соответствуем требованиям безопасности.

Решение: необходимо использовать сертификат с более стойким алгоритмом шифрования, например sha256. Чтобы получить такой сертификат с помощью утилиты openssl нужно добавить ключ **-sha256** (в инструкции выше используется именно такой подход).

2. lib permission denied

При попытке работы с каталогом lib, сервис выдает ошибку **permission denied**.

Причина: при использовании chroot в proftpd используется модуль RLimitChroot, который запрещает работу с «чувствительными» каталогами — lib, etc и так далее.

Решение: если у нас есть необходимость постоянно работать с каталогами, защищенными модулем RLimitChroot, то его действие можно отключить.

Открываем конфигурационный файл:

```
    nano /etc/proftpd.conf
```

Добавляем строку:

```
    RLimitChroot off
```

Чтобы настройка применилась, перезапускаем сервис:

```
systemctl restart proftpd
```

Revision #6
Created 26 October 2023 12:11:41 by Admin
Updated 5 December 2023 04:04:20 by Admin