

01. Модуль 2. Задание 1

Задание

Настройте доменный контроллер Samba на машине BR-SRV.

- ▶ Создайте 5 пользователей для офиса HQ: имена пользователей формата user№.hq. Создайте группу hq, введите в эту группу созданных пользователей
- ▶ Введите в домен машину HQ-CLI
- ▶ Пользователи группы hq имеют право аутентифицироваться на клиентском ПК
- ▶ Пользователи группы hq должны иметь возможность повышать привилегии для выполнения ограниченного набора команд: cat, grep, id. Запускать другие команды с повышенными привилегиями пользователи группы не имеют права
- ▶ Выполните импорт пользователей из файла users.csv. Файл будет располагаться на виртуальной машине BR-SRV в папке /opt

Реализация



Будет рассмотрен пример на основе настроек **МОДУЛЯ-1**



Имеем установленный и настроенный **DNS сервер на HQ-SRV**. Настройки аналогичны **Модуль-1, Задание-10**.

Дополнительная настройка Bind

1. На HQ-SRV открываем конфигурационный файл DNS сервера `/etc/named.conf`

```
1 | # nano /etc/named.conf
```

и дописываем строчку

```
1 | allow-transfer { 192.168.200.2; };
```

где: 192.168.200.2 - IP адрес *BR-SRV*

```
GNU nano 7.2 /etc/named.conf
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
options {
    listen-on port 53 { any; };
    listen-on-v6 port 53 { none; };
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    secroots-file "/var/named/data/named.secroots";
    recursing-file "/var/named/data/named.recursing";
    allow-query { any; };
    forwarders { 77.88.8.8; };
    allow-transfer { 192.168.200.2; };
}
/*
- If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
- If you are building a RECURSIVE (caching) DNS server, you need to enable
  recursion.
- If your recursive DNS server has a public IP address, you MUST enable access
  control to limit queries to your legitimate users. Failing to do so will
  cause your server to become part of large scale DNS amplification
  attacks. Implementing BCP38 within your network would greatly
  reduce such attack surface
*/
recursion yes;
```

Перезагружаем службу

```
1 | # systemctl restart named
```

Установка сервера SAMBA DC на BR-SRV



[База знаний РЕД.ОС - Установка сервера SAMBA DC](#)

Переводим SELinux в режим уведомлений

```
1 | # setenforce 0
```

Проверяем что сервер имеет полное доменное имя

```
1 | # hostnamectl
```

Установка необходимых пакетов

```
1 | # dnf install samba* krb5* -y
```

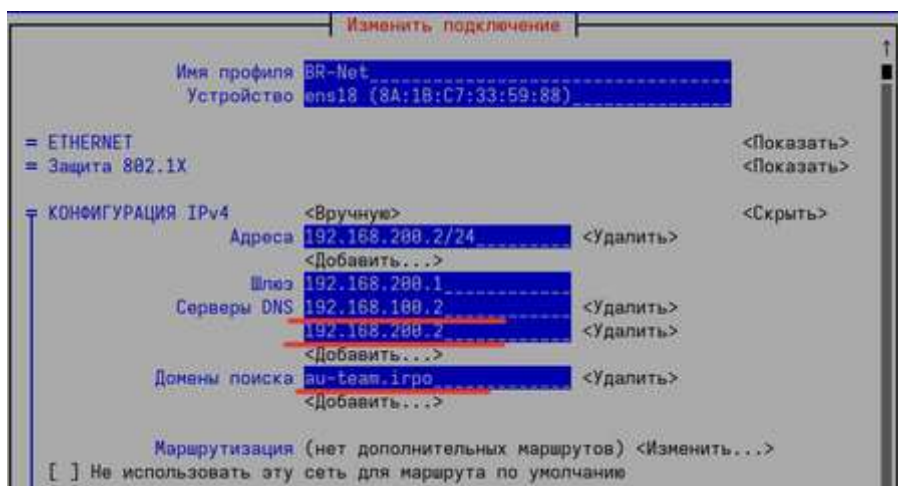
Настройка сетевого интерфейса через утилиту `nmtui`

В настройках сетевого интерфейса `BR-SRV` в конфигурации `IPv4` необходимо внести следующие значения:

IP-адрес первого DNS-сервера – IP-адрес `HQ-SRV`

IP-адрес второго DNS-сервера – IP-адрес создаваемого контроллера домена (`BR-SRV`)

Домены поиска – `au-team.irpo`



Отключаем DNS-службы `systemd-resolved` в файле `/etc/systemd/resolved.conf`

```
1 | # nano /etc/systemd/resolved.conf
```

Устанавливаем параметр `DNSStubListener` в значение `no`, отключив прослушивание `systemd-resolved` на порту `53`.

```
[Resolve]
# Some examples of DNS servers which may be used
# Cloudflare: 1.1.1.1#cloudflare-dns.com 1.0.0.1
# Google:      8.8.8.8#dns.google 8.8.4.4#dns.goo
# Quad9:       9.9.9.9#dns.quad9.net 149.112.112.
#DNS=
#FallbackDNS=
#Domains=
#DNSSEC=no
#DNSOverTLS=no
#MulticastDNS=no
#LLMNR=resolve
#Cache=yes
#CacheFromLocalhost=no
DNSStubListener=no
#DNSStubListenerExtra=
#ReadEtcHosts=yes
#ResolveUnicastSingleLabel=no
-
```

Перезапускаем systemd-resolved и NetworkManager

```
1 | # systemctl restart systemd-resolved.service NetworkManager
```

Проверяем изменения в настройках

```
1 | # cat /etc/resolv.conf
```

В выводе должен быть указан адрес отличающийся от **127.0.0.53** и Домен поиска (**search**)

```
[root@br-srv ~]#
[root@br-srv ~]# cat /etc/resolv.conf | grep -v "#"
nameserver 192.168.100.2
nameserver 192.168.200.2
search au-team.irpo
[root@br-srv ~]#
```

Создание домена под управлением Samba DC

Переименовываем файл **/etc/smb.conf**, он будет создан в процессе выполнения команды **samba-tool**

Данный файла при запуске полуавтоматической конфигурации может вызвать ошибку.

```
1 | # mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
```

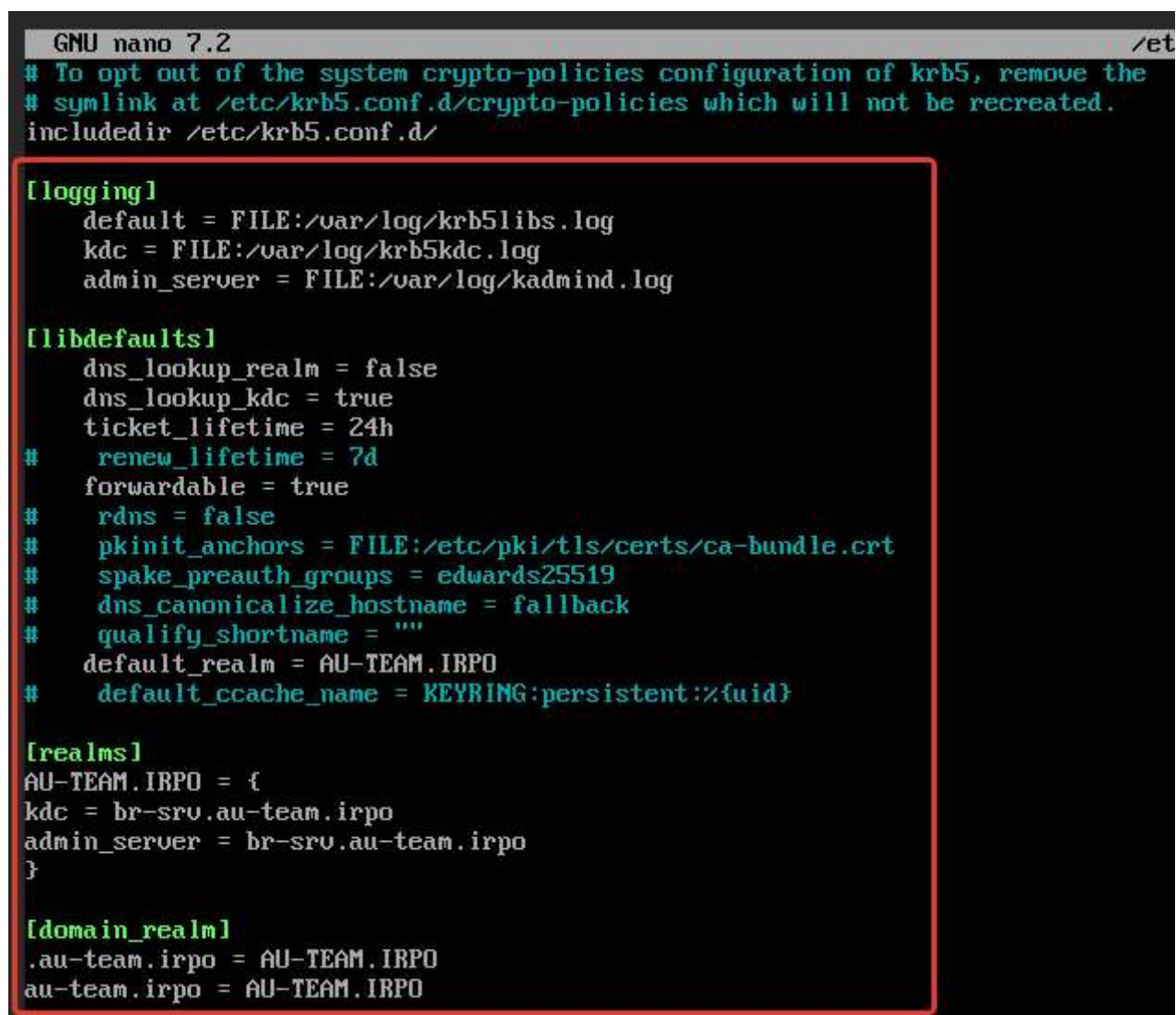
Создаем резервную копию конфигурационного файла `kerberos` , используемого по умолчанию

```
1 | # cp /etc/krb5.conf /etc/krb5.conf.bak
```

Настройка конфигурации Kerberos `/etc/krb5.conf`

Данный файл приводим к следующему виду

```
1 | # nano /etc/krb5.conf
```



```
GNU nano 7.2 /et
# To opt out of the system crypto-policies configuration of krb5, remove the
# symlink at /etc/krb5.conf.d/crypto-policies which will not be recreated.
includedir /etc/krb5.conf.d/

[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
dns_lookup_realm = false
dns_lookup_kdc = true
ticket_lifetime = 24h
# renew_lifetime = 7d
forwardable = true
# rdns = false
# pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
# spake_preauth_groups = edwards25519
# dns_canonicalize_hostname = fallback
# qualify_shortname = ""
default_realm = AU-TEAM.IRPO
# default_ccache_name = KEYRING:persistent:%{uid}

[realms]
AU-TEAM.IRPO = {
kdc = br-srv.au-team.irpo
admin_server = br-srv.au-team.irpo
}

[domain_realm]
.au-team.irpo = AU-TEAM.IRPO
au-team.irpo = AU-TEAM.IRPO
```

Полуавтоматическое конфигурирование сервера с помощью утилиты `samba-tool`

Конфигурирование в интерактивном режиме выполняется командой:

```
1 | # samba-tool domain provision --use-rfc2307 --interactive
```

```

root@br-srv:~#
root@br-srv:~#
root@br-srv:~# samba-tool domain provision --use-rfc2307 --interactive
Realm [AU-TEAM.IRPO]: Enter
Domain [AU-TEAM]: Enter
Server Role (dc, member, standalone) [dc]: dc
DNS backend (Samba_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [Samba_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding) [192.168.100.2]: Enter
Administrator password: 
Retype password:

```

Запуск и проверка работоспособности

Запуск и добавление в автозагрузку службы samba:

```
1 | # systemctl enable --now samba
```

Проверка статуса службы:

```
1 | # systemctl status samba
```

Проверяем работу домена

```

1 | # samba-tool domain info 127.0.0.1
2 |
3 | # samba-tool domain info 192.168.200.2

```

```

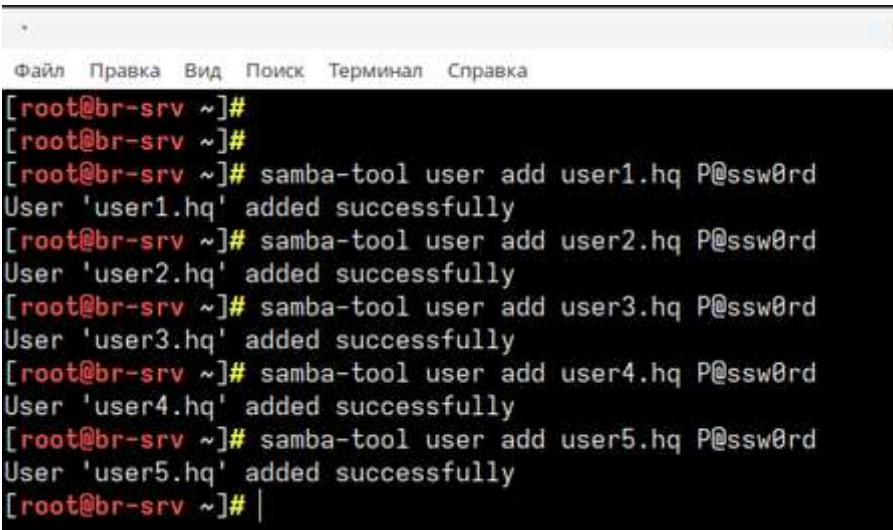
root@br-srv:~#
root@br-srv:~# samba-tool domain info 127.0.0.1
Forest           : au-team.irpo
Domain           : au-team.irpo
Netbios domain   : AU-TEAM
DC name          : br-srv.au-team.irpo
DC netbios name  : BR-SRV
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name
root@br-srv:~#
root@br-srv:~#
root@br-srv:~# samba-tool domain info 192.168.200.2
Forest           : au-team.irpo
Domain           : au-team.irpo
Netbios domain   : AU-TEAM
DC name          : br-srv.au-team.irpo
DC netbios name  : BR-SRV
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name
root@br-srv:~#

```


Добавление пользователей

Создаем 5 пользователей

```
1 # samba-tool user add user1.hq P@ssw0rd
2
3 # samba-tool user add user2.hq P@ssw0rd
4
5 # samba-tool user add user3.hq P@ssw0rd
6
7 # samba-tool user add user4.hq P@ssw0rd
8
9 #samba-tool user add user5.hq P@ssw0rd
```



```
[root@br-srv ~]#
[root@br-srv ~]#
[root@br-srv ~]# samba-tool user add user1.hq P@ssw0rd
User 'user1.hq' added successfully
[root@br-srv ~]# samba-tool user add user2.hq P@ssw0rd
User 'user2.hq' added successfully
[root@br-srv ~]# samba-tool user add user3.hq P@ssw0rd
User 'user3.hq' added successfully
[root@br-srv ~]# samba-tool user add user4.hq P@ssw0rd
User 'user4.hq' added successfully
[root@br-srv ~]# samba-tool user add user5.hq P@ssw0rd
User 'user5.hq' added successfully
[root@br-srv ~]# |
```

Создаем группу и добавляем туда созданных пользователей

```
1 # samba-tool group add hq
2
3 # samba-tool group addmembers hq user1.hq,user2.hq,user3.hq,user4.hq,user5.hq
```



```
[root@br-srv ~]#
[root@br-srv ~]#
[root@br-srv ~]# samba-tool group add hq
Added group hq
[root@br-srv ~]#
[root@br-srv ~]# samba-tool group addmembers hq user1.hq,user2.hq,user3.hq,user4.hq,user5.hq
Added members to group hq
[root@br-srv ~]# |
```

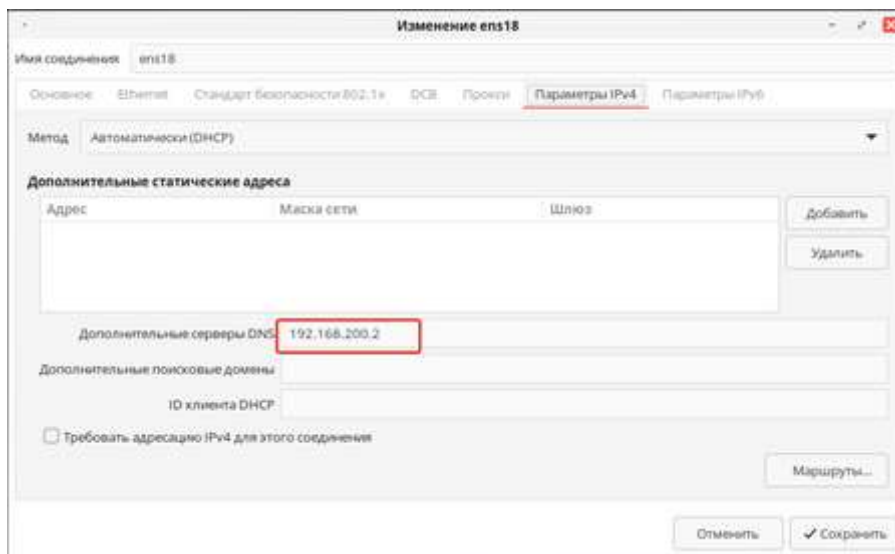
Вывод списка пользователей Samba DC

```
1 # samba-tool user list
```

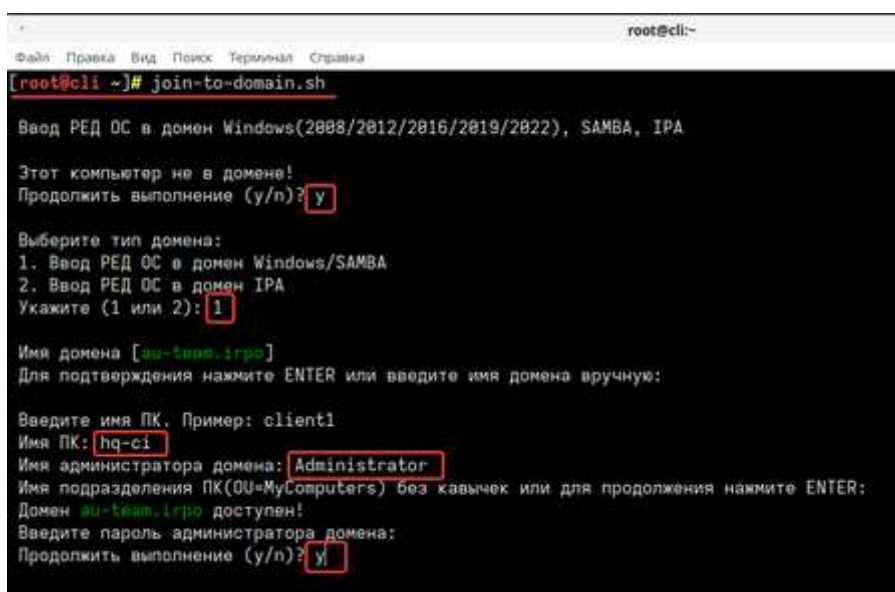
Ввод клиента HQ-CLI в домен



В настройке сетевого интерфейса **HQ-CLI** добавляем **Дополнительные серверы DNS** – прописав IP адрес **BR-SRV**



В терминале **HQ-CLI** запускаем скрипт **join-to-domain.sh** с привилегиями суперпользователя



Вводим пароль, который вводили при настройке домена через **samba-tool**

Перезагружаем **HQ-CLI** и входим под **доменным пользователем**

Проверка



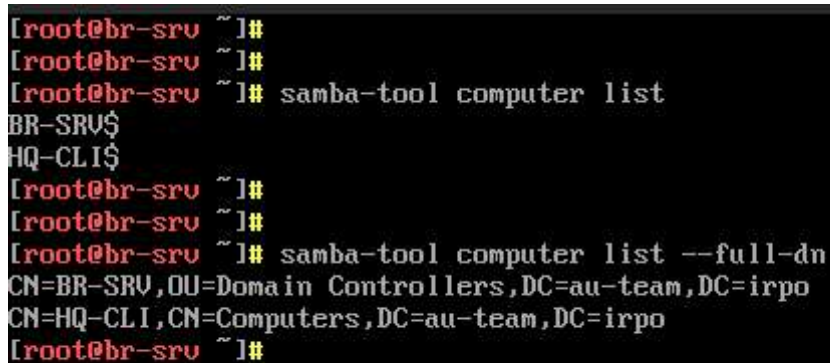
На **BR-SRV** проверяем

Пример получения списка имен (SAM) компьютеров:


```
1 | # samba-tool computer list
```

Пример получения списка уникальных составных имен компьютеров (DN):

```
1 | # samba-tool computer list --full-dn
```



```
[root@br-srv ~]#  
[root@br-srv ~]#  
[root@br-srv ~]# samba-tool computer list  
BR-SRV$  
HQ-CLI$  
[root@br-srv ~]#  
[root@br-srv ~]#  
[root@br-srv ~]# samba-tool computer list --full-dn  
CN=BR-SRV,OU=Domain Controllers,DC=au-team,DC=irpo  
CN=HQ-CLI,CN=Computers,DC=au-team,DC=irpo  
[root@br-srv ~]#
```

Пример получения полного списка учетных записей в домене

```
1 | # samba-tool user list
```

Пример получения списка уникальных составных имен пользователей (DN):

```
1 | # samba-tool user list --full-dn
```

Привилегии для выполнения набора команд

Создаем файл в `/etc/sudoers.d/hq` на `HQ-CLI`

```
1 | # nano /etc/sudoers.d/hq
```

Прописываем следующую строку

Повышение привилегий с вводом пароля

```
1 | %hq ALL=(ALL) /usr/bin/cat, /usr/bin/grep, /usr/bin/id
```

Повышение привилегий без ввода пароля

1 | %hq ALL=(ALL) NOPASSWD:/usr/bin/cat, /usr/bin/grep, /usr/bin/id



где `/usr/bin/cat`, `/usr/bin/grep`, `/usr/bin/id` - полный путь к запускаемым командам

Нахождение полного пути к команде



Which в Linux — это утилита для нахождения местоположения исполняемых файлов. Она анализирует пути, указанные в переменной окружения `PATH`, и возвращает путь к первому найденному файлу, соответствующему запрошенному имени.

```
Файл  Правка  Вид  Поиск  Терминал  Справка
[ root@hq-cli ~ ]#
[ root@hq-cli ~ ]# which cat
/usr/bin/cat
[ root@hq-cli ~ ]#
[ root@hq-cli ~ ]# which grep
alias grep='grep --color=auto'
/usr/bin/grep
[ root@hq-cli ~ ]#
[ root@hq-cli ~ ]# which id
/usr/bin/id
[ root@hq-cli ~ ]#
```

Импорт пользователей



Пользователи импортированные из скачанного файла [Users.csv](#) с <https://de.firpo.ru> могут не авторизоваться (не верный пароль) из-за кодировки символов.
Модернизированный файл [Users.csv](#)

Открываем файл `/opt/Users.csv` с помощью команды `head`, Для просмотра имен полей таблицы `Users.csv`

1 | # head /opt/Users.csv

Имена полей необходимы для команды `read` в Bash скрипте

```

192.168.10.165:8006 QEMU (BR-SRV) - noVNC
[root@br-srv opt]#
[root@br-srv opt]#
[root@br-srv opt]# head Users.csv
First Name;Last Name;Role;Phone;OU;Street;ZIP/Postal Code;City;Country/Region;Password
Nolan;Barry;Overall;500 570 389;Overall;Rua Montes Claros 367;88104-660;Iumen;Russia;P0ssw0rd1
Althea;Battle;Overall;0845 46 42;Overall;Rua Petropolis 1748;01254-030;Glazov;Russia;P0ssw0rd1
Keefe;Becker;Overall;500 130 448;Overall;Rua Amazonas 1700;18607-496;Votkinsk;Russia;P0ssw0rd1
Zenia;Berg;Overall;(016977) 3041;Overall;Avenida Indianopolis 1270;04062-002;Sarapul;Russia;P0ssw0rd1
Deirdre;Bernard;Overall;(014537) 92989;Overall;Rua D 1936;35044-640;Kambarka;Russia;P0ssw0rd1
Raphael;Bird;Overall;5 548 711 314;Overall;Rua Francisco Cabrera Gomes 1887;08676-280;Balezino;Russia;P0ssw0rd1
Rachel;Blackburn;Overall;9 758 588 839;Overall;Rua F2 em Deus 1790;53550-035;Lubertzi;Russia;P0ssw0rd1
Abbot;Blackwell;Overall;(016977) 5178;Overall;Rua dos Galchhos 341;94945-230;Shatura;Russia;P0ssw0rd1
Mark;Blanchard;Overall;7 681 547 481;Overall;Rua Trinta e Quatro 1343;17039-350;Armavir;Russia;P0ssw0rd1
[root@br-srv opt]#

```



Создаем **Bash** скрипт добавления пользователей из **.csv** файла в **Samba AD**

```
1 | # nano samba-user-add.sh
```

Указываем путь к **.CSV** файлу с пользователями

```

1 | #!/bin/bash
2 |
3 | FILE="/opt/Users.csv"

```

Построчно в цикле читаем файл с разбивкой на строки с использованием разделителя **;**

```
1 | while IFS=';' read -r firstname lastname role phone ou street zip city country
```

Добавляем пользователя **Samba**

```
1 | samba-tool user add "$firstname.$lastname" "$password"
```

Завершаем цикл и исключаем строку заголовка из выходных данных **tail -n +2**

```
1 | done < <(tail -n +2 "$FILE")
```



Скрипт

```
1  #!/bin/bash
2
3  FILE="/opt/Users.csv"
4
5  while IFS=';' read -r firstname lastname role phone ou street zip city country
6      samba-tool user add "$firstname.$lastname" "$password"
7  done < <(tail -n +2 "$FILE")
```

Сохраняем файл скрипта, выдаём ему право на выполнение и запускаем его

```
1  # chmod +x /root/samba-user-add.sh
2
3  # cd /root
4
5  # ./samba-user-add.sh
```



Скрипт отрабатывает продолжительное время. Можно пока выполнять другой пункт задания

Содержимое доступно в соответствии с Всеобщее достояние, от Кабинет 2.20. | Powered by [Wiki.js](#)