


Включение записи в журналы Kerberos

При установке службы Kerberos в конфигурационном файле этой службы `/etc/krb5.conf` указываются настройки записи журналов в файлы, находящиеся в каталоге `/var/log`.

Пример записей в конфигурационном файле:

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


 Данная статья применима к:

- ОС ОН Орёл 2.12
- ОС СН Смоленск 1.6
- ОС СН Ленинград 8.1

Однако, так как каталог `/var/log` доступен для записи только привилегированному пользователю, запись в эти файлы производиться не будет.

При необходимости включить запись журналов Kerberos следует выполнить следующие действия:

1. Воспользовавшись текстовым редактором от имени привилегированного пользователя (в ОС СН Смоленск и Ленинград - привилегированного пользователя с высокой целостностью) в файлах запуска служб Kerberos (юниты Kerberos) `/lib/systemd/system/krb5-admin-server.service` и `/lib/systemd/system/krb5-kdc.service` в строку

```
 ReadWriteDirectories=-/var/tmp /tmp /var/lib/krb5kdc -/var/run /run
```

добавить каталог журналов `/var/log`:

```
 ReadWriteDirectories=-/var/tmp /tmp /var/lib/krb5kdc -/var/run /run /var/log
```

2. После сохранения изменений в файлах выполнить обновление службы `systemd` и перезапуск системных служб:

```
sudo systemctl daemon-reload
```

3. В случае использования службы FreeIPA помимо вышеуказанных действий перезапустить сервисы, контролируемые FreeIPA, командой:

```
sudo ipactl restart
```

Сценарий для ленивых:

```
sudo sed -i.bak -e "s~^[[:space:]]*ReadWriteDirectories=\\(.*\\)
~ReadWriteDirectories=\\1 /var/log~" /lib/systemd/system/{krb5-admin-server,
krb5-kdc}.service
sudo systemctl daemon-reload
```