Kerberos-

- http://web.mit.edu/kerberos/
- https://help.ubuntu.com/community/Kerberos
- https://help.ubuntu.com/18.04/serverguide/kerberos.html
- http://k5wiki.kerberos.org/wiki/Pkinit_configuration

Kerberos

Kerberos - , . Kerberos MIT's Kerberos site. Designing an Authentication System , Kerberos.

, Kerberos- .

Kerberos. MIT , Linux. Heimdal , .

Microsoft's **Active Directory** - Kerberos . Active Directory. Active, KDC **Domain Controller (DC)**. Active Directory Domain, .

Kerberos - **Key Distribution Center (KDC)**, . Kerberos, , KDC. , realm.

realm . , realm . , example.com EXAMPLE.COM realm.

1. USB- .
2. USB- :

```
$ lsusb
```

USB-:

```
[dmitrieva@localhost ~]$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 004: ID 0a89:0030 Aktiv Rutoken ECP
Bus 002 Device 003: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 002 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
```

, : **Aktiv Rutoken ECP**

Astra Linux 1.4.

.

- .

- `<username> = testuser`
- `<realm> = AKTIV-TEST.RU`
- `<server> = server.aktiv-test.ru`
- `<client> = client.aktiv-test.ru`

, realm Kerberos . realm . .

Host Names

Kerberos realm **Fully Qualified Domain Name (FQDN)**.

Kerberos , FQDN reverse-resolvable. IP , rdns false krb5. conf

Active Directory DNS, Active Directory Domain Controller DNS.
, FQDN , .

FQDN, forward reverse :

```
$ nslookup server.example.com
$ nslookup <server ip address>
```

Astra Linux ( ), nslookup, dnsutils.

Synaptic Package Manager $ apt-get install dnsutils

IP . FQDN .

FQDN DNS , hosts (/etc) :

```
127.0.0.1 server.aktiv-test.ru localhost server
```

```
<IP-address> server.aktiv-test.ru <IP-address> server
```

IP-address - IP . 10.0.0.1.

DNS nslookup .

ping FQDN:

```
$ ping server.aktiv-test.ru
PING server.aktiv-test.ru (10.0.0.1) 56(84) bytes
of data.
64 bytes from server.aktiv-test.ru (10.0.0.1):
icmp_seq=1 ttl=128 time=0.176ms
```

ping IP FQDN, . , .

ping .

Kerberos : , . - **Network Time Protocol (NTP)** . Astra Linux 1.4 - NTP-. NTP- (, UbuntuTime Ubuntu).

Active Directory Domain Controllers NTP .

, Kerberos . Kerberos System Administration Manual , .

KDC

KDC

```
$ sudo apt-get install krb5-kdc krb5-admin-server
krb5-pkinit opensc pcscd
```

.

KDC - /etc/krb5kdc/kdc.conf.
- KDC , . realm. , .

kdc.conf

/etc/krb5kdc/kdc.conf :

```
[kdcdefaults]
        kdc_ports = 750,88
        default_realm = AKTIV-TEST.RU

[realms]
AKTIV-TEST.RU = {
    database_name = /var/lib/krb5kdc/principal
    admin_keytab = FILE:/etc/krb5kdc/kadm5.keytab
    acl_file = /etc/krb5kdc/kadm5.acl
    key_stash_file = /etc/krb5kdc/stash
    kdc_ports = 750,88
    max_life = 10h 0m 0s
    max_renewable_life = 7d 0h 0m 0s
    master_key_type = des3-hmac-sha1
    supported_enctypes = des3-hmac-sha1:normal des-
cbc-crc:normal des:normal des:v4 des:norealm des:
onlyrealm
    default_principal_flags = +preauth
}

[logging]
    kdc = FILE:/var/local/krb5kdc/kdc.log
    admin_server = FILE:/var/local/krb5kdc/kadmin.
log
```

' '

```
$ sudo mkdir /var/local/krb5kdc
```

' .

. Kerberos

krb5.conf

/etc/krb5.conf :

```
[libdefaults]
    default_realm = AKTIV-TEST.RU

# The following krb5.conf variables are only for
MIT Kerberos.
    krb4_config = /etc/krb.conf
    krb4_realms = /etc/krb.realms
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true

# The following libdefaults parameters are only
for Heimdal Kerberos.
    v4_instance_resolve = false
    v4_name_convert = {
        host = {
            rcmd = host
            ftp = ftp
        }
        plain = {
            something = something-else
        }
    }
    fcc-mit-ticketflags = true

[realms]
    AKTIV-TEST.RU = {
        kdc = server.aktiv-test.ru
        admin_server = server.aktiv-test.ru
        default_domain = aktiv-test.ru
    }

[domain_realm]
    .aktiv-test.ru = AKTIV-TEST.RU
    aktiv-test.ru = AKTIV-TEST.RU

[login]
    krb4_convert = true
    krb4_get_tickets = false
```

Kerberos

Kerberos :

```
$ krb5_newrealm
```

Kerberos Access Control List (ACL) Kerberos admin daemon. - /etc/krb5kdc/kadm5.acl. - realm, , .

```
# This file is the access control list for krb5
administration.
# When this file is edited run /etc/init.d/krb5-
admin-server restart to activate
# One common way to set up Kerberos administration
is to allow any principal
# ending in /admin  is given full administrative
rights.
# To enable this, uncomment the following line:
*/admin@AKTIV-TEST.RU    *
```

Principals

Principals Kerberos, . , Kerberos realm principal, Kerberos.

principals principal@REALM.NAME.

, tom realm AKTIV-TEST.RU principal tom@AKTIV-TEST.RU Kerberos.

Principal service/server.fqdn@REALM.NAME. , FTP lab.example.com realm AKTIV-TEST.RU principal ftp/lab.example.com@AKTIV-TEST.RU Kerberos.

principal .

kadmin

Kerberos realm kadmin. , , , realm principle. kadmin , Kerberos realm, , . , , kadmin KDC.

kadmin.local. kadmin.local root KDC principal. .

kadmin :

```
$ kadmin -p <principal>
```

<principal> principal. -, principal admin/admin realm, :

```
$ kadmin -p admin/admin
```

- :

```
$ kadmin: addprinc user
```

realm - principal .

- :

```
$ kadmin: delprinc user
```

- principal:

```
$ kadmin: listprincs
```

- :

```
$ addprinc service/server.fqdn
```

realm - principal .

-

```
$ kadmin: delprinc service/server.fqdn
```

.

```
$ sudo kadmin.local
# username = testuser
# password = test
kadmin.local:$ addprinc <username>
# ...
kadmin.local:$ quit

$ kinit <username>
...
$ klist
...
$ kdestroy
```

klist, :

```
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: testuser@AKTIV-TEST.RU

Valid starting       Expires              Service
principal
06.10.2016 16:58:08  07.10.2016 02:58:08  krbtgt
/AKTIV-TEST.RU@AKTIV-TEST.RU
        renew until 07.10.2016 16:58:06
```

,,, .

Kerberos

```
$ sudo apt-get install krb5-user libpam-krb5
libpam-krb5 krb5-pkinit libengine-pkcs11-openssl
opensc pcscd
```

krb5-config

krb5-config /etc/krb5.conf file. :

```
$ sudo dpkg-reconfigure krb5-config
```

:

- realm - AKTIV-TEST.RU
- Kerberos realm - server.aktiv-test.ru
- realm - server.aktiv-test.ru

: /etc/krb5.conf

krb5-config - , Kerberos /etc/krb5.conf. , krb5-config.
.

```
[libdefaults]
    default_realm = AKTIV-TEST.RU

# The following krb5.conf variables are only for
MIT Kerberos.
    krb4_config = /etc/krb.conf
    krb4_realms = /etc/krb.realms
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true

# The following libdefaults parameters are only
for Heimdal Kerberos.
    v4_instance_resolve = false
    v4_name_convert = {
        host = {
            rcmd = host
            ftp = ftp
        }
        plain = {
            something = something-else
        }
    }
    fcc-mit-ticketflags = true

[realms]
    AKTIV-TEST.RU = {
        kdc = server.aktiv-test.ru
        admin_server = server.aktiv-test.ru
    }

[domain_realm]
    .aktiv-test.ru = AKTIV-TEST.RU
    aktiv-test.ru = AKTIV-TEST.RU


[login]
    krb4_convert = true
    krb4_get_tickets = false
```

Kerberos, Ticket-Granting Ticket (TGT) kinit, .

realm .

```
# username = testuser
# password = test
$ kinit -p testuser@AKTIV-TEST.RU
Password for testuser@AKTIV-TEST.RU: <password>
...
$ klist
...
$ kdestroy
```

klist, :

```
Default principal: testuser@AKTIV-TEST.RU

Valid starting       Expires              Service
principal
06.10.2016 17:27:10  07.10.2016 03:27:10  krbtgt
/AKTIV-TEST.RU@AKTIV-TEST.RU
        renew until 07.10.2016 17:27:07
```

CA, :

```
$ openssl genrsa -out CA_key.pem 2048
$ openssl req -key CA_key.pem -new -x509 -out
CA_cert.pem
```

pkinit_extensions

pkinit_extensions

```
[ kdc_cert ]
basicConstraints=CA:FALSE

# Here are some examples of the usage of
nsCertType. If it is omitted
keyUsage = nonRepudiation, digitalSignature,
keyEncipherment, keyAgreement

#Pkinit EKU
extendedKeyUsage = 1.3.6.1.5.2.3.5

subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer

# Copy subject details

issuerAltName=issuer:copy

# Add id-pkinit-san (pkinit subjectAlternativeName)
subjectAltName=otherName:1.3.6.1.5.2.2;SEQUENCE:
kdc_princ_name

[kdc_princ_name]
realm = EXP:0, GeneralString:${ENV::REALM}
principal_name = EXP:1, SEQUENCE:kdc_principal_seq

[kdc_principal_seq]
name_type = EXP:0, INTEGER:1
name_string = EXP:1, SEQUENCE:kdc_principals

[kdc_principals]
princ1 = GeneralString:krbtgt
princ2 = GeneralString:${ENV::REALM}

[ client_cert ]

# These extensions are added when 'ca' signs a
request.

basicConstraints=CA:FALSE

keyUsage = digitalSignature, keyEncipherment,
keyAgreement

extendedKeyUsage =  1.3.6.1.5.2.3.4
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer


subjectAltName=otherName:1.3.6.1.5.2.2;SEQUENCE:
princ_name


# Copy subject details

issuerAltName=issuer:copy

[princ_name]
realm = EXP:0, GeneralString:${ENV::REALM}
principal_name = EXP:1, SEQUENCE:principal_seq

[principal_seq]
name_type = EXP:0, INTEGER:1
name_string = EXP:1, SEQUENCE:principals

[principals]
princ1 = GeneralString:${ENV::CLIENT}
```

KDC, :

```
$ openssl genrsa -out KDC_key.pem 2048
#
$ openssl req -new -out KDC.req -key ./KDC_key.pem
#
$ REALM=AKTIV-TEST.RU; export REALM
$ CLIENT=server.aktiv-test.ru; export CLIENT
$ openssl x509 -req -in ./KDC.req -CAkey ./CA_key.
pem -CA ./CA_cert.pem -out ./KDC.pem -extfile .
/pkinit_extensions -extensions kdc_cert -
CAcreateserial
```

/var/lib/krb5kdc/:

- KDC.pem
- KDC_key.pem
- CA_cert.pem

:

```
$ sudo cp ./KDC.pem ./KDC_key.pem ./CA_cert.pem
/var/lib/krb5kdc
```

preauth . kdcdefaults /etc/krb5kdc/kdc.conf :

/etc/krb5kdc/kdc.conf

```
[kdcdefaults]
        ...
    pkinit_identity = FILE:/var/lib/krb5kdc/kdc.
pem,/var/lib/krb5kdc/kdckey.pem
    pkinit_anchors = FILE:/var/lib/krb5kdc/cacert.
pem
```

preauth :

```
$ sudo kadmin.local
kadmin.local$: modprinc +requires_preauth testuser
```

PKCS#11

http://www.rutoken.ru/support/download/pkcs/

testuser. .

```
$ pkcs11-tool --module /usr/lib/librtpkcs11ecp.so
--keypairgen --key-type rsa:2048 -l --id 45
...
$ openssl
OpenSSL> engine dynamic -pre SO_PATH:/usr/lib
/engines/engine_pkcs11.so -pre ID:pkcs11 -pre
LIST_ADD:1 -pre LOAD -pre MODULE_PATH:/usr/lib
/librtpkcs11ecp.so
(dynamic) Dynamic engine loading support
[Success]: SO_PATH:/usr/lib/openssl/engines
/engine_pkcs11.so
[Success]: ID:pkcs11
[Success]: LIST_ADD:1
[Success]: LOAD
[Success]: MODULE_PATH:opensc-pkcs11.so
Loaded: (pkcs11) pkcs11 engine
OpenSSL> req -engine pkcs11 -new -key 0:45 -
keyform engine -out client.req
engine "pkcs11" set.
PKCS#11 token PIN:
...
OpenSSL> quit
```

librtpkcs11ecp.so, opensc-pkcs11.so engine_pkcs11.so

CA

```
$ REALM=AKTIV-TEST.RU; export REALM
$ CLIENT=server.aktiv-test.ru; export CLIENT
$ openssl x509 -CAkey ./CA_key.pem -CA ./CA_cert.
pem -req -in ./client.req -extensions client_cert -
extfile ./pkinit_extensions -out client.pem
```

PEM CRT:

```
$ openssl
OpenSSL> x509 -in client.pem -out client.crt -
outform DER
```

:

```
$ pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -
l -y cert -w ./client.crt --id 45
```

- client.pem - .

(client.pem) /etc/krb5/

CA (cacert.pem) c /etc/krb5/

Kerberos, /etc/krb5.conf

/etc/krb5.conf

```
[libdefaults]
        default_realm = AKTIV-TEST.RU
        pkinit_anchors = FILE:/etc/krb5/CA_cert.pem
#
#        pkinit_identities = FILE:/etc/krb5/client.
pem,/etc/krb5/clientkey.pem
#
        pkinit_identities = PKCS11:/usr/lib/x86_64-
linux-gnu/opensc-pkcs11.so
```

:

```
$ kinit <username>
```