

Kerberos apache2 Astra Linux

-
-
- [apache2](#)
- [Kerberos](#) [FreeIPA](#)
- [Kerberos](#) [ALD](#)
-
- [web-](#)
 - [web- Mozilla Firefox](#)
 - [web- Konqueror](#)



:

- Astra Linux Special Edition .10015-01 (1.7), .10015-10
- Astra Linux Special Edition .10015-17
- Astra Linux Special Edition .10015-37 (7.7)
- Astra Linux Special Edition .10015-03 (7.6)
- Astra Linux Special Edition .10152-02 (4.7)
- Astra Linux Special Edition .10015-01 (1.6)
- Astra Linux Special Edition .10015-16 . 1
- Astra Linux Special Edition .10015-16 . 2
- Astra Linux Special Edition .10265-01 (8.1)
- Astra Linux Common Edition 2.12

Kerberos [web- apache2](#) [FreeIPA](#) [ALD](#). [web-](#), Kerberos. :

1. : [ipadomain0.ru](#);
2. :
 - a. : [ipa0.ipadomain0.ru](#);
3. Web-:
 - a. [web-](#) , ;
 - b. : [web.ipadomain0.ru](#)

[web-](#) , [web-](#) . [web-](#) , . [web-](#) curl, [web-](#) .

[web-](#) Astra Linux [apache2](#). [apache2](#) , .



Astra Linux Special Edition:

, Astra Linux Special Edition (SSH), , .
[apache2](#) , :

```
systemctl start apache2  
systemctl enable apache2
```

[apache2](#) , :

```
sudo apt install apache2
```

Kerberos [apache2](#) Astra Linux :

- [libapache2-mod-auth-gssapi](#) - ;
- [libapache2-mod-auth-kerb](#) - .

:

- ([libapache2-mod-auth-gssapi](#)):

```
sudo apt install libapache2-mod-auth-gssapi
```

- ([libapache2-mod-auth-kerb](#)):

```
sudo apt install libapache2-mod-auth-kerb
```





() [FreeIPA](#) apache2 , Kerberos .

apache2

web-, apache2, . :

1. /etc/apache2/sites-available/auth-kerberos.conf :
 - . libapache2-mod-auth-gssapi:

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    <Directory /var/www>
        AuthType GSSAPI
        AuthName "test"
        #GssapiBasicAuth On
        GssapiCredStore keytab:<__>
        # 3 , ( web- Kerberos )
        #GssapiUseSessions On
        #Session On
        #SessionCookieName myapp_web_gssapi_session path=/my_url;httponly;secure;
        Require valid-user
    </Directory>
</VirtualHost>
```

web- apache2;

- . libapache2-mod-auth-kerb:

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html/
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    <Directory /var/www/html/>
        AuthType Kerberos
        # (realm) -
        KrbAuthRealms <_>
        # ,
        KrbServiceName HTTP/<__>
        # ,
        Krb5Keytab /etc/apache2/keytab
        KrbMethodNegotiate on
        KrbMethodK5Passwd off
        require valid-user
        KrbSaveCredentials on
    </Directory>
</VirtualHost>
```

KrbMethodK5Passwd: on, web- Kerberos. web-;

2. web-, apache2:

```
sudo a2dissite 000-default.conf
```

3. web-:

```
sudo a2ensite auth-kerberos
```

4. /var/www/html/auth-kerberos web-:

```
sudo mkdir /var/www/html/auth-kerberos
```

5. /var/www/html/auth-kerberos /var/www/html/auth-kerberos/index.html web-:

```
<html>
<body>
<div style="width: 100%; font-size: 40px; font-weight: bold; text-align: center;">
    Kerberos.
</div>
</body>
</html>
```

6. web- /etc/apache2/apache2.conf :

```
AddDefaultCharset UTF-8
```

7. Astra Linux Special Edition: /etc/apache2/apache2.conf AstraMode off:

```
AstraMode off
```

Kerberos FreeIPA

1. :
a. :

```
kinit admin
```

- b.

```
ipa service-add HTTP/<__web->
```

2. web-:
a. :

```
sudo kinit admin
```

- b. :

```
sudo ipa-getkeytab -s ipa0.ipadomain0.ru -k /etc/apache2/keytab -p  
HTTP/`hostname`
```

- c. :

```
sudo chown www-data:www-data /etc/apache2/keytab
```

3. apache2:

```
sudo systemctl restart apache2
```

Kerberos ALD

ALD , FreeIPA, . ALD :

1. :

```
ald-admin service-add HTTP/<__web->
ald-admin sgroup-svc-add HTTP/<__web-> --sgroup=mac
```

2. web- :

```
keytab="/etc/apache2/keytab"
ald-client update-svc-keytab HTTP/`hostname` --ktfile="$keytab"
chown www-data "$keytab"
chmod 644 "$keytab"
```

3. apache2:

```
sudo systemctl restart apache2
```

apache2 http://<__web->. curl. , Kerberos Kerberos, KRB5CCNAME. , KRB5CCNAME .

1. :

a. web- :

```
curl http://`hostname`/auth-kerberos

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
are authorized to access the document
requested. Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
<hr>
<address>Apache/2.4.46 (Debian) Server at web.ipadomain0.ru Port
80</address>
</body></html>
```

b. Kerberos:

```
kdestroy
```

c. Kerberos:

```
curl --negotiate -u : http://`hostname`/auth-kerberos/

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
```

```
are authorized to access the document
requested. Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
<hr>
<address>Apache/2.4.46 (Debian) Server at web.ipadomain0.ru Port
80</address>
</body></html>
```

2. ;

a. Kerberos:

```
kinit admin
```

b. , KRB5CCNAME ,:

```
echo $KRB5CCNAME
KEYRING:persistent:67200
```

(Kerberos) ., , :

```
FILE:/tmp/krb5cc_1000
```

klist: klist .:

i. :

```
klist

Ticket cache: KEYRING:persistent:1000:1000
Default principal: admin@IPADOMAIN0.RU

Valid starting      Expires            Service principal
03.11.2021 11:26:24  04.11.2021 11:26:22  krbtgt/IPADOMAIN0.
RU@IPADOMAIN0.RU
```

ii. :

```
export KRB5CCNAME=KEYRING:persistent:1000:1000
```

c. Kerberos:

```
curl --negotiate -u : http://`hostname`/auth-kerberos/

<html>
<body>
<div style="width: 100%; font-size: 40px; font-weight: bold; text-
align: center;">
    Kerberos.
</div>
</body>
</html>
```

web-

web-, , web- negotiate.

web- Mozilla Firefox

web- Mozilla Firefox , about:config, negotiate.

```
network.negotiate-auth.trusted-uris
```

, , http- https-,,,:

```
http://, https://
```

Mozilla Firefox

```
network.negotiate-auth.delegation-uris
```

, . KRB5CCNAME., php :

```
putenv("KRB5CCNAME=".$_SERVER['KRB5CCNAME']);
```

web- Konqueror

Konqueror .