Kerberos / Spnego

**Kerberos** is a network authentication protocol for client/server applications, and **SPNEGO** provides a mechanism for extending **Kerberos** to Web applications through the standard HTTP protocol.

# Kerberos Server on Linux, pgAdmin on MAC & Browsing pgAdmin through FireFox from Linux Client

This is a multi-node setup (on Ubuntu), with a client, Kerberos Server and pgAdmin server on MAC. All three machines could be the same, but that would make the instructions confusing for people trying to use multiple nodes.

1. Ensure all hosts are in DNS or hosts files on each machine:  
     
   192.168.26.167 krb5.pgadmin.org (KDC)

192.168.86.1 mytest.pgadmin.local (pgAdmin)

192.168.26.168 krb5-client.pgadmin.org (Client/Browser machine)

1. On krb5-server, install the required software:  
     
   $ sudo apt install krb5-kdc krb5-admin-server  
     
   When prompted, set the realm to PGADMIN.ORG and the server and admin server to krb5.pgadmin.org.  
     
   Note that the krb5 service may fail to start. Don't worry about that.
2. Create the new realm:  
     
   $ sudo krb5\_newrealm
3. Start the kerberos server:  
     
   $ sudo systemctl start krb5-kdc
4. Create the admin user to manage principals:  
     
   $ sudo kadmin.local  
   Authenticating as principal root/admin@PGADMIN.ORG with password.  
   kadmin.local: addprinc root/admin  
   WARNING: no policy specified for root/admin@PGADMIN.ORG; defaulting to no policy  
   Enter password for principal "root/admin@PGADMIN.ORG":  
   Re-enter password for principal "root/admin@PGADMIN.ORG":  
   Principal "root/admin@PGADMIN.ORG" created.  
   kadmin.local: exit
5. Create the access control file for the admin principal:  
     
   $ sudo vim /etc/krb5kdc/kadm5.acl  
   root/admin@PGADMIN.ORG \*
6. Restart the admin service:  
     
   $ sudo systemctl restart krb5-admin-server
7. Run a quick test:  
     
   $ klist  
   klist: No credentials cache found (filename: /tmp/krb5cc\_1000)  
   $ kinit root/admin  
   Password for root/admin@PGADMIN.ORG:  
   $ klist  
   Ticket cache: FILE:/tmp/krb5cc\_1000  
   Default principal: root/admin@PGADMIN.ORG  
     
   Valid starting Expires Service principal  
   2020-08-12 17:18:58 2020-08-13 03:18:58 krbtgt/PGADMIN.ORG@PGADMIN.ORG  
   renew until 2020-08-18 17:18:51
8. krb5-client, install the client packages:  
     
   $ sudo apt install krb5-user libpam-krb5 libpam-ccreds  
     
   Enter the server and realm details as before.
9. Add the principal for the Linux user account:$ sudo kadmin.local  
   kadmin.local: addprinc khushboovashi  
   WARNING: no policy specified for khushboovashi@PGADMIN.ORG; defaulting to no policy  
   Enter password for principal "khushboovashi@PGADMIN.ORG":  
   Re-enter password for principal "khushboovashi@PGADMIN.ORG":  
   Principal "khushboovashi@PGADMIN.ORG" created.
10. Add the principal for HTTP (This would be used for Spnego):  
      
    $ sudo kadmin.local  
    kadmin.local: addprinc -randkey HTTP/mytest.pgadmin.local

WARNING: no policy specified for HTTP/mytest.pgadmin.local@PGADMIN.ORG; defaulting to no policy  
Enter password for principal "HTTP/mytest.pgadmin.local@PGADMIN.ORG":  
Re-enter password for principal "HTTP/mytest.pgadmin.local@PGADMIN.ORG":  
Principal "HTTP/mytest.pgadmin.local@PGADMIN.ORG" created.

1. Create a keytab file for HTTP:  
     
   $ sudo kadmin.local

kadmin.local: ktadd -k pgadmin.keytab HTTP/mytest.pgadmin.local

Entry for principal HTTP/mytest.pgadmin.local with kvno 2, encryption type aes256-cts-hmac-sha1-96 added to keytab WRFILE:pgadmin.keytab.

Entry for principal HTTP/mytest.pgadmin.local with kvno 2, encryption type aes128-cts-hmac-sha1-96 added to keytab WRFILE:pgadmin.keytab.  
kadmin.local: exit

1. Copy the pgadmin.keytab file to mytest.pgadmin.local (pgadmin server) machine and ensure it's owned by the local user
2. On Mac, install pgAdmin or setup dev environment:

Set below parameters into config\_local.py

AUTHENTICATION\_SOURCES = [**'kerberos'**]

KERBEROS\_AUTO\_CREATE\_USER = **True**

KRB\_APP\_HOST\_NAME = 'mytest.pgadmin.local' (if not set, will take the default\_server value)

If you haven’t set the default\_keytab\_name in krb5.conf or haven’t set the *KRB\_KTNAME environment variable then, explicitly set this*

*KRB\_KTNAME = '/Users/khushboovashi/Desktop/pgadmin\_latest.keytab'*

1. On Mac, install kerberos  
   brew install krb5
2. Edit krb5.conf file

sudo vi /etc/krb5.conf

[libdefaults]

default\_realm = PGADMIN.ORG

default\_keytab\_name = file:/<pgadmin.keytab location>

[domain\_realm]

.org = PGADMIN.ORG

Pgadmin.org = PGADMIN.ORG

1. Check that authentication works on krb5-client:  
     
   khushboovashi@krb5-client:~$ klist  
   klist: No credentials cache found (filename: /tmp/krb5cc\_1000)  
   khushboovashi@krb5-client:~$ kinit khushboovashi  
   Password for khushboovashi@PGADMIN.ORG:  
   khushboovashi@krb5-client:~$ klist  
   Ticket cache: FILE:/tmp/krb5cc\_1000  
   Default principal: khushboovashi@PGADMIN.ORG  
     
   Valid starting Expires Service principal  
   2020-08-12 18:21:48 2020-08-13 04:21:48 krbtgt/PGADMIN.ORG@PGADMIN.ORG  
   renew until 2020-08-13 18:21:38
2. On krb5-client, set the Firefox browser to use the Spnego/Kerberos

* Open **Firefox** and enter about:**config** in the address bar. Dismiss any warnings that appear.
* In the Filter field, enter **negotiate**.
* Double-click the network.negotiate-auth.trusted-uris preference.
* In the dialog box, enter the domain, mytest.pgadmin.local
* Click the OK button. The domain that you just entered in the network.
* Now browse mytest.pgadmin.local:<port> from the linux firefox browser

WSGI application under Apache HTTPD:

<Virtualhost \*:80>

ServerName mytest.pgadmin.local

WSGIDaemonProcess pgadmin user=www-data group=www-data threads=5 python-home=/home/khushboovashi/venv3.6

WSGIScriptAlias /pgadmin /home/khushboovashi/venv3.6/lib/python3.6/site-packages/pgadmin4/pgAdmin4.wsgi

<Directory /home/khushboovashi/venv3.6/lib/python3.6/site-packages/pgadmin4>

**WSGIScriptReloading On**

**WSGIPassAuthorization On**

WSGIProcessGroup pgadmin

WSGIApplicationGroup %{GLOBAL}

Require all granted

</Directory>

</Virtualhost>