Single-sign-on (SSO) authentication is now required more than ever. Nowadays, almost every website requires some form of authentication to access its features and content. With the number of websites and services rising, a centralized login system has become a necessity. This guideline explaining how SSO authentication is implemented for the web and provide a working example using Apache server with mod\_mellon(for apache).

Main goal to provide access to application on port 80 to customer with authorization through idP.

Requirements:

I) CentOS 7 64-bit

Docker container with application on localhost port 80

SSL certificate generated.

II) Console configuration:

Commands for apache:

sudo systemctl restart httpd

sudo systemctl stop httpd

sudo systemctl start httpd

logs - /var/log/httpd

1) Versions of installed packages:

rpm -qa | grep httpd

httpd-tools-2.4.6-40.el7.centos.4.x86\_64

httpd-2.4.6-40.el7.centos.4.x86\_64

rpm -qa | grep mellon

mod\_auth\_mellon-0.11.0-1.el7.x86\_64

yum install httpd mod\_ssl

yum install mod\_auth\_mellon.x86\_64

vim sudo /etc/httpd/httpd.conf

2) Apache config files:

2.1) Conf.d:

<VirtualHost \*:443>

ServerName projects.com

SSLEngine on

ProxyRequests Off

ProxyPreserveHost On

<Proxy \*>

AddDefaultCharset off

Order deny,allow

Allow from all

</Proxy>

SSLCertificateFile /etc/pki/tls/certs/tkmi-repl.projects.com.cer

SSLCertificateKeyFile /etc/pki/tls/private/tkmi-repl.projects.com.key

RequestHeader set X-Forwarded-Proto "https"

RequestHeader set X-Forwarded-Port "443"

#Proxy for mellon is disabled!!!

ProxyPass /mellon/ !

#Reverse proxy to application

ProxyPass / http://localhost:80/

ProxyPassReverse / http://localhost:80/

</VirtualHost>

<Location />

Require all granted

AuthType "Mellon"

MellonEnable "auth"

MellonSPMetadataFile /etc/httpd/mellon/https\_questions.tkmi\_repl.projects.com.xml

MellonSPPrivateKeyFile /etc/httpd/mellon/https\_questions.tkmi\_repl.projects.com.key

MellonSPCertFile /etc/httpd/mellon/https\_questions.tkmi\_repl.projects.com.cert

MellonIdPMetadataFile /etc/httpd/mellon/MetadataFile.xml

MellonIdPCAFile /etc/httpd/mellon/ADFS\_Cert\_base64.cer

MellonPostReplay On

MellonCookiePath /

MellonSecureCookie Off

MellonEndpointPath /mellon

MellonVariable "sso-cookie"

MellonUser "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"

MellonSetEnv "upn" "<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn>"

#set available field in request

RequestHeader unset LOGON\_USER

RequestHeader set LOGON\_USER "%{MELLON\_upn}e" env=MELLON\_upn

</Location>

Listen 443

2.2) Conf.ssl

sudo vim /etc/httpd/conf.d/ssl.conf

#For disabling SSLv3 proto

SSLProtocol All -SSLv2 -SSLv3

#Listen 443 https

SSLCertificateFile /etc/pki/tls/certs/tkmi-repl.projects.com.cer

SSLCertificateKeyFile /etc/pki/tls/private/tkmi-repl.projects.com.key

3) Creating certificates for mellon:

/usr/libexec/mod\_auth\_mellon/mellon\_create\_metadata.sh https://projects.com https://projects.com/mellon

4) Ensure that NameID policy in Metadata.xml (mellon metadata file generated on step 4) set to unspecified:

<NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat>

5) Comment out SAML Redirect Binding metadata in Metadata.xml as follows:

Metadata.xml comment block

<!--SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="idP URL"/-->

II)

https://idpSite.com:44301/entries/view?id=https%3A%2F%2Fprojects.com&kind=RelyingParty

Tab General:

Identifiers https://projects.com

Tab SAML-SECURITY (add mellon cert):

Signed SAML requests requiredNo

Signature algorithmSHA-1

Signing certificates

Subj: CN=projects.com, Valid: mm/dd/yyyy-mm/dd/yyyy

Tab SAML:

Assertion Consumer POST Yes 0 https://projects.com/mellon/postResponse