Manual:Extension/LDAPAuthentication/SSO

Contents

About this manual

In this manual we will use certain placeholders. Replace them due to the following steps analogical to your system environment.

- `example.local` = your domain name
- `webserver.example.local` = FQDN of your bluespice webserver
- `dc.example.local` = FQDN of your domain controller

Preparation

Please make sure that you configured a working "A" record at your DNS server for `webserver.example.local` **and** (really necessary!) an reverse DNS record (PTR). Please make also sure that the system clocks do not differ more than 5 minutes.

Needed users in the Active Directory

You need to create the following users in your Active Directory

- One user for your Kerberos authentication (We will call it "KerberosProxy" at this manual)
- One user for your BlueSpice AD proxy user (We will call it "LdapProxy" at this manual)

Please create these users and configure the passwords to "never expire".

Create a keytab file

Create a keytab file at your domain controller using this command (works on Windows >= 2018 R2):

```
$ ktpass -princ HTTP/webserver.example.local@EXAMPLE.LOCAL
-mapuser KerberosProxy@EXAMPLE.LOCAL
-crypto RC4-HMAC-NT
-ptype KRB5_NT_PRINCIPAL
-pass <password-of-KerberosProxy>
-out bluespice.keytab
```

Move this file to your BlueSpice server (folder `/etc`).

Install required packages on CentOS

Install all packages you need for Kerberos:

```
$ yum install krb5-workstation mod_auth_kerb
```

Create Kerberos configuration

Create a backup of `/etc/krb5.conf` and clear the file content. Insert this new content:

```
[libdefaults]
         default_realm = EXAMPLE.LOCAL

[realms]
         EXAMPLE.LOCAL = {
                 kdc = dc.example.local
                 admin_server = dc.example.local
         }

[domain_realm]
         example.local = EXAMPLE.LOCAL
         .example.local = EXAMPLE.LOCAL
```

Test authentication with your Keytab-file

Now you can test your authentication with the keytab file which was created before:

```
$ kinit -VV -k -t /etc/bluespice.keytab HTTP/webserver.example.local
```

If everything is configured correctly you should get a success message:

```
Authenticated to Kerberos v5
```

Secure your BlueSpice webroot with Kerberos

Now you have to secure the BlueSpice DocumentRoot with. Open your VirtualHost config and insert the following:

```
<VirtualHost *:443>
        ...
        <Directory /path/to/DocumentRoot>
                AuthType Kerberos
                KrbAuthRealms EXAMPLE.LOCAL
                KrbServiceName HTTP/webserver.example.local@EXAMPLE.LOCAL
                Krb5Keytab "/etc/bluespice.keytab"
                KrbMethodNegotiate on
                KrbMethodK5Passwd on
                Require valid-user
        </Directory>
        ...
</VirtualHost>
```

Restart your apache2 webserver.

Testing

Create a file `test.php` at the DocumentRoot of BlueSpice and insert this code:

```
<?php
echo $_SERVER['REMOTE_USER'];
```

If everyting works fine you should be able to open `test.php` with a webbrowser (not Firefox!) without getting an authentication window and you can see your windows user name at the `test.php`. Now delete `test.php`.

User permission to autocreate account

Make sure that the wiki user group `*` has the `autocreateaccount` permission in the PermissionManager of BlueSpice.

PHP-extension for ldap

Make sure that `php-ldap` is installed and loaded at your apache2 server.