

SSO AD

Introdução

Pretende-se o desenvolvimento de uma funcionalidade no ecrã de login do portal, que permita aos utilizadores de domínio da CM Porto, entrarem diretamente no sistema (SSO - Single Sign On).

Uma vez que o portal está instalado num servidor linux, com apache como serviço http web, a integração passa por instalar e configurar um conjunto de extensões que permitem a comunicação entre este servidor e o servidor de domínio da AD (Active Directory).

Configurar Controlador de Dominio (KDC)

No Controlador de Domínio

Criar um utilizador no controlador de dominio, para efeitos de autenticação do servidor web na AD.

- Nome de utilizador: humanportal
- Definir uma palavra passe forte
- Definir "password nunca expira"
- Utilizador tem de pertencer ao grupo "Utilizadores de Domínio" (Domain Users)

Definir SPN (Service Principal Name) para webservice (mapeia SPN HTTP/<servidor web>.cm-porto.net ao utilizador humanportal):

- Abrir terminal "PowerShell" como administrador
- Executar os seguintes comandos:
 - > setspn -A HTTP/<web server> CM-PORTO\humanportal
 - > mkdir c:\temp
 - > ktpass -princ HTTP/<web server>@CM-PORTO.NET -mapuser CM-PORTO\humanportal -pass <password> -out C:\temp\webserver.keytab -pType KRB5_NT_PRINCIPAL -crypto **AES256-SHA1**
 - enviar ficheiro C:\temp\webserver.keytab à humansoft
 - * enviar credenciais do utilizador humanportal à humansoft, para efeitos de testes em qualidade
 - * o ficheiro keytab será usado para autenticação kerberos, no servidor web.

No servidor web:

- copiar o ficheiro gerado c:\temp\webserver.keytab para o webserver linux em /etc/apache2/webserver.keytab

- atribuir o owner como o apache: `sudo chmod www-data:www-data /etc/apache2/webserver.keytab`
- atribuir permissões: `chmod 600 /etc/apache2/webserver.keytab`
- verificar se ficheiro está bem definido: `klist -k -t /etc/apache2/webserver.keytab`
 - klist deverá mostrar o *principal* HTTP/<webserver>.cm-porto.pt@CM-PORTO.NET
- usar o comando kinit para autenticar SPN (Service Principal Name):
 - `> kinit -k -t /etc/apache2/webserver.keytab HTTP/<web server>@CM-PORTO.NET`
 - este comando irá obter um ticket kerberos para o webservice ospedado no servidor linux.

Instalar Kerberos e LDAP (servidor web)

```
> sudo apt install php8.3-ldap libsasl2-modules-gssapi-mit libsasl2-dev
```

```
> sudo apt-get install krb5-config krb5-locales libpam-krb5
```

```
> sudo apt-get install libapache2-mod-auth-gssapi (ou mod_auth_gssapi)
```

verificar a instalação:

```
> kinit --version
```

```
> ls /usr/lib/apache2/modules/ | grep gssapi
```

Ativar mod_auth_gssapi no apache:

```
> sudo a2enmod auth_gssapi
```

```
> sudo service apache2 restart
```

```
> sudo apache2ctl -M | grep gssapi
```

Configurar Kerberos

```
> sudo nano /etc/krb5.conf
```

[libdefaults]

```
default_realm = CM-PORTO.NET
dns_lookup_realm = false
dns_lookup_kdc = false
ticket_lifetime = 365d
forwardable = true
```

[realms]

```
CM-PORTO.NET = {
```

```
kdc = <controlador de dominio>.cm-porto.net
admin_server = <controlador de dominio>.cm-porto.net
}
```

```
[domain_realm]
.cm-porto.net = CM-PORTO.NET
cm-porto.net = CM-PORTO.NET
```

* Substituir CM-PORTO.NET pelo FQDN (Fully Qualified Domain Name) do controlador de domínio (KDC)

Verificar resolução do nome do controlador de dominio, a partir do servidor web:

```
> nslookup <controlador de dominio>.cm-porto.net ou

> ping <controlador de dominio>.cm-porto.net

* se falhou, adicionar a /etc/hosts
```

Verificar se porta do KDC está aberta:

```
> telnet dc1.humansoft.pt 88
```

Verificar se ficheiro keytab está bem configurado:

```
> sudo klist -k /etc/krb5.keytab
```

Configurar Apache

```
<VirtualHost *:433>
ServerName webserver.humansoft.pt
...
<Directory <pasta do portal>/sessions/doLoginSsoAd>
AuthType GSSAPI
AuthName "Kerberos Login"
GssapiCredStore keytab:/etc/apache2/webserver.keytab
Require valid-user
# Enable SPNEGO support (Negotiate protocol)
GssapiUseSessions On
GssapiLocalName On
</Directory>
...
</VirtualHost>
```

Configurar os browsers para usarem kerberos automaticamente

Microsoft Edge (on Windows):

1. Abrir **Opções de Internet** (a partir do Painel de Controlo ou a partir do browser).
2. Clicar no separador **Segurança**.
3. Selecionar a zona (**Intranet** ou **Trusted Sites** dependendo das configurações da rede).
4. Adicionar o url do portal.

Revision #5

Created 2 October 2024 08:45:07 by humansoft

Updated 9 October 2024 16:44:36 by humansoft