3.27 – Active Directory, Azure AD, LDAP, RADIUS integration

> **Create configuration files easily**
>
> Click here to go to the customizer for the integration of authentication services. Fast, simple, secure. No data is stored on the server!
>
> To the customizer →

You can authenticate your users against Active Directory, LDAP or RADIUS server. Please configure your users.json as followings:

Active Directory or LDAP

```
{
  "source": {
    "type": "AD",
    "properties": {
      "server": "192.168.12.128:389", //can also be specified without the port
      "domain": "mydomain.com",
      "groups": "sales, support",
      "transferCredential": false
    }
  }
}
```

You can let gateway fetch servers from the AD. The following example will fetch all the servers from the "otherLoginWorkstations" attribute:

```
{
  "source": {
    "type": "AD",
    "properties": {
      "server": "192.168.12.128:389",
      "domain": "mydomain.com",
      "groups": "sales, support",
      "transferCredential": false,
      "serversAttr": "otherLoginWorkstations"
    }
  }
}
```

Gateway can also change AD user password if:

1. AD has SSL enabled.
2. Export the AD certificate (Public key only) in Base-64 encoded X.509 file format.
3. Import the AD certificate to Java keystore with following commands:

   ```
   cd JRE\bin (use JDK\bin instead if JRE is not found, for example, OpenJDK11).
   keytool -importcert -alias "anyName" -keystore \lib\security\cacerts -storepass changeit -file
   "C:\Users\username\Desktop\exported.cer"
   ```

   Please check Microsoft Tech Community Blog for more details on how to setup LDAPS on Windows.
4. users.json:

   ```
   {
     "source": {
       "type": "AD",
       "properties": {
         "server": "192.168.12.128:389",
         "secProtocol": "tls",
         "domain": "mydomain.com",
         "groups": "sales, support",
         "transferCredential": false,
         "serversAttr": "otherLoginWorkstations"
       }
     }
   }
   ```

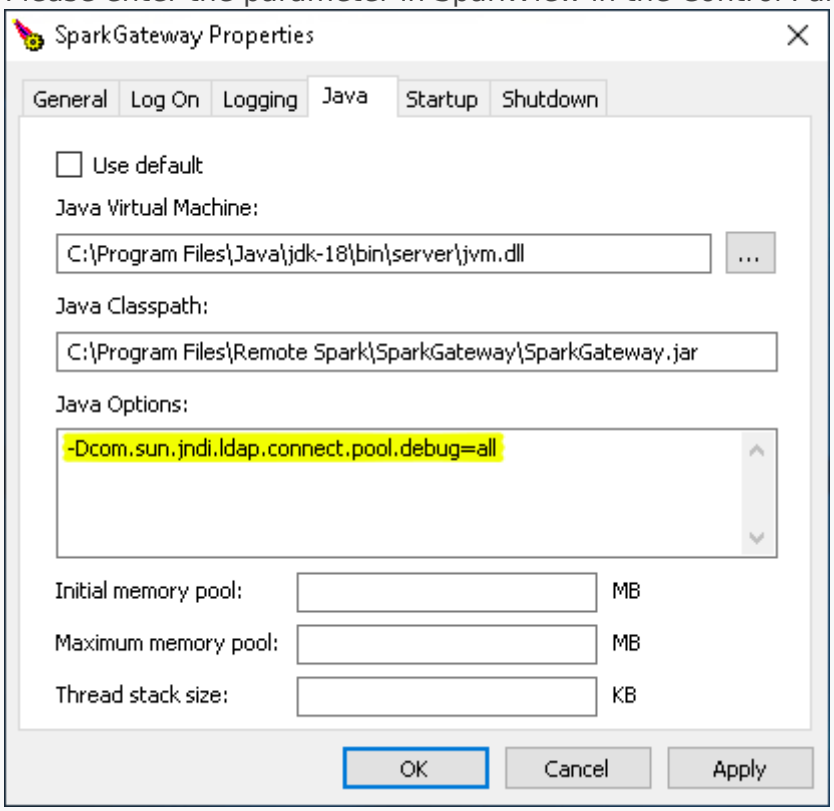
   "tls" or "ssl" can be used for the security protocol (secProtocol).

LDAP debugging

Get LDAP debug logs

If errors occur when trying to connect via LDAP, the following Java parameter can be stored in order to obtain more error information and logging for LDAP:
`-Dcom.sun.jndi.ldap.connect.pool.debug=all`

Please enter the parameter in SparkView in the Control Panel:



Prevent unmatched name issue

If the LDAP server is specified via an IP address and not the host name, unmatched name issues may occur. To prevent this, set the following Java parameter:
`-Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true`

RADIUS

```
{
  "source": {
    "type": "RADIUS",
    "properties": {
      "server": "192.168.12.128",
```

```
    "port": "1812",
    "accountingPort": "1813",
    "sharedSecret": "test123"
   }
  }
}
```

The sharedSecret can be gateway wide, can also be passed from the client side. Please check the source code of login.html for more information.

You also need to configure the servers in servers.json.

Azure AD

The Azure AD connection is essentially an OAuth2 connection. You can find more information about OAuth2 here.

To connect Azure AD, you need to create a JSON file (e.g. `providers.json`) with the following content, or extend an existing OAuth2 JSON file:

```
{
 "providers" : [
  {
   "name" : "Live",
   "client_id" : "40e0b9e5-a534-4bbe-98d2-f3ff0139b67f",
   "client_secret" : "UVH8Q~_e3MxQknUYzbo.bSy_lYafDBO_-R8pTWaCt",
   "request_uri" : "https://login.microsoftonline.com/common/oauth2/v2.0/authorize",
   "redirect_uri" : "https://www.mygateway.com/oauth2callback",
   "access_token_uri": "https://login.microsoftonline.com/common/oauth2/v2.0/token",
   "scope": "openid profile email"
  }
 ]
}
```

Please replace `https://www.mygateway.com` with the address of your SparkView server.

In the gateway.conf file, this file must then be linked (if not already done with an existing file):

`oauth2 = C:\\data\\oauth\\providers.json`

Please note that the endpoint name "common" in the URL may be different for you. You can find more information about this here:

https://learn.microsoft.com/en-us/azure/active-directory/develop/active-directory-v2-

protocols#endpoints

Revision #9
Created 5 April 2022 14:50:39 by Julian
Updated 10 January 2024 13:22:56 by Julian