org.clazzes.login.ldap

Functionality

The LDAP login service authenticates against users in an ADS domain or against users in an LDAP server configured for an individual domain.

The function `tryLogin()` needs credentials if run against a legacy LDAP Server.

For AD DS servers, an additional non-search authentication method `bindAds` is implemented for `tryLogin()`, which tries to bind using a principal in the form `user@domain`.

The functions `searchUser()`, `getGroups()`, `getGroupMembers()` need bind credentials and will only work in AD DS environments.

Sample Configuration for authentication against an ADS-Domain

The following sample configuration is the most common configuration OSGi configuration in PID `org.clazzes.login.ldap`, which allows you to authenticate users against an Active Directory Domain.

All you need to know is the Windows/NetBIOS Name of your domain and the corresponding DNS name used to physically locate the Active Directory server.

In our example we use `EXAMPLE` as the Windows/NetBIOS domain name with its DNS counterpart `example.com`.

Key	Value
`defaultDomain`	`EXAMPLE`
`domain.EXAMPLE.controllerUri`	`ads://example.com`
`domain.EXAMPLE.authMethod`	`bindAds`

Detailed Configuration

The LDAP login service may be configured using the OSGi configuration PID `org.clazzes.login.ldap` using these configuration values:

Key	Default Value	Description
`defaultDomain`		The domain to use for principals, which do not contain a domain.
`domain.<domain>.controllerUri`		The server to contact. Supported URL schemes: `ldap`, `ldaps`, `ads`. See below
`domain.<domain>.authMethod`	`searchAndBind`	The method for authenticating a user. Supported methods: `searchAndBind`, `bindAds`.
`domain.<domain>.bindUser`		The DN used for binding before searching something in the domain <domain>. For `tryLogin()` this applies only to the authMethod `searchAndBind`.
`domain.<domain>.bindPassword`		The password used for binding searching something in the domain <domain>. For `tryLogin()` this applies only to the authMethod `searchAndBind`.
`domain.<domain>.userAttribute`	`samAccountName`	The LDAP attribute to use for finding a given user name.
`domain.<domain>.prettyNameAttribute`	`cn`	The LDAP attribute to try to use as pretty name for users and groups.

`domain.<domain>.eMailAddressAttribute`	`mail`	The LDAP attribute to try to use as primary e-mail address for users.
`domain.<domain>.mobileAttribute`		The LDAP attribute to try to use as mobile phone number for users. This number is used to send ephemerals OTP for two-factor-authentication to the user. If this option is activated, two-factor signons are mandatory for this domain. Usually, this option is configured to the value `mobile` in order to activate ephemeral OTP two-factor-authentication.
`domain.<domain>.tokenIdsAttribute`		The LDAP attribute to try to use as a space separated list of 12-character YubiKey token IDs (like `cccccceiiuch`) for users. These token IDs are used to check token OTPs for two-factor-authentication to the user. If this option is activated, two-factor signons are mandatory for this domain. Usually, this option is configured to the value `pager` in order to activate token-based OTP two-factor-authentication.

There may be multiple domains in a configuration.

Controller Schemes

The URL schemes for a domain controller are ldap, ldaps and ads.

ADS controller scheme

The `ads` URL scheme for the URL `ads://mydomain.com` undertakes a lookup for the DNS records

```
SRV _ldap._tcp.mydomain.com
TXT _ldap._tcp.mydomain.com
```

to auto-detect the apropriate `ldap(s)` URI.

LDAP controller scheme

When directly specifying the LDAP-Server using an URL like `ldap://ldap-01.mydomain.com` it is possible to specify the baseDN for searches using a pseudo-path like in `ldap://ldap-01.mydomain.com/dc=mydomain,dc=com`

Manual installation in OSGi container

I some software product has pointed to this page for configuration details, the bundle is probably already installed in the OSGi container the software product runs in.

OSGi administrators maintaining an individual OSGi container can install the ldap-login-service bundle using these osgi commands:

```
obr:addurl http://maven.clazzes.org/repository.xml
obr:deploy ldap-login-service
```

Developer information

The maven artifact is:

```
<groupId>org.clazzes.login</groupId>
<artifactId>ldap-login-service</artifactId>
```