ldap.properties ファイルの変更

ldap.properties ファイルの変更

LDAP の URLや baseDN 、パスワードなどのプロパティ値を ldap.properties ファイルに設定します。
ここでは、 LDAP の標準ポートへ接続するプロパティ値を設定します。

/opt/shibboleth-idp/conf/ldap.properties ファイルを以下のように編集してください。

```
## Connection properties ##
idp.authn.LDAP.ldapURL = ldap://localhost  ← ポート指定を削除します。
idp.authn.LDAP.useStartTLS = false  ← 先頭の#を削除してコメントを解除し、falseを設定します。

（省略）

# Search DN resolution, used by anonSearchAuthenticator, bindSearchAuthenticator
# for AD: CN=Users,DC=example,DC=org
idp.authn.LDAP.baseDN = o=test_o,dc=ac,c=JP
idp.authn.LDAP.subtreeSearch = true  ← 先頭の#を削除してコメントを解除し、trueを設定します。
idp.authn.LDAP.userFilter = (uid={user})
# bind search configuration
# for AD: idp.authn.LDAP.bindDN=adminuser@domain.com
idp.authn.LDAP.bindDN = cn=olmgr,o=test_o,dc=ac,c=JP
```

他の設定がデフォルトのままであればbindDN/bindDNCredentialは属性取得でのみ使用されます。パスワード検証時は使用されず、匿名で接続しようとします。この後者の挙動を変更する場合は、anonSearchAuthenticatorと指定している部分をbindSearchAuthenticatorに修正してください。

なお、bindDN/bindDNCredentialに指定する値は、Shibboleth IdPバージョン2ではattribute-resolver.xmlのLDAP DataConnectorにprincipal/principalCredentialとして直接記述していたものです。また、古い学認テンプレートを使用している場合はここで記述したものが反映されませんので、可能な限り最新のattribute-resolver.xmlテンプレートを使用してください。

また、*.propertiesでは、パスワード等に&や<などの記号が含まれている場合でも&や<のような書き方はせずに&や<とそのまま記述してください。

最後に、運用開始後*.propertiesを更新することが必要になった場合は、reload-service.shによるリロードでは更新が反映されませんので、更新後Jettyを再起動してください。

BACK TOP NEXT