Grouper web services - authentication - Grouper LDAP

Grouper has built-in LDAP authentication for web service. This feature is in 2.1.4+. Pass the user/pass in basic auth (over SSL), and Grouper can bind to an ldap server. The username will be the subject id or identifier (or it can be manipulated).

Manage users

Manage users in your LDAP

Configure

Note the file locations in the container are listed in the v2.5 container documentation

File	Value	Description
grouper.hibernate.properties	grouper.is.ws.basicAuthn=false	This is the default provided with container, do not overlay
web.xml	Should be an empty element	This is the default provided with container, do not overlay
server.xml	ajp 8009 connector element: tomcatAuthentication="false"	This is the default provided with container, do not overlay Tomcat is not doing authn so that attribute needs to be false

grouper-ws.properties	<pre># to provide custom authentication (instead of the default httpServletRequest.getUserPrincipal()
	# for non-Rampart authentication. Class must implement the interface:
	# edu.internet2.middleware.grouper.ws.security.WsCustomAuthentication
	# class must be fully qualified. e.g. edu.school.whatever.MyAuthenticator
	# blank means use default: edu.internet2.middleware.grouper.ws.security.WsGrouperDefaultAuthentication
	# kerberos: edu.internet2.middleware.grouper.ws.security.WsGrouperKerberosAuthentication
	# ldap: edu.internet2.middleware.grouper.ws.security.WsGrouperLdapAuthentication
	ws.security.non-rampart.authentication.class = edu.internet2.middleware.grouper.ws.security.WsGrouperLdapAuthentication
	
	# if ldap authn should cache results
	ws.authn.ldap.cacheResults = true
	
	# if ldap authn should be used, which ldap connection name in the grouper-loader.properties should
	# be used for the connection to the ldap
	ws.authn.ldap.grouperLoaderLdapConfigId = personLdap
	
	# OPTION 1 - use loginDnPrefix and loginDnSuffix
	# if ldap authn should be used, this is the prefix of the userId when connecting to ldap, e.g. uid=
	ws.authn.ldap.loginDnPrefix =
	
	# if ldap authn should be used, this is the suffix to the userId when connecting to ldap, e.g. ,ou=users,dc=school,dc=edu
	ws.authn.ldap.loginDnSuffix =
	
	# OPTION 2 - use findUserBase and findUserFilter (available Grouper v2.5.23+)
	# if ldap authn should be used, this is the search base to find the user, e.g. dc=school,dc=edu
	ws.authn.ldap.findUserBase =
	
	# if ldap authn should be used, this is the filter to find the user. {username} is substituted with what's provided as the username. e.g. (uid={username})
	ws.authn.ldap.findUserFilter =</pre>
		Overlay the grouper-ws.properties or configure in the database. Note the LDAP config is in the grouper-loader.properties file

grouper-www.conf	Do not have any authn directives here	This is the default provided with container, do not overlay

DEBUG

Note, if you want to debug this, put this in the log4j.properties:

```
log4j.logger.edu.internet2.middleware.grouper.ws.security.WsGrouperLdapAuthentication = DEBUG
```