External systems configuration

In Grouper v2.5.24+ there is re-organized configuration for external systems. In general this will consolidate most the credentials that grouper uses (except to its own database and morphString).

In the Grouper UI you can review all the configured external systems in one place with an easy-to-use UI.

In general the configuration will not change so that few or no changes are needed to leverage the new functionality, though a few of the provisioners will need to be adjusted.

This will assume you are storing configuration in the database, since the UI needs to save its settings. If you do not want encrypted passwords in the database you will be able to enter a scriptlet to get the password from an environment variable or secrets manager or other place.

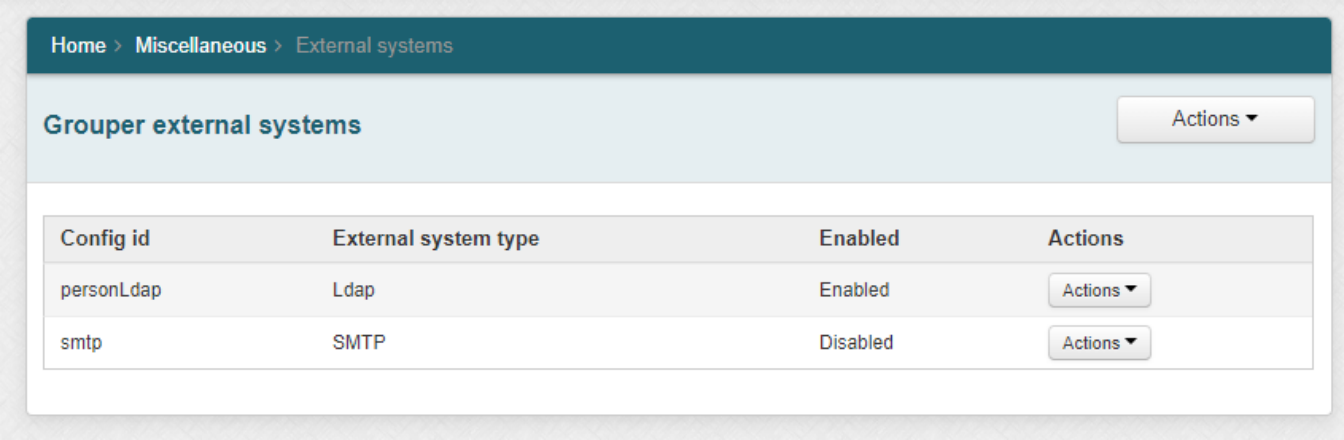
External systems in UI

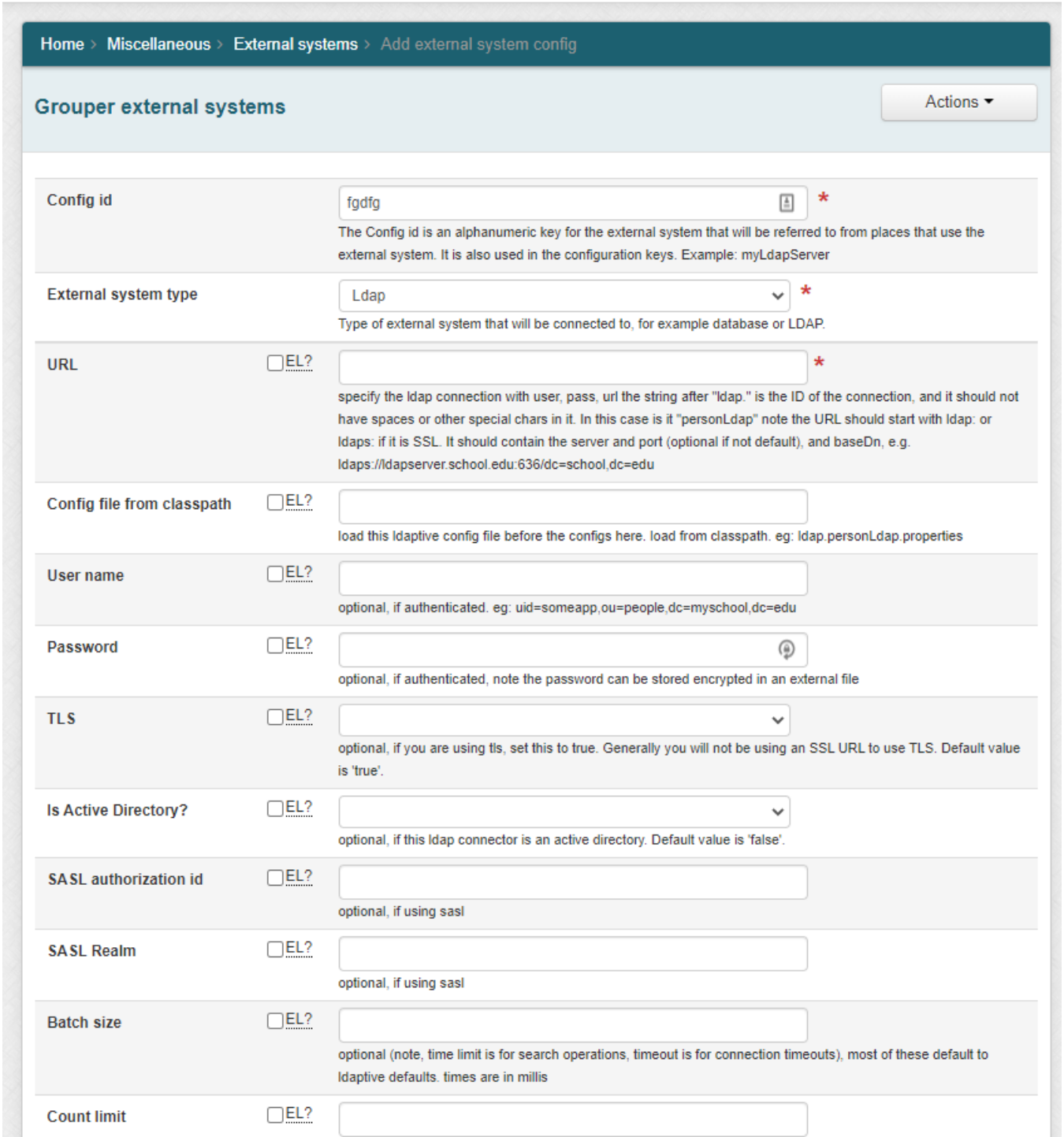
Access the configurations in Miscellaneous Administration External systems

Initial notes and limitations

- The enable/disable feature does not currently work. It is in the API so that Grouper features that use external systems can use that indicator to decide if it should enable/disable itself
- There is not a "test" button for all external systems, we need to implement those. Currently there is a "test" for SQL and LDAP.
- We will eventually have a screen that lists where each external system is used, it's not there yet.
- You probably need to restart Grouper when making changes to external systems

Screenshots





Identify the external systems and properties

Note, these lists will get out of date but they show the current configurations as of v2.5.24

LDAP connections in grouper-loader.properties

ldap.<connectionId>.attributeName

e.g. ldap.personLdap.url

https://www.ldaptive.org/v1/docs/guide/connections/pooling.html

Attribute	Type	Default	Notes
url	String		required. Explain that for provisioning the URL should point to one node for consistency
user	String		optional
pass	String		encrypted if a password. Save this like the configuration editor saves
configFileFromClasspath	String		
isActiveDirectory	Boolean		
tls	Boolean		
saslAuthorizationId	String		
saslRealm	String		
batchSize	Integer		
countLimit	Integer		
timeLimit	Integer		time limit for search operations in millis
timeout	Integer		timeout to get a connection in millis
minPoolSize	Integer	3	
maxPoolSize	Integer	10	
validateOnCheckIn	Boolean		
validateOnCheckOut	Boolean		defaults to true if all other validate methods are false
validatePeriodically	Boolean		
validateTimerPeriod	String	PT30M	
pruneTimerPeriod	String		
pagedResultsSize	Integer		needs to be equal to or less than the max result size server setting
referral	String		set to 'follow' if using AD and using paged results size and need this for some reason (generally you shouldnt)
validator	String		drop down. validator setup, currently supports CompareLdapValidator and SearchValidator. additional properties below for CompareLdapValidator.
validatorCompareDn	String		required for CompareLdapValidator. check this DN exists when saving connection. e.g. ou=people,dc=example,dc=com
validatorCompareAttribute	String		required for CompareLdapValidator. e.g. ou check this DN exists when saving connection
validatorCompareValue	String		required for CompareLdapValidator. e.g. people
searchResultHandlers	String		comma-delimited list of classes to process LDAP search results. Useful if AD returns a ranged attribute for large # groups (e.g., member;range=0-1499); include the GrouperRangeEntryHandler to handle progressive fetching.
searchIgnoreResultCodes	String		comma-delimited list of result codes (org.ldaptive.ResultCode) to ignore, e.g. TIME_LIMIT_EXCEEDED, SIZE_LIMIT_EXCEEDED, PARTIAL_RESULTS
enabled	Boolean	true	if this connector is enabled

Database from grouper-loader.properties

db.<connectionId>.attributeName

e.g. db.warehouse.url

Attribute	Type	Default	Notes
url	String		Required e.g. mysql: jdbc:mysql://localhost:3306/grouper?useSSL=false e.g. p6spy (log sql): [use the URL that your DB requires] e.g. oracle: jdbc:oracle:thin:@server.school.edu:1521:sid e.g. hsqldb (a): jdbc:hsqldb:dist/run/grouper;create=true e.g. hsqldb (b): jdbc:hsqldb:hsql://localhost:9001/grouper e.g. postgres (a): jdbc:postgresql://localhost:5432/database e.g. postgres (b): jdbc:postgresql://localhost:5432/database?currentSchema=mySchema e.g. mssql: jdbc:sqlserver://localhost:3280;databaseName=grouper
user	String		
pass	String		Save this like the configuration editor saves

driver	String		note: you probably dont have to enter a driver, it will detect from URL. If it cant detect, then specify it here. If this is not mysql, or postgres, make sure jar is in container. These are the defaults e.g. mysql: com.mysql.jdbc.Driver e.g. oracle: oracle.jdbc.driver.OracleDriver e.g. hsqldb: org.hsqldb.jdbcDriver e.g. postgres: org.postgresql.Driver
c3p0.max_size	Integer		optional pooling params, these will default to the grouper.hibernate(.base).properties pooling settings (get that value for the UI from that config)
c3p0.min_size	Integer		
c3p0.timeout	Integer		seconds
c3p0.max_statements	Integer		
c3p0.idle_test_period	Integer		
c3p0.acquire_increment	Integer		
c3p0.validate	Boolean		
c3p0. debugUnreturnedConnectionStackTraces	Boolean		if unreturnedConnectionTimeout is non zero, then if connection takes too long it will be logged as stack
c3p0.unreturnedConnectionTimeout	Integer		
enabled	Boolean	true	if this connector is enabled

Mail SMTP in grouper.properties

There is only one SMTP server in Grouper

mail.smtp.attributeName (configId is "default")

	Type	Default	Notes
server	String		required
user	String		
pass	String		use method from config editor to save
from.address	String		required. this is the default email address where mail from grouper will come from e.g. noreply@school.edu
ssl	Boolean		
starttls.enable	Boolean		
ssl.trust	String		if you are doing SSL/TLS, you should put the smtp server here so it is trusted
port	Integer	25 for non-ssl, 465 for ssl	
transport.protocol	String	smtp	
use.protocol.in.property. names	Boolean		in the java mail settings if "smtp" or whatever the protocol is should be in the property names
smtp.ssl.protocols	String		if you have trouble connecting to SSL/TLS, try a different SSL protocol, e.g. TLSv1.2
smtp.socketFactory.class	String		generally saying SSL true is enough, though you might need to set a class. generally leave this blank
smtp.socketFactory.fallback	Boolean		generally you will leave this blank unless doing something advanced
subject.prefix	String		prefix all email's subjects. e.g. TEST:
test.address	String		when running junit tests, this is the address that will be used
debug	Boolean		if debug info from java mail should be printed
enabled	Boolean	true	if this connector is enabled

SFTP server in grouper.properties

grouperSftp.site.configId.attributeName

e.g. grouperSftp.site.depot.host

Attribute	Type	Default	Notes

host	String		required
user	String		
password	String		password if not using private key
secret.privateKey	String textarea		note this is stored in secret.privateKey_0, secret.privateKey_0, if longer than 4k you can encrypt the private key to connect with. if its more than 4k encrypted, then take it in chunks and they will be concatenated # and use _0, _1, _2, etc. Note, replace newlines with $newline$ so it fits in a textfield
secret. privateKeyPassphrase			
knownHostsEntry			connect to the host, and copy the known_hosts entry for the host to connect to e.g. host.whatever ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEA3B00cx5W9KPSjzik3E
deleteTempFilesAfterSession			if any temporary files (e.g. private key and known hosts) should be deleted after session, default true
timeoutMillis		10000	timeout in millis
enabled	Boolean	true	if this connector is enabled

Azure endpoint in grouper.properties

grouper.azureConnector.<configId>.attributeName

e.g. grouper.azureConnector.myAzure.loginEndpoint

Attribute	Type	Default	Notes
loginEndpoint	String		login endpoint to get a token e.g. https://login.microsoftonline.com
DirectoryID	String		azure directory id e.g. 6c4dxxx0d
client_id	String		azure client id e.g. fd805xxxxdfb
client_secret	String, password		
resource	String		resource. generally same as graph endpoint e.g. https://graph.microsoft.com
graphEndpoint	String		e.g. https://graph.microsoft.com
graphVersion	String		e.g. v1.0
groupLookupAttribute	String		e.g. displayName
groupLookupValueFormat	String		e.g. ${group.getName()}
requireSubjectAttribute	String		e.g. netId
subjectIdValueFormat	String		${subject.getAttributeValue("netId")}@school.edu
enabled	Boolean	true	if this connector is enabled

Googleapps endpoint in grouper.properties

This is not externalized and is configured with the change log consumer, so this will need to be adjusts in the google provisioner code

grouper.googleConnector.<configId>.attributeName

e.g. grouper.googleConnector.myGoogle.domain

Attribute	Type	Default	Notes
domain	String		required. The Google managed domain name. (e.g. example.org)
serviceAccountEmail	String		required. The service account email address created by Google.
serviceAccountPKCS12File Path	String		required (either this or pass). The path of the PKCS12 file created and downloaded from Google. The OS account running Grouper needs to have read permissions to this file. Access to this file should be limited.
serviceAccountPKCS12Pass	String		required (either this or file path. If not reading from a file, this is the secret that is in the file
serviceImpersonationUser	String		This is the account that all actions will be made by. It needs to exists and will be the creator and modifier account associated with the Google auditing logs.
enabled	Boolean	true	if this connector is enabled

O365 endpoint in grouper.properties

See documentation at http://graph.microsoft.io/en-us/docs. Note the google provisioner will need to be adjust to read this config

grouper.o365Connector.<configId>.attributeName

e.g. grouper.o365Connector.myO365.tenantId

Attribute	Type	Default	Notes
tenantId	String		required
clientId	String		required
clientSecret	String password		required
idAttribute	String		
groupJexl	String		
enabled	Boolean	true	if this connector is enabled

Box connector

Note the box provisioner needs to be refactored to read this config

grouperClient.boxConnector.<configId>.attributeName

e.g. grouperClient.boxConnector.myConnector.privateKeyFileName

Attribute	Type	Default	Notes
privateKeyContents_0	String password		private key contents, can use multiple 0, 1, 2
privateKeyFileName	String		if not putting pem in database, you can put it on the filesystem, list the filename Note, either this or privateKeyContents_0 is required
privateKeyPass	String password		required
publicKeyId	String		required
enterpriseId	String		required
clientId	String		required
clientSecret	String password		required
proxyHost	String		
proxyPort	Integer		required if proxyHost is provided, cant be set if not
enabled	Boolean	true	if this connector is enabled

ActiveMQ in grouper.properties

grouper.activeMqConnector.<configId>.attributeName

e.g. grouper.activeMqConnector.myConnector.host

Note: activeMq needs refactoring to use these configs

Attribute	Type	Default	Notes
host	String		required
port	Integer	5672	
username	String		required
password	String password		
enabled	Boolean	true	if this connector is enabled

RabbitMQ in grouper.properties

grouper.rabbitMqConnector.<configId>.attributeName

e.g. grouper.rabbitMqConnector.myConnector.host

Attribute	Type	Default	Notes
host	String		required, host address of rabbitmq queue
virtualhost	String		virtual host address of rabbitmq queue
port	Integer		port of rabbitmq queue
username	String		required
password	String password		
tlsVersion	String		set the following three properties if you want to use TLS connection to rabbitmq. All three need to be populated. TLS Version. e.g. TLSv1.1
pathToTrustStore	String		path to trust store file
trustPassphrase	String password		trust passphrase
enabled	Boolean	true	if this connector is enabled

SQS in grouper.properties

grouper.sqsConnector.<configId>.propertyName

e.g. grouper.sqsConnector.myConnector.accessKey

Attribute	Type	Default	Notes
accessKey	String		required
secretKey	String password		required
enabled	Boolean	true	if this connector is enabled

Duo in grouper.properties

grouper.duoConnector.<configId>.propertyName

e.g. grouper.duoConnector.myConnector.adminDomainName

Attribute	Type	Default	Notes
adminDomainName	String		required endpoint domain name
adminIntegrationKey	String		required
adminSecretKey	String password		required
enabled	Boolean	true	if this connector is enabled

Remedy in grouper.properties

grouper.remedyConnector.<configId>.attributeName

e.g. grouper.remedyConnector.myConnector.url

Attribute	Type	Default	Notes
url	String		required
username	String		required
password	String password		required
enabled	Boolean	true	if this connector is enabled

Remedy digital marketplace in grouper.properties

grouper.remedyDigitalMarketplaceConnector.<configId>.attributeName

e.g. grouper.remedyDigitalMarketplaceConnector.myConnector.url

Attribute	Type	Default	Notes
url	String		required

username	String		required
password	String password		required
enabled	Boolean	true	if this connector is enabled

See also

Grouper Provisioning Framework