

Documento de Instalación

Proyecto

Sistema Gestor Documental SCJ



Historial de Revisiones

| **VERSIÓN** | **AUTOR** | **DESCRIPCIÓN** | **FECHA** |
| --- | --- | --- | --- |
| 1.0.0 | Dante Medina | Documento versión inicial | 19-06-2020 |
| 1.0.1 | Cristián Durán | Correcciones y mejoras al documento | 18-11-2020 |

Aprobaciones

| **APROBADO POR** | **NOMBRE** | **VERSIÓN**  **APROBADA** | **FECHA** |
| --- | --- | --- | --- |
| Jefe de Proyecto | Isabel Ulloa Naranjo | 1.0.0 |  |

INDICE

[**1.** Introducción 1](#_Toc60133464)

[1.1. Documentación Relacionada 2](#_Toc60133465)

[**2.** Consideraciones 3](#_Toc60133466)

[2.1. Consideraciones de instalación 3](#_Toc60133467)

[**3.** Instalaciones 4](#_Toc60133468)

[3.1. Instalación de Alfresco 4](#_Toc60133469)

[3.2. Configuracion de postgres 5](#_Toc60133470)

[3.3. Configuracion de alfresco 7](#_Toc60133471)

[3.3.1. Aplicar AMPs Alfresco 7](#_Toc60133472)

[3.3.2. Creación carpetas, permisos y aplicación de reglas 9](#_Toc60133473)

[3.4. Configuraciones sobre alfresco 11](#_Toc60133474)

[3.5. Configuracion de Wildfly 12](#_Toc60133475)

[3.6. Configuracion de aplicación web (SCJ) 13](#_Toc60133476)

[3.7. Configuracion de aplicación Carga Camunda (PHP) 15](#_Toc60133477)

[3.8. Configuracion de JMS transferencia archivo nacional 16](#_Toc60133478)

[3.9. Configuración BPM de prueba de sistema 17](#_Toc60133479)

1. Introducción

Este documento tiene como finalidad ser una guía para la instalación y configuración del sistema de Gestor Documental y todo su ecosistema. Esta guía muestra cómo realizar la instalación usando componentes de carácter comunitarios, Alfresco Community, Wildfly 19, LDAP, Tomcat y Postgresql. Todos estos componentes quedan instalados bajo una sola máquina. Se mostrara como realizar la configuración de cada uno de los componentes antes mencionados.

* 1. Documentación Relacionada

Para la construcción de este documento, se consideraron las siguientes referencias:

| **DOCUMENTO** | **ORGANIZACIÓN** | **DESCRIPCIÓN** |
| --- | --- | --- |
| ACHN0005-DOC\_Propuesta\_Tecnica\_Economica.doc | Tecnova | Documento que da el margen de trabajo propuesto por Tecnova aprobado por Archivo Nacional |
| ACHN0005 Documento\_Disenio\_Solucion.doc | Tecnova | Documento de diseño de solución presentado por Tecnova aprobado por Archivo Nacional |

Tabla 1: Documentación relacionada

1. Consideraciones
   1. Consideraciones de instalación

La instalación se realizó sobre una plataforma VMware de Archivo Nacional.

* Sistema Operativo Centos 7 KernelLinux 3.10.0-1127.10.1.el7.x86\_64
* Servidor de aplicaciones Wildfly 19
* Versión de componentes AlfrescoCommunity 5.1.0
  + Versión de PostgreSQL 9.4.4
  + Solr versión 4.0
  + Apache Tomcat 7.0.59
  + Activiti 5.20.0.0

1. Instalaciones
   1. Instalación de Alfresco

Prerrequisitos:

* El instalador es una herramienta grafica por lo que debe tener acceso a un ambiente con entorno gráfico.
* Ningún servicio debe estar ocupando el puerto 25 en la maquina donde se instalará Alfresco, para este propósito ejecute los siguientes comandos, como usuario root:
  + service postfix stop
  + chkconfig postfix off

El instalador se encuentra en /Gestor/alfresco en la Maquina o Dirección

* chmod a+x alfresco-community-installer-201602-linux-x64.bin
* ./alfresco-community-installer-201602-linux-x64.bin
* Seleccionar Idioma

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

* Tipo de Instalación Fácil: Instalación con configuración predeterminada

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

* Seleccionar carpeta  /opt/alfresco-community (HOME\_ALFRESCO)
* Especificar contraseña de administrador de Alfresco, (guardar la password)
* Registrar AlfrescoCommunity como servicio y continuar.
* En el paso final, seleccionar lanzar AlfrescoCommunity.
  1. Configuracion de postgres

La instalación de Alfresco posee una instancia de postgres que instala para su funcionamiento.

Para conocer y realizar la configuración seguir los siguientes pasos:

* service alfresco stop
* vim HOME\_ALFRESCO/alf\_data/postgresql/postgresql.conf
* descomentar la línea listen\_addresses y el valor debe ser ‘\*’ quedando de la siguiente forma, listen\_addresses = ‘\*’
* vim HOME\_ALFRESCO/alf\_data/postgresql/pg\_hba.conf (debe quedar como se adjunta la imagen, se recomienda respaldar la configuración anterior), posteriormente reiniciar servicio alfresco “service alfresco start”

Imagen que contiene Escala de tiempo

Descripción generada automáticamente

* Ingresar en una terminal “cd HOME\_ALFRESCO/postgresql/bin” y luego “./psql -U postgres”
  + postgres=# \password postgres
  + ingresar password y confirmar password
  + salir con \q
* Detener servicio alfresco (“service alfresco stop”) e ingresar vim HOME\_ALFRESCO/alf\_data/postgresql/pg\_hba.conf (cambiar la configuración como se ve en la imagen adjunta, guardar y reiniciar servicio alfresco)

Imagen que contiene Tabla

Descripción generada automáticamente

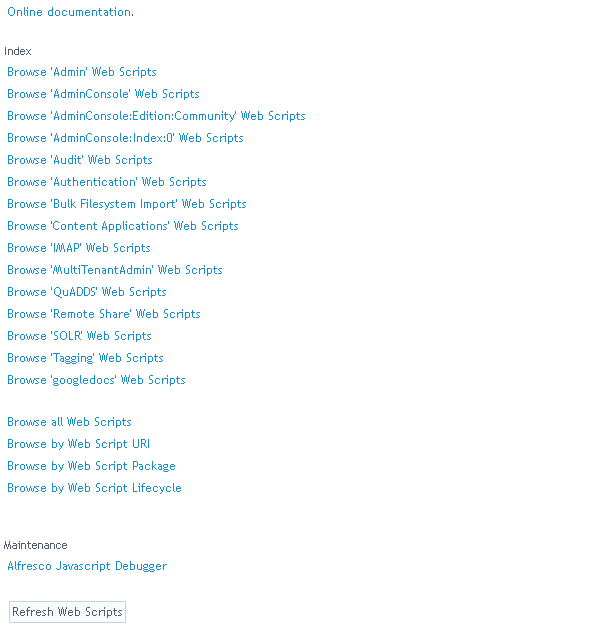
* Ingresar en una terminal “cd HOME\_ALFRESCO/postgresql/bin” y luego “./psql -U postgres”
* Ingresar las siguientes instrucciones:
  + postgres=# ALTER ROLE alfresco SUPERUSER NOCREATEDB CREATEROLE INHERIT LOGIN;
  + postgres=# \q
  + cd HOME\_ALFRESCO/postgresql/bin” y luego “./psql -U alfresco”
  + alfresco=#CREATE SCHEMA sgdp AUTHORIZATION alfresco;
  + alfresco=#ALTER SCHEMA sgdp OWNER TO alfresco;
  + alfresco=# CREATE USER sgdp WITH LOGIN NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE NOREPLICATION;
  + alfresco=# ALTER USER sgdp PASSWORD ‘xxxxxxxx’;
  + alfresco=# ALTER SCHEMA sgdp OWNER TO sgdp;
  + \q
* Ingresar a la Ruta del repositorio (Servicios\_Gestor/BD) y descargar los siguientes scripts y ejecutar en secuencia:
  + 00-ESTRUCTURA\_BD.sql
  + 01-CREATE\_SGDP\_ACCESOS.sql
  + 02-CREATE\_SGDP\_INSTANCIA\_PROCESO\_METADATA.sql
  + 03-CREATE\_SGDP\_TIPOS.sql
  + 04-ALTER\_SGDP\_INSTANCIAS\_DE\_PROCESOS.sql
  + 05-CREATE\_SGDP\_ARCHIVOS\_INST\_DE\_TAREA\_METADATA.sql
  + 06-ALTER\_SGDP\_ARCHIVOS\_INST\_DE\_TAREA.sql
  + 07-CREATE\_SGDP\_PARAMETROS\_ARCHIVO\_NACIONAL.sql
  + 08-CREATE\_SGDP\_CARGAS.sql
  + 09-CREATE\_SGDP\_DETALLES\_CARGA.sql
  + 10-CREATE\_SGDP\_LOG\_CARGA.sql

En el siguiente paso, es necesario modificar algunas rutas a servicios que se utilizaran en el gestor previamente a realizar la carga inicial del modelo de datos. Para realizar esta tarea es necesario conocer la IP de servidor donde está instalado alfresco, anotarla y luego realizar un reemplazo de la ip “192.168.1.92” a la ip del servidor de instalación.

* + 11-INSERT\_CARGA\_INICIAL.sql
  1. Configuracion de alfresco

Para terminar la instalación correcta de Alfresco, es necesario realizar los siguientes pasos:

* + 1. Aplicar AMPs Alfresco
* Detener servicio de alfresco y ejecutar las siguientes instrucciones:
  + service alfresco stop tomcat
  + rm -f HOME\_ALFRESCO/alf\_data/solr4/index/workspace/SpacesStore/index/\*
  + rm -f HOME\_ALFRESCO/alf\_data/solr4/index/archive/SpacesStore/index/\*
  + rm -f HOME\_ALFRESCO/alf\_data/solr4/model/\*
  + rm -rf HOME\_AFRESCO/alf\_data/solr4/content/\*
* Descargar del repositorio (Servicios\_Gestor\instalacion\amp) y copiar los archivos amp all-in-one-repo-amp-1.0-SNAPSHOT.amp y all-in-one-share-amp-1.0-SNAPSHOT.amp a los directorios HOME\_ALFRESCO/amps y a HOME\_AFRESCO/amps\_share respectivamente.
* Una vez copiados los archivos aplicar los amps ejecutar los siguientes comandos.
  + cd ALFRESCO\_HOME/bin
  + ./apply\_amps.sh
* Detener el servicio de alfresco y ejecutar los siguientes comandos:
  + service alfresco stop tomcat
  + rm -f HOME\_ALFRESCO/alf\_data/solr4/index/workspace/SpacesStore/index/\*
  + rm -f HOME\_ALFRESCO/alf\_data/solr4/index/archive/SpacesStore/index/\*
  + service alfresco start tomcat
  + curl <http://localhost:8080/solr4/admin/cores?action=FIX>
* Detener el servicio de alfresco y ejecutar los siguientes comandos:
  + service alfresco stop tomcat
  + cd HOME\_ALFRESCO/tomcat/webapps/alfresco/WEB-INF/classes/alfresco/extension/templates/webscripts/
  + rm -f subirCartas.post.json.ftl subirCartas.post.js subirCartas.post.desc.xml
  + ingresar al repositorio (Servicios\_Gestor\instalacion\xml) y reemplazar los archivos, sgdp-carpetas.xml y sgdp-documentos.xml en la carpeta HOME\_ALFRESCO/tomcat/webapps/alfresco/WEB-INF/classes/alfresco/module/all-in-one-repo-amp/model
  + service alfresco start tomcat
  + Abrir los puertos de la máquina virtual creada:
    - firewall-cmd --permanent --add-port=8080/tcp
    - firewall-cmd --reload
  + Ingresar http://<IP Instalación>:8080/alfresco/s/index .
  + Solicitará el password generado para el administrador de alfresco.



* Presionar sobre el botón “Refresh Web Script”.
  + 1. Creación carpetas, permisos y aplicación de reglas
* Ingresar a Alfresco share, http://<IP Instalación>:8080/share/page , ingresar las credenciales Nombre de usuario y contraseña.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

* Seleccionar el tab “Repositorio”, al cargar la pantalla seleccionar la opción crear la siguiente estructura de carpetas a partir de la Raiz:

.

└── Repositorio

├── Codigos\_QR

├── Imagenes

└── SCJ\_WORKSPACE

├── ARCHIVOS\_TEMPORALES

└── OPARTES

Seguir el orden de creación en la siguiente secuencia:

Nombre: SCJ\_WORKSPACE

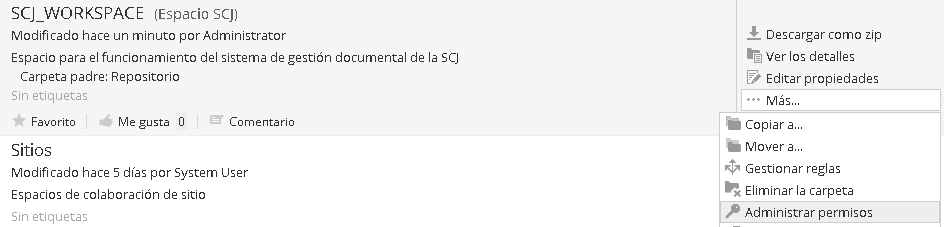
Título: Espacio SCJ

Descripción: Espacio para el funcionamiento del sistema de gestión documental de la SCJ

Carpeta padre: Repositorio

Inicialmente se heredarán permisos sobre esta carpeta, es necesario quitarlos.

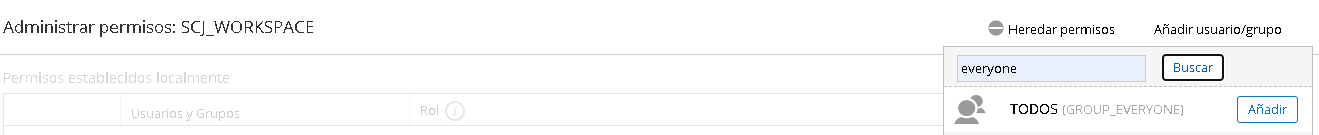
* En interfaz de repositorio ir a interfaz inicialmente creada, y presionar sobre más acciones y administrar permisos.



Luego presionar sobre “Heredar permisos”, esta opción quedara deshabilitada para esta carpeta.



Luego presionar sobre añadir usuario/grupo, y buscar el grupo “everyone” y presionar añadir:



Luego cambiar el rol a colaborador y guardar como se muestra en la siguiente imagen:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Nombre: OPARTES

Título: Oficina de Partes

Descripción: Espacio para el funcionamiento del sistema de gestión documental de la SCJ

Carpeta padre: SCJ\_WORKSPACE

Nombre: ARCHIVOS\_TEMPORALES

Título: ARCHIVOS\_TEMPORALES

Descripción: ARCHIVOS\_TEMPORALES

Carpeta padre: SCJ\_WORKSPACE

Nombre: Codigos\_QR

Título: Codigos\_QR

Descripción: Imágenes con los códigos QR de cada usuario

Carpeta padre: Repositorio

Nombre: Imagenes

Título: Imagenes

Descripción: Imagenes de firma simple

Carpeta padre: Repositorio

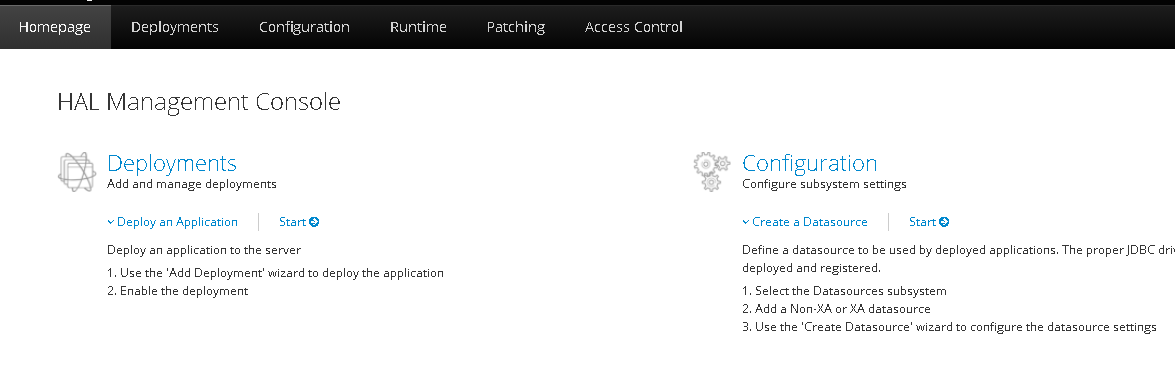
* 1. Configuraciones sobre alfresco

En los siguientes pasos en necesarios realizar otras configuraciones sobre alfresco.

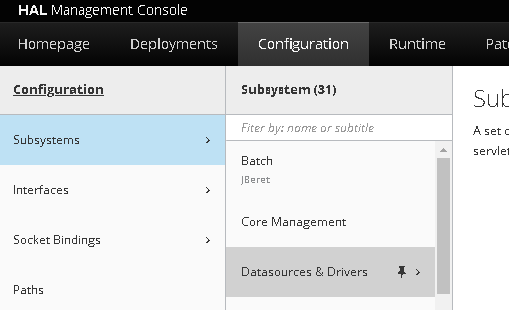
* Primero detener el servicio de tomcat de alfresco “service alfresco stop tomcat”.
* Obtener desde el repositorio (“Servicios\_Gestor\custom-authentication-repo”) el archivo “custom-authentication-repo-1.0-SNAPSHOT.jar” y copiarlo a la ruta: “/HOME\_ALFRESCO/tomcat/webapps/alfresco/WEB-INF/lib”.
* Reemplazar en la ruta: HOME\_ALFRESCO/tomcat/webapps/alfresco/WEB-INF/classes/alfresco/extension/templates/webscripts/, con los archivos que se encuentran en el repositorio en “Gestor\alfresco\web-scripts-alfresco-sgdp”.
* Reiniciar tomcat “service alfresco start tomcat”.
  1. Configuracion de Wildfly

En esta sección vamos a configurar el servidor de aplicaciones WildFly 19 que aloja la aplicación que trabaja con el gestor documental.

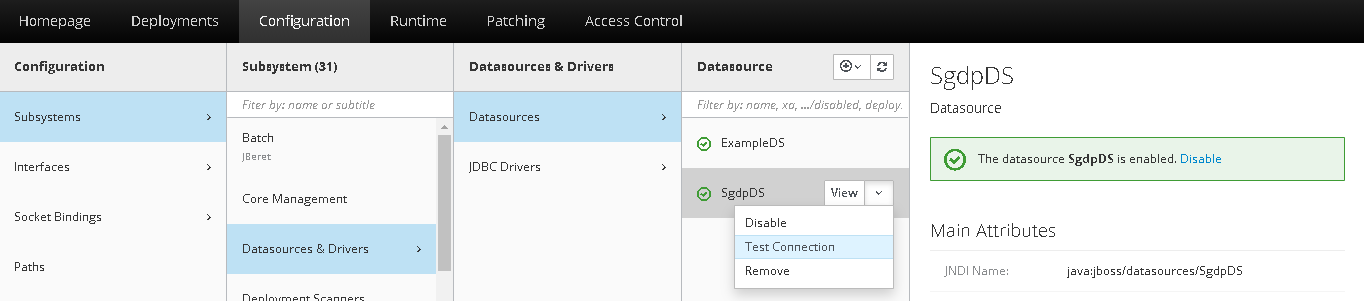
* Ingresar al repositorio y descargar el archivo wildfly-19.1.0.Final.zip, descomprimir en una ruta adecuada de trabajo que llamaremos HOME\_WILDFLY.
* Es necesario primero instalar el jdk de java con el siguiente comando (ejemplo en Centos 7):
  + sudo yum install java-1.8.0-openjdk.x86\_64
* Ingresar con un terminal a la ruta HOME\_WILDFLY y ejecutar los siguientes comandos:
  + cd HOME\_WILDFLY/bin
  + sh ./add-user.sh
  + Crear un usuario “Management User” y apuntar sus datos ya que serán requerimos para la administración del servidor de aplicaciones.
  + Cuando realice la pregunta “Is this new user going to be used for one AS process to connect to another AS process? e.g. for a slave host controller connecting to the master or for a Remoting connection for server to server EJB calls.”, Indicar No.
* Abrir puertos para wildfly y consola de administración (8180 y 9990, respectivamente:
  + firewall-cmd --permanent --add-port=8180/tcp
  + firewall-cmd –reload
  + firewall-cmd --permanent --add-port=9990/tcp
  + firewall-cmd --reload
* Iniciar el servidor de aplicaciones con los siguientes comandos:
  + cd HOME\_WILDFLY/bin
  + sh ./standalone.sh -Djboss.bind.address=**<IP de la Maquina>** -bmanagement=**<IP de la Maquina>**
  + Nota: las dos ultimas propiedades es para que sea visible desde la IP donde esta la maquina.
* Configuracion DataSource wildfly
  + Abrir consola de administración http://<IP de la Maquina>:9990/, e ingresar usuario y password generado para wildfly.
  + Ir a Configuración:



* Ir a subsystems, datasources and drivers:



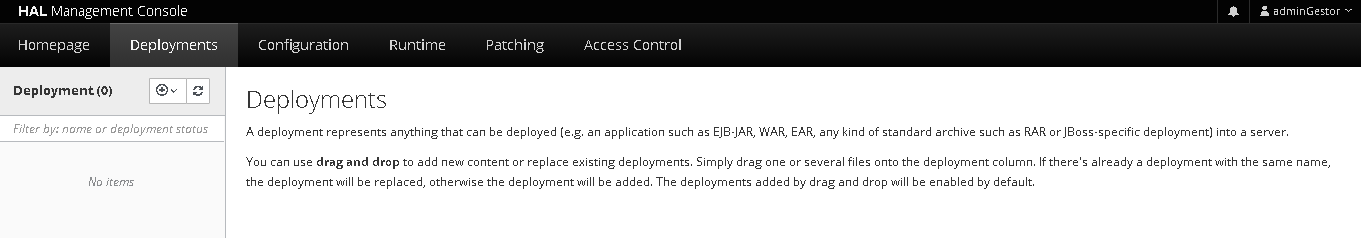
* Presionar sobre Datasources->SGDP y sobre el botón para más acciones y presionar test connection.



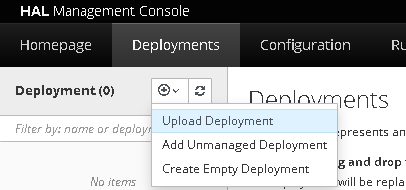
* Debe decir conexión exitosa a base de datos.
  1. Configuracion de aplicación web (SCJ)

En esta sección vamos a configurar el acceso al LDAP de la institución para la autenticación y autorización al sistema, además de las variables de entorno para archivo nacional. (Nota: esta configuración se debe trabajar en un ambiente con Maven 3.0.5 >= y OpenJDK version 1.8.0\_252)

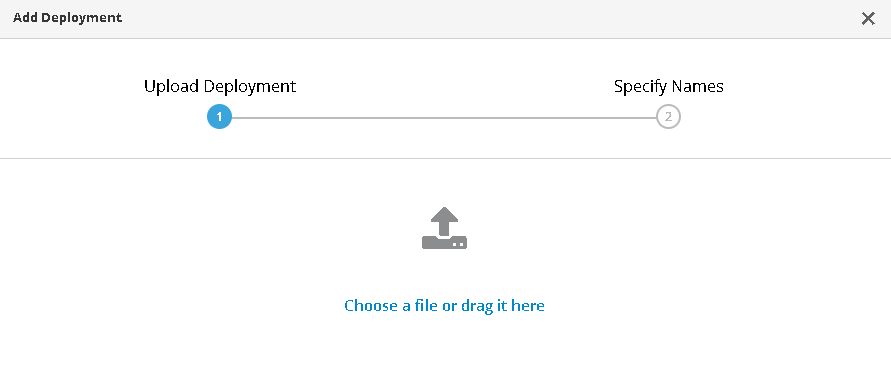
* Ingresar al repositorio y descargar las fuentes del sistema en una ruta adecuada para el trabajo que llamaremos HOME\_SCJ, buscar el archivo security-context.xml (“Servicios\_Gestor\SGDP\src\cl\gob\scj\sgdp\config”) y editar las siguientes propiedades:
  + Buscar el bean id=”contextSource” y editar las tres propiedades que este posee.
  + ldap://<ip ldap>:<puerto ldap>/<propiedades ldap>
  + name=”userDn” value=”<propiedades del ldap>”
  + name=”password” value=”<password>” (password del admin ldap)
* Compilar el client api:
  + Ubicado en Servicios\_Gestor\integracion-client-api
  + Ejecutar mvn install -Dmaven.test.skip=true
* Ingresar a un terminal cd HOME\_SCJ y ejecutar el siguiente comando:
  + mvn clean install -DskipTests
  + cd HOME\_SCJ/target
  + respaldar el archivo sgdp-0.0.1-SNAPSHOT.war en una ruta apropiada.
* Desplegar el war generado.
  + Abrir consola de wildfly http://<IP de la Maquina>:9990/console/index.html.
  + Presionar sobre Deployments.



* Luego sobre el símbolo +, seleccionar la opción upload deployment, como se muestra en la siguiente imagen:



* Presionar sobre Choose a file or drag it here.



* Seleccionar war generado y presionar el botón “Next”. Luego presionar finish
  1. Configuracion de aplicación Carga Camunda (PHP)

(aca)En esta sección se realiza la configuración de la aplicación Carga de subprocesos a SGDP, para la correcta configuración son necesarios los siguientes prerrequisitos en la máquina.

1. Contar con PHP instalado Versión 5.4.16 php -v (Nota: yum install php)
2. Contar con los módulos pdo\_pgsql y pgsql instalados, php -m (Nota: yum install php-pgsql)
3. Habilitar las conexión de BD setsebool httpd\_can\_network\_connect\_db 1

* Ingresar al repositorio y descargar las fuentes de la aplicación carga subprocesos SGDP.
* Copiar la carpeta sgdoc en /var/www/html/
* Ejecutar el siguiente comando y editar la conexión de base de datos al usuario sgdp creado anteriormente en los siguientes archivos:
  + vim /var/www/html/sgdoc/proceso/bpm/connect.php
  + vim /var/www/html/sgdoc/proceso/bpm/logica/connect.php
* Dar permisos a usuario apache sobre sistema PHP:
  + chown -R apache:apache /var/www/html/sgdoc/
  + chcon -t httpd\_sys\_content\_t /var/www/html/sgdoc/proceso/bpm/diagramas –R
  + chcon -t httpd\_sys\_rw\_content\_t /var/www/html/sgdoc/proceso/bpm/diagramas -R
* Reiniciar PHP con el comando “service httpd restart”
* Abrir puerto 80:
  + firewall-cmd --permanent --add-port=80/tcp
  + firewall-cmd –reload
  1. Configuracion de JMS transferencia archivo nacional

En esta sección se realizará la instalación de la aplicación springboot que se encargará de enviar los archivos hacia archivo nacional.

* Ingresar al repositorio y descarga las fuentes de la aplicación /carga y almacenar en una ruta adecuada para su trabajo, que de ahora en adelante llamaremos HOME\_CARGA.
* Ingresar a la ruta donde está la aplicación y ejecutar los siguientes comandos y editar las conexiones de bd, ip de la máquina y destino del log.
  + vim /HOME\_CARGA/carga/src/main/resources/application.yml
  + Editar y guardar las siguientes propiedades destacadas con negrita.

producer:

url-endpoint: http://**<ip maquina instalacion>**:6038/api/v3/producer

*# Database*

datasource:

driver-class-name: org.postgresql.Driver

url: jdbc:postgresql://**<ip maquina bd alfresco>**:5432/alfresco

username: sgdp

password: **<PASSWORD>**

*# Logger configuration*

logging:

pattern:

console: "%d %-5level %logger : %msg%n"

file: "%d %-5level [%thread] %logger : %msg%n"

level:

cl.archivo.nacional: DEBUG

org.springframework: DEBUG

org.hibernate: warn

file: **<RUTA ALCENAR LOG>/**application-carga.log

*#Propiedades*

properties:

archivo.nacional.ip.sftp: **<Ip Server SFTP Ingesta>**

archivo.nacional.port.sftp: **<puerto comunicación server sftp ingesta>**

archivo.nacional.url.login: http://**<IP publica ingesta>**/uaa/oauth/token?grant\_type=password&password={password}&username={username}

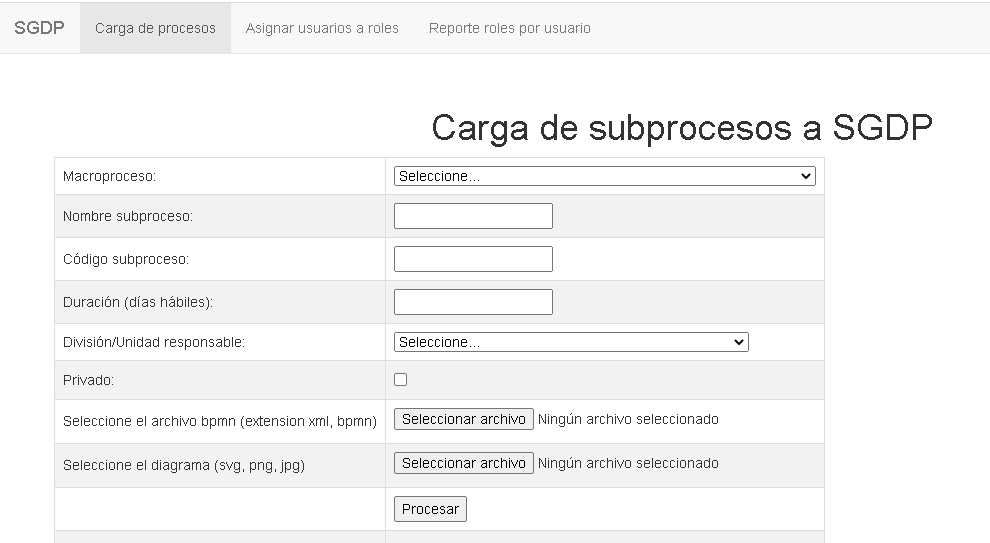
archivo.nacional.url.consolidacion: http://**<Ip Publica Ingesta>**/api-integracion/api/consolidacion

archivo.nacional.basic.login: Basic YXBpLnNlcnZpY2VzOmFwaS5zZXJ2aWNlcw==

* Ejecutar el siguiente comando mvn /HOME\_CARGA/carga clean install -DskipTests
* Al finalizar copiar el archivo /HOME\_CARGA/carga/target/carga-0.0.1-SNAPSHOT.jar en una ruta apropiada.
* En la carpeta donde se encuentra carga-0.0.1-SNAPSHOT.jar abrir un terminal y ejecutar el siguiente comando:
  + java –jar carga-0.0.1-SNAPSHOT.jar
  1. Configuración BPM de prueba de sistema

Para verificar la instalación y realizar pruebas sobre ellas, en necesario configurar nuestro primer Flujo BPM para el proceso. Para realizar esta tarea se debe realizar lo siguiente:

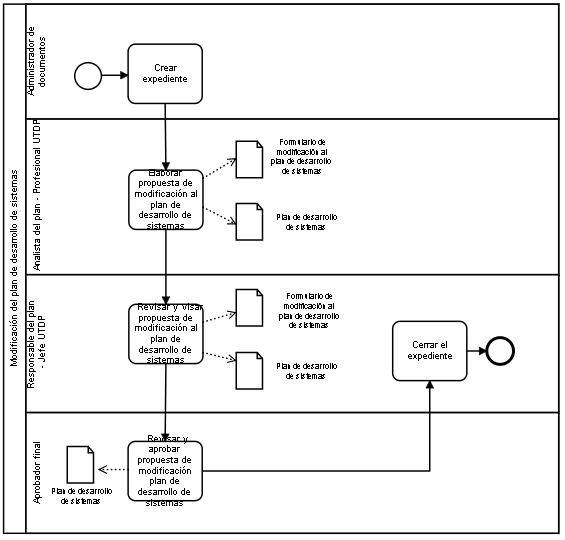
* Ir a la URL: http://<IP de la Maquina>/sgdoc/proceso/bpm/index.php



En la imagen anterior, se debe completar la información requerida por el formulario, en detalle:

* Macroproceso: es solo informativo, se refiere al macroproceso al cual pertenecerá el flujo BPM a subir.
* Nombre Subproceso: este es un texto el cual debe ser el nombre exacto de la serie documental previamente configurada en los sistemas de archivos nacional.
* Codigo subproceso: código utilizado solo como referencia interna.
* Duración de días hábiles: duración total de días del Flujo BPM, por ejemplo “120”
* División/Unidad responsable: seleccionar algunos de los disponibles, es solo informativo.
* Seleccione el archivo BPMN: acá se debe utilizar el diagrama de BPM utilizado como ejemplo para las instituciones. Este se encuentra modelado en Camunda, y se puede descargar desde el repositorio en la ruta “Gestor\alfresco\Diagrama\_Camunda”, archivo “76 02 Modificación del plan de desarrollo de sistemas.bpmn”.
* Seleccione el diagrama: adjuntar el diagrama encontrado en la misma ubicación del paso anterior. Este es el diagrama en imagen del BPMN que se utiliza como informativo en el sistema.

El diagrama BPMN que se utilizará para este proceso es:



Una vez terminado de completar el formulario anterior, se debe presionar el botón Procesar, y luego presionar al fin de la interfaz el botón “Grabar Proceso”.

Adicionalmente se deben configurar los usuarios que utilizarán el gestor en Base de Datos, estos usuarios son mantenidos por medio de LDAP en su autentificación, pero en la asignación de roles a estos usuarios de deben completar manualmente en base de datos.

En la base de datos SGDP, en la tabla SGDP\_USUARIOS\_ROLES, se debe completar la información de los usuarios que existan en el LDAP. A Continuación se entrega un script de BD con datos de ejemplo para los usuarios de prueba entregados:

INSERT INTO sgdp."SGDP\_USUARIOS\_ROLES" ("ID\_ROL","ID\_USUARIO","ID\_UNIDAD","B\_ACTIVO","B\_FUERA\_DE\_OFICINA","A\_NOMBRE\_COMPLETO","A\_RUT") VALUES

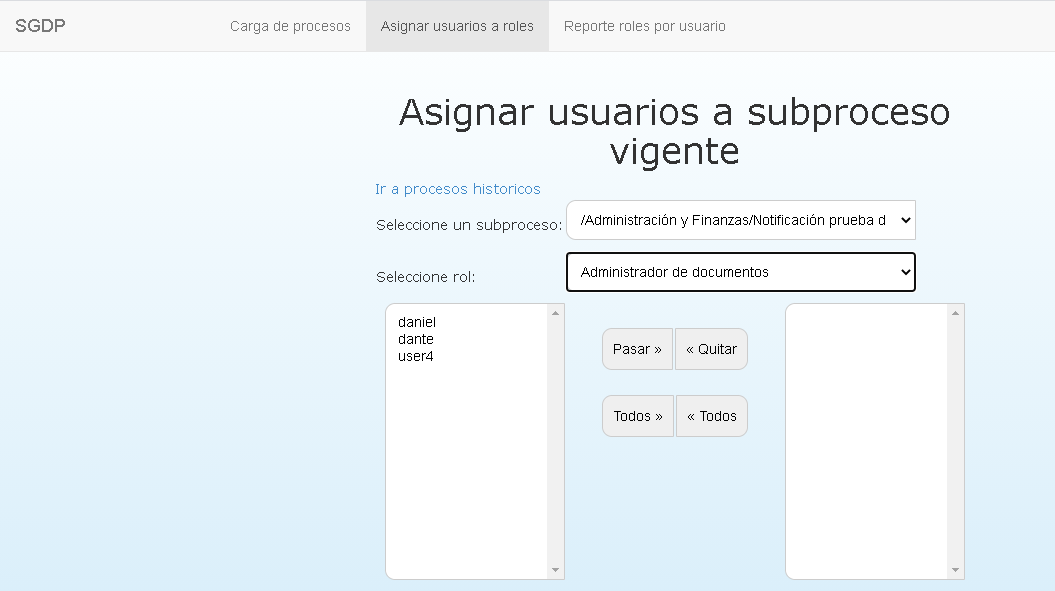
(9,'dante',1,true,false,'Dante','3-5'),

(1,'dante',1,true,false,'Dante','3-5'),

(2,'user4',1,true,false,'User4','2-7'),

(2,'daniel',1,true,false,'Daniel','1-9');

* El siguiente paso es realizar la asociación de usuarios a roles del sistemas, para eso en el sistema de carga de subprocesos, se debe seleccionar la funcionalidad “Asignar usuarios a roles”.



Seleccionar el proceso cargado en paso anterior y por cada rol existente en el BPM asociar los usuarios que se desee, pasando estos usuarios hacia la derecha. Luego para grabar la operación presionar el botón “Guardar Asignación”.

1. LDAP

Si fuese necesario instalar un LDAP, esta sección entrega una ayuda para poder realizar una correcta instalación de los servicios necesarios.

* 1. Instalación

Para instalar el producto se ejecuta el siguiente comando.

% yum -y install openldap compat-openldap openldap-clients openldap-servers openldap-servers-sql openldap-devel

* 1. Configuración Inicial y Arranque

Los siguientes comandos permiten arrancar el servicio OpenLDAP, definido como slapd y habilitarlo como servicio.

% systemctl start slapd

% systemctl enable slapd

* 1. Configuración de Directorio para Aplicación PMI

La instalación de OpenLDAP y posterior configuración, supone las siguientes características:

* Usuario de administración ldapadm
* Estructura del árbol dc=app,dc=local
* Creación de OU’s para contener los distintos elementos necesarios por la aplicación

La siguiente figura muestra el detalle del árbol a configurar.



Los siguientes pasos permiten configurar el servicio, de acuerdo con las necesidades del proyecto. Todas las configuraciones deben ser ejecutadas en base a archivos ldif y con los comandos para agregar objetos al directorio.

* 1. Contraseña de administrador

Se genera una contraseña para ser usada en la configuración del directorio.

% slappasswd -h {SSHA} -s ***<contraseña>***

En negrita se muestra lo que se debe configurar:

* Contraseña, valor establecido por el operador.

Este comando entregará un texto codificado con algoritmo SSHA.

* 1. Configuración inicial del directorio

Las siguientes tareas permiten configurar la estructura inicial del directorio.

Crear archivo 1-db-setup.ldif



Ejemplo, con los datos a configurar:

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcSuffix

olcSuffix: ***dc=app,dc=local***

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcRootDN

olcRootDN: ***cn=ldapadm,dc=app,dc=local***

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcRootPW

olcRootPW: ***{SSHA}d/thexcQUuSfe3rx3gRaEhHpNJ52N8D3***

En negrita se muestra lo que se debe configurar:

* Esquema del árbol (olcSuffix).
* Nombre de la cuenta de administración, en este proceso se crea la cuenta ldapadm (olcRootDN).
* Contraseña, el resultado del comando ***slappasswd*** en punto 3.3.1 (olcRootPW).

Ejecutar las modificaciones:

% ldapmodify -Y EXTERNAL -H ldapi:/// -f 1-db-setup.ldif

* 1. Ajustar permiso de monitoreo de accesos sólo a ldapadm

Crear y editar archivo 2-monitor-setup.ldif



Ejecutar las modificaciones

% ldapmodify -Y EXTERNAL -H ldapi:/// -f 2-monitor-setup.ldif

* 1. Cargar Esquemas necesarios

Se debe agregar esquemas para la creación de objetos necesarios.

Ejecutar los siguientes comandos:

% ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif

% ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif

% ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif

% ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/ppolicy.ldif

% ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/openldap.ldif

* 1. Creación de Esquema Base para Directorio

Editar archivo 3-base-setup.ldif para crear estructura base de directorio.



Se ejecuta el siguiente comando para cargar la estructura.

% ldapadd -x -W -D "cn=ldapadm,dc=app,dc=local" -f 3-base-setup.ldif

* 1. Crear Estructura para Aplicación PMI

Editar archive 4-pmi-setup.ldif con el siguiente contenido.



Ejecutar la creación de OU.

% ldapadd -x -W -D "cn=ldapadm,dc=app,dc=local" -f 4-pmi-setup.ldif

* 1. Configuración de Políticas de Contraseñas

Los siguientes pasos se realizan para crear la estructura que contiene las políticas de contraseñas para las cuentas creadas en el Directorio.

1. Crear OU para almacenar políticas.

Crear archivo 5-myoupolicy.ldif para estructura donde se almacenarán las políticas.



Ejecutar la creación de OU.

% ldapadd -x -W -D "cn=ldapadm,dc=app,dc=local" -f 5-myoupolicy.ldif

1. Habilitar librería de políticas

Crear archivo 6-addmodule.ldif



Ejecutar instrucciones:

% ldapadd -Y EXTERNAL -H ldapi:/// -f 6-addmodule.ldif

1. Cargar módulo de políticas

Crear archivo 7-ppmodule.ldif



Ejecutar instrucciones:

% ldapadd -Y EXTERNAL -H ldapi:/// -f 7-ppmodule.ldif

1. Cargar configuración de políticas a directorio

Crear archivo 8-ppolicyoverlay.ldif



Ejecutar instrucciones:

% ldapadd -Y EXTERNAL -H ldapi:/// -f 8-ppolicyoverlay.ldif

1. Cargar política de contraseñas

Crear archivo 9-passwordpolicy.ldif



Ejecutar instrucciones:

% ldapadd -D cn=ldapadm,dc=app,dc=local -w ***<contraseña>*** -f 9-passwordpolicy.ldif

En negrita se muestra lo que se debe configurar:

* Contraseña, valor establecido por el administrador de sistemas pasos anteriores (no el encriptado, el real configurado)