



Tot plugin Ranger

Control de versiones	2
Modelo de integración	2
Gobierno activo	3
Credenciales requeridas	6
Generación y uso de los certificados	6
Proceso de activación de SSL/TLS con CDP	6
Preliminares	6
Asistente	6
Asistente::Generar la CA	7
Asistente::Resumen	8
PostInstalación	8
TrustStores y Keystores	8
Conexión de SSL/TLS con CDP	9
Credenciales del usuario	9
HDFS	11
Hive	12
Rol de Anjana	14
Limitaciones Ranger	14
Limitaciones Anjana	15
Acciones del plugin	16
Crear/Ampliar política	16
Eliminar/reducir política	16
Ejemplo de configuración	16

Control de versiones

Versión	Fecha de modificación	Responsable	Aprobador	Resumen de cambios
1.0	11/05/2023	Anjana Data Producto	Anjana Data Producto	Creación del documento

Modelo de integración

Gobierno activo

La gestión de acceso requiere el plugin “Tot plugin Ldap” para que genere los grupos que representan a los DSA e inserte o elimine usuarios a dichos grupos.

A su vez se requiere que Ranger sincronice dichos grupos para poder utilizarlos en sus políticas.

Las variables mostradas en las siguientes capturas son las propiedades que tendrán que adaptarse a la configuración del LDAP y Ranger que se tenga.

Source for Syncing User and Groups

ranger.usersync.source.impl.class
[ranger.usersync.source.impl.class](#)

Ranger Usersync Default Group ↩

- org.apache.ranger.unixusersync.process.UnixUserGroupBuilder
- org.apache.ranger.unixusersync.process.FileSourceUserGroupBuilder
- org.apache.ranger.ldapusersync.process.LdapUserGroupBuilder

Usersync LDAP/AD URL

ranger.usersync.ldap.url
[ranger.usersync.ldap.url](#)

Ranger Usersync Default Group ↩

[REDACTED]

Usersync Bind User

ranger.usersync.ldap.binddn
[ranger.usersync.ldap.binddn](#)

Ranger Usersync Default Group ↩

CN=cdpadadm,OU=ANJANA,DC=cdp,DC=local

Usersync Bind User Password

ranger.usersync.ldap.ldapbindpassword
[ranger_usersync_ldap_ldapbindpassword](#)

Ranger Usersync Default Group ↩

.....

Usersync Incremental Sync

ranger.usersync.ldap.deltasync
[ranger.usersync.ldap.deltasync](#)

Ranger Usersync Default Group

Usersync Enable STARTTLS

ranger.usersync.ldap.starttls
[ranger.usersync.ldap.starttls](#)

Ranger Usersync Default Group

Usersync User Search Base

ranger.usersync.ldap.user.searchbase
[ranger.usersync.ldap.user.searchbase](#)

Ranger Usersync Default Group ↩

OU=ANJANA,DC=cdp,DC=local

Usersync User Search Scope

ranger.usersync.ldap.user.searchscope
[ranger.usersync.ldap.user.searchscope](#)

Ranger Usersync Default Group

- sub
- base
- one

Usersync User Object Class

ranger.usersync.ldap.user.objectclass

 [ranger.usersync.ldap.user.objectclass](#)

Usersync User Search Filter

ranger.usersync.ldap.user.searchfilter

 [ranger.usersync.ldap.user.searchfilter](#)

Usersync User Name Attribute

ranger.usersync.ldap.user.nameattribute

 [ranger.usersync.ldap.user.nameattribute](#)

Usersync Referral

ranger.usersync.ldap.referral

 [ranger.usersync.ldap.referral](#)

Usersync Username Case Conversion

ranger.usersync.ldap.username.caseconversion

 [ranger.usersync.ldap.username.caseconversion](#)

Usersync Groupname Case Conversion

ranger.usersync.ldap.groupname.caseconversion

 [ranger.usersync.ldap.groupname.caseconversion](#)

Usersync Enable User Search

ranger.usersync.user.searchenabled

 [ranger.usersync.user.searchenabled](#)

Usersync Group Search Base

ranger.usersync.group.searchbase

 [ranger.usersync.group.searchbase](#)

Ranger Usersync Default Group

user

Ranger Usersync Default Group

Ranger Usersync Default Group

sAMAccountName

Ranger Usersync Default Group

ignore

follow

throw

Ranger Usersync Default Group

none

lower

upper

Ranger Usersync Default Group [Deshacer](#)

none

lower

upper

Ranger Usersync Default Group

Ranger Usersync Default Group

OU=ANJANA,DC=cdp,DC=local

<p>Usersync Enable User Search <small>ranger.usersync.user.searchenabled</small>  ranger.usersync.user.searchenabled</p>	<p><input checked="" type="checkbox"/> Ranger Usersync Default Group</p>		
<p>Usersync Group Search Base <small>ranger.usersync.group.searchbase</small>  ranger.usersync.group.searchbase</p>	<p>Ranger Usersync Default Group </p> <input type="text" value="OU=ANJANA,DC=cdp,DC=local"/>		
<p>Usersync Group Object Class <small>ranger.usersync.group.objectclass</small>  ranger.usersync.group.objectclass</p>	<p>Ranger Usersync Default Group </p> <input type="text" value="group"/>		
<p>Usersync Group Name Attribute <small>ranger.usersync.group.nameattribute</small>  ranger.usersync.group.nameattribute</p>	<p>Ranger Usersync Default Group </p> <input type="text" value="cn"/>		
<p>Usersync Group Member Attribute <small>ranger.usersync.group.memberattributename</small>  ranger.usersync.group.memberattributename</p>	<p>Ranger Usersync Default Group </p> <input type="text" value="member"/>		
<p>Usersync Group Hierarchy Levels <small>ranger.usersync.ldap.grouphierarchylevels</small>  ranger.usersync.ldap.grouphierarchylevels</p>	<p>Ranger Usersync Default Group</p> <input type="text" value="0"/>		
<p>Usersync Ldap Group Names <small>ranger.usersync.ldap.groupnames</small>  ranger.usersync.ldap.groupnames</p>	<p>Ranger Usersync Default Group</p> <p></p>		
<p>Usersync Sleeptime interval <small>ranger.usersync.sleeptimeinmillisbetweensynccycle</small>  ranger.usersync.sleeptimeinmillisbetweensynccycle</p>	<p>Ranger Usersync Default Group </p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;">3</td> <td style="width: 50%; text-align: center;">minuto(s) </td> </tr> </table>	3	minuto(s) 
3	minuto(s) 		

El presente plugin creará o actualizará las políticas de HDFS y/o Hive para dar o quitar permisos a los grupos representados por DSAs.

Credenciales requeridas

Para permitir al plugin conectarse a Ranger se requieren dos cosas: un usuario de servicio con los permisos y credenciales correspondientes y certificados en la JVM para habilitar la conexión SSL a Ranger.

Generación y uso de los certificados

Para permitir la conexión entre el plugin y CDP es necesario realizar una serie de pasos previos para habilitar el SSL en el cluster y generar los certificados necesarios que el plugin requiere.

Proceso de activación de SSL/TLS con CDP

Actualmente con *Cloudera* es necesario activar *SSL/TLS* para poder hacer uso de *Ranger*. Si el asistente de este proceso falla hay muchas probabilidades de dejar el cluster completamente inoperable.

Preliminares

Durante la ejecución del asistente *Cloudera Manager* ha de conectarse, en nuestro caso con el usuario *root*, a todos los servidores del entorno, usando contraseña o bien usando claves pública/privada.

Para el par de claves público/privada hay que desplegar la clave pública de *root* a todos los nodos, además de habilitar el *root login* en la configuración del servidor *SSH*

```
Unset
sed -i 's/#PermitRootLogin prohibit-password/PermitRootLogin
yes/g' /etc/ssh/sshd_config

sed -i 's>PasswordAuthentication no/PasswordAuthentication
yes/g' /etc/ssh/sshd_config
```

Se recomienda realizar previamente un test de conexión manual desde el *Cloudera Manager* a todos los servidores del *Cluster*.

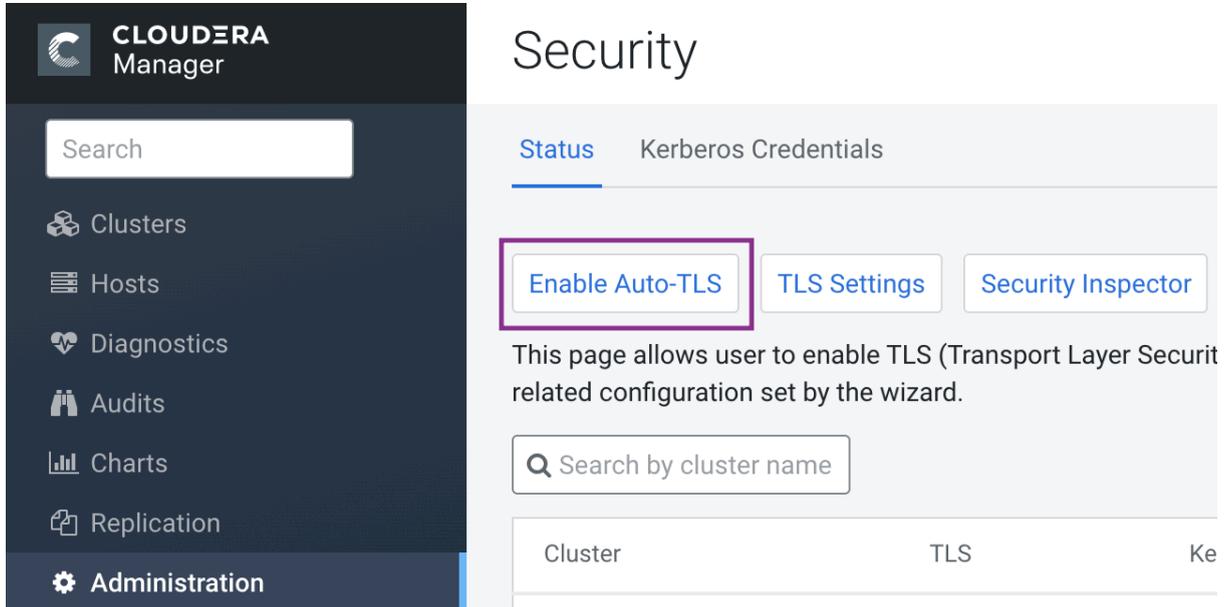
Asistente

El asistente consta de dos fases

- Generar la CA
- Pantalla de Resumen

Quando se nos muestra la pantalla de resumen, sólo hemos de pulsar el botón de finalizar en la pantalla de resumen cuando finalice la operativa que nos describe que hagamos.

El asistente que se lanza desde al menú Administración > Seguridad > Enable TLS



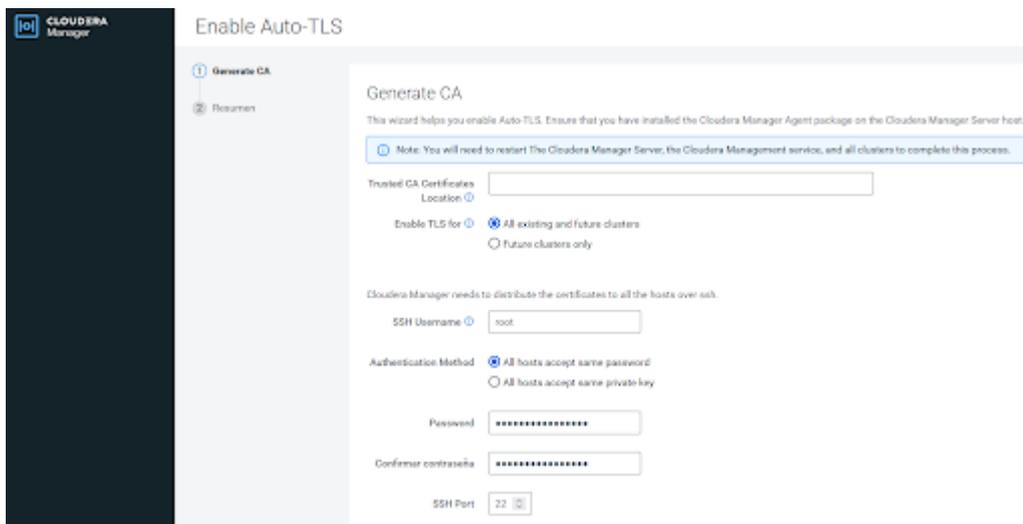
The screenshot shows the Cloudera Manager interface. On the left is a dark sidebar with the Cloudera Manager logo and a search bar. Below the search bar are menu items: Clusters, Hosts, Diagnostics, Audits, Charts, Replication, and Administration (highlighted with a blue bar). The main content area is titled 'Security' and has two tabs: 'Status' (active) and 'Kerberos Credentials'. Under the 'Status' tab, there are three buttons: 'Enable Auto-TLS' (highlighted with a purple box), 'TLS Settings', and 'Security Inspector'. Below the buttons is a text description: 'This page allows user to enable TLS (Transport Layer Security) related configuration set by the wizard.' There is also a search bar labeled 'Search by cluster name' and a table with columns 'Cluster', 'TLS', and 'Ke'.

Asistente::Generar la CA

Esta primera pantalla del asistente nos permite o bien usar una CA que nos proporcionen o bien Cloudera genera una CA autofirmada.

En nuestro caso marcamos las opciones:

- All existing clusters and future clusters.
- All hosts accept the same password.
- ssh user name y password en nuestro caso root



The screenshot shows the 'Enable Auto-TLS' wizard in Cloudera Manager. The wizard has two steps: 'Generate CA' (active) and 'Resumen'. The 'Generate CA' step includes the following fields and options:

- Trusted CA Certificates Location:** A text input field.
- Enable TLS for:** Two radio button options:
 - All existing and future clusters
 - Future clusters only
- SSH Username:** A text input field with the value 'root'.
- Authentication Method:** Two radio button options:
 - All hosts accept same password
 - All hosts accept same private key
- Password:** A password input field with masked characters.
- Confirmar contraseña:** A password input field with masked characters.
- SSH Port:** A dropdown menu with the value '22'.

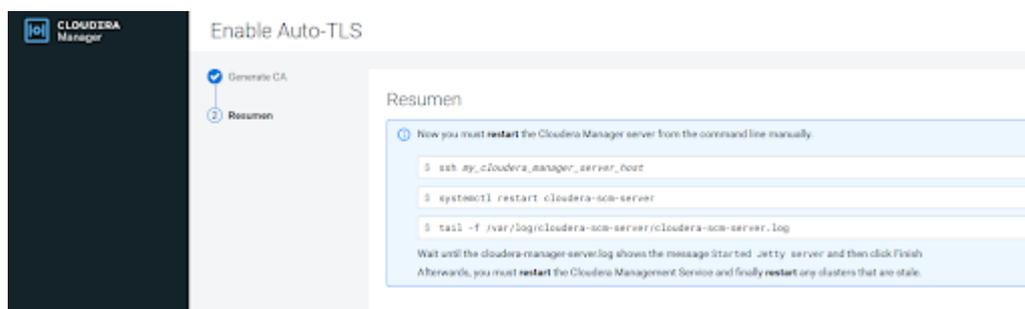
Asistente::Resumen

En esta pantalla **NO** debemos presionar finalizar hasta que se complete la operativa que nos muestra.

La operativa es:

1. conectarse a la máquina de *Cloudera Manager*
2. Reiniciar *Cloudera Manager*
3. Verificar en el log cuando se ha terminado de reiniciar

Sólo cuando esté completamente reiniciando el servido *Cloudera Manager* finalizaremos el asistente



PostInstalación

Después de la finalización del asistente tendremos que actualizar las configuraciones obsoletas de los clientes y aplicaciones.

TrustStores y Keystores

Cloudera almacena los JKS para certificados y claves en: `/var/lib/cloudera-scm-agent/agent-cert`

- cm-auto-in_cluster_truststore.jks
- cm-auto-in_cluster_ca_cert.pem
- cm-auto-global_truststore.jks
- cm-auto-global_cacerts.pem
- cm-auto-host_key_cert_chain.pem
- cm-auto-host_key.pw
- cm-auto-host_key.pem
- cm-auto-host_cert_chain.pem
- cm-auto-host_keystore.jks

El password se puede sacar usando este comando:

Unset

```
grep -Eo "Djavax.net.ssl.trustStorePassword=[[:alnum:]]*"
$(find /run/cloudera-scm-agent/process/ -name "proc.json" |
grep HIVESERVER2 | sort | head -1) | sed
's/Djavax.net.ssl.trustStorePassword=/'
```

Conexión de SSL/TLS con CDP

El plugin utiliza una librería de Java para conectar por SSL a Ranger, es necesario que el plugin tenga acceso a los certificados generados anteriormente para conectar.

Existen dos maneras de hacerlo:

- Incluir el certificado en el comando de arranque del plugin incluyendo las siguientes variables de la JVM (deben):

```
-Djavax.net.ssl.trustStore={ruta}\cm-auto-global_truststore.jks
-Djavax.net.ssl.trustStorePassword=****
```

- Instalar los certificados en la JVM donde se ejecuta el plugin

Credenciales del usuario

Se requiere la creación de un usuario de servicio de tipo User, ya sea creado desde Ranger o sincronizado desde LDAP.

Users/Groups/Roles > User Edit

User Detail

User Name * ⓘ

First Name ⓘ

Last Name ⓘ

Email Address ⓘ

Select Role * ▼

Group *Please select*

Sync Details :

Name	Value
sync_source	LDAP/AD

Dicho usuario necesita estar presente en ciertas políticas de HDFS y Hive que le permitan modificar todos los elementos que se quieren gobernar.

Si se quiere que las políticas estén en una zona de seguridad en particular (configurable) es necesario que el usuario de servicio sea administrador de la zona de seguridad, ya sea nominal o por pertenencia a un grupo.

☰ purchases

Zone Administrations	
Admin Users	<code>admin</code> <code>hive</code> <code>usr_luis</code> <code>usr_apis_anjana</code>
Admin Usergroups	<code>grp_dev</code>
Auditor Users	--
Auditor Usergroups	<code>grp_dev</code>

HDFS

En la política definida por defecto "all - path" creada por Ranger en HDFS añadir al usuario que utilizará Anjana otorgándoles todos los permisos y marcando la opción "Delegate Admin"

Service Manager > cm_hdfs Policies > Edit Policy

Edit Policy

Policy Details:

Policy Type: **Access**

Policy ID: **76**

Policy Name *: **Enabled** **Normal**

Policy Label:

Resource Path *: **Recursive**

Description:

Audit Logging: **Yes**

Allow Conditions: hide ^

Select Role	Select Group	Select User	Permissions	Delegate Admin	
<input type="text" value="Select Roles"/>	<input type="text" value="Select Groups"/>	<input type="text" value="x hdfs x mapred x usr_apis_anjana"/>	<input type="button" value="Read"/> <input type="button" value="Write"/> <input type="button" value="Execute"/>	<input checked="" type="checkbox"/>	<input type="button" value="x"/>
<input type="text" value="Select Roles"/>	<input type="text" value="Select Groups"/>	<input type="text" value="x rangerlookup"/>	<input type="button" value="Read"/>	<input type="checkbox"/>	<input type="button" value="x"/>

Hive

De manera similar a HDFS en la política definida por defecto "all - database, table, column" de Hadoop SQL añadir al usuario que utilizará Anjana otorgándoles todos los permisos y marcando la opción "Delegate Admin".

Edit Policy

Policy Details:

Policy Type **Access**

Policy ID **9**

Policy Name *

Enabled Normal

Policy Label

<div style="display: flex; align-items: center; margin-bottom: 10px;"> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">database</div> <div style="margin: 0 5px;">*</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px; margin-right: 5px;">x *</div> <div style="margin-left: 20px;">Include <input checked="" type="checkbox"/></div> </div>
<div style="display: flex; align-items: center; margin-bottom: 10px;"> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">table</div> <div style="margin: 0 5px;">*</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px; margin-right: 5px;">x *</div> <div style="margin-left: 20px;">Include <input checked="" type="checkbox"/></div> </div>
<div style="display: flex; align-items: center; margin-bottom: 10px;"> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">column</div> <div style="margin: 0 5px;">*</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px; margin-right: 5px;">x *</div> <div style="margin-left: 20px;">Include <input checked="" type="checkbox"/></div> </div>

Description

Audit Logging **Yes**

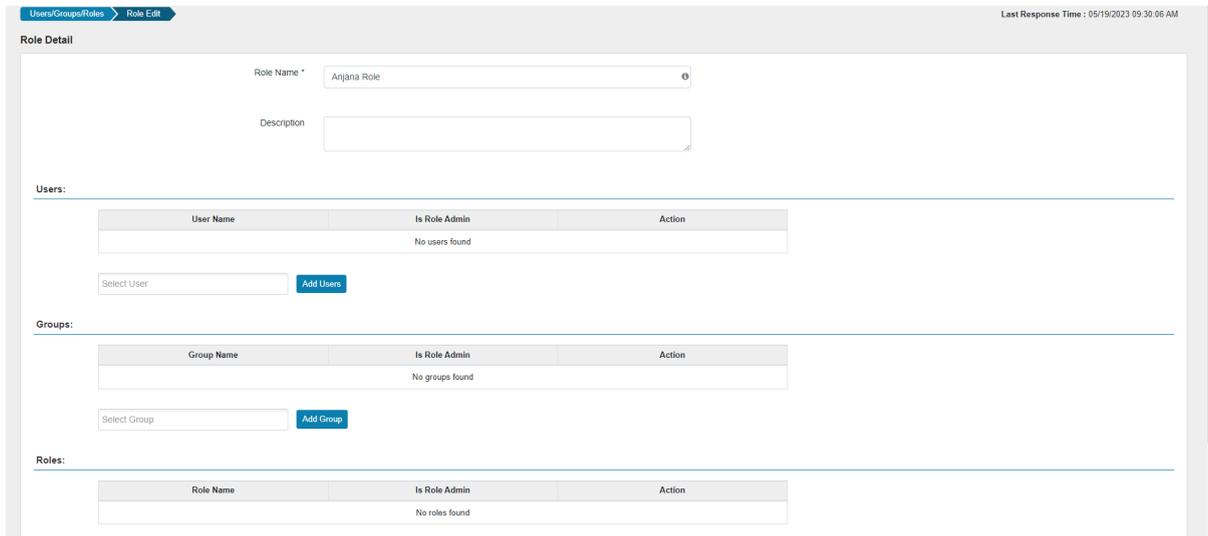
Allow Conditions:

hide

Select Role	Select Group	Select User	Permissions	Delegate Admin
<input data-bbox="260 1800 547 1832" type="text" value="Select Roles"/>	<input data-bbox="563 1800 850 1832" type="text" value="Select Groups"/>	<div style="display: flex; flex-wrap: wrap; gap: 5px;"> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">x hive</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">x beacon</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">x dpprofiler</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">x hue</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">x admin</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">x impala</div> <div style="border: 2px solid red; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">x usr_apis_anjana</div> </div>	<div style="display: flex; flex-wrap: wrap; gap: 5px;"> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">select</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">update</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">Create</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">Drop</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">Alter</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">Index</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">Lock</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">All</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">Read</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">Write</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">RepAdmin</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">Service Admin</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">Temporary UDF Admin</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">Refresh</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;">RW Storage</div> </div>	<input checked="" type="checkbox"/> <input type="checkbox"/>

Rol de Anjana

Para la agrupación de los permisos gobernados por Anjana es necesario crear un rol en Ranger que no contenga ningún usuario, grupo ni rol, a modo práctico funcionará como un tag en un registro de permisos. El nombre del rol debe ser Anjana Role.



Users/Groups/Roles > Role Edit Last Response Time : 05/19/2023 09:30:06 AM

Role Detail

Role Name *

Description

Users:

User Name	Is Role Admin	Action
No users found		

Groups:

Group Name	Is Role Admin	Action
No groups found		

Roles:

Role Name	Is Role Admin	Action
No roles found		

Limitaciones Ranger

Sólo es posible tener una política habilitada sobre un conjunto de objetos en particular (p.ej.: no es posible tener 2 políticas que actúan sobre el mismo fichero o tabla a la vez, pero sí una política que actúe sólo sobre el fichero y otra que actúe sobre el fichero y otro más), por ese motivo el plugin sólo actuará sobre políticas que apliquen a un solo recurso, ya sea un fichero/carpeta (HDFS) o una tabla (Hive).

Para facilitar saber qué políticas el plugin ha creado/modificado se le aplicará un tag a la política (Anjana Governed). Además de que todos los permisos gobernados por Anjana estarán agrupados en un único registro con el rol vacío creado anteriormente.

Policy Type: **Access** Add Validity Period

Policy ID: **1860**

Policy Name: Anj_4 Enabled Normal

Policy Label: **x Anjana_Governed**

Resource Path: **x /Test/Permission** Recursive

Description:

Audit Logging: **Yes**

Allow Conditions:

Select Role	Select Group	Select User	Permissions	Delegate Admin	
Select Roles	x public	Select Users	Write	<input type="checkbox"/>	<input checked="" type="checkbox"/>
x Anjana Role	x grp_oscar_test x grp_dev x grp_anjana	Select Users	Read Execute	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Con dicho tag se puede filtrar fácilmente qué políticas está interviniendo anjana y dentro de las mismas que permisos son los gobernados por el plugin, para que en caso de que se requiera modificar la política manualmente se puede identificar que fue creado por el plugin (y que no se debe de modificar).

SEARCH: POLICY LABEL: Anjana_Governed Add New Policy

Policy ID	Policy Name	Policy Labels	Status	Audit Logging	Roles	Groups	Users	Action
1843	Anj_1	Anjana_Governed	Enabled	Disabled	--	grp_oscar_test	--	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>
1848	Jorge_Policy	Anjana_Governed	Enabled	Disabled	--	public	--	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>
1860	Anj_4	Anjana_Governed	Enabled	Enabled	Anjana Role	public grp_oscar_test grp_dev grp_anjana	--	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>

Limitaciones Anjana

Por el procesamiento de los path a nivel de Hive, el path del objeto en Anjana que represente una tabla de Hive debe tener el path compuesto de una de estas dos maneras:

- catálogo u origen de datos/base de datos/tabla (EX: hive/db1/table1)
- base de datos/tabla (EX: db1/table1)

Siendo el carácter separador del path "/" configurable (mirar el ejemplo de configuración)

En los casos en los que se utilice el Active Directory y se utilice sAMAccountName, por restricciones de dicha tecnología, el nombre de los grupos no debe ser mayor de 20 caracteres.

Acciones del plugin

Crear/Ampliar política

Esta acción se ejecuta cuando se aprueba un DSA en Anjana que contenga algún objeto gobernado con la tripleta configurada en el plugin. Esta acción se ejecutará con un retraso configurable en el plugin, porque hay que esperar a que Ranger sincronice con el LDAP el grupo que se creó previamente en el plugin de Ldap.

Como se ha explicado en las limitaciones, primero se buscará si existe una política que actúa únicamente sobre el recurso que el objeto representa, en caso de no encontrarla se creará una. Sobre esta política se creará un nuevo registro de acceso sobre el grupo que el DSA representa y le dará los permisos correspondientes (read/execute en HDFS y select en Hive), además de incluir el tag Anjana Governed para visibilidad.

Añadir que toda política de esta acción estará automáticamente habilitada. En caso de que existiera una sobre el recurso deshabilitada, se limpiará de todo permiso o exclusiones previos que tuviera antes de tratar sobre ella.

En el caso de políticas de HDFS, si la política que apunta al recurso no es recursiva, el plugin la pasará a recursiva quedando del mismo modo que si la hubiera creado el plugin.

Eliminar/reducir política

Esta acción se ejecuta cuando se expira un DSA en Anjana que contenga algún objeto gobernado con la tripleta configurada en el plugin o cuando se expira el objeto gobernado y está presente en algún DSA. Sobre la política asociada al recurso se eliminarán los registros de acceso.

En los casos de que todavía queden acceso gobernados por Anjana y se encuentra la política deshabilitada, se volverá a habilitar.

En los casos en los que al eliminar el acceso de Anjana todavía queden accesos gestionados por el cliente se eliminará el tag de Anjana Governed para indicar que Anjana ya no gobierna sobre dicho recurso y en el caso de que fueran los únicos registros existentes se eliminará la política también.

Ejemplo de configuración

```
server:  
  port: 15021  
  
totplugin:
```

```
location: http://totpluginrangerserver:15021/plugin/ranger/api/v1
server:
  url: http://totserver:15000/tot/
aris:
  - ari: "anja:totplugin:im:/cloudera/hive/devQA/"
    imAri: "anja:totplugin:im:/ldap/ldap/ldap/"
  - ari: "anja:totplugin:im:/cloudera/hdfs/devQA/"
    imAri: "anja:totplugin:im:/ldap/ldap/ldap/"
  - ari: "anja:totplugin:im:/cloudera/ranger/devQA/"
    imAri: "anja:totplugin:im:/ldap/ldap/ldap/"
connection:
  urlBaseRanger: "https://ip-10-150-100-136.eu-central-1.compute.internal:6182"
  userRanger: "usr_apis_anjana"
  pwdRanger: "*****"
delayInSeconds: 0
securityZone: "sales"
hive:
  hiveService: cm_hive
  valueTechnologyHive: hive
  hiveAuditLogin: true
  replaceHiveClientPolicyByAnjanaPolicyName: true
  pathSplit: "/"
hdfs:
  hdfsService: cm_hdfs
  valueTechnologyHdfs: hdfs
  hdfsAuditLogin: true
  replaceHdfsClientPolicyByAnjanaPolicyName: true
```

Se han de revisar las configuraciones comunes en el doc de configuraciones Anjana Data 4.4 - DS - Configuración técnica de Portal y microservicios

Configuraciones específicas:

- Connection:
 - urlBaseRange: Url de acceso a Ranger
 - userRanger: Usuario de servicio del plugin
 - pwdRanger: Contraseña del usuario de servicio
- delayInSeconds: Delay en segundos, usado en la aprobación del DSA, es recomendado ponerlo a un poco más que el tiempo de sincronización con LDAP configurado Ranger. Su valor predeterminado es 0.
- securityZone: Campo opcional, si relleno indica la zona de seguridad donde se van a crear las políticas.
- hive:
 - hiveService: Nombre del servicio de Hive dentro de Ranger sobre el que se quiere aplicar las políticas.

- valueTechnologyHive: El valor en el campo technology que deben de tener los objetos gobernados para ser identificados como Hive y creadas sus políticas en su servicio.
 - hiveAuditLogin: Campo opcional, indica si se quiere que las políticas creadas o actualizadas de hive por el plugin se auditen. Es false por defecto.
 - replaceHiveClientPolicyByAnjanaPolicyName: Campo opcional, indica si se quiere permitir que el plugin modifique el nombre de las políticas de hive que actualiza con el nombre Anj_<Id del objeto que representa la tabla>. Es false por defecto.
 - pathSplit: Campo opcional, el carácter por el cual se procesa el path de un objeto de hive para obtener su base de datos y que tabla representa. (EX: para database/table seria el caracter /).
- hdfs:
 - hdfsService: Nombre del servicio de HDFS dentro de Ranger sobre el que se quiere aplicar las políticas.
 - valueTechnologyHdfs: El valor en el campo technology que deben de tener los objetos gobernados para ser identificados como HDFS y creadas sus políticas en su servicio.
 - hdfsAuditLogin: Campo opcional, indica si se quiere que las políticas creadas o actualizadas de HDFS por el plugin se auditen. Es false por defecto.
 - replaceHdfsClientPolicyByAnjanaPolicyName: Campo opcional, indica si se quiere permitir que el plugin modifique el nombre de las políticas de hdfs que actualiza con el nombre Anj_<Id del objeto que representa el/los fichero/s>. Es false por defecto.