**MANUAL D’instal.lació i configuració de WSO2 Identity Server**

**ÍNDEX**

[1. SIGLES I DEFINICIONS 3](#_Toc533163064)

[1.1 Sigles 3](#_Toc533163065)

[1.2 Definicions 3](#_Toc533163066)

[2. Introducció 4](#_Toc533163067)

[3. instal.lació i configuració del WSO2 Identity server 5](#_Toc533163068)

[3.1 Configuració global 5](#_Toc533163069)

[3.2 WSO2 Identity Server 6](#_Toc533163070)

[3.2.1 Instal·lació 6](#_Toc533163071)

[3.2.2 Configuració 7](#_Toc533163072)

[3.2.3 Configuració de la seguretat 7](#_Toc533163073)

[3.2.4 Afegir el magatzem d’usuaris al Directori Actiu 8](#_Toc533163074)

[3.2.4.1 Crear un nou magatzem d’usuaris 8](#_Toc533163075)

[3.2.4.2 Configurar la connexió LDAPS 8](#_Toc533163076)

[3.2.5 Configurar WSO2 com a KDC server 8](#_Toc533163077)

[3.3 Accés al Directori Actiu en mode únicament de lectura 9](#_Toc533163078)

[3.4 Single-Sign-On basat en el Protocol SAML 9](#_Toc533163079)

[3.5 Autenticació Kerberos 9](#_Toc533163080)

# SIGLES I DEFINICIONS

## Sigles

A continuació, trobareu una llista ordenada alfabèticament de les sigles que s'utilitzen en aquest document.

| **Terme** | **Definició** |
| --- | --- |
| WSO2 |  |
| IAM | Identity Access Management |
| SAML | Security Assertion Markup Language |
| LDAP | Lightweight Directory Access Protocol |
|  |  |

## Definicions

A continuació, trobareu una llista ordenada alfabèticament dels termes que s'utilitzen en aquest document.

| **Terme** | **Definició** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Introducció

El present document descriu el procediment d’instal·lació i configuració de WSO2 Identity Server.

El procediment d’instal·lació cobreix els següents punts:

* La configuració global,
* WSO2 Identity Server:
  + La instal·lació,
  + La configuració,
  + La configuració de la seguretat.
* La configuració del magatzem d’usuaris d’un Directori Actiu.
* La configuració dels proveïdors de servei:
  + El proveïdor de servei Kerberos per Cloudera
  + El proveïdor de servei SAML per Cloudera Manager
  + El proveïdor de servei SAML per Cloudera Navigator

# instal.lació i configuració del WSO2 Identity server

## Configuració global

El Sistema Operatiu ha d’estar preparat abans d’instal·lar el WSO2 Identity Server. Per tant, les següents passes s’han d’haver realitzat:

* Actualitzar el Sistema Operatiu:

*# yum update*

* Instal·lar el Packet:

*# yum install zip unzip -y*

*# yum install net-tools -y*

*# yum install nano -y*

* Definir els hostnames:

*# nano /etc/hosts*

El kid Oracle Java SE Developement (JDK) hauria també d’estar instal·lat per tal que WSO2 funcioni correctament. A continuació es detallen les passes que s’han de seguir per a la seva instal·lació:

* Descarregar l’ultima versió de JDK en la següent adreça: <http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>
* Instal·lar el Java:

*# cd /opt/*

*# tar xzf jdk-8u121-linux-x64.tar.gz*

*# cd /opt/jdk1.8.0\_121/*

*# alternatives --install /usr/bin/java java /opt/jdk1.8.0\_121/bin/java 2*

*# alternatives --config java*

* Instal·lar el Javac i el Jar:

*# alternatives --install /usr/bin/jar jar /opt/jdk1.8.0\_121/bin/jar 2*

*# alternatives --install /usr/bin/javac javac /opt/jdk1.8.0\_121/bin/javac 2*

*# alternatives --set jar /opt/jdk1.8.0\_121/bin/jar*

*# alternatives --set javac /opt/jdk1.8.0\_121/bin/javac*

* Comprovar la versió instal·lada de Java:

*# java -version*

* Configurar les variables de l’entorn:

*# nano /etc/bash.bashrc*

*export JAVA\_HOME=/opt/jdk1.8.0\_121*

*export JRE\_HOME=/opt/jdk1.8.0\_121/jre*

*export PATH=$PATH:${JAVA\_HOME}/bin:${JRE\_HOME}/bin*

*# nano ~/.bashrc*

*export JAVA\_HOME=/opt/jdk1.8.0\_121*

*export JRE\_HOME=/opt/jdk1.8.0\_121/jre*

*export PATH=$PATH:${JAVA\_HOME}/bin:${JRE\_HOME}/bin*

## WSO2 Identity Server

### Instal·lació

Primer de tot, cal descarregar-se l’ultima versió de WSO2 Identity Server a la següent adreça: <http://wso2.com/products/identity-server/>.

Després, cal executar la següent línia de comandes:

* Afegir l’usuari WSO2:

*# useradd -d /opt/wso2 wso2*

* Instal·lar WSO2 IS:

*# cd /opt/wso2/*

*# unzip wso2is-5.3.0.zip*

* Canviar el propietari del directori WSO2:

*# chown -R wso2 /opt/wso2*

Per tal de fer funcionar WSO2 IS com un servei:

* Introduir la variable CARBON\_HOME:

*# nano /etc/bash.bashrc*

*export CARBON\_HOME=/opt/wso2is-5.3.0*

*# nano ~/.bashrc*

*export CARBON\_HOME=/opt/wso2is-5.3.0*

* Crear el script d’inici:

*# cd /etc/init.d*

*# nano wso2is*

*#! /bin/bash*

*#*

*# wso2is Start/Stop WSO2 Identity Server*

*#*

*# chkconfig: 2345 55 25*

*# description: Start/Stop WS02 Identity Server at boot time.*

*export JAVA\_HOME="/opt/jdk1.8.0\_121"*

*export CARBON\_HOME="/opt/wso2is-5.3.0"*

*startcmd='${CARBON\_HOME}/bin/wso2server.sh start > /dev/null &' restartcmd='${CARBON\_HOME}/bin/wso2server.sh restart > /dev/null &'*

*stopcmd='${CARBON\_HOME}/bin/wso2server.sh stop > /dev/null &'*

*wso2user='wso2'*

*case "$1" in*

*start)*

*echo "Starting WSO2 Application Server ..."*

*su -c "${startcmd}" ${wso2user}*

*;;*

*restart)*

*echo "Re-starting WSO2 Application Server ..."*

*su -c "${restartcmd}" ${wso2user}*

*;;*

*stop)*

*echo "Stopping WSO2 Application Server ..."*

*su -c "${stopcmd}" ${wso2user}*

*;;*

*\*)*

*echo "Usage: $0 {start|stop|restart}"*

*exit 1*

*esac*

*# chmod +x wso2is*

*# chkconfig --add wso2is*

*# chkconfig wso2is on*

* Iniciar el servei:

*# service wso2is start*

### Configuració

La configuració bàsica consisteix en:

* Canviar el hostname de la configuració dels arxius següents:
  + repository/conf/carbon.xml,
  + repository/conf/security/sso-idp-config.xml,
  + repository/conf/security/saml2.federation.properties,
  + repository/deployment/server/jaggeryapps/dashboard/apis/gadget.json,
  + repository/deployment/server/jaggeryapps/portal/gadgets/account-recovery/gadget.xml,
  + repository/deployment/server/jaggeryapps/portal/gadgets/identity\_management/gadget.xml,
  + repository/deployment/server/jaggeryapps/portal/gadgets/pwd\_change/gadget.xml,
  + repository/deployment/server/jaggeryapps/portal/gadgets/user\_auth\_apps/gadget.xml,
  + repository/deployment/server/jaggeryapps/portal/gadgets/user\_profile/gadget.xml,
  + repository/deployment/server/jaggeryapps/dashboard/apis/gadget.json.
* Canviar la contrasenya de l’administrador de l’arxiu de configuració:
  + repository/conf/user-mgt.xml

### Configuració de la seguretat

La securització de WSO2 Identity Server consisteix en crear un nou keystore privat, firmat amb els certificats de l’usuari. Les etapes necessàries per a realitzar aquesta configuració són les següents:

* Crear un nou keystore privat

* Comprovar el contingut del fitxer CSR (<https://www.sslshopper.com/csr-decoder.html>) fins al final amb la firma de l’autoritat.
* Exportar els certificats i la clau privada del keystore:
  + Convertir JKS al format PKCS12
  + Visualitzar el contingut del keystore pkcs12
  + Exportar el certificat
  + Exportar la clau privada (no encriptada)
* Importar el certificat firmat en el keystore privat:
  + Importar el certificate d’arrel i els certificats intermediaris
  + Importar el certificate firmat
* Afegir la clau pública al truststore del client:
  + Exportar la clau pública del keystore
  + Importar la clau pública
* Configurar el nou keystore:
  + Identificar l’arxiu per modificar
  + Substituir la instància wso2carbon.jks per el nou keystore (I el mateix per la contrasenya)

### Afegir el magatzem d’usuaris al Directori Actiu

#### Crear un nou magatzem d’usuaris

Des de la consola de seguretat, s’afegeix un nou magatzem d’usuaris, seleccionant el menú de l’esquerra “User stores / Add” i introduint els paràmetres corresponents en el en el format corresponent

#### Configurar la connexió LDAPS

Des de la línia de comanda:

* Accedir a la carpeta client-truststore
* Exportar la clau pública del Directori Actiu
* Importar la clau pública en el client-trustore

### Configurar WSO2 com a KDC server

Activar el servidor KDC des de la línia de comanda

Des de la consola de gestió WSO2 IS, crear el servei principal. Seleccionar en el menú de l’esquerra “Service provider/Add”:

* Nom: Cloudera Kerberos
* Descripció: KDC Cloudera

En el proveïdor de servei, accedir a “Inbound Authentication Configuration/Kerberos KDC” i clicar a “Configure”:

* Nom del servei
* Descripció
* Contrasenya
* Entra de nou la contrasenya

## Accés al Directori Actiu en mode únicament de lectura

WSO2 Identity Server està configurat per a proveir únicament accés de lectura al Directori Actiu. El Directori Actiu està configurat com un magatzem d’usuaris.

WSO2 llista els usuaris i els grups presents en el Directori Actiu.

Els usuaris i rols del Directori Actiu són llistats (read-only) en la consola de gestió de WSO2 IS.

## Single-Sign-On basat en el Protocol SAML

L’ús del Protocol SAML ha estat escollit per autenticar els usuaris del Directori Actiu al Cloudera Manager (SP) i al Cloudera Navigator (SP).

WSO2 IS integra una eina especifica per a provar l’autenticació utilitzant el Protocol SAML.

## Autenticació Kerberos

Cloudera (SP) necessita l’autenticació Kerberos per a realitzar les tasques tals com l’encriptació. Per tant, WSO2 IS és configurat com a central MIT KDC.