Resum de seguretat DE CLOUDERA I POSSIBLES RISCOS

ÍNDEX

[1. Sigles i definicions 3](#_Toc533346467)

[1.1 Sigles 3](#_Toc533346468)

[1.2 Definicions 3](#_Toc533346469)

[2. Introducció 4](#_Toc533346470)

[3. Encriptació 5](#_Toc533346471)

[3.1 Data-in-transit 5](#_Toc533346472)

[3.2 Gestió de claus 5](#_Toc533346473)

[3.3 Data-at-rest 5](#_Toc533346474)

[3.4 Possibles riscos 5](#_Toc533346475)

[4 Autenticació 7](#_Toc533346476)

[4.1 SAML 7](#_Toc533346477)

[4.2 Kerberos 7](#_Toc533346478)

[4.3 Possibles riscos 7](#_Toc533346479)

[5 Autorització 8](#_Toc533346480)

[5.1 Cloudera Manager i Cloudera Navigator 8](#_Toc533346481)

[5.2 Servei Apache Sentry 8](#_Toc533346482)

[5.3 Possibles riscos 8](#_Toc533346483)

[6 Auditoria 9](#_Toc533346484)

[7 Documents relacionats 10](#_Toc533346485)

# 1. Sigles i definicions

## 1.1 Sigles

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

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

## 1.2 Definicions

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

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

# 2. Introducció

Aquest document serveix per establir els passos principals que s'han de dur a terme per configurar la seguretat de Cloudera i els possibles riscos als que està exposat el sistema, després de ser securitzat, posant èmfasi en els aspectes que s'han de vigilar un cop configurats.

# 3. Encriptació

Cloudera proveu amb diversos mecanismes per protegir dades persistides al disc o a altres medis d’emmagatzematge (data-at-rest) i per protegir dades que es mouen entre els processos del cluster o per la resta de la xarxa (data-in-transit).

## 3.1 Data-in-transit

* Generació i signat de certificats
* Importació dels certificats signats
* Configuració bàsica TLS/SSL per a Cloudera Manager i Cloudera Navigator
* Configuració de TLS/SSL de tots els agents contra el servidor de Cloudera
* Configuració de TLS/SSL entre tots els agents
* Configuració dels diferents serveis de Cloudera per aplicar SSL

## 3.2 Gestió de claus

* Instal·lació de Cloudera Navigator Key Trustee Server
* Instal·lació de Key Trustee Key Management Server
* Instal·lació de Cloudera Navigator Encrypt
* Habilitar HDFS Transparent Encryption
* Afegir el servei Key Trustee Server
* Afegir el servei Key Trustee KMS
* Crear usuari d'administració de les claus
* Crear zones d'encriptació a HDFS
* Afegir el fitxers a les zones d'encriptació de HDFS

## 3.3 Data-at-rest

* Configuració de diversos serveis per fer encriptació a HDFS. Es fa servir l’algoritme d’encriptació AES-CTR.

## 3.4 Possibles riscos

* L'encriptació de comunicacions evita per complet els atacs del tipus man-in-the-middle. Cada connexió és privada i genera un parell de claus d'encriptació simètrica. Qualsevol persona que es volgués ficar dins d'una connexió hauria d'esbrinar la clau privada del parell de claus, que és essencial per fer la desencriptació de les dades que viatgen a través del fil entre els dos punts que conformen aquella connexió.
* Per la banda de l'encriptació de les dades en repòs, alguna persona podria fer-se amb les credencials d'un usuari administrador i extreure les claus, per poder fer la desencriptació a part.
* També en refer7ncia a les claus d'encriptació de dades en repòs, un usuari malintencionat podria fer servir un algorisme de força bruta per esbrinar totes les claus que Key Management Server emmagatzema. Aquest és un procés bastant costós per suposar un risc real. Les mesures a prendre per evitar això seria fer canvis en les claus cada cert temps per frenar qualsevol avanç al descobriment de les claus existents.

# 4 Autenticació

L’autenticació és el procés de confirmar que algú és qui diu ser. A Cloudera farem servir dos mètodes d’autenticació: per una part configurarem Cloudera Manager i Cloudera Navigator per autenticar usuaris utilitzant SAML mentre que la resta de processos i serveis faran servir Kerberos per autenticar-se.

## 4.1 SAML

A continuació es detallen els passos a seguir per configurar SAML:

* Rebre el fitxer de metadades de SAML.
* Configurar de Cloudera Manager i Cloudera Navigator per a autenticar via SAML.
* Generar fitxer de metadades amb les urls de resposta per a l'intercanvi de missatges amb SAML.

## 4.2 Kerberos

A continuació es detallen els passos a seguir per configurar Kerberos:

* Crear l'usuari per accedir al KDC.
* Crear els usuaris a KDC que farà servir Cloudera per importar-los.
* Generar els fitxers de keytab de les comptes de Cloudera per importa-los.
* Crear l'script per importar els fitxers de keytab.
* Importar les credencials que falten per autenticar serveis amb Kerberos.
* Configurar els serveis per autenticar a través de Kerberos.

## 4.3 Possibles riscos

* S'ha de posar especial atenció al fitxers de keytab que es generen. Sempre estaran emmagatzemats al servidor de Cloudera, amb accés només per a usuaris amb privilegis. Si un fitxer de keytab acaba sortint, qualsevol podria iniciar sessió a Kerberos només amb el nom principal de KDC sense necessitar la contrasenya. Per això és important tenir cura de la seva custòdia. Si es perd, s’ha de regenerar las credencials en Cloudera. Aquesta acció regenera els keytabs.
* Amb els usuaris, la major part dels riscos vénen de contrasenyes no massa robustes o que segueixin patrons.

# 5 Autorització

Amb l’autorització podem escollir quina informació veu cada usuari o grups d’usuaris. A Cloudera farem servir dos formes d’identificar els usuaris: una per rols, amb els perfils d’usuari de Cloudera Manager i Cloudera Navigator i altra, utilitzant el servei Sentry que s’inclou a Cloudera.

## 5.1 Cloudera Manager i Cloudera Navigator

* Configuració de SAML per distingir de quina manera es recollirà el grup de l'usuari i l’assignació als diferents perfils.

## 5.2 Servei Apache Sentry

* Instal·lació del servei Sentry a Cloudera
* Creació dels diferents rols d'usuari
* Creació dels permisos per permetre accedir a les diferents dades de Cloudera associant-los amb els rols creats

## 5.3 Possibles riscos

* Un usuari podria accedir amb les credencials d'un altre usuari per aconseguir dades a les què, en principi, no hauria de tenir accés.

# 6 Auditoria

És crític, per a una organització, entendre d'on venen les dades i com estan sent utilitzades. L'objectiu de l'auditoria és capturar un registre complet i immutable de tota l'activitat dins del sistema.

L'auditoria juga un rol central a tres activitats claus dins de l'empresa:

* Primer, l'auditoria és part de la seguretat del sistema i pot explicar què, quan i a qui ha passat en cas que hi hagi una bretxa o altre incident maliciós.
* La segona activitat és l’acompliment. L'auditoria participa satisfent els requeriments central de regulacions associades amb dades sensibles. L'auditoria proveu dels punts necessaris per construir el camí de qui, com, quan i amb quina freqüència les dades són produïdes, visualitzades i manipulades.
* Finalment, la informació d'auditoria ajuda a entendre com diferents usuaris utilitzen les dades. A més, pot ajudar a establir patrons d'accés d'aquestes dades.

Les eines utilitzades a Cloudera per obtenir dades d'auditoria són Cloudera Navigator Audit Server i Cloudera Navigator Data Management.

* Instal·lació del rol d'instància Cloudera Navigator Audit Server.
* Instal·lació del rol d’instància Cloudera Navigator Data Management Component.

# 7 Documents relacionats

SP12\_Disseny de Seguretat del Sistema Informàtic