

installer et configurer Apereo/CAS 6.3.2 sur debian 10 (Buster)

- 1 [Configurer la Debian](#)
 - 1.1 [Ajouter les backports dans le dépôt](#)
 - 1.2 [Mettre à jour le système](#)
 - 1.3 [Installation des paquets nécessaire](#)
 - 1.4 [Configurer la variable d'environnement JAVA](#)
 - 1.5 [Vérifier la variable d'environnement](#)
 - 1.6 [Configurer Tomcat9](#)
 - 1.7 [Configurer le Tomcat9 manager](#)
 - 1.8 [Redémarrer Tomcat](#)
- 2 [Pré-installe Apereo / CAS](#)
 - 2.1 [Ajout de module LDAP \(Dépendance\)](#)
 - 2.2 [Ajouter dans le fichier cas.properties la configuration LDAP](#)
 - 2.3 [Vérification du port de connexion LDAP 389](#)
 - 2.4 [Vérification du port de connexion LDAP 636](#)
 - 2.5 [Création du dossier log pour CAS](#)
 - 2.6 [Copie des fichiers cas.log et cas_audit.log](#)
 - 2.7 [Droit sur le dossier](#)
 - 2.8 [Installation de Gradle](#)
 - 2.9 [Création de la clé #](#)
- 3 [Choix de la Configuration des applications](#)
- 4 [Configuration du Json](#)
 - 4.1 [Configurer le fichier cas.properties](#)
 - 4.2 [Création du dossier services](#)
 - 4.3 [Ajouter les applications](#)
 - 4.4 [Création du fichier json](#)
 - 4.5 [Configuration des applications](#)

Configurer la Debian

Ajouter les backports dans le dépôt

```
echo "deb http://deb.debian.org/debian buster-backports main contrib non-free" >> /etc/apt/sources.list
```

Mettre à jour le système

```
#apt update
```

```
#apt upgrade
```

Installation des paquets nécessaire

```
#apt install tomcat9 tomcat9-admin tomcat9-user openjdk-11-jdk openjdk-11-jre maven build-essential git
```

Configurer la variable d'environnement JAVA

```
#echo "JAVA_HOME=/usr/lib/jvm/java-11-openjdk-amd64/" >> /etc/environment
```

```
#source /etc/environment
```

Vérifier la variable d'environnement

```
echo $JAVA_HOME
```

Configurer Tomcat9

Aller dans /etc/default
Ouvrir le **fichier tomcat9**
Rajouter la ligne suivante :

```
JAVA_HOME=/usr/lib/jvm/java-11-openjdk-amd64
```

Vérifier de nouveau si vous avez Java 11

```
update-alternatives --display java
```

Configurer le Tomcat9 manager

Aller dans /etc/tomcat9
Ouvrir le fichier **tomcat-users.xml**
Tout en bas du fichier mettre

```
<role rolename="admin-gui"/>  
<user username="admin" password="toor" roles="manager-gui,admin-gui"/>
```

Redémarrer Tomcat

```
systemctl restart tomcat9
```

Mettre TOMCAT9 en HTTPS.

Vérifier que le port 80 et 443 sort bien vers l'extérieur.

Maintenant nous allons utiliser Let's Encrypt

Pour installer cerbot via les paquet

```
apt install python-certbot-apache
```

Utiliser la commande suivante pour avoir le domaine en https :

```
certbot --apache -d cas.domaine-univ.fr
```

il vous demande de mettre votre adresse mail.

Suivre les indications.

Récupérer le chemin où se trouve le fichier pem qui vous donne let's encrypt

Il vous donne le chemin où se trouve le fichier pem.

IMPORTANT NOTES:

- Congratulations! Your certificate and chain have been saved at:
/etc/letsencrypt/live/cas.domaine-univ.fr/fullchain.pem

Your key file has been saved at:
/etc/letsencrypt/live/cas.domaine-univ.fr/privkey.pem

- Your cert will expire on 2021-06-31. To obtain a new or tweaked version of this certificate in the future, simply run certbot again with the "certonly" option.
To non-interactively renew *all* of your certificates, run "certbot renew"
- Your account credentials have been saved in your Certbot configuration directory at **/etc/letsencrypt**. You should make a secure backup of this folder now.
This configuration directory will also contain certificates and private keys obtained by Certbot so making regular backups of this folder is ideal.

Créer le dossier pour les fichiers SSL

J'ai créé un dossier dans **/opt/tomcat/conf**

```
Mkdir /opt/tomcat/conf
```

```
Mkdir /opt/tomcat
```

```
Mkdir /opt/tomcat/conf
```

J'ai copié les trois fichiers dans **/opt/tomcat/conf** :

```
cp cert.pem chain.pem privkey.pem /opt/tomcat/conf
```

J'ai mis les droits pour les fichiers *.pem :

```
chown tomcat:tomcat *.pem
```

Ajouter des lignes SSL sur le serveur Tomcat9

Je suis allé dans **/etc/tomcat9/server.xml**

J'ai ajouté les lignes suivantes :

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150" SSLEnabled="true">
  <SSLHostConfig>
    <Certificate certificateFile="/opt/tomcat/conf/cert.pem"
      certificateKeyFile="/opt/tomcat/conf/privkey.pem"
      certificateChainFile="/opt/tomcat/conf/chain.pem" />
    </SSLHostConfig>
  </Connector>
```

J'ai redémarré tomcat

Pré-installer Apereo / CAS

Nous commençons par installer le projet nécessaire à l'utilisation de cas-overlay-Template

Récupérer le projet

Aller dans le dossier /opt

```
#git clone https://github.com/apereo/cas-overlay-template
```

Ouvrir le dossier cas-overlay-template

```
#cd cas-overlay-template
```

Ajout de module LDAP (Dépendance)

Ouvrir le **fichier build.gradle**

Ajouter les 3 lignes en gras ci-dessous :

```
dependencies {
    // Add modules in format compatible with overlay casModules property
    if (project.hasProperty("casModules")) {
        def dependencies = project.getProperty("casModules").split(",")
        dependencies.each {
            def projectsToAdd = rootProject.subprojects.findAll {project ->
                project.name == "cas-server-core-${it}" || project.name == "cas-server-support-${it}"
            }
            projectsToAdd.each {implementation it}
        }
    }
    // CAS dependencies/modules may be listed here statically...

implementation "org.apereo.cas:cas-server-webapp-init:${casServerVersion}"
implementation "org.apereo.cas:cas-server-support-ldap:${project.cas.version}"
implementation "org.apereo.cas:cas-server-support-json-service-registry:${casServerVersion}"
}
```

Enregistrer le fichier

Ajouter dans le fichier cas.properties la configuration LDAP

Aller dans /opt/cas-overlay-template/etc/cas/config/cas.properties

```
cas.server.name=https://cas.domaine-univ.fr:8443
cas.server.prefix=${cas.server.name}/cas
logging.config: file:/etc/cas/config/log4j2.xml
```

ATTENTION ENLEVER LE # POUR ÊTRE EN VERSION PRODUCTION

cas.authn.accept.users=

```
#### Desactivation des comptes locaux

cas.authn.accept.users=
#### Connexion LDAP
cas.authn.ldap\[0\].providerClass=org.ldaptive.provider.unboundid.UnboundIDProvider
cas.authn.ldap\[0\].type=AUTHENTICATED
cas.authn.ldap\[0\].useSsl=false
cas.authn.ldap\[0\].ldapUrl=ldap://domaine-univ.fr:389
cas.authn.ldap\[0\].baseDn= dc= domaine-univ,dc=fr
cas.authn.ldap\[0\].subtreeSearch=true
cas.authn.ldap\[0\].searchFilter=sAMAccountName=\{user\}
cas.authn.ldap\[0\].principalAttributeList=cn,givenName,mail

#### Credential to connect to LDAP
cas.authn.ldap\[0\].bindDn=CN=Admincas,CN=CasAdmin,DC= domaine-univ,DC=fr
cas.authn.ldap\[0\].bindCredential=P@ssw0rd
```

Activation en LDAPS

Par contre si vous voulez mettre le LDAP en LDAPS

Il vous faudra activer userSsl=true

```
cas.authn.ldap\[0\].useSsl=false
```

Vérification du port de connexion LDAP 389

```
telnet domaine-univ.fr 389
```

Si vous avez ce message-là :
Trying 192.168.0.54...
Connected to [domaine-univ.fr](#).
Escape character is '^['.
C'est ok.

Vérification du port de connexion LDAP 636

```
telnet domaine-univ.fr 636
```

Si vous avez ce message-là :
Trying 192.168.0.54...
Connected to [domaine-univ.fr](#).
Escape character is '^['.
C'est ok.

Création du dossier log pour CAS

Créer un dossier dans /var/log/cas

```
mkdir /var/log/cas
```

Copie des fichiers cas.log et cas_audit.log

Copier ou créer les fichiers cas.log et cas_audit.log dans le dossier

Droit sur le dossier

Pour mettre les droits sur le dossier faire la commande suivante :

```
chown -R tomcat:adm /var/log/cas
```

Modifier le fichier log4j2.xml dans le dossier cas-overlay-template-master/etc/cas/config

Mettre à la place de

```
<Property name="baseDir">/var/log</Property>
```

```
<Property name="baseDir">/var/log/cas</Property>
```

Enregistrer le fichier

Installation de Gradle

```
./gradlew clean
```

#.

```
./gradlew clean copyCasConfiguration build
```

Création de la clé

#

```
./gradlew createKeystore
```

Il faut récupérer le fichier

Copier le fichier cas.war

```
cp /opt/cas-overlay-template/build/libs/cas.war /var/lib/tomcat9/webapps/
```

Relancer le service de Tomcat9

```
systemctl restart tomcat9.service
```

Maintenant nous allons tester la connexion

Pour ici l'adresse ip est : <https://cas.domaine-univ.fr:8443/cas>

Cliquer sur « **se connecter** »



Connexion



Entrez votre identifiant et votre mot de passe.

Identifiant :

Mot de passe :

SE CONNECTER

 [Mot de passe oublié ?](#)

Pour des raisons de sécurité, veuillez vous [déconnecter](#) et fermer votre navigateur lorsque vous avez fini d'accéder aux services authentifiés.

Connexion non sécurisée

Vous accédez actuellement au serveur CAS via une connexion non sécurisée. L'authentification unique NE FONCTIONNERA PAS. Pour faire fonctionner l'authentification unique, vous devez vous authentifier en HTTPS.

Liens vers les ressources CAS

-  [Actuator Endpoints](#)
-  [Documentation](#)
-  [Pull Requests](#)
-  [Guide pour les contributeurs](#)
-  [Listes de diffusion](#)
-  [Salon de discussion](#)
-  [Blog](#)

Copyright © 2005–2018 Apereo, Inc. Powered by Apereo Central Authentication Service 6.0.4 2019-05-21T07:23:20Z

Quand vous êtes connectés, vous devez avoir ce message-là : **Connexion réussie**

Connexion réussie

Bienvenue **admincas**. Vous vous êtes authentifié(e) auprès du Service Central d'Authentification. Toutefois, vous voyez cette page car CAS ne connaît pas votre destination finale ni comment vous y rediriger. Examinez la requête d'authentification et assurez-vous qu'une application ou service cible autorisé et enregistré auprès de CAS est spécifié.

[Click here](#) to view attributes resolved and retrieved for **admincas**.

Pour des raisons de sécurité, veuillez vous [déconnecter](#) et fermer votre navigateur lorsque vous avez fini d'accéder aux services authentifiés.

Liens vers les ressources CAS

- [Actuator Endpoints](#)
- [Documentation](#)
- [Pull Requests](#)
- [Guide pour les contributeurs](#)
- [Listes de diffusion](#)
- [Salon de discussion](#)
- [Blog](#)

Copyright © 2005–2018 Apereo, Inc. Powered by Apereo Central Authentication Service 6.0.4 2019-05-21T07:23:20Z

En cliquant sur

Connexion réussie

Bienvenue **admincas**. Vous vous êtes authentifié(e) auprès du Service Central d'Authentification. Toutefois, vous voyez cette page car CAS ne connaît pas votre destination finale ni comment vous y rediriger. Examinez la requête d'authentification et assurez-vous qu'une application ou service cible autorisé et enregistré auprès de CAS est spécifié.

[Click here](#) to view attributes resolved and retrieved for **admincas**.

Pour des raisons de sécurité, veuillez vous [déconnecter](#) et fermer votre navigateur lorsque vous avez fini d'accéder aux services authentifiés.

Attribute	Value(s)
cn	[Admincas]
givenName	[Cas]

Nous pouvons voir les attributs de l'active Directory.

Choix de la Configuration des applications

Nous avons le choix pour configurer les applications soit avec :

- Avec Json
- Base de donnée module JPA

Pour démarrer nous allons utiliser le Json.

Configuration du Json

Vérifier que dans le fichier **build.gradle** nous avons bien :

```
implementation "org.apereo.cas:cas-server-support-json-service-registry:${project.'cas.version'}"
```

Une fois vérifier nous pouvons commencer.

Configurer le fichier cas.properties

Ouvrir le fichier cas.properties

```
cd \opt\cas-template-overlay
```

```
nano etc/cas/config/cas.properties
```

Ajouter la ligne ci-dessous :

Configuration de JSON

```
cas.serviceRegistry.json.location: file:/etc/cas/services
```

Une fois que la ligne a été ajouté nous devons créer un dossier.

Création du dossier services

Nous utilisons la commande mkdir pour créer le dossier

```
mkdir /etc/cas/services
```

Ajouter les applications

Nous allons créer pour chaque applications un fichier en « .json »
Il est recommandé de nommer les nouveaux fichiers JSON comme suit:

```
serviceName-serviceNumericId.json"
```

Pour créer l'ID nous utilisons la commande suivant :

```
date +%s
```

Voici ce qui donne

```
root@cas:/opt/cas-overlay-template# date +%s  
1559915619
```

Ce numéro est notre ID.
Donc le fichier sera « application-1559915619.json »
Le fichier doit être dans /etc/cas/services/

Création du fichier json

« Application » est le nom de votre application dans cette exemple

```
touche application-1559915619.json
```

Configuration des applications

Ouvrir le fichier que nous venons de créer

```
nano application-1559915619.json
```

Attention l'exemple ci-dessous à éviter à l'utilisation

```
{
/*
Ne pas utiliser cette définition dans un environnement de production.
*/
"@class" : "org.apereo.cas.services.RegexRegisteredService",
"serviceId" : "^(https|imaps)://.*",
"name" : "HTTPS and IMAPS wilcard",
"id" : 1503925297,
"evaluationOrder" : 99999
}
```

Voici pour l'application Rocketchat

Ouvrir le fichier http_rocketchat-1559902436.json

```
nano http_rocketchat-15599902436
```

```
{
"@class" : "org.apereo.cas.services.RegexRegisteredService",
"serviceId" : "^(http://192.168.0.111/_cas/.*)",
"name" : "Rocketchat",
"id" : 1503925297,
"evaluationOrder" : 99999
}
```

Aller dans RocketChat mettre les informations du serveur cas.

URL de base pour SSO : <https://cas.domaine-univ.fr:8443/cas>

URL de login SSO : <https://cas.domaine-univ.fr:8443/cas/login>

CAS

Annuler

Sauvegarder les modifications

Activé ☒ Oui ☐ Non

↺

URL de base pour SSO

↺

URL de base pour votre service externe de connexion SSO, par exemple: http://sso.example.com/sso/

URL de login SSO

↺

URL de connexion pour votre service externe de connexion SSO, par exemple : http://sso.example.com/sso/

Version CAS

2.0

↺

Utiliser seulement une version de CAS supportée par votre service CAS SSO

Réinitialiser les paramètres de la section

Réinitialiser

Vous devez mettre vos attributs



Toujours synchroniser les données utilisateur ☒ Oui ☐ Non

Toujours synchroniser les données externes de l'utilisateur CAS avec les attributs disponibles après connexion. Note : dans tous les cas, les attributs sont toujours synchronisés après la création du compte.

Attributs de carte

`{"cn":"name", "mail":"email"}`



Utilisez cette entrée JSON pour créer des attributs internes (clé) à partir d'attributs externes (valeur).

Exemple: `{" email ":"% email% "," name ":"% prénom%,% nom% "}`

La carte d'attributs est toujours interpolée. Dans CAS 1.0, seul l'attribut `username` est disponible. Les attributs internes disponibles sont: nom d'utilisateur, nom, adresse e-mail, chambres: rooms est une liste de pièces séparées par des virgules à joindre lors de la création de l'utilisateur, par exemple: ("rooms": "% team%% department%") rejoindrait les utilisateurs CAS lors de la création de leur équipe et canal départemental.

Réinitialiser les paramètres de la section

Réinitialiser

Ouvrir la page de RocketChat pour ici c'est 192.168.0.113:3000

Cliquer sur AUTHENTIFICATION CAS



ROCKET.CHAT

AUTHENTIFICATION CAS

Adresse e-mail ou nom d'utilisateur

Mot de passe

Se connecter

Créer un nouveau compte

Mot de passe oublié

By proceeding you are agreeing to our [Terms of Service](#), [Privacy Policy](#) and [Legal Notice](#).

Powered by [Open Source Chat Platform Rocket.Chat](#).

English Version

La page s'ouvre et nous voyons que RocketChat est bien dans CAS

Mettre son identifiant et son mot de passe du serveur AD

Connexion



Entrez votre
identifiant et votre
mot de passe.

Identifiant :

Mot de passe :

SE CONNECTER

 [Mot de passe oublié ?](#)

Pour des raisons de sécurité,
veuillez vous [déconnecter](#) et
fermer votre navigateur lorsque
vous avez fini d'accéder aux
services authentifiés.

RocketChat

RocketChat



Liens vers les ressources CAS

 [Actuator Endpoints](#)

 [Documentation](#)

 [Pull Requests](#)

 [Guide pour les
contributeurs](#)

 [Listes de diffusion](#)

 [Salon de discussion](#)

 [Blog](#)



Discussions

Canaux

 # general

Groupes privés

Vous ne faites partie d'aucun canal pour le moment.

Messages Privés

Vous ne faites partie d'aucun canal pour le moment.

 ROCKET.CHAT

Home

Welcome to Rocket.Chat!

The Rocket.Chat desktops apps for Windows, macOS and Linux are available to download [here](#).

The native mobile app, Rocket.Chat, for Android and iOS is available from [Google Play](#) and the [App Store](#).

For further help, please consult the [documentation](#).

If you're an admin, feel free to change this content via **Administration → Layout → Home Body**. Or clicking [here](#).