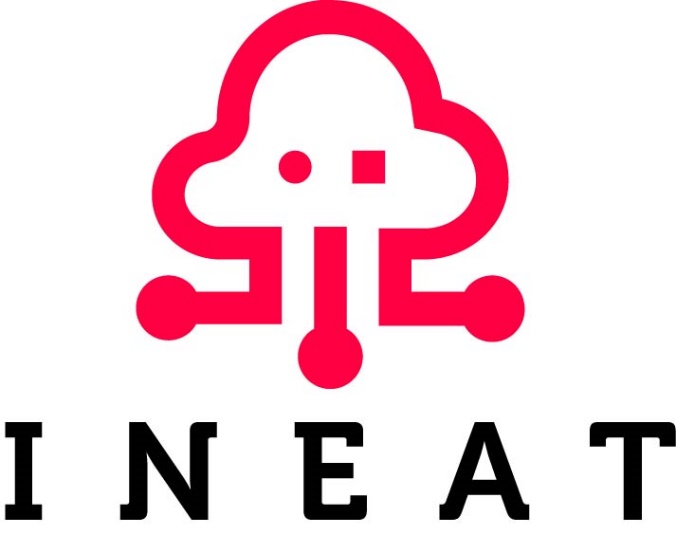
Mise en Production



GAMMELIN Anthony

**Gestion des versions**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Auteur | Etat | Modifications |
| 1.0 | 01/09/17 | GAMMELIN Anthony |  | Création du Document |

**DIFFUSION**

|  |  |  |  |
| --- | --- | --- | --- |
| Entité | Destinataires | Pour validation | Pour information |
| INEAT | Jimmy PAEPEGAEY | x |  |
| INEAT |  |  | x |
| Ease |  |  | x |

Sommaire

[1. Description de la plateforme 3](#_Toc492041604)

[1.1 Sizing & Applicatifs des machines 3](#_Toc492041605)

[1.1.1 Préproduction 3](#_Toc492041606)

[1.1.2 Production 5](#_Toc492041607)

[2 Patch Management 7](#_Toc492041608)

[2.1 Procédure Générale 7](#_Toc492041609)

[2.2 Utilisation de apt 7](#_Toc492041610)

[3 SSL Management 8](#_Toc492041611)

[3.1 Génération d’un Certificat 9](#_Toc492041612)

[4 Mise en Production 10](#_Toc492041613)

[4.1 Tomcat 10](#_Toc492041614)

[4.2 Base de Données 10](#_Toc492041615)

# Description de la plateforme

La plateforme Ease est hébergée sur le Cloud INEAT (ATE) les machines virtuelles composant la plateforme sont gérées via HyperV et administrées via la console SCVMM.

## Sizing & Applicatifs des machines

### Préproduction

La plateforme de préproduction est composée de 2 machines (Front & Back), elle est isolée de la production et a pour but de recetter l’applicatif sur des versions de composants système ISO Prod.

Le schéma d’infrastructure de préproduction est le suivant :



Le sizing des machines (Iso Prod) est le suivant :

* Une Virtual Machine VM EASE-PPR-FE (Nginx)

|  |  |  |
| --- | --- | --- |
| **Model VM** | **OS / Soft** | **NIC / @ip** |
| (1 cores, 4 GB memory) | Linux Debian 9.1  Tomcat 8.5.14  Apache 2.4 | Eth0 / 10.12.218.10 |

* Une Virtual Machine VM EASE-PPR-DB (Mariadb)

|  |  |  |
| --- | --- | --- |
| **Model VM** | **OS / Soft** | **NIC / @ip** |
| (1 cores, 4 GB memory) | Linux Debian 9.1  MariaDB 10.1.26 | Eth0 / 10.12.218.11 |

Les composants système en place en préproduction sont les suivants :

* Serveur Web Tomcat (80 / 443) – Front
* Serveur Apache (80 / 443) – Front
* MariaDB – Back

### Production

La plateforme de production est composée de 2 machines ( 1 Front & 1 Back ), elle est isolée de la préproduction.

Le schéma d’infrastructure de production est le suivant :



Le sizing des machines est le suivant :

* + - VM EASE-PROD-FE (Tomcat)

|  |  |  |
| --- | --- | --- |
| **Modèle VM** | **OS / Soft** | **NIC / @ip** |
| (1 cores, 4 GB memory) | Linux Debian 9.1  Tomcat 8.5.14  Apache 2.4 | Eth0 / 10.12.217.10 |

* + - VM EASE-PROD-DB1 (MariaDB)

|  |  |  |
| --- | --- | --- |
| **Modèle VM** | **OS / Soft** | **NIC / @ip** |
| (1 cores, 4 GB memory) | Linux Debian 9.1  MariaDB 10.1.26 | Eth0 / 10.12.217.11 |

Les composants système en place en production sont les suivants :

* Front :
  + Apache2 & Mod\_Security
  + Tomcat8
* Backs :
  + MariaDB

# Patch Management

## Procédure Générale

Attention il faut toujours consulter le client avant chaque mise à jour système

Afin de palier à d’éventuels problèmes applicatif suite aux patchs des machines, il faut effectuer un Snapshot des VMs avant toutes mise à jour de plus il faut effectuer le patch de la préproduction en avance de phase.

## Utilisation de apt

Mise à jours d’un système Debian.

|  |
| --- |
| # sudo apt-get update;sudo apt-get upgrade;sudo apt-get dist-upgrade; sudo apt-get autoremove |

# SSL Management

Ce chapitre décrit la procédure de changement de certificat SSL sur la plateforme Ease.  
Afin de sécuriser au maximum le trafic, le certificat est desservi par le WAF ainsi que par Tomcat, il est donc nécessaire de le changer pour chaque composant.

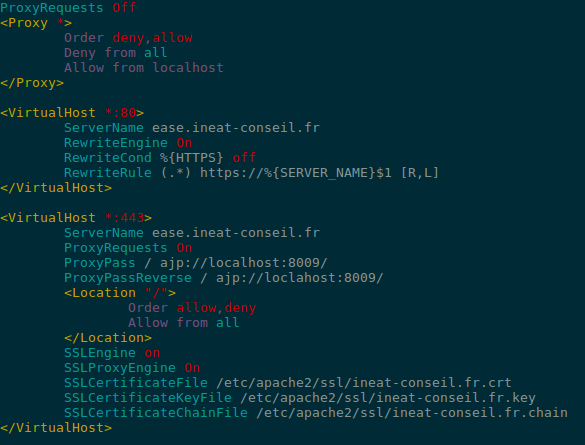
Le tomcat embarque les certificats dans un conteneur JKS qui se devra d’être généré. Il sera stocké au même emplacement que les certificats d’apache

Pour le FRONT les certificats sont stocké dans :

|  |
| --- |
| root@easeweb001:~# ll **/etc/apache2/ssl/**  total 28  drwxrwxr-x 2 root root 4096 août 29 10:10 .  drwxr-xr-x 9 root root 4096 août 29 10:10 ..  -rw-r--r-- 1 root root 1590 août 29 10:10 ineat-conseil.fr.chain  -rw-r--r-- 1 root root 1920 août 29 10:10 ineat-conseil.fr.crt  -rw-r--r-- 1 root root 4312 août 29 10:10 ineat-conseil.fr.jks  -rw-r--r-- 1 root root 1705 août 29 10:10 ineat-conseil.fr.key |

La configuration du certificat pour la partie Apache est dans le fichier suivants :

**/etc/apache2/sites-enabled/waf.conf :**



La configuration pour la partie tomcat ce fait dans le fichier **server.xml** à la racine de **/etc/tomcat8/**

|  |
| --- |
| <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"  useSendfile="false"  compression="force"  compressionMinSize="1024"  noCompressionUserAgents="gozilla, traviata"  compressableMimeType="text/html,text/xml,text/javascript,text/css,application/javascript"  maxThreads="150" SSLEnabled="true" scheme="https" secure="true"  clientAuth="false" sslProtocol="TLS"  keystoreFile="**/etc/apache2/ssl/ease-keystore.jks**"  keystorePass="**PASSWORD**" keyAlias="**ease-keystore**"  keyPass="**PASSWORD**" /> |

## Génération d’un Certificat

Pour sécuriser la plateforme nous utiliserons un certificat SSL généré par Lets’encryt, ce chapitre décrit la procédure de génération d’un nouveau certificat ainsi que la création d’un Keystore pour Tomcat.

Pour générer un nouveau certificat nous utiliserons **certbot** c’est un applicatif mis à disposition par Let’s Encrypt qui effectue les vérifications nécessaires à la délivrance d’un certificat et le génère ensuite. Cette applicatif s’utilise directement sur le serveur FRONT de la manière suivante :

|  |
| --- |
| ./certbot-auto certonly --webroot --webroot-path /var/www/html --domain ease.space --email ease-support@ineat-conseil.fr |

Une fois les certificats généré nous pouvons créer un keystore pour Java, cependant nous devons d’abord passer par un Keystore au format PKCS12, pour cela nous utiliserons les commandes suivantes :

|  |
| --- |
| openssl pkcs12 -export -in ease.space.crt -inkey ease.space.key -out ease.space.p12 |

Une fois le Keystore PKCS12 créé nous pourrons le convertir en Keystore JKS via la commande suivante :

|  |
| --- |
| keytool -importkeystore -destkeystore ease.space.jks -srckeystore ease.space.p12 -srcstoretype pkcs12 |

La création des Keystore implique la mise en place de mot de passe. Ceux-ci doivent être stocker dans les Coffres Fort numérique du Cloud Ineat et mis à jour au niveau de la configuration du tomcat.

# Mise en Production

Ce chapitre décrit la procédure de mise en production pour la plateforme Ease.

Les étapes décrites sont identiques que ce soit pour la production ou la pré-production à la différence que pour la production, le **WAR** à récupérer dans **SharePoint** est nommé **Prod.war** et pour le pré-production, il est nommé **Preprod.war**

## PREMIERE MISE EN PRODUCTION

Pour effectuer la première mise en production, nous effectuerons les étapes suivantes :

* Upload de l’archive sur le serveur WEB depuis le **SharePoint** commun avec **Ease**
* Eteindre l’ancien serveur Ease à l’adresse **51.255.82.184**

|  |
| --- |
| root@easeweb001: **ssh jimmy@ease.space**  root@old\_ease**: sudo systemctl stop tomcat8** |

* Effectuer le dump de la base de données

|  |
| --- |
| root@old\_ease**: mysqldump -u jimmy -p --add-drop-table --complete-insert --databases ease > ease\_backup.sql** |

* Récupération de la base de données via **scp**

|  |
| --- |
| root@easeweb001**: scp jimmy@ease.space:ease\_backup.sql ease\_backup.sql** |

* Stop de tomcat et purge du dossier **/var/li/tomcat8/webapps/**

|  |
| --- |
| root@easeweb001**: systemctl stop tomcat8**  root@easeweb001**: cd /var/lib/tomcat8/webapps**  root@easeweb001**: rm -rf \*** |

* Initialisations de la base de données

|  |
| --- |
| MariaDB [(none)]> **DROP DATABASE ease;**  Query OK, 87 rows affected (2.37 sec)  MariaDB [(none)]> **CREATE DATABASE ease CHARACTER SET utf8 COLLATE utf8\_general\_ci;**  Query OK, 1 row affected (0.00 sec) |

|  |
| --- |
| root@easeweb001**: mysql –u root –p ease < ease\_backup.sql** |

* Copie du nouveau .war dans **/var/lib/tomcat8/webapps/** ( Le fichier doit s’appeler ROOT.war, remplacer **Prod.war** par **Preprod.war** au besoin)

|  |
| --- |
| root@easeweb001: **cp /home/admin/PROD.war ROOT.war** |

* Redémarrage de **tomcat**

|  |
| --- |
| root@easeweb001: **systemctl start tomcat8** |

## Base de Données

En cas de mise à jour de la base de données nous procéderons de la manière suivante.

* Upload du script SQ sur le serveur de la base de données depuis le **SharePoint** commun avec **Ease**
* Eteindre **tomcat** sur le serveur tomcat8 pour éviter l’altération des données

|  |
| --- |
| root@easeweb001**: systemctl stop tomcat8** |

* Backup de la base actuelle en cas de RollBack

|  |
| --- |
| root@easebdd001:/var/lib/mysql/backup# **mysqldump -u root -p --add-drop-table --complete-insert --databases ease > ease\_backup.sql** |

* Une fois le Dump effectué on exécute le script d’update de la base de données

|  |
| --- |
| root@easebdd001: **mysql –u root –p ease < update.sql** |

## Tomcat

Pour la partie tomcat, en cas de mise en production le client nous fournira une archive de l’application au format .WAR  
Pour effectuer la mise en production nous effectuerons les étapes suivantes :

* Upload de l’archive sur le serveur WEB depuis le **SharePoint** commun avec **Ease**
* Eteindre **tomcat**

|  |
| --- |
| root@easeweb001**: systemctl stop tomcat8** |

* Purge du dossier **/var/lib/tomcat8/webapps/**

|  |
| --- |
| root@easeweb001**: cd /var/lib/tomcat8/webapps**  root@easeweb001**:** **rm -rf \*** |

* Copie du nouveau .war dans **/var/lib/tomcat8/webapps/** ( Le fichier doit s’appeler ROOT.war, remplacer **Prod.war** par **Preprod.war** au besoin)

|  |
| --- |
| root@easeweb001: **cp /home/admin/Prod.war ROOT.war** |

* Une fois l’archive en place il faut redémarrer le tomcat et vérifier son fonctionnement

|  |
| --- |
| root@easeweb001: **systemctl start tomcat8** |