|  |  |
| --- | --- |
| https://upload.wikimedia.org/wikipedia/fr/thumb/6/6e/Maroc_telecom_logo.svg/langfr-220px-Maroc_telecom_logo.svg.png | **TMA GRC**  Configuration WAS- V{REF\_LIVRAISON} |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Diffusion** | | | | |
| **Destinataire** | **Organisme ou entreprise** | **Nombre** | **Pour action** | **Pour info** |
| {CP\_PRESTATAIRE} | ATOS | 1 | X |  |
| Khadija TAA | IAM | 1 |  | X |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Mises à jour** | | | |
| **Version** | **Date** | **Auteur** | **Motifs** |
| 1.0 | {DATE} | YAM | Création |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **Dépôt** | | |
| **URL** | **Accès anonyme ?** | **Administrateur** |
|  |  |  |
|  |  |  |

***SOMMAIRE***

# AJOUT des fichiers properties

## Objet

L’accès au WebService nécessite un ajout au niveau du fichier webservices.properties

## Procédure

* Connectez-vous avec le compte système virtuser **Sur les deux machines** : 10.100.11.203 et 10.100.11.205
* Positionnez-vous sur le répertoire /opt/grc/IBM/WebSphere/ext/GRCCluster1/properties/ en lançant la commande :

cd /opt/grc/IBM/WebSphere/ext/GRCCluster1/properties/

* Ajouter les lignes suivantes

savdegroupageforwana.username=DEGROUPAGE

savdegroupageforwana.password=ENC(bU5Dxk7duI1gbetZA2x0tKNGxx1o9eaC)

wanaDegroupage.user=dsl-eligibility

wanaDegroupage.password=ENC(JF/TsuEAmm9I4I4vfZaVp3iwj7SznWLFh1k/lpARpDM=)

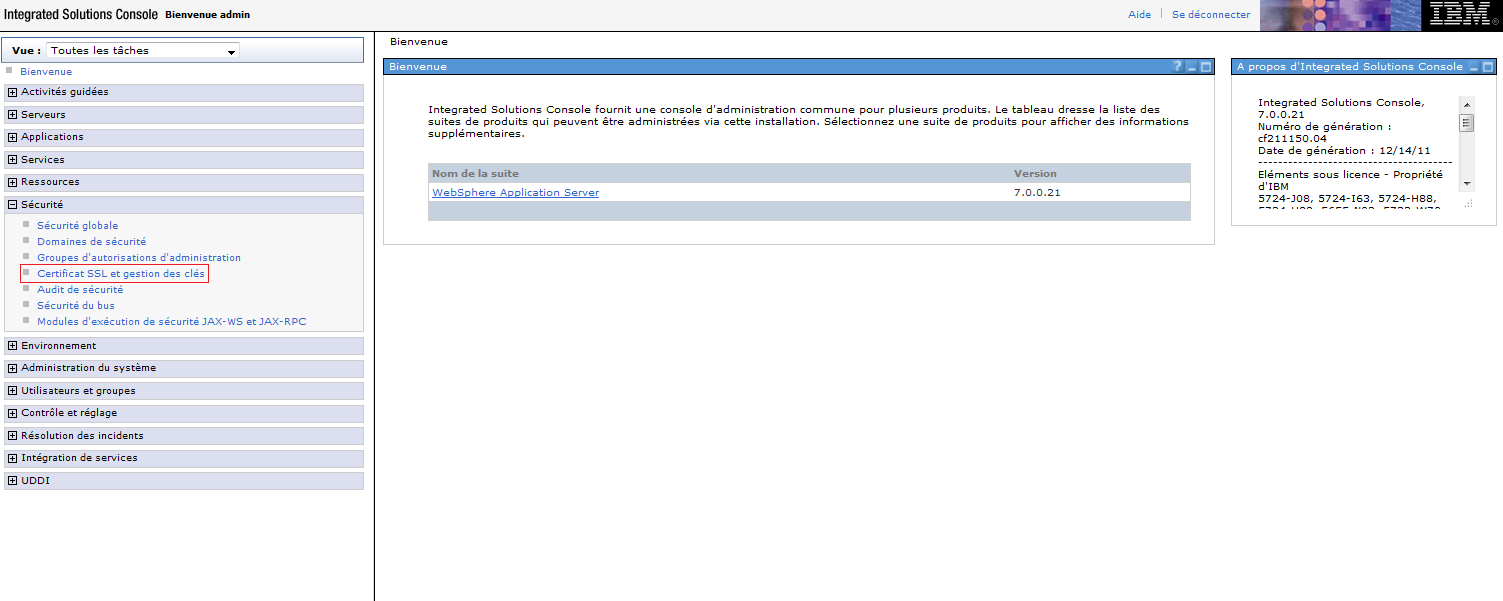
* Refaire la même procédure on se connectant cette fois au Cluster 2 :

cd /opt/grc/IBM/WebSphere/ext/GRCCluster2/properties/

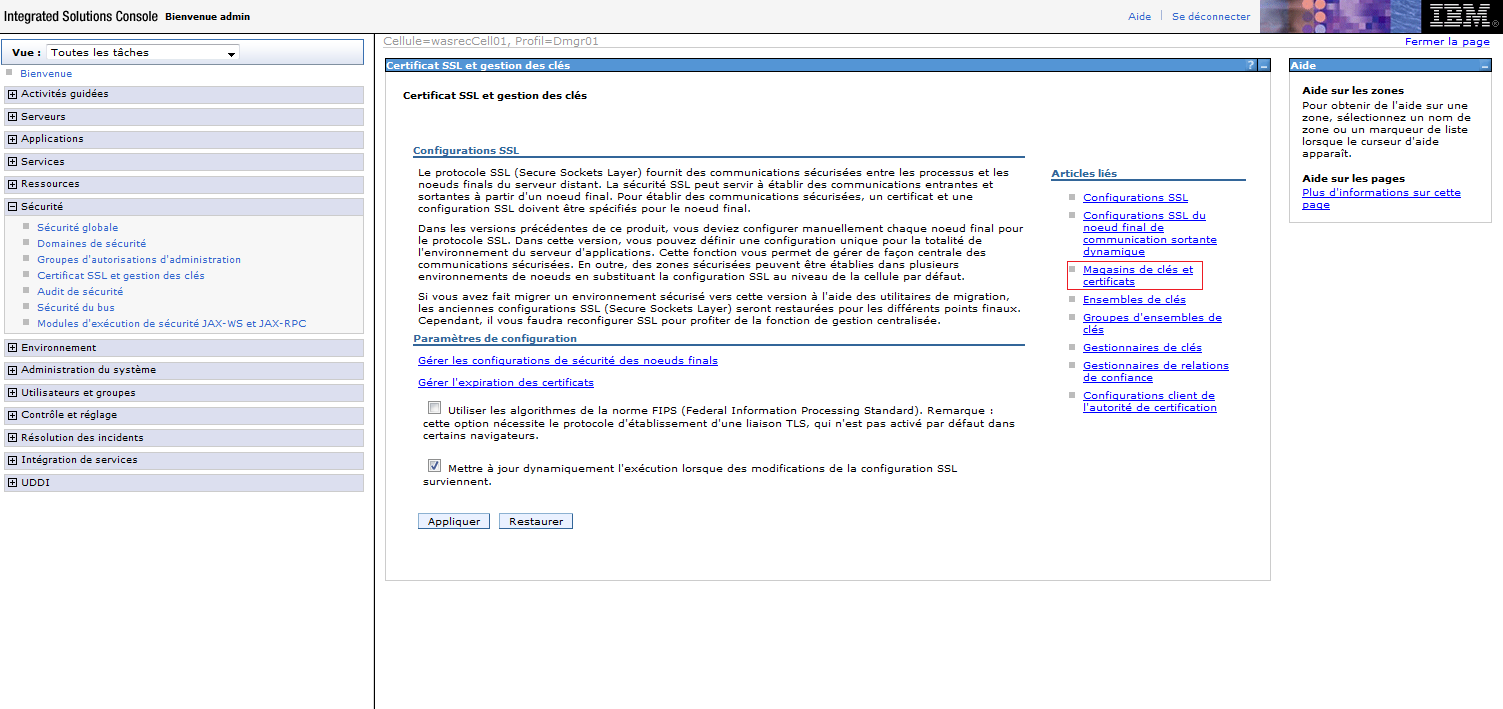
# Ajout de la certification WS

Se connecter à la console WAS GRC prod : <https://10.100.11.205:9043/ibm/console/> avec un utilisateur ayant les droits nécessaires d’administration WAS.

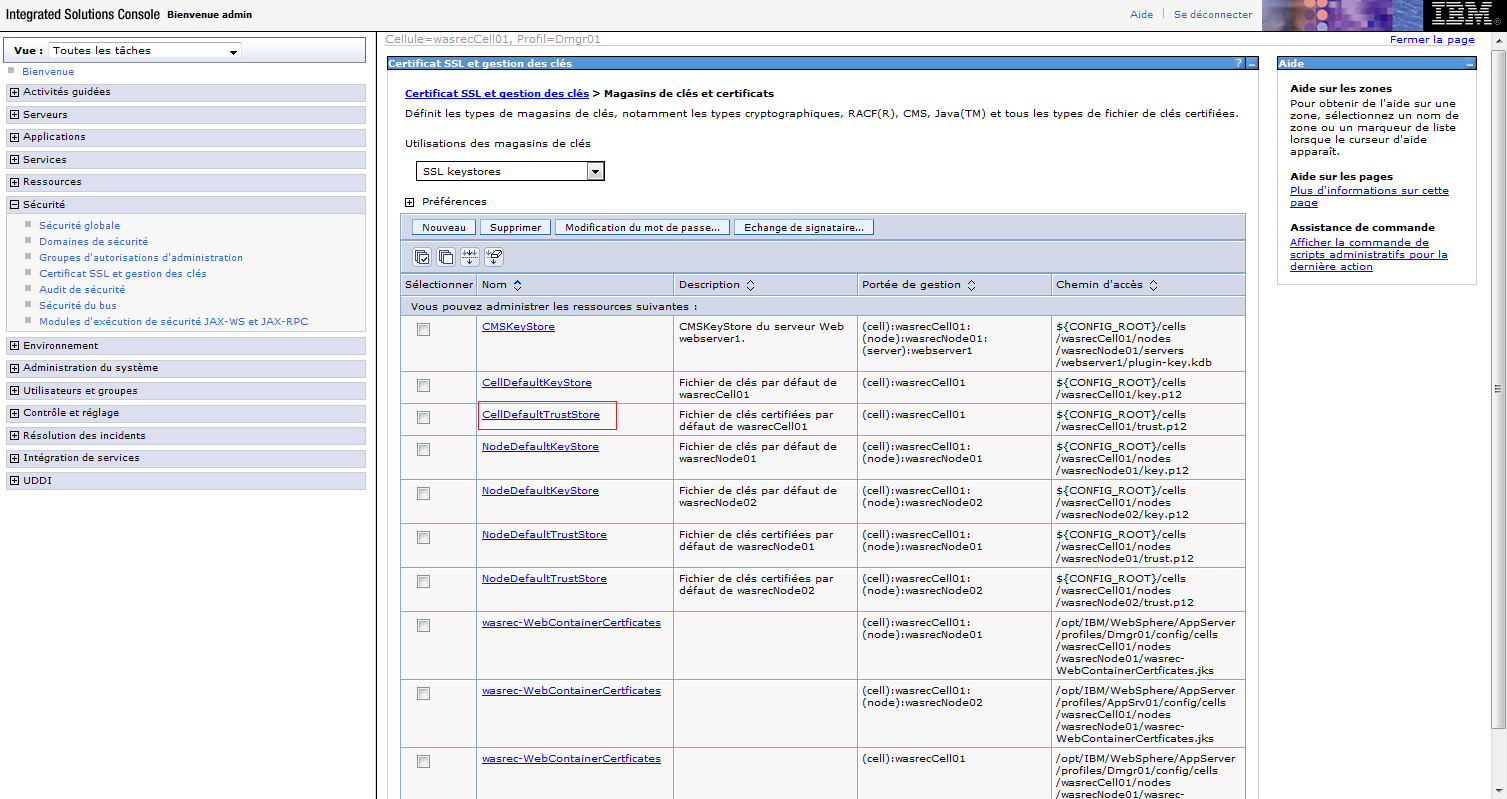
1 - Dérouler le menu Sécurité et choisir « Certificat SSL et gestions des clés »



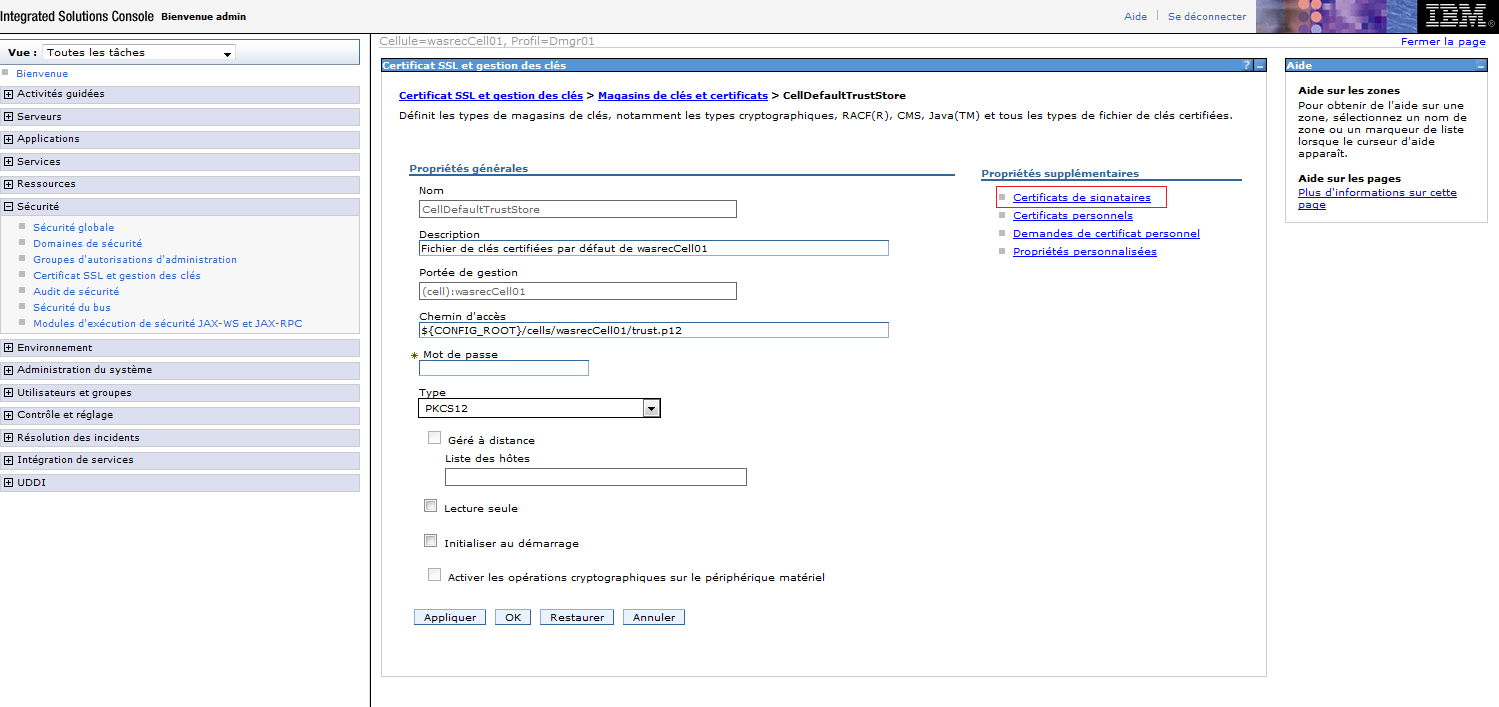
2 – Aller dans le menu « Magasins de clés et certificats »



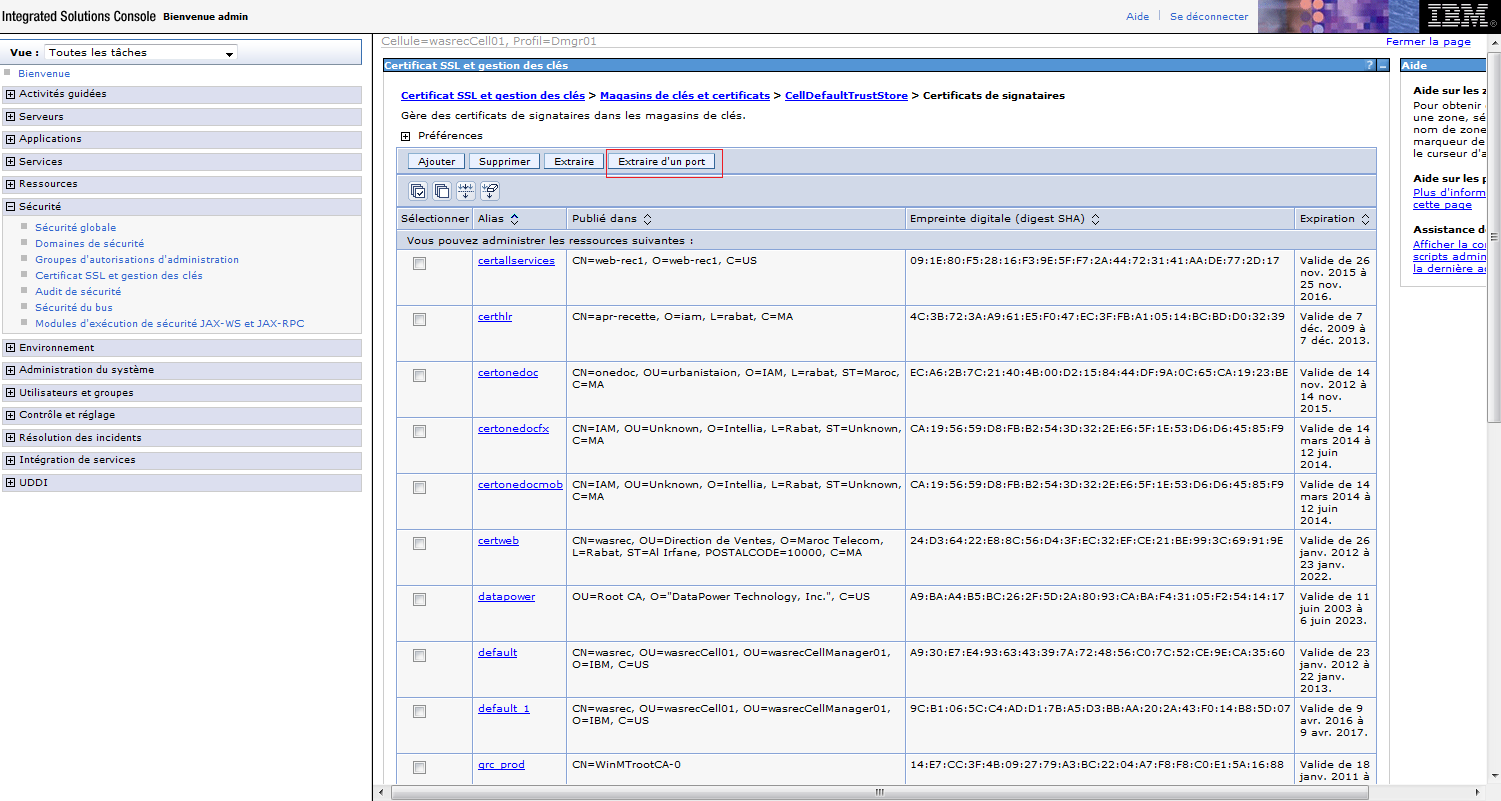
3 – Choisir « CellDefaultTrustStore »



4 - Aller dans le menu « Certificats de signataires »



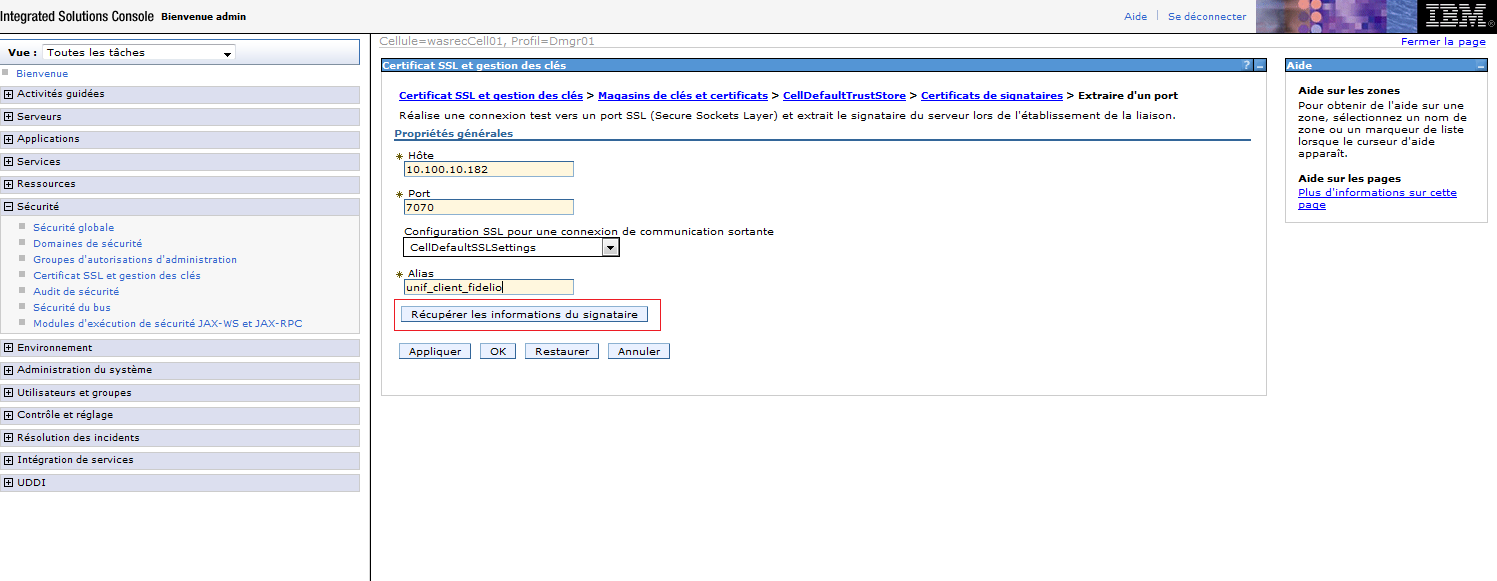
5 - Cliquer sur le bouton « Extraire d’un port »



6 – Rentrer les informations suivantes et cliquer sur le bouton « Récupérer les informations du signataire » :

* Hôte : 172.17.12.26
* Port : 443
* Configuration SSL : CellDefaultSSLSettings
* Alias : WANA\_PROXY

**N.B :** Si Websphere affiche un message indiquant que le certificat existe déjà, ignorer cette étape.



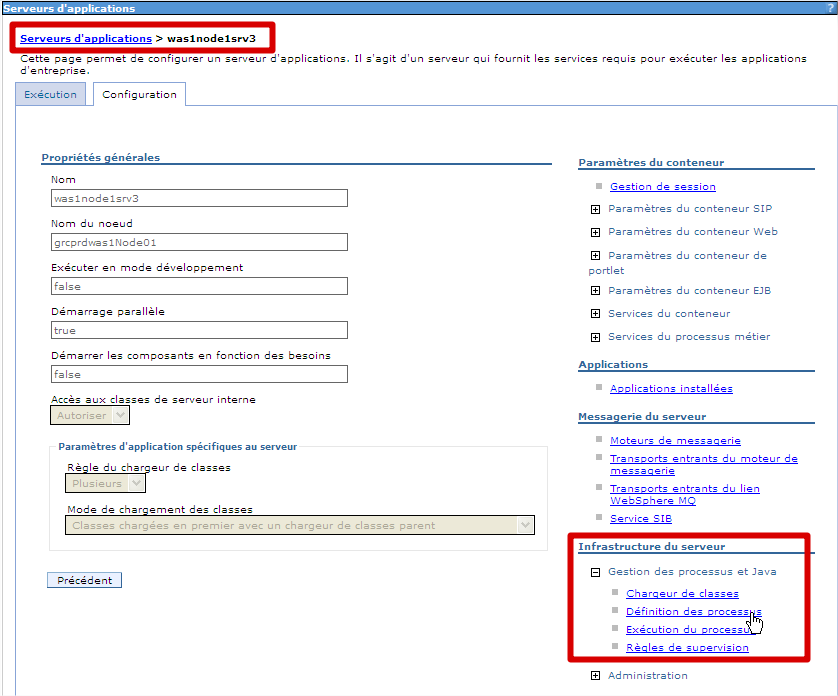
7 - Cliquer sur « OK » et sauvegarder la configuration.

# variable du batch

Se connecter à la console WAS GRC prod : <https://10.100.11.205:9043/ibm/console/> avec un utilisateur ayant les droits nécessaires de modification.

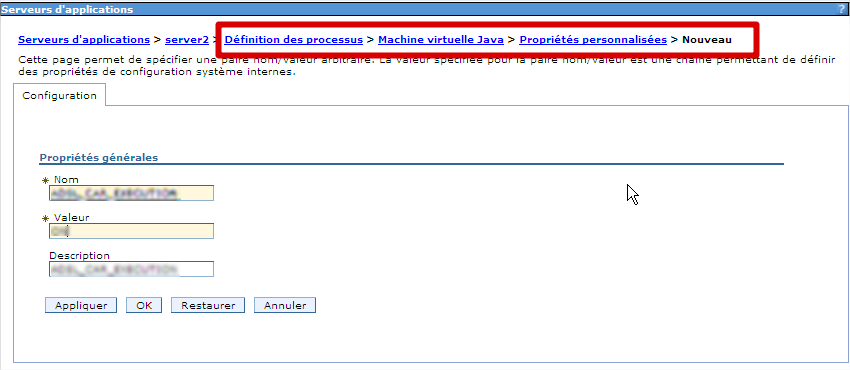
Accéder au serveur [was1node1srv4](https://10.100.11.205:9043/ibm/console/applicationServerCollection.do?csrfid=2119819430&EditAction=true&contextId=cells%3AGRCPRDWAS1Cell01%3Anodes%3AGRCPRDWAS1Node01%3Aservers%3Awas1node1srv4&resourceUri=server.xml&perspective=tab.configuration)

Aller sur le lien : « Infrastructure du serveur  Gestion des processus Java  définition des processus »



Ensuite, aller sur le menu : « Définition des processus  Machine virtuelle Java  Propriétés personnalisées »

Modifier la valeur de la variable SAV\_DEGROUPAGE\_BATCH\_EXECUTION et la positionner à la valeur ON si cette dernière n’a pas cette valeur (SAV\_DEGROUPAGE\_BATCH\_EXECUTION à **ON**)



Cliquer sur OK.

# Ajout du certificat AU NIVEAU DU jdk

* Connectez-vous avec le compte virtuser
* Sur les trois machines suivantes :
  + 10.100.11.204 (waspure4.iamdg.net.ma)
  + 10.100.11.203 (waspure3.iamdg.net.ma)
  + 10.100.11.205 (waspure5.iamdg.net.ma)

Rajouter la ligne suivante au niveau du fichier /etc/hosts

10.100.233.145 EdpPrdApp-0.iamdg.net.ma

Lancer la commande suivante pour rajouter le certificat MTCASH au niveau du JDK1.8 (Opération à effectuer sur les trois machines)

cd */opt/IBM/WebSphere/AppServer*/java\_1.8.64/jre/lib/security

openssl s\_client -connect 10.100.233.145:9443 </dev/null | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > iam-mtcash.cert

keytool -import -noprompt -trustcacerts -alias iam-mtcash -file iam-mtcash.cert -keystore cacerts

**FIN DU DOCUMENT**