Etude de l'ENT de l'Université de Paris 5

Recommandations des experts suite à la journée du 29 octobre 2009

Objet	Recommandations des experts suite à la journée du 29 octobre 2009
Référence	ESUP-ETU-P5-C
Date de la première version	29 octobre 2009
Date de la dernière version	8 février 2010
Rédacteurs	• Pascal AUBRY – Université de Rennes 1 • Julien MARCHAL – Université de Nancy 2
Diffusion	• depuis le 8 février 2010 : adhérents du consortium ESUP-Portail

Le déplacement des experts sur place a permis d'échanger de vive voix sur les choix techniques adoptés par l'Université de Paris 5, et comprendre ces choix pour pouvoir proposer des améliorations en adéquation avec les contraintes locales.

Ce document présente une analyse sommaire de l'incident du samedi 17 octobre qui a bloqué le fonctionnement du portail pendant quelques heures, et donne les recommandations des experts pour l'amélioration du système.

A. Analyse de l'incident du samedi 17 octobre 2009

Symptômes observés

Le portail répondait une page blanche.

Le mécanisme de redémarrage du portail en cas de panne n'a pas fonctionné, ce qui a entrainé une absence de service pendant environ cinq heures.

Cause probable

Un *deadlock* au niveau du portail ou d'une application (*portlet* ou canal *uPortal*), repérable par les messages suivants dans les *logs*, qui indiquent que le portail augmente le nombre de *threads* allouable :

```
esup     WARN [TP-Processor7] portal.ChannelRendererFactoryImpl.[] sept./22 09:27:36 -
queueSize: 51 activeCount: 20 largestPoolSize: 20
esup     WARN [TP-Processor46] portal.ChannelRendererFactoryImpl.[] sept./22 09:27:52
- queueSize: 93 activeCount: 20 largestPoolSize: 20
esup     WARN [TP-Processor46] portal.ChannelRendererFactoryImpl.[] sept./22 09:27:52
- queueSize: 94 activeCount: 20 largestPoolSize: 20
esup     WARN [TP-Processor46] portal.ChannelRendererFactoryImpl.[] sept./22 09:27:52
- queueSize: 95 activeCount: 20 largestPoolSize: 20
esup     WARN [TP-Processor46] portal.ChannelRendererFactoryImpl.[] sept./22 09:27:52
- queueSize: 96 activeCount: 20 largestPoolSize: 20
```

L'origine la plus probable de ce *deadlock* est la *portlet esup-lecture* en version 1.3.0, comme indiqué dans le *ChangeLog* de l'application :

```
Version 1.3.2 (2009-09-04)
Fixed: Blocked Thread because of bad timeout management during source or category call
```

En conséquence, le portail ne pouvait plus s'allouer de *thread* pour le rendu, et renvoyait une page blanche (vide).

Le script de détection des pannes du portail n'a pas fonctionné car la réponse vide était néanmoins sans erreur (statut HTTP 200 OK).

B. Recommandations

n°1. Utiliser plusieurs serveurs virtuels

Description

Un seul serveur virtuel est aujourd'hui utilisé pour l'exécution de *uPortal*, a priori dimensionné de manière suffisante (8Go). Il vaut mieux utiliser plusieurs serveurs virtuels plus petits à la place d'un seul.

L'observation des statistiques d'utilisation et des charges du serveur en place a permis de déterminer que 4 serveurs de 2Go n'auront aucun problème à absorber la charge actuelle.

Par ailleurs, l'expérience acquise sur d'autres installations a permis de déterminer que l'ajout de *portlets* supplémentaires influait peu sur les ressources nécessaires, mais qu'en revanche le temps de démarrage du portail était impacté de manière non négligeable.

Importance/urgence

L'application de cette recommandation est importante, mais n'est pas urgente dans la mesure où le système en place actuellement peut très bien fonctionner.

Gains

- Un meilleur support de la part de la communauté, grâce à l'adoption d'une configuration plus standard.
- Une meilleure tolérance aux pannes, toujours possible dans le futur même après correction des problèmes actuels.
- La souplesse dans la mise à jour incrémentale des logiciels (portail, applications) par l'arrêt progressif des serveurs à mettre à jour et le redémarrage des serveurs mis à jour.
- Possibilité d'ajouter simplement des serveurs supplémentaires pour faire face à une montée en charge de l'utilisation, simple grâce notamment à la virtualisation.

Effets de bord

La mise en place d'un tel système distribué nécessite :

- La reconfiguration du frontal (*Apache*) pour rediriger les clients vers les serveurs virtuels (*load-balancing*)

Des scripts de mise à jour des images des serveurs virtuels, par exemple à base de *rsync*. Les images des serveurs sont très semblables mais de petites différences doivent néanmoins être appliquées, concernant notamment certaines propriétés nécessaires au fonctionnement du mode *proxy* CAS.

Aide des experts

- Scripts de mise à jour des serveurs

n°2. *Frontal* Apache *: désactiver le connecteur HTTP de* Tomcat *(8080)*

Description

Le connecteur HTTP de *Tomcat* sur le port 8080 est utilisé pour la détection des arrêts de service de Tomcat, il doit être arrêté, la réponse sur le port 8080 n'indiquant en rien que *Tomcat* fonctionne par ailleurs pour le protocole AJP.

Importance/urgence

Peu important, non urgent.

Gains

- Permet d'éviter tout accès qui ne serait pas tracé au niveau *Apache.*

Effets de bord

- Modifier le script de détection de l'activité de *Tomcat*.

n°3. *Frontal* Apache *: passer à Apache 2 et mod_proxy*

Description

mod_jk (*Apache* 1.3) utilisé aujourd'hui n'est plus supporté, il doit être remplacé par *mod_proxy* (*Apache* 2)

Importance/urgence

Important, non urgent (à faire avant ou en même temps que le passage à plusieurs serveurs virtuels).

Gains

- Possibilité de mise à jour pour la suite.

Effets de bord

- Modifier le script de détection de l'activité de *Tomcat*.

Aide des experts

Configuration type de *mod_proxy*.

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
ProxyPass / ajp://localhost:8009/
```

n°4. JVM : utilisation d'une JVM 32bits

Description

Une machine virtuelle 64bits est utilisée sur le serveur hébergeant le portail, notamment pour passer outre la limite de 2Go de la mémoire imposée par les JVM 32bits.

La JVM 64bits n'apportant par ailleurs aucun autre gain, il vaut mieux revenir à une JVM 32bits.

Importance/urgence

L'application de cette recommandation est urgente dans la mesure où les experts ne sont pas capables de déterminer quel est l'impact de l'utilisation d'une JVM 64bits.

Gains

- Un meilleur support de la part de la communauté, grâce à l'adoption d'une configuration plus standard.

Aide des experts

Cette recommandation ne peut être appliquée qu'après passage à plusieurs serveurs virtuels pour l'hébergement du portail (cf recommandation n°1).

n°5. JVM : optimiser les arguments de lancement

Description

Dans l'installation actuelle, toute la mémoire utilisable est allouée dès le démarrage de la JVM. Les paramètres de la JVM doivent être optimisés.

Importance/urgence

Peu important, non urgent.

Gains

- Charge moins importante des serveurs virtuels grâce à l'optimisation des paramètres mémoire.

Aide des experts

Paramètres utilisés à Nancy 2 :

```
-server -Xms256m -Xmx1500m -XX:MaxPermSize=256m -XX:+UseParallelGC
-Dnetworkaddress.cache.ttl=3600
-Dcom.sun.management.jmxremote
-Djava.awt.headless=true
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
-Djava.util.logging.config.file=/home/uportal/up-3/tomcat/conf/logging.properties
-Djavax.net.ssl.trustStore=/Cert/esup-portail.keystore
-Djava.endorsed.dirs=/home/uportal/up-3/tomcat/endorsed
-classpath :/home/uportal/up-3/tomcat/bin/bootstrap.jar
-Dcatalina.base=/home/uportal/up-3/tomcat
-Dcatalina.home=/home/uportal/up-3/tomcat
-Djava.io.tmpdir=/home/uportal/up-3/tomcat/temp
```

Paramètres utilisés à Rennes 1 :

```
-server -Xms2500m -Xmx2500m -Xss128k -XX:+AggressiveOpts -XX:MaxPermSize=512m
-XX:+CMSClassUnloadingEnabled  -XX:+CMSPermGenSweepingEnabled
-Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=9054 -Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false
-Djava.io.tmpdir=/data/webapps/ent.univ-rennes1.fr/tomcat/temp
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
-Djava.util.logging.config.file=/data/webapps/ent.univ-
rennes1.fr/tomcat/conf/logging.properties
-Xdebug -Xrunjdwp:transport=dt_socket,address=55554,server=y,suspend=n
-Djava.endorsed.dirs=/opt/tomcat-5.5-uPortal2.6/common/endorsed
-Dcatalina.base=/data/webapps/ent.univ-rennes1.fr/tomcat
-Dcatalina.home=/opt/tomcat-5.5-uPortal2.6
```

HTTPS

Tous les accès au portail se font via le protocole HTTPS, ce qui n'est *a priori* pas recommandé. C'est une volonté politique que tous les accès soient sécurisés, et le chiffrement est assuré par un frontal *Apache* sur un serveur dédié qui ne rencontre pas de problème de performance.

En conséquence, aucune recommandation n'est émise sur ce point.

n°6. Serveur CAS : mettre à jour le serveur CAS en version 3

Description

La version 2 du serveur CAS n'est plus supportée depuis quelques années, une mise à jour vers la version 3 est nécessaire, notamment pour combler certaines failles de sécurité.

Importance/urgence

Important et urgent.

Gains

- Plus de sécurité par le comblement de certaines attaques XSS en version 2.
- Plus de flexibilité dans la configuration du serveur Cas (grâce à Spring).
- Possibilité de redonder le serveur CAS, avec reprise sans interruption de service grâce à *memCache*.

Possibilité de faire les mises à jour du serveur CAS sans interruption de service (toujours grâce à *memCache*).

Effets de bord

Tous les clients doivent être compatibles avec la version 3 du serveur (mise à jour nécessaire vers les dernières versions disponibles).

Modifier le script *Perl* maison d'authentification du serveur de messagerie (Courrier IMAP)

Modifier le workflow du serveur Cas pour intégrer la phase d'interrogation concernant le respect de la charte de l'université.

Aide des experts

Exemple de patch du *workflow* du serveur CAS

```
<action-state id="submit">
  <action bean="authenticationViaFormAction" method="submit" />
  <transition on="warn" to="warn" />
  <transition on="success" to="statusCheck" />
  <!-- <transition on="success" to="sendTicketGrantingTicket" /> -->
  <transition on="error" to="viewLoginForm" />
</action-state>

<action-state id="statusCheck">
    <action bean="statusCheckAction"/>
    <transition on="warn" to="showStatusWarnView"/>
    <transition on="success" to="sendTicketGrantingTicket" />
</action-state>

<end-state id="showStatusWarnView" view="casStatusWarnView" />
```

n°7. Serveur CAS : modifier les sources d'authentification du serveur CAS

Description

Ajouter une source d'authentification basée sur un fichier pour tous les comptes ne figurant pas dans l'annuaire LDAP ou la base de données GRHUM.

Note : l'accès actuel à deux sources d'utilisateurs (la base GRHUM et l'annuaire LDAP) dont la plupart des comptes sont dupliqués est source de confusion. Cette situation étant essentiellement guidée par l'historique des évolutions du SI.I, aucune recommandation n'est émise sur ce point. Une réflexion globale sur le S.I. semble néanmoins souhaitable.

Importance/urgence

Important, non urgent (à faire lors de la migration vers CAS v3).

Gains

- Séparation claire des comptes du S.I. des comptes de gestion.
- Suppression de l'URL */private* de *uPortal* (cf recommandation n°11).

n°8. Serveur CAS : redonder le serveur CAS

Description

Si la mise en place d'une solution redondante basée sur la version 3 de Cas n'est pas possible rapidement, prévoir une solution de *spare* pour le serveur actuel pour faire face à toute panne.

Importance/urgence

Très important, urgent si la migration vers CAS v3 ne peut être faite rapidement.

Gains

- Continuité du service d'authentification en cas de panne du serveur CAS.

n°9. uPortal : sécuriser certaines URLs sensibles

Description

Les URLs suivantes sont accessibles par n'importe quel client et doivent être sécurisées (par IP par exemple) :

- https://ent.univ-paris5.fr/uPortal/monitor
- https://ent.univ-paris5.fr/uPortal/private

Importance/urgence

Important, non urgent.

Gains

- Eviter les authentifications administrateur dans le portail depuis n'importe où (sans log)
- Eviter de que tous ne puisse voir les statistique et performance du serveur

Aide des experts

Configuration type de protection par IP :

```
<Location /private>
  Order allow,deny
  Allow from xxx.xxx.xxx.xxx
</Location>
```

n°10. uPortal : supprimer les comptes uPortal

Description

Les comptes d'administration de *uPortal* (par ex. *admin*) sont déclarés dans la base de données de *uPortal*. Il est recommandé de n'utiliser que des comptes CAS, au besoin en déclarant ces comptes spécifiques dans une source séparée (cf recommandation n°8)

Importance/urgence

Peu important, non urgent.

Gains

- Plus de souplesse dans la gestion de ces comptes
- Simplification des accès au portail par la suppression de l'URL https://ent.univ-paris5.fr/uPortal/private

n°11. uPortal : diminuer la durée d'expiration des sessions des invités

Description

Par défaut, le temps d'expiration des sessions des invités est le même que celui des sessions des utilisateurs authentifiés. Il en résulte un grand nombre de sessions inutiles.

Importance/urgence

Important, non urgent.

Gains

- Moins de sessions actives
- Moins de mémoire consommée

Aide des experts

Dans le fichier *portal.properties*, la valeur de la propriété, positionner la propriété suivante :

```
org.jasig.portal.PortalSessionManager.unauthenticatedUserSessionTimeout=600
```

n°12. uPortal : ajouter des outils de monitoring du portail

Description

Par défaut, la *servlet EsupMonitor*, qui fournit des informations en temps-réel sur l'état du portail, n'est pas active. Il faut l'activer en positionnant la propriété *esup.monitor* à *true* dans *config.properties* (suivre par *ant init deploy*).

Pour mémoriser l'historique de l'état du portail, il faut ajouter un script d'interrogation qui enregistre régulièrement l'état du portail.

Importance/urgence

Important, urgent.

Gains

- Surveillance en temps-réel du portail pour détecter d'éventuelles anomalies
- Traces pour reconstituer les problèmes a posteriori en cas d'incident.

Aide des experts

Cette recommandation a été mise en place le 29 octobre, mais un redémarrage du serveur était nécessaire pour prendre en compte les paramètres *JMX Remote* nécessaires (variable *JVM_OPTS* dans *start-esup.sh*).

Les URLs suivantes sont désormais accessibles :

- https://ent.univ-paris5.fr/analysis/threads.jsp
- https://ent.univ-paris5.fr/analysis/datasources.jsp
- https://ent.univ-paris5.fr/analysis/EsupMonitor

Les experts pourront participer à l'installation d'un serveur *Cacti* pour une meilleure lecture des informations récupérées lors des prochaines journées.

n°13. uPortal : renommer un attribut du portail

Description

L'attribut *facsimileTelephoneNumber*, mappé sur l'attribut *xxx* de l'annuaire LDAP, contient le type d'utilisateur (ENSEIGNANT, VISITEUR, …). Il faut le renommer.

Importance/urgence

Peu important, non urgent.

Gains

- Lisibilité des attributs du portail.

Effets de bord

Les applications s'appuyant sur cet attribut risquent de ne plus fonctionner après renommage.

Aide des experts

Pour assurer la continuité de fonctionnement des applications, il est possible de dupliquer l'attribut au lieu de le renommer.

n°14. uPortal : supprimer l'authentification LDAP

Description

L'authentification LDAP du portail est activée alors que seules les authentifications via CAS sont souhaitées. L'authentification LDAP doit être désactivée en positionnant la propriété *xxx* à *false* dans *security.properties*.

Par ailleurs, l'activation de l'authentification LDAP génère de très nombreuses traces inutiles dans les logs.

Importance/urgence

Important, urgent.

Gains

- Meilleur contrôle des accès au portail.
- Meilleure lisibilité des logs

Aide des experts

Cette recommandation a été mise en place le 29 octobre.

n°15. uPortal : modifier le script de surveillance du portail

Description

Le script de surveillance de l'état du portail fait une simple vérification de la réponse (ou non) de la première page du portail. Lors du dernier incident, le portail ne fonctionnait plus, mais répondait quand même (une page blanche), avec un code de retour HTTP égal à 200 (OK), ce qui fait que la panne du portail n'a pas été détecté (et le serveur n'a pas été automatiquement relancé). Le script doit effectuer un contrôle plus strict de la réponse du portail, par exemple en contrôlant la présence d'un élément clé de la page de réponse.

Par ailleurs, une session invité est générée à chaque interrogation de la page d'accueil ; l'identifiant de session doit être conservé entre chaque interrogation pour éviter cela.

Importance/urgence

Peu important dans la mesure où les experts pensent qu'une relance automatique du serveur n'est à terme pas souhaitable, non urgent.

Gains

- Meilleure détection des pannes.
- Possibilité d'interroger l'état du portail plus souvent (sans création d'une session supplémentaire à chaque interrogation.

Aide des experts

Option de *wget* pour repasser l'identifiant de session à chaque requête :

```
--cookies=on --load-cookies=/tmp/cookie.tmp
```

n°16. uPortal : centraliser les logs

Description

La surveillance des logs est rendue plus compliquée par la mise en place de solutions distribuées. Il est recommandé de centraliser les logs sur un serveur syslog.

Un serveur syslog est déjà opérationnel et peut-être utilisé.

Importance/urgence

Important, non urgent (à faire néanmoins dès la mise en place de plusieurs serveurs pour le portail).

Gains

- Meilleure lisibilité des logs.

Effets de bord

Les applications du portail doivent également être branchées sur le serveur *syslog*.

Aide des experts

Exemple de configuration de log4j pour envoyer les logs sur un serveur syslog :

```
log4j.rootLogger=ERROR, syslog

log4j.appender.syslog=org.apache.log4j.net.SyslogAppender
log4j.appender.syslog.SyslogHost=syslog.univ.fr
log4j.appender.syslog.Facility=LOCAL5
log4j.appender.syslog.layout=org.apache.log4j.PatternLayout
log4j.appender.syslog.layout.ConversionPattern=portlet-XXX %d %p [%c] - %m%n
```

n°17. uPortal : mettre à jour la portlet esup-lecture

Description

La *portlet esup-lecture* doit être mise à jour (version 1.3.2 au moins, 1.4.0 préférable) pour éviter les problèmes de *deadlocks* présents dans la version 1.3.0 actuellement installée.

Importance/urgence

Important, urgent.

Gains

- Fiabilisation de l'ENT.

n°18. Serveur LDAP : redonder le serveur LDAP

Description

Le serveur LDAP n'est aujourd'hui pas redondé (à cause d'un problème lié à la présence de signes '+' dans certains DN qui empêche la diffusion des mises à jour de l'annuaire maître vers les annuaires esclaves dans la version utilisée d'*OpenLdap*). La non redondance du serveur LDAP est aussi critique que celle du serveur CAS.

Importance/urgence

Très important, urgent.

Gains

- Continuité du service d'authentification en cas de panne du serveur CAS.

Effets de bord

Une fois la redondance mise en place, il est recommandé d'indiquer cette redondance aux applications qui en ont la capacité.

n°19. Webmail : sécuriser le webmail

Description

Les URLs suivantes sont accessibles à tous les clients :

- https://webmail.etu.univ-paris5.fr/horde3/test.php
- http://webmail.univ-paris5.fr/horde3/test.php

Il faut les sécuriser, par exemple par IP.

Note : IMP tourne aujourd'hui dans une *iframe*, pour garantir l'homogénéité de présentation de toutes les applications. Ce ne sera pas possible avec DIMP (le successeur de IMP). La solution sera de personnaliser DIMP pour lui donner le même *look* que le portail et le faire tourner dans une fenêtre séparée.

Importance/urgence

Important, urgent.

Gains

- Continuité du service d'authentification en cas de panne du serveur CAS.

Effets de bord

Une fois la redondance mise en place, il est recommandé d'indiquer cette redondance aux applications qui en ont la capacité.

n°20. Bases de données : migrer les bases applicatives vers MySql 5

Description

Les applications du portail et le portail lui-même utilisent un serveur MySql 4 (sur le même serveur qu'Oracle). Un serveur MySql 5 est déjà opérationnel, il s'agit donc simplement de migrer les bases d'un serveur vers un autre, en gérant au mieux les interruptions de service.

Importance/urgence

Important, peu urgent.

Gains

- Meilleure surveillance des *pools* de connexion
- Détection de problèmes d'accès aux données depuis les applicatifs.

n°21. Bases de données : configurer et surveiller les pools de connexion

Description

L'accès aux données peut être ralenti par une mauvaise configuration des pools de connexion ou par une mauvaise utilisation des *pools* de connexion par les applications. Une surveillance de ces *pools* peut être mise en place très simplement grâce à *Lambda Probe*.

Importance/urgence

Important, urgent.

Gains

- Meilleure surveillance des *pools* de connexion
- Détection de problèmes d'accès aux données depuis les applicatifs.

Aide des experts

Indiquer l'utilisation des paramètres *validationQuery* et *autoReconnect* :

```
<Resource name="jdbc/PortalDb"
          auth="Container"
          type="javax.sql.DataSource"
          username="XXXXX" password="XXXXX"
          driverClassName="com.mysql.jdbc.Driver"
          url="jdbc:mysql://sql.univ.fr/uPortal?autoReconnect=true"
          maxActive="100" maxIdle="30" maxWait="10000"
          poolPreparedStatements="true"
          validationQuery="SELECT 1"
          removeAbandoned="true"
          removeAbandonedTimeout="300"
          logAbandoned="true" />
```

n°22. Bases de données : traquer les requêtes SQL critiques

Description

Mettre en place le traçage des requêtes critiques (*slow queries*) de MySql.

Importance/urgence

Important, urgent.

Gains

- Traquer dans les applications non connues des experts d'éventuelles fautes de programmation.
- Repérer l'absence d'index dans les tables des applications connues.

Aide des experts

Indiquer le traçage des requêtes critiques dans le fichier *my.cnf* :

```
slow_query_log = 1
slow_query_log_file = /var/log/mysql.slow.log
```

n°23. Bases de données : séparer les données dans des bases distinctes

Description

Des applications utilisent la base de données de *uPortal* pour stocker leurs données. Il est recommandé de les placer dans des bases de données séparées.

Importance/urgence

Moyennement important, non urgent.

Gains

- Simplifier la sauvegarde et la restauration des bases.
- Ne pas être limité par le nombre de connexion par base.

n°24. Bases de données : séparer Oracle et MySql

Description

Oracle et MySql sont hébergés sur le même serveur physique. Outre le fait qu'un dysfonctionnement du serveur Oracle a déjà eu des incidences sur le serveur MySql, provoquant ensuite une panne du portail, il est recommandé d'héberger les deux SGBD sur des machines (physiques ou virtuelles) différentes.

Importance/urgence

Important, non urgent.

Gains

- Rendre indépendants les serveurs de données.