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

Synthèse de l'intervention des experts les 9-10 novembre 2009 et dernières recommandations

Objet	Synthèse de l'intervention des experts les 9-10 novembre 2009 et dernières recommandations
Référence	ESUP-ETU-P5-E
Date de la première version	10 novembre 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

Ce document résume les opérations effectuées par les experts les 9 et 10 novembre 2009, et propose une dernière série de recommandation pour la consolidation de l'ENT de l'Université de Paris 5.

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

A. Synthèse de l'étude

La mise en œuvre, l'optimisation, et l'évolution de l'ENT ESUP-Portail est délicate :

- Les compétences nécessaires sont nombreuses et transversales (de l'architecture système au développement logiciel),
- Les meilleures solutions sont le plus souvent empiriques, issues de l'expérience gagnée au fil des années d'exploitation.

Malgré la mise en place tardive de ESUP-Portail (en comparaison avec d'autres universités en production depuis 2003), l'équipe rencontrée par les experts possède toutes ces compétences et la motivation pour mener à terme la consolidation de l'ENT de l'Université de Paris 5.

Améliorations apportées au système

Les gains attendus après les opérations effectuées lors des dernières semaines sont les suivants :

- **Meilleur suivi des incidents**, grâce à la mise en place d'outils de *monitoring* et la centralisation des *logs*.
- **Fiabilité**, grâce à l'ajustement de nombreux paramètres de configuration.
- **Performance**, grâce à la répartition de charge entre les serveurs.
- **Souplesse de l'évolutivité pour la montée en charge**, grâce au mécanisme de réplication qui permet une extension de la ferme des serveurs en quelques minutes.
- **Facilité de support**, grâce à l'adoption d'options partagées par un grand nombre d'établissement de notre communauté.

Evolutions à venir

Les préconisations données par les experts le 2 novembre, ainsi que les dernières présentées en fin de ce document, doivent permettre d'achever la consolidation de l'ENT de l'Université de Paris 5.

L'ajout de fonctionnalités, par le remplacement progressif des canaux (*iFrame* et *uPortal*) par des applications plus intégrées (*portlets*), peut désormais se faire sans diminution de qualité de service ni baisse de performance.

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

B. Description de l'intervention des 9-10 novembre 2009

Préparation de l'architecture distribuée

Mise à jour de la portlet esup-lecture

Cause probable des incidents observés récemment, la portlet *esup-lecture* est mise à jour en version 1.3.2.

Ajout d'un nouveau frontal virtuel

Un alias *enttest.univ-paris5.fr* est créé sur le serveur hébergeant le frontal *Apache* (*ent.univ-paris5.fr*).

Sur ce frontal, les modules *mod_proxy*, *mod_proxy_ajp* et *mod_proxy_balancer* sont activés (cf **recommandation n°3**), et un serveur Apache virtuel (*VirtualHost*) est déclaré sur *enttest.univ-paris5.fr*.

Les URLs */monitor* et */private* du portail ont été sécurisées par IP (cf **recommandation n°9**).

Voir : **recommandation n°25** Frontal *Apache* : configuration SSL

Ajout du serveur maître de la ferme

Une machine virtuelle supplémentaires est créée par recopie de la machine d'exploitation en place (*millenium.dsi.univ-paris5.fr*). Cette machine est appelée *salander.dsi.univ-paris5.fr*, alias DNS *ent1.univ-paris5.fr*. Ce nouveau serveur virtuel est taillé de manière plus raisonnable que l'ancien (2Go de mémoire contre 8Go précédemment, cf **recommandation n°1**). Ce serveur va devenir le serveur maître de la ferme de serveurs, celui à partir duquel seront créés les autres serveurs virtuels réplicas.

Les privilèges nécessaires sont positionnés sur le serveur *MySql* pour donner droit d'accès à la base *uPortal* et les bases applicatives (*Moodle*).

Configuration du serveur maître

Les modifications suivantes sont apportées à la machine *salander* :

- Une JVM 32 *bits* est utilisée en place d'une machine 64 *bits* (cf **recommandation n°4**). Le portail, les *portlets* et tous les canaux ont été recompilés. Les librairies de connexion aux bases de données ont été déplacées de */java/jre/lib/ext* vers */tomcat/common/lib*.
- Le connecteur HTTP de *Tomcat* a été désactivé (cf **recommandation n°2**).
- Les paramètres de lancement de la JVM ont été améliorés, notamment en ce qui concerne la configuration de l'utilisation de la mémoire (cf **recommandation n°5**). Ces options peuvent certainement être affinées après observation du comportement des JVM sur les serveurs.
- La propriété *esup.real.port.https* a été corrigée, le mécanisme de *proxy* CAS ne pouvait pas fonctionner. Le fonctionnement validé à l'aide du canal *CasTest*.
- Un « *Manager pathname* » vide est positionné pour tous les contextes *Tomcat* (pas de sauvegarde des sessions de *uPortal* pour un redémarrage plus rapide du portail). Note : avec l'implémentation actuelle de *Pluto*, les sessions des *portlets* sont stockées dans la session principale, il est donc inutile de préciser un *PathManager* pour les contextes des *portlets*.
- La durée d'expiration des sessions des invités a été réduite (cf **recommandation n°11**).
- Une sonde *Lambda Probe* a été installée sur tous les serveurs du portail (cf **recommandation n°14**) accessible par *http://ent.univ-paris5.fr/probe**n***.
- Le répertoire *work* de *Tomcat* est supprimé à chaque redémarrage.

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

- Le contexte de *uPortal* est déplacé de */uPortal/* à */*, ce qui permet de ne pas avoir à ajouter de contexte à chaque fois que l'on ajoute une *portlet*. L'ancien chemin */uPortal/* est automatiquement redirigé vers */* pour garder valides les signets des utilisateurs.
- Les attributs *reloadable* de tous les contextes sont passés à *false* pour éviter les rechargements automatiques intempestifs.

Validation du serveur maître

Le fonctionnement du serveur *salander* est validé à travers le frontal *enttest.univ-paris5.fr*.

Ajout d'un serveur syslog sur le serveur maître

Syslog-ng est installé sur le serveur maître pour centraliser tous les logs des réplicas de la ferme (cf **recommandation n°16**).

La configuration de *uPortal* est modifiée pour envoyer tous les logs au serveur *syslog* (*Logger.properties*).

Les configurations *log4j* des applications (*portlets* et canaux) sont également modifiées de la même manière.

Les scripts de génération des statistiques à partir des *logs* sont modifiés pour prendre en compte la nouvelle localisation des *logs*.

Ajout du premier réplica

Une machine virtuelle supplémentaires est créée par recopie du serveur maître (salander.*dsi.univ-paris5.fr*). Cette machine est appelée *larsson.dsi.univ-paris5.fr*, alias DNS *ent2.univ-paris5.fr*.

Tous les applicatifs du serveur sont supprimés après la duplication, ils seront maintenus grâce à une synchronisation depuis le serveur maître.

Synchronisation du réplica

Des clés sont échangées entre *salander* et *larsson* pour permettre la synchronisation.

Les scripts de synchronisation des serveurs sont mis en place :

- *sync.sh* sur le serveur maître
- *syncDist.sh* pour les réplicas

Les scripts sont adaptés pour la configuration locale.

Mise en place du load-balancing

La configuration du frontal Apache est modifiée pour implémenter la répartition de charge entre les deux serveurs de la ferme.

L'accès au gestionnaire du répartiteur de charge est réservé à une plage d'adresses IP privilégiée (*https://enttest.univ-paris5.fr/balancer-manager*).

Validation de l'architecture de test

L'architecture de test est validée à travers le frontal enttest.univ-paris5.fr (répartition de charge, accès aux bases de données, tests fonctionnels rapides de tous les canaux, fonctionnement proxy de CAS, accès aux sondes, …).

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

Mise en production

Basculement de l'architecture répartie en production

Le basculement s'est fait par une simple modification du frontal Apache (*enttest.univ-paris5.fr* devient *ent.univ-paris5.fr*), avec possibilité de retour en arrière en quelques minutes si nécessaire.

Validation de l'architecture définitive

Aucune anomalie n'a été détectée sur la nouvelle architecture.

Instructions pour l'ajout d'un nouveau réplica

Les instructions suivantes donnent la méthodologie pour ajouter un serveur à la ferme du portail.

- Dupliquer un des réplicas, lui donner un nom DNS
- Rajouter un CNAME sur le frontal (*ent**n***).
- Ajuster les paramètres système du nouveau serveur (adresse IP, ne pas oublier */etc/hosts*).
- Adapter le script *syncDist.sh* en positionnant la propriété LOCAL_ID.
- Synchroniser le nouveau réplica avec le serveur maître.
- Démarrer le réplica.
- Modifier la configuration du frontal pour prendre en compte le nouveau réplica.

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

C. Avancement de la mise en œuvre des premières recommandations (2 novembre 2009)

n°1. Utiliser plusieurs serveurs virtuels (appliquée)

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

2 machines virtuelles de 2Go chacune ont été mises en place par les experts, suffisantes au vu des charges observées.

Une troisième machine virtuelle a été mise en production à partir en seulement 15 minutes, ce qui montre la souplesse d'utilisation du système distribué.

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

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

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*.

Aide des experts

Le connecteur a été désactivé.

n°3. Frontal Apache : passer à Apache 2 et mod_proxy (appliquée)

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

Les modules ont été installés et configurés pour la mise en place du frontal de répartition de charge.

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

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.

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

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 (appliquée)

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

Les paramètres de lancement utilisés sont les suivants :

```
-server
-Dcom.sun.management.jmxremote
-Xms256m
-Xmx1500m
-XX:MaxPermSize=256m
-XX:+CMSClassUnloadingEnabled
-XX:+CMSPermGenSweepingEnabled
```

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.

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

- 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).

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

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 (appliquée)

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

Les URLs ci-dessus ont été protégées par IP.

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

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

- 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 (appliquée)

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 propriété suivante a été positionnée :

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

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

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

La servlet *EsupMonitor* a été mise en place, avec nécessité d'utiliser 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

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

Une sonde *Lambda Probe* a été installée sur tous les serveurs du portail (*http://ent.univ-paris5.fr/probe**n***).

Les experts recommandent l'installation d'un serveur *Cacti* pour une meilleure lecture des informations récupérées.

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 (appliquée)

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.

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

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 (appliquée)

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

Un serveur *syslog* a été installé sur le serveur maître et tous les *logs* du portail et des applications sont désormais centralisés.

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

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

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.

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

Gains

- Sécuriser les informations affichées par les webmails

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" />
```

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

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.

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

D. Dernières recommandations (12 novembre 2009)

n°25. Cluster *: sortir le serveur maître de la ferme*

Description

Le serveur maître a aujourd'hui un rôle spécifique dans la ferme des serveurs du portail, et sert pourtant *uPortal* comme les autres serveurs. Il serait logique de sortir ce serveur spécifique de la ferme afin de n'y conserver que des machines strictement identiques.

Notes :

- Certains exploitants conservent le serveur maître dans la ferme malgré sa spécificité.
- Le serveur maître peut être conservé pour d'autres services annexes, comma par exemple l'exécution des tâches asynchrones.

Importance/urgence

Important, non urgent.

Gains

- Simplification de l'analyse en cas d'incident.

n°26. Cluster *: synchroniser des réplicas*

Description

Afin d'être sûr de la cohérence des serveurs, il est important de programmer la synchronisation automatique des réplicas avant le redémarrage quotidien du portail.

Importance/urgence

Important, urgent.

Gains

- Assurance de la cohérence des serveurs.

n°27. Frontal Apache *: configuration SSL*

Description

La configuration SSL est dupliquée dans plusieurs fichiers de configuration, il est souhaitable de regrouper tout ce qui concerne SSL dans un seul fichier de configuration (*ssl.conf*) et l'inclure là où nécessaire.

Importance/urgence

Peu important, non urgent (mais facilitera la future migration des certificats serveurs).

Gains

- Meilleure maintenance de la configuration du frontal *Apache*.

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

n°28. uPortal *: chemin des canaux* iFrame

Description

Nombre de canaux *iFrame* du portail ont une URI de la forme */uPortal/xxx*. Ces chemins sont toujours valides malgré la suppression du chemin */uPortal/* pour la racine grâce à une redirection de */uPortal/* en */*. Il convient néanmoins de mettre à jour ces chemins en modifiant les paramètres de publication des canaux correspondants.

Importance/urgence

Important, non urgent.

Gains

- Meilleure lisibilité de la configuration.

Effets de bord

Des liens externes vers les applications peuvent subsister pour accéder aux applications sans passer par le portail, ils doivent être mis à jour.

n°29. uPortal *: utilisation de* custom.properties

Description

Les propriétés de configuration du portail sont définies dans le fichier *config.properties*. Il convient d'utiliser le fichier *custom.properties* (dont les propriétés prennent le pas sur celles du fichier *config.properties*), qui ne contient alors que les propriétés propres à la configuration locale.

Importance/urgence

Important, non urgent.

Gains

- Simplification de la mise à jour du portail.

n°30. uPortal *: application* HarpWeb

Description

L'application *HarpWeb* est intégrée en *iFrame*. Avant la modification de la propriété *esup.real.port.https*, elle demandait une authentification (formulaire propre à l'application). Il semble que le passage d'un Proxy Ticket valide ait modifié le comportement de l'application, qui affiche désormais une erreur.

Importance/urgence

Important, urgent.

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

n°31. syslog *: rotation des fichiers de* log

Description

Aucun mécanisme n'est en place pour limiter l'espace occupé sur le serveur *syslog* par les fichiers de *log*, cela doit être corrigé dès que possible, par exemple avec *logrotate*.

Importance/urgence

Important, urgent.

Gains

- Prévention contre la saturation de l'espace disque.

n°32. syslog *: mettre un alias DNS sur le serveur* syslog

Description

Le nom du serveur *syslog* est précisé à plusieurs endroits dans la configuration du portail et de ses applications. L'utilisation d'un alias DNS permettrait de pouvoir déplacer simplement le serveur *syslog* sans avoir à modifier la configuration du portail et des applications.

Importance/urgence

Important, non urgent.

Gains

- Maintenabilité des applications.
- Souplesse de la gestion des logs.

Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.