Améliorer la qualité de la gestion du Centre informatique

Par Benjamin LISAN, mars 2008.

1 Introduction

Ce document a été rédigé à destination d'un responsable informatique qui me demandait conseil sur la gestion d'un DATA CENTER, qu'il allait diriger.
Ces conseils proviennent de la propre expérience de l'auteur, en tant que créateur puis responsable d'un centre informatique, chez Renault Montigny-le-Bretonneux, pendant 3 ans puis en tant que responsable de l'informatique d'une startup I.S.O. à Saint-Cloud, pendant 1,5 ans et enfin en tant qu'ingénieur système Solaris, pour un grand compte, où je travaille actuellement, depuis juillet 2007. Voici ces conseils :

2 Eviter les problèmes hardware

1) Eviter les températures trop élevées dans la salle machine (avoir une température constante de 18 °C).
2) Eviter d'avoir à gérer un parc vieillissant. Pour éviter cela, par exemple, vous pouvez souscrire à un contrat avec le constructeur ou fournisseur, qui reprendra régulièrement vos anciennes machines en échange d'une nouvelle, dès que les machines les plus anciennes dépasseront une certaine date.
3) Pour diminuer le nombre de problèmes réseau, éviter de dé-brasser puis re-brasser sans cesse les serveurs, opérations risquant d'augmenter les risques de faux-contacts ou/et d'avoir des câbles réseau ou SAN défectueux.
4) Simplifier le réseau (moins de routeurs, moins de sous-réseaux …). Partout où c'est possible utiliser le 1000 Mbps (1 GoBytes) FDX, en autoneg à 1 (le 100 FD étant alors réservé au « jumpstart » et autres cas rares) ou bien quand cela n'est pas possible, tout à 100 FDX. A noter : il existe maintenant du 10 Go.
5) Standardiser, homogénéiser, le parc informatique. Eviter de se retrouver face au « SICOB informatique », à une hétérogénéité informatique totale, avec trop de constructeurs et trop de modèles différents.
6) Supprimer les serveurs les plus anciens,
7) Ne garder qu'un nombre limité de gros serveurs récents (avec une gamme de modèles réduites …) (Sun 25k, Sun T5220 …, M5000/M8000, IBM Regata, HP Superdome … Utilisation de VMWare, avec serveurs Windows (Wintel …), quand c'est possible).

8) Avoir une cellule d'assistance technique hardware, présente sur (dédiée à) chaque site, en permanence, pouvant remplacer à chaud certains équipements (disques durs dans les baies de disques…),
9) Constituer un stock de pièce détaché avant (quand c'est possible) _ en tout cas, un stocks de disques hot-plug….
10) Disposer des sondes de températures sur les plus gros châssis (en général, celles sont déjà souvent livrées en standard avec les châssis).

3 Eviter les problèmes système

1) Mettre en place des outils (par exemple, à base de scripts shell, de perl …) pour la surveillance, la supervision de toutes les ressources systèmes, affichant des alertes de dépassements de seuils (taux occupation CPU, RAM, disque, partitions, volumétries en tout genre _ tables oracles, augmentation des FS, des swaps, affichant des alertes dès que le seuil de saturation d'un « File system » dépasse, par exemple, 80 %) etc …). (Ces scripts peuvent être lancés par crontab ou Control-M) ou des outils comme Patrol.
2) Faire des sauvegardes de toutes les données importantes, régulières, si possible, chaque soir,
3) Avoir un plan de reprise d'activité (PRA), fonctionnant en relation avec un site de secours, ultra-testé, y compris au niveau des procédures d'interventions humaines.
4) Anticiper, chaque année, l'augmentation annuelle de la volumétrie par machine et application, ce qui nécessite une planification prévisionnelle de l'augmentation régulière de la volumétrie. Celle-ci se fait lors d'une négociation, à renouveler chaque début d'année, avec le client ou le chef de projet. On doit alors demander à chaque chef de projet applicatif qu'est-ce qu'il prévoit comme augmentation de la volumétrie de ses applications, pour l'année en cours … pour la prévision de l'année en cours, lors de plusieurs réunions. Accorder à priori officiellement une quantité X de la volumétrie demandée (et en fait, accorder X + 20 % de plus, par rapport à la volumétrie accordée officiellement à chacun des chefs de projets, sans qu'il le sache).
5) Planifier longtemps à l'avance, les UPGRADES, les MEP _ mises en production _ … (par plusieurs réunions entre tous les intervenants …), avec une check-list très détaillée, minutée des futures interventions de chaque intervenant dans la MEP. … avec répétition de la MEP sur des machines de test/intégration avant (avant de faire la grosse MEP en prod).
6) Faire que la salle informatique dispose d'une dizaine (?) de petites machines de test, que chaque chef de projet peut réserver pour un temps a priori limité, au travers un planning des réservations de ces serveurs.
7) Faire des audits réguliers de la situation de l'état de l'infomatique de ce centre informatique … => ce qui permettra l'élaboration ou la mise en place d'un **nouveau schéma et plan directeur** _ à faire à chaque début d'année _, pour anticiper/prévoir l'évolution de l'informatique du CENTRE INFORMATIQUE.
8) **Normaliser tout** : normaliser le SOCLE de base technique ou le MASTER _ l'OS etc … servant aux installations des machines _, normaliser toutes les installations, qu'elles soient OS, réseau etc… Tout doit être normalisé, jusqu'au nom des programmes, des variables, des triggers…

9) Eviter que l'information utile au centre informatique soit disséminée partout. Il faut qu'elle soit centralisée au niveau d'un serveur de fichier unique (ou d'un site web unique) à l'arborescence logique. Il y aura, par exemple, a) un point d'accès unique accessible soit par le navigateur IE, b) un partage ou disque réseau unique ou en nombre restreint (sur un serveur d'info, elle pourra être créé par Wiki ou CMS).
10) Si possible, mettre en place une informatique totalement centralisée, avec une base de données relationnelle centrale, très exhaustive, avec un modèle conceptuel de données très complet, et bien étudié (par exemple, à base de technologie relationnelle Oracle, en cluster, en système de haute disponibilité Oracle RAC).

4 Politique de sécurité

1) On doit se connecter à ces machines qu'avec son compte nominatif (ce qui permet de tracer les logins). Et certaines personnes connectées avec leur compte nominatif auront le droit de faire un « su – » ou « sudo ». On ne peut pas se connecter directement « root » sur ces machines. Toutes les machines critiques seront eTrustées ou/et ne seront accessibles qu'en accès SSH protégé.
2) De plus, il existera un tunnel VPN pour accéder à certains serveurs sensibles (ou critiques)…
3) Les serveurs auront des noms standards (type « su0090 » …).
4) Seuls un nombre très restreint de personnes habilitées connaîtront le mot de passe du compte Unix « root ».
5) Le mot de passe de « root » devra être changé tous les mois, voire tous les 15 jours.
6) Il faut limiter au maximum le nombre de comptes qui ont les droits « root » super-utilisateurs (tels rootinst, rootsecu, rootinst2, rootinst3, rootinv, rootsvg, rootdba, dtsecu …).
7) L'accès au local du CENTRE INFORMATIQUE sera protégé par un badge … ou par un digicode (voire au travers d'un sas d'accès/d'entrée).

5 Politique de sauvegardes

1) Avoir une politique de sauvegarde système régulière de tous les serveurs.
2) Avoir éventuellement un serveur de sauvegarde centralisé [1] (en cluster ou sauvé lui même par un dispositif PRA (i.e. « Plan de Reprise d'Activité »).
3) Les sauvegardes du PRA concerneront tous les serveurs de production …
4) L'outil de sauvegarde ou de PRA doit être convivial, pour éviter de faire des erreurs, ou de paniquer, quand il faudra l'utiliser.
5) Il faut que chaque personne s'entraîne à remonter un serveur à partir d'une sauvegarde image système du PRA, pour éviter d'être paniquer quand il faudra effectivement avoir recours au PRA.
6) Disposer d'un serveur de test (à l'image d'un serveur de production), sur lequel on peut s'entraîner à remonter un système Unix à partir d'une sauvegarde du

[1] Donc la volumétrie prévue pour les sauvegardes devra être conséquente.

PRA (ou à partir d'une image « ufsdump » Sun sauvée, sur le serveur de sauvegarde centralisé (par exemple dans /catalog/dumps/*nom_du_serveur*).

6 politique de reboot

1) Mettre en place une politique de reboot auto, au moins sur les machines de production qui doivent être rebootées tous les mois, voire les 2 mois …

7 Gestion humaine

1) Eviter trop d'entités et de services cloisonnés…
2) Favoriser la communication horizontale.
3) Eviter la hiérarchie … et la concurrence entre les gens, sauf si c'est dans le cadre d'une émulation amicale, positive et non destructrice.
4) Eviter le management par le stress et le harcèlement. Favoriser plutôt la collaboration, la solidarité entre les collaborateurs (par des évènements qui créent du lien _ par exemple, grâce à des réunions, des formations, de pots, des rencontres au restaurant, lors de WE (?) …). Il est important de créer un vrai esprit d'équipe, un esprit qui fait qu'on a envie de faire le maximum pour le CENTRE INFORMATIQUE (un esprit qui contribue à ce que les collaborateurs ont envie de s'épauler mutuellement en cas de problème).
5) Favoriser les idées (boîtes aux idées …), par exemple par le brainstorming entre les membres de l'équipe informatique.
6) Faire en sorte que toute l'équipe soit ensemble, dans le même OpenSpace, pour une meilleure communication directe (faire en sorte que les personnes communique directement plutôt de vive voix quand cela est possible, plutôt que par mail).
7) Avec une salle de réunion équipée à côté (avec Barco _ vidéoprojecteur _, vidéo-conférence, PC connecté au réseau, paperboard …).
8) Avoir un armoire avec tous les bouquins techniques essentiels (surtout d'administration Solaris, Windows …).
11) Faire que les gens soient responsabilisés (en leur donnant des responsabilités et des objectifs, plutôt que, par exemple, de contrôler leurs horaires …).

8 Divers

1) Il faut éviter que les collaborateurs soient débordés de mails, chaque jour.
2) Pour cela, on édictera pour cela quelques règles de bonne conduite dans l'utilisation de sa messagerie. Par exemple,
3) Les collaborateurs n'envoieront des mails, que lorsque cela est vraiment nécessaire.
4) Sinon, il sera préférable, pour eux, de recourir au téléphone ou d'aller voir directement la personne ou encore d'utiliser l'outil MS-Messenger.
5) Ils éviteront, si possible, de mettre leurs mails en copie de tout le monde. d) Les titres des mails seront normalisés, lisibles et parlants : l'objet des mails sera

normalisé et court (avec par exemple, 1) un code du sujet ou du problème abordé, 2) le/les serveur(s) concernés …).

6) Sinon, le système ou les utilisateurs créeront des règles sous Outlook pour ranger automatiquement ses mails, avec une arborescence des répertoires de sauvegarde normalisée.
7) L'utilisateur devra être précis, concis et factuels, dans ses mails.
8) Le responsable du centre informatique ne doit pas uniquement se cantonner aux tâches administratives (quelles soient des tâches de gestions humaines et financières). Il doit de temps en temps pouvoir maintenir son niveau de compétence technique, en pouvant continuer de mettre la main à la patte, donner l'exemple au niveau de ses subordonnées. Il doit pouvoir se former techniquement régulièrement et être au courant, en permanence, des nouvelles technologies et évolutions informatiques. (Il devrait sinon (vœux pieux) d'avoir toutes les qualités : être un bon gestionnaire financier, être humain, concret, réaliste, bon technicien. Il connaît bien les technologies, au niveau des matériels et des logiciels…).
9) Le logement du responsable informatique et de quelques membres importants de l'équipe sera à proximité du site du CENTRE INFORMATIQUE (sinon à défaut, ils peuvent y accéder à distance par leur connexion Internet au travers d'un VPN).
10) Tous doivent pouvoir accéder par leur connexion Internet, à leur domicile, par un portail Internet/firwall, et par un VPN (CISCO …) au réseau du CENTRE INFORMATIQUE, en télétravail.
11) Les membres doivent pouvoir intervenir sur le centre à tout moment, 7J/7, 24H/24, dans le quart d'heure qui suit l'incident…

9 Conclusion

Toutes ces préconisations devraient réduire les interventions de nuits et le nombre d'incidents évitables.
L'efficacité du travail de l'équipe peut être, sans cesse, améliorée … si elle a des capacités d'anticipations pour prévenir et éviter les incidents à venir, par un travail de développement constructif anticipatif _ au niveau outils et scripts de supervision, architecture système (une solution de facilité pouvant être déjà de surdimensionner, au niveau CPU, RAM, volumétrie disque, les serveurs, en particulier, au moment de leur l'acquisition etc …