

Capitoul

Introduction à la Haute Disponibilité

16/10/2008

*Marie-Dominique Cabanne
Philippe Orth
Giles Carré*

16/10/2008

Capitoul - Haute Disponibilité

1

Sommaire



- Introduction
- Solutions
 - Environnementales
 - Organisationnelles
 - Informatique
 - architecture
 - sécurité
 - matériel
 - logiciel
- Conclusion

Disponibilité

- **dépendance aux services**
 - rendre les systèmes fiables ?
 - anticiper la panne, solutions de substitution
 - accélérer la reprise

Disponibilité

- **dépendance aux services**

- rendre les systèmes fiables ?

- PREVENTION**, choix des éléments, surveillance

- anticiper la panne, solutions de substitution

- accélérer la reprise

Disponibilité

- **dépendance aux services**

→ rendre les systèmes fiables ?

PREVENTION, choix des éléments, surveillance

→ anticiper la panne, solutions de substitution

→ accélérer la reprise

PRA Plan de Reprise d'Activité

Disponibilité

- **dépendance aux services**

→ rendre les systèmes fiables ?

PREVENTION, choix des éléments, surveillance

→ anticiper la panne, solutions de substitution

HAUTE-DISPONIBILITE

→ accélérer la reprise

PRA Plan de Reprise d'Activité

Disponibilité

- **dépendance aux services**

→ rendre les systèmes fiables ?

PREVENTION, choix des éléments, surveillance

→ anticiper la panne, solutions de substitution

HAUTE-DISPONIBILITE

→ accélérer la reprise

PRA Plan de Reprise d'Activité

Quantifier la disponibilité ?

- la règle des "9"
- durée d'arrêt cumulée sur 1 an

Nombre de 9	Arrêt du service sur 1 an
2 neuf : 99 %	environ 4 jours
3 neuf : 99,9 %	environ 9 heures
4 neuf : 99,99 %	environ 1 heure
5 neuf : 99,999 %	environ 5 minutes

Quantifier la disponibilité ?

- la règle des "9"
- durée d'arrêt cumulée sur 1 an

Nombre de 9	Arrêt du service sur 1 an
2 neuf : 99 %	environ 4 jours
3 neuf : 99,9 %	environ 9 heures
4 neuf : 99,99 %	environ 1 heure
5 neuf : 99,999 %	environ 5 minutes

HAUTE-
DISPONIBILITE

Quantifier la disponibilité ?

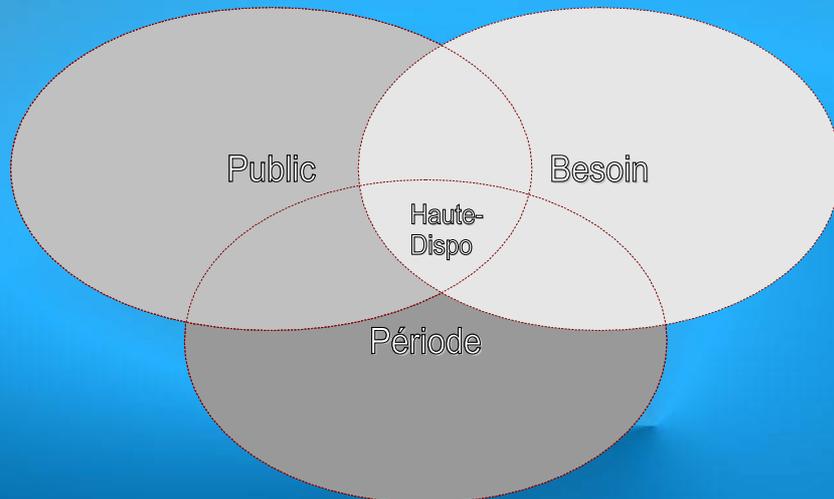
- la règle des "9"
- durée d'arrêt cumulée sur 1 an

Nombre de 9	Arrêt du service sur 1 an
2 neuf : 99 %	environ 4 jours
3 neuf : 99,9 %	environ 9 heures
4 neuf : 99,99 %	environ 1 heure
5 neuf : 99,999 %	environ 5 minutes

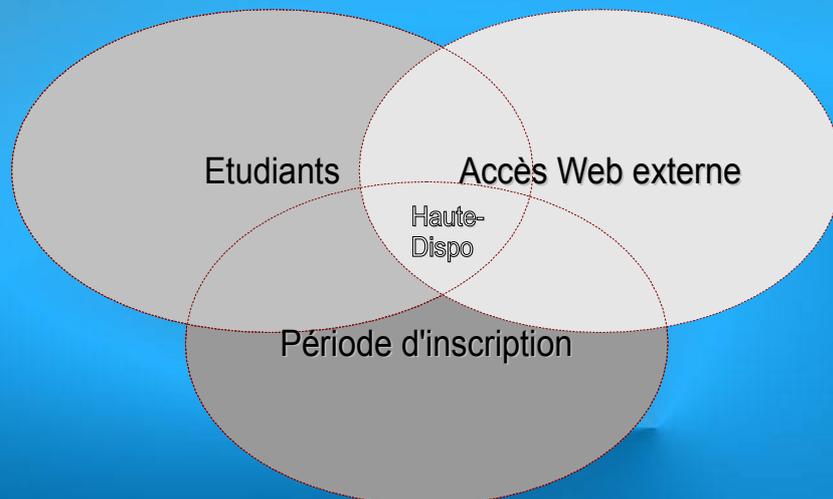
Fréquence ?

HAUTE-
DISPONIBILITE

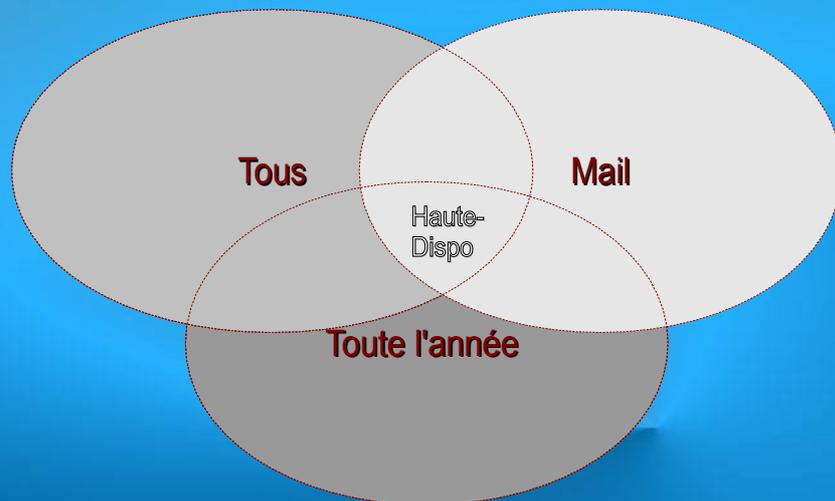
Une piste pour aborder le problème



Une piste pour aborder le problème



Une piste pour aborder le problème



Le maillon faible ...

- définir la chaîne complexe assurant le service
- identifier les "SPOF" (Single Point Of Failure)

Disponibilité
du service = Disponibilité du
SPOF le plus faible

Sommaire

- Introduction
- ➔ • Solutions
 - ➔ – Environnementales
 - Organisationnelles
 - Informatique
 - architecture
 - sécurité
 - Matériel
 - Logiciel
- Conclusion

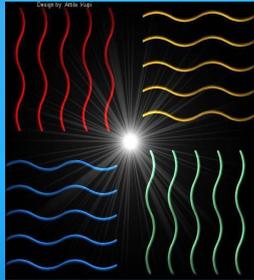
Les risques environnementaux

- 1) **Extérieur** (les 4 éléments)
- 2) **Energie** (électricité)
- 3) **Chaleur intrinsèque**

Pour **assurer une haute disponibilité** des équipements présents dans une salle machine, il faut d'abord penser à **se prémunir** des principaux **risques environnementaux**.

La salle serveur

1) choisir le lieu idéal



- **Eau** (sous sol inondable, gouttière, canalisation, etc)
- **Terre** (accès physique à la salle, vandalisme, propreté, **ordre**)
- **Air** (serveur = bouteille de vin => limiter les variations T°C et Hygro au maximum)
- **Feu** (détecteurs, gaz inhibiteurs FM200)

16/10/2008

Capitoul - Haute Disponibilité

17

- **AIR :**
 - Choisir une pièce non sensible aux variations climatiques (sous-sol de préférence, isolation thermique)
 - Laisser de l'espace autour des baies de serveur :
 - Intervention plus facile
 - Meilleure circulation de l'air (éviter les points chaud)
- **EAU :**
 - Se prémunir des dégâts des eaux (sous-sol inondable, canalisation d'eau passant au dessus des serveurs, gouttière en cas de fortes pluies, etc)
- **TERRE :**
 - prévoir l'accès physique pour charges lourdes et encombrants
 - Accès des personnes :
 - Limiter aux seules personnes nécessaires
 - Attention aux fenêtres. Prévoir barres de protection.
 - Laisser la salle propre et rangée
 - Prévoir une place pour chaque chose et étiqueter.
 - Faire des documentations synthétiques (fiches) :
 - Plus facile à maintenir
 - Plus fonctionnelle en cas d'urgence
 - Prévoir un câblage fonctionnel et bien étiqueté
 - Réseau ethernet
 - Réseau Fiber channel
 - KVM
 - Électrique (circuit 1 et circuit 2)
 - Attention au choix des étiquettes. Elles doivent tenir le temps et les actions mécaniques (vent, froid, manutention)
- **FEU :**
 - Mettre en place des détecteurs (circuits redondants)
 - Gaz inhibiteur (FM200 par exemple) pour neutraliser le feu (sans tuer l'administrateur système)

La salle serveur

2) Alimentation électrique

- Risques en amont
 - Panne du fournisseur électrique
 - Maintenance annuelle du TGBT
- Risques internes
 - Intervention sur circuit électrique



Se prémunir de :

- Rupture d'une boucle EDF
- Maintenance prévue en amont du TGBT
- Maintenance annuelle du TGBT (4h à l'UT1)
- Incidents internes : court circuit sur tableau électrique de la salle serveur
-> prévoir une séparation intégrale des circuits d'alimentations

La salle serveur

2) Alimentation électrique: un exemple de solution



La salle serveur

TGBT
principal

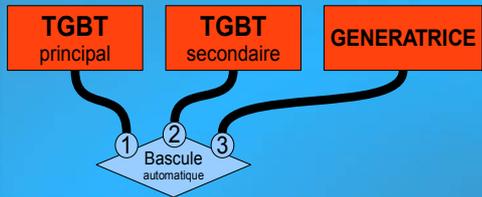
TGBT
secondaire

GENERATRICE

2) Alimentation électrique: un exemple de solution



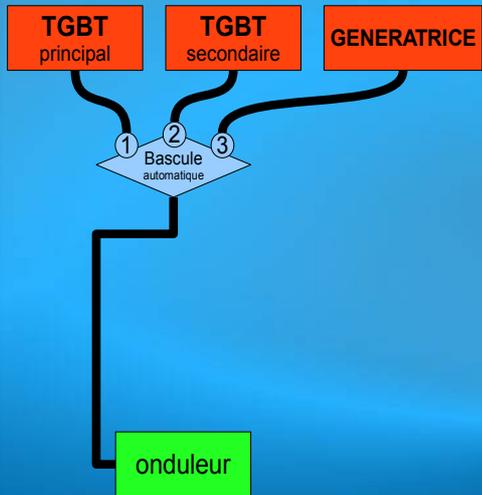
La salle serveur



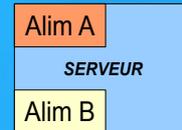
2) Alimentation électrique: un exemple de solution



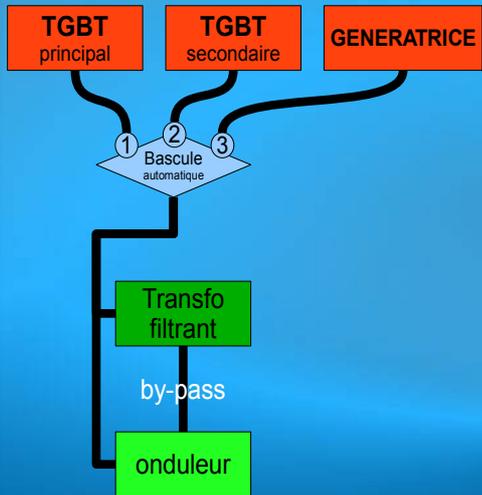
La salle serveur



2) Alimentation électrique: un exemple de solution



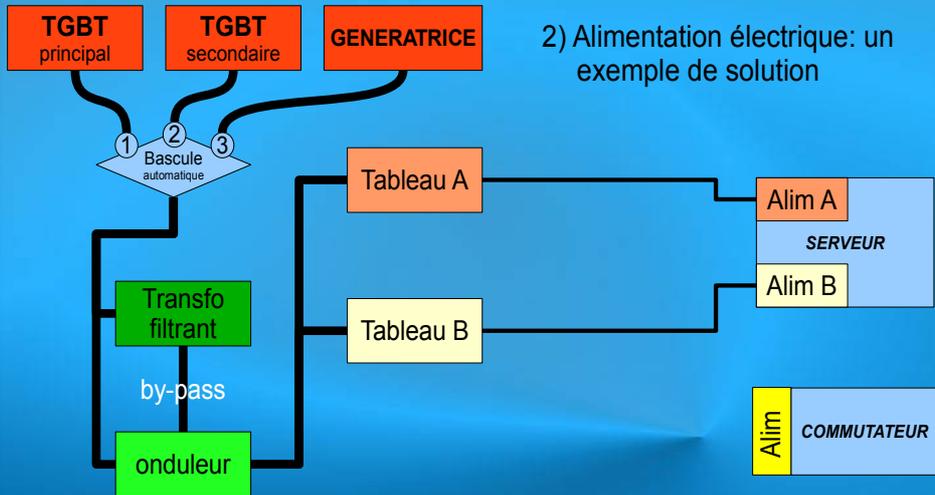
La salle serveur



2) Alimentation électrique: un exemple de solution

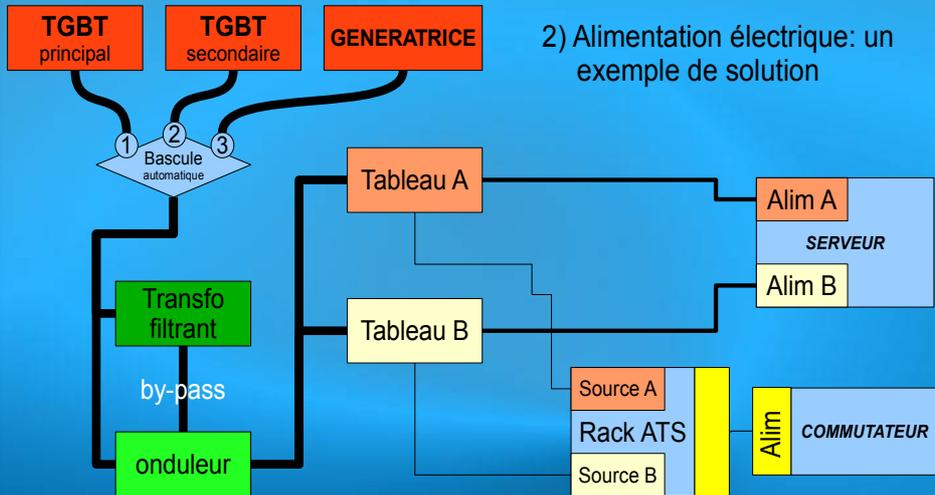


La salle serveur



2) Alimentation électrique: un exemple de solution

La salle serveur



2) Alimentation électrique: un exemple de solution

La salle serveur

3) gérer la chaleur intrinsèque



- Dimensionnement
- Éviter les points chauds
- Circulation de l'air
- Apporter l'air froid au plus près de l'équipement
- Penser au secours

- Prévoir une bonne circulation d'air
- Éviter les « points chauds »
- apporter l'air froid au plus près de l'entrée de l'équipement (face avant)
- Éviter de croiser les flux d'air
- Penser à secourir la climatisation
 - Redondance des circuits de refroidissement (au moins pour assurer niveau 1 et 2)
 - Electriquement (sinon T° augmente de +1°C par minute à UT1)
 - Le cas échéant, prévoir un extracteur d'air chaud ondulé (attention à prévoir une entrée d'air compatible avec les règles anti-incendie)
- Autres technologies :
 - Puit canadien ?
 - Eau glacée
 - Système APC

La salle serveur

Utiliser la « défragmentation de salle serveur »



16/10/2008

Capitoul - Haute Disponibilité

27

Le changement de la clim principale ou des travaux dans la salle serveur peuvent aider l'administrateur système à y voir plus clair dans sa salle.

Une photo prise quelques jours avant le début des travaux.

Les 6 baies de serveurs sont sur la droite (en noir).

La salle serveur



- 2 semaines d'arrêt (sauf pour les services de niveau 1 et 2)
- 70 serveurs physiques
- 1 SAN
- 5 commutateurs
- 3 KVM
- 1 robot de sauvegarde
- 3 Km de câbles
- 3 à 10 personnes

16/10/2008

Capitoul - Haute Disponibilité

28

Une fois « défragmentée », la salle ne contient plus que 5 baies...

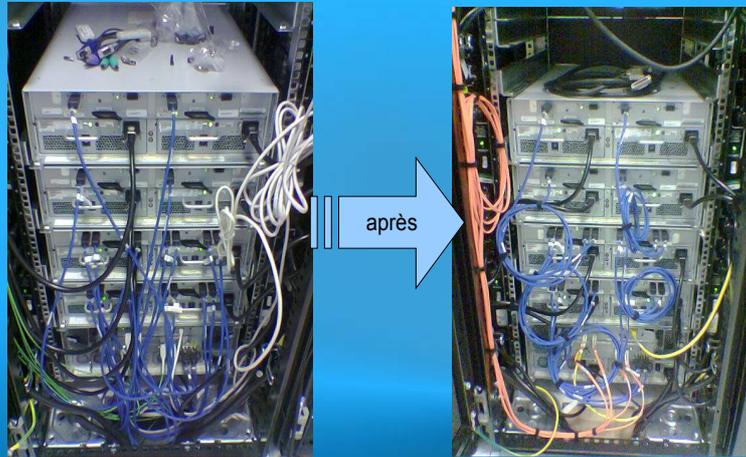
2 jours à 8 personnes pour démonter
5 jours à 5 personnes pour remonter

Conseils :

- Bien recenser les étapes
- Faire un diagramme de gantt
- Coordonner les équipes
- Jouer le scénario avant pour ne rien oublier...

La salle serveur

Propreté et ordre



16/10/2008

Capitoul - Haute Disponibilité

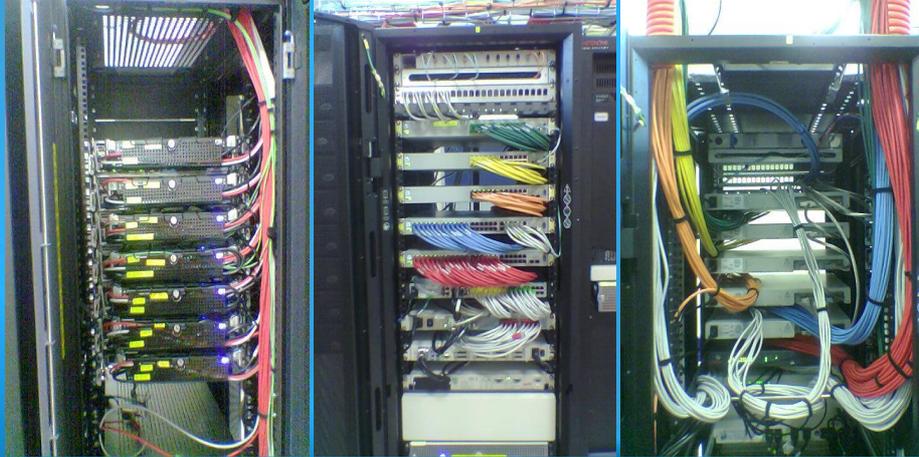
29

Câblage du SAN.

Remplacement d'un module facilité
après re-câblage

La salle serveur

Propreté et ordre



Utiliser des codes couleurs simples et fonctionnels

16/10/2008

Capitoul - Haute Disponibilité

30

Un câblage ordonné et identifié facilite énormément l'exploitation quotidienne de la salle serveur. Cela évite les erreurs sources de pannes.

En cas de soucis, l'identification du problème est facilitée et le délais de retour à la normale raccourci.

Ce que nous avons utilisé :

- Un code couleur par équipement (réseau et kvm) : vert, jaune, orange, bleu, ...
- Chaque câble est identifié avec un numéro correspondant au port de l'équipement
- Le câble jaune avec le numéro 5 branché sur le serveur X est donc connecté au commutateur « jaune », sur le port N°5.

La salle serveur

Propreté et ordre

La « nature a horreur du vide »



16/10/2008

Capitoul - Haute Disponibilité

31

La nature n'aime pas le vide, paraît-il...

Conserver une salle serveur prête en cas d'urgence n'est pas toujours facile surtout si elle est vaste.

La salle serveur

Propreté et ordre

La « nature a horreur du vide »



16/10/2008

Capitoul - Haute Disponibilité

32

La nature n'aime pas le vide, paraît-il...

Conserver une salle serveur prête en cas d'urgence n'est pas toujours facile surtout si elle est vaste.

Sommaire

- Introduction
- ➔ • Solutions
 - Environnementales
 - ➔ - Organisationnelles
 - Informatique
 - architecture
 - sécurité
 - matériel
 - logiciel
- Conclusion

Aspects organisationnels ==> solutions non technologiques

Certaines de ces solutions ont déjà été citées ou le seront ailleurs, mais leur regroupement dans cette section correspond à un point de vue.

Point de vue humain

- Rappel des risques
 - Déterioration
 - involontaire
 - volontaire
 - Attaques
- Facteurs psychologiques
 - Le stress

16/10/2008

Capitoul - Haute Disponibilité

34

On considère l'humain à la fois comme :

- Source éventuelle de problème
- Agent de solutions

Déterioration involontaire :

- Casser un équipement (se prendre les pieds dans les câbles)
- Erreur de manipulation (utilisateur, administrateur) → peut-être la source la plus fréquente d'indisponibilité

Psychologie :

- Bien redéfinir le besoin exprimé par l'utilisateur
- Apparition du stress en situation de panne

Des solutions contre la détérioration

- Limitation des accès physiques
- Responsabilisation des personnes qui interviennent
- Rangement des salles de serveur

Accès

- Très limité en salle des machines
- Pas de ménage
- Verrouillage des armoires de distribution réseau

Responsabilisation, en particulier envers les intervenants extérieurs

Rangement : la « beauté » de l'installation peut être un indicateur de qualité

Des solutions contre les attaques

- Outils logiciels de surveillance
- Voir la partie sécurité

Une documentation

- Procédures documentées
- Documentation spécialisée pour l'intervention
- Accessibilité permanente de la documentation
 - Forme papier
 - Forme électronique
 - Documentation à jour

16/10/2008

Capitoul - Haute Disponibilité

37

Spécialisation de la documentation →
distinguer :

- Documentation technique de conception, d'installation
- Documentation d'intervention
 - On ne doit pas se poser de question
 - Informations nécessaires et suffisantes

Accès à la documentation

- Papier : accès facile et permanent mais mise à jour plus difficile
- Électronique : à jour, mais être sûr de l'accessibilité en particulier en cas de panne des services (documentation sur clé USB ou sur portable autonome)

Une installation adaptée

- Organisation de la salle informatique
 - Clarté (repérage)
 - Logique (disposition)

Une organisation humaine

- Permanences
 - présence (rotations, etc)
 - compétence
- Responsable de référence

Sommaire

- Introduction
- ➔ • Solutions
 - Environnementales
 - Organisationnelles
 - ➔ - Informatique
 - ➔ • architecture
 - sécurité
 - matériel
 - logiciel
- Conclusion

Les solutions "informatiques"

- architecture
- outils

classification des services par niveau d'importance

→ *retrouver cette classification sur les baies*

les services de niveau 1

- Serveurs secondaires
 - DNS (synchro OK, config clients)
 - DHCP (synchro à prévoir, plages séparées pour les @ dynamiques)

les services de niveau 1

- Serveurs secondaires
 - services d'authentification
 - LDAP (synchro OK, client)
 - AD (synchro contrôleurs OK)
 - CAS (clusterisation possible)
 - radius (synchro à prévoir, client)
 - pare-feu

les services de niveau 1

- autonomie (pas de machines virtuelles !)
- machines différentes
- logiciels différents
- sites différents -> PRA ?

les services de niveau 2

- le service de mail
 - plusieurs MX
 - réseaux différents
 - sites différents
 - capacité du MX secondaire
 - filtrage de spam
 - délai de rétention

les services de niveau 2

- le service de mail
 - les boîtes aux lettres
 - 1 serveur de boîte
 - fiabilisation du stockage
 - sauvegarde (fréquence ?)
 - clusterisation du serveur de boîtes
 - duplication , journalisation des données

les services de niveau 2

- le service Web et autres ...
 1. redondance du serveur
 - mécanisme de heartbeat
 - IP virtuel (Fake, Ultramonkey)
 - données communes (SAN) ou réplication

les services de niveau 2

- le service Web et autres ...
 2. virtualisation avec 2 (ou +) machines physiques (VmWare ESX,Xen)
 - données communes (baie SAN)
 - mécanisme de migration à chaud (Vmotion)

les serveurs de données

- accès et intégrité des données
- clusterisation des NAC (NetApp)
- baie SAN
- redondance des éléments réseaux
- sauvegardes

les bases de données

- sauvegardes des BDD
- clusterisation (Oracle RAC)
- replication/sauvegarde entre DBB hétérogènes (Daffodil replicator)

les services de niveau 3

- C'est le niveau « métier »
- Gestion
 - caractéristiques
 - criticité par période
 - association quasi systématique à un serveur de base de données
 - respect scrupuleux des spécifications (⇒ séparation des applications)

16/10/2008

Capitoul - Haute Disponibilité

51

Gestion : contraintes fortes imposées par les éditeurs (révision de l'OS, des bibliothèques, de Java, etc)

les services de niveau 3

- ... gestion
 - ne pas patcher en période critique
 - \Rightarrow anticiper ou différer
 - Δ conditions de support
 - le plus important : la pérennité
 - complémentarité des dispositifs de sauvegarde

Importance de la pérennité : données souvent non reconstituables en rejouant les actions des opérateurs → nécessité de solutions technologiques

les services de niveau 3

- ... gestion
 - redondance des données
 - continuité assurée par un partenaire (éventuellement en mode dégradé)
 - travailler de manière sûre \Rightarrow 3 bases
 - application en production avec accès à base de production + base de test à jour
 - application et base de mise au point

les services de niveau 3

- Calcul
 - criticité : ne pas interrompre les calculs de longue durée (plusieurs semaines ou mois)
 - grappes avec mécanismes de migration ; parallélisme
 - préférer les centres de calcul

Préconisation ?

- Eviter les petites configurations de calcul isolées (la machine assemblée avec son petit Linux, isolée, peu maintenue)
- Au profit des centres de calcul

les services de niveau 3

- Serveurs d'application
 - déploiement et maintenance facilités (synchronisme des versions d'application)
 - serveurs multiples : partage et équilibrage de charge
 - applications web

les services de niveau 3

- Base de données
 - noyau sophistiqué (procédures de récupération automatiques)
 - hiérarchie de sauvegarde
 - ▷ nombreux besoins
 - à chaud, à froid
 - mixte (RAID + sauvegarde système + instantanés + sauvegarde BD)

les services de niveau 3

- Licences
 - mutualisation de jetons (optimisation + niveau de service)
 - FlexLM
 - serveurs multiples
 - continuité de service tant que $n/2 + 1$ serveurs sont accessibles

Service de licence : pourrait être envisagé au niveau 2

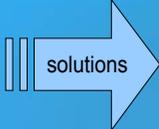
Sommaire

- Introduction
- ➔ • Solutions
 - Environnementales
 - Organisationnelles
 - ➔ - Informatique
 - ➔ • architecture
 - sécurité
 - matériel
 - logiciel
- Conclusion

Risques informatique : sécurité

- Externe
 - Attaques humaines
 - Attaques automatiques
- Interne
 - Malveillance
 - Accident

Risques informatique : sécurité

- Externe
 - Attaques humaines
 - Attaques automatiques
 - Interne
 - Malveillance
 - Accident
- 
- Parefeu
 - Antivirus (passerelle et individuelle)
 - Antispam
 - Sondes, procédures automatiques réactives (auto défense)
 - ...

Sommaire

- Introduction
- ➔ • Solutions
 - Environnementales
 - Organisationnelles
 - ➔ - Informatique
 - architecture
 - sécurité
 - ➔ • matériel
 - logiciel
- Conclusion

Le matériel : les éléments

- Disques durs
- Alimentations
- Ventilateurs
- Mémoires
- Interfaces
- cpu

Le matériel : les éléments

- Disques durs
- Alimentations
- Ventilateurs
- Mémoires
- Interfaces
- cpu
- **RAID, hot plug, spare**

RAID

- Matériel à préférer car indépendant de l'OS (partition de boot gérée)
- Logiciel (à minima)
- RAID 1 (miroir)
- RAID 5 (N+1, mini 3, parité répartie)
- RAID 6 (N+2, mini 4, 2 disques de parité)

Le matériel : les éléments

- Disques durs
- Alimentations
- Ventilateurs
- Mémoires
- Interfaces
- cpu
- RAID, hot plug, spare
- **Redondance, hot plug, spare, ATS**

Attention à la fausse redondance
Architecture blade

Système Automatic Transfert Switch de
chez APC permet de gérer la haute
dispo électrique des équipements
mono alimentation

http://www.apc.com/resource/include/techspec_index.cfm?base_sku=AP7723

Le matériel : les éléments

- Disques durs
- Alimentations
- Ventilateurs
- Mémoires
- Interfaces
- cpu
- RAID, hot plug, spare
- Redondance, hot plug, ATS
- **Redondance, hot plug**

Architecture serveur:

Redondance

Sur dimensionnement

Hot plug

Le matériel : les éléments

- Disques durs
- Alimentations
- Ventilateurs
- Mémoires
- Interfaces
- cpu
- RAID, hot plug, spare
- Redondance, hot plug, ATS
- Redondance, hot plug
- **RAID, ECC, spare**

Mémoire Error Correction Coding (bits dédiés à la correction d'erreur)

RAID 1 Mémoire possible sur certaines cartes mères .

Hot plug possible sur certaines architectures

Le matériel : les éléments

- Disques durs
- Alimentations
- Ventilateurs
- Mémoires
- Interfaces
- cpu
- RAID, hot plug, spare
- Redondance, hot plug, ATS
- Redondance, hot plug
- RAID, ECC, spare
- **Redondance, stack**

Le matériel : les éléments

- Disques durs
- Alimentations
- Ventilateurs
- Mémoires
- Interfaces
- cpu
- RAID, hot plug, spare
- Redondance, hot plug, ATS
- Redondance, hot plug
- RAID, ECC, spare
- Redondance, stack
- **Redondance, hot plug**

Le matériel : les éléments

- Disques durs
- Alimentations
- Ventilateurs
- Mémoires
- Interfaces
- cpu
- RAID, hot plug, spare
- Redondance, hot plug, ATS
- Redondance, hot plug
- RAID, ECC, spare
- Redondance, stack
- Redondance, hot plug

Maintenance

« pro-active » (SAN)

Ajuster en fonction de l'âge de l'équipement

Le matériel : l'équipement

- Carte mère : difficilement redondante
- ⇒ **redondance du serveur en entier**
- En réel
 - En virtuel
 - mixte

En réel:

- Équilibrage de charge (NLB sous windows)
- Reprise

En virtuel:

- Virtualisation en cluster (2 machines physiques minimum + partage des données (SAN ou NAS))

En mixte:

- Mélange des deux technologies

Le matériel : l'équipement

- Carte mère : difficilement redondante
- ⇒ **redondance du serveur en entier**

- En réel
- En virtuel
- mixte

CONTRAT DE MAINTENANCE

En réel:

- Équilibrage de charge (NLB sous windows)
- Reprise

En virtuel:

- Virtualisation en cluster (2 machines physiques minimum + partage des données (SAN ou NAS))

En mixte:

- Mélange des deux technologies

Sommaire

- Introduction
- ➔ • Solutions
 - Environnementales
 - Organisationnelles
 - ➔ - Informatique
 - architecture
 - sécurité
 - matériel
 - ➔ • logiciel
- Conclusion

Les logiciels

- Risque principal : le Bug
- Solutions :
 - Extreme programming
 - Programmation parallèle

Les logiciels

- Risque principal : le Bug
- Solutions :
 - Extreme Programming
 - Programmation parallèle

CONTRAT DE MAINTENANCE

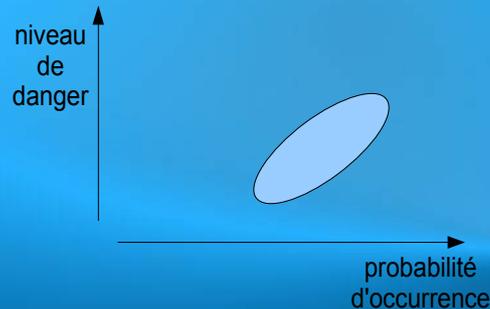
Sommaire

- Introduction
- Solutions
 - Environnementales
 - Organisationnelles
 - Informatique
 - architecture
 - sécurité
 - matériel
 - logiciel
- Conclusion



Conclusion Pourquoi la HD ?

- La HD n'est pas un absolu
- Évaluer le risque



16/10/2008

Capitoul - Haute Disponibilité

76

La Haute Disponibilité n'est pas un absolu à atteindre a priori

- Ne pas prendre le problème à l'envers (que faut-il mettre en oeuvre pour faire de la HD ?) → commencer par définir une politique
- Puis voir si on a les moyens de mettre en oeuvre cette politique

Conclusion

Les solutions

- Se situer
 - Adéquation coût / besoin
- Les solutions
 - Large éventail (Environnementales, organisationnelles, informatiques)
 - Rechercher la simplicité
 - Garder à l'esprit le nivellement par le bas

16/10/2008

Capitoul - Haute Disponibilité

77

Rechercher l'adéquation

- Évaluer le risque (intersection entre le niveau de danger et la probabilité d'occurrence) et se situer
- Évaluer son besoin
- Formaliser (public / besoin / période)
- Chiffrer

L'éventail des solutions est large

(solutions environnementales, organisationnelles et informatiques).

De nombreuses solutions sont simples, et une petite mesure bien pensée peut permettre d'élever fortement le niveau de disponibilité.

Il ne faut pas oublier le principe de nivellement par le bas qui fait que le niveau de disponibilité global est lié à l'élément le moins disponible.

Références

- <http://fr.wikipedia.org/wiki/>
 - Haute_disponibilité
 - Plan_de_continuité
 - Plan_de_continuité_d'activité_(informatique)
 - Plan_de_reprise_d'activité_(informatique)
- <https://www.clusif.asso.fr/fr/production/ouvrages/pdf/>
 - PlanContinuiteActivite.pdf
- http://lionel.tricon.free.fr/Articles/ha/ha_article.html
- http://www.alcove.fr/IMG/pdf/white_paper_HA.pdf