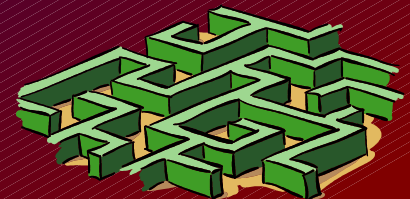


*Plan de secours informatique  
à chaud,  
virtualisation,  
et autres recettes...*

Groupe de travail OSSIR

12 mars 2007

<http://bruno.kerouanton.net>





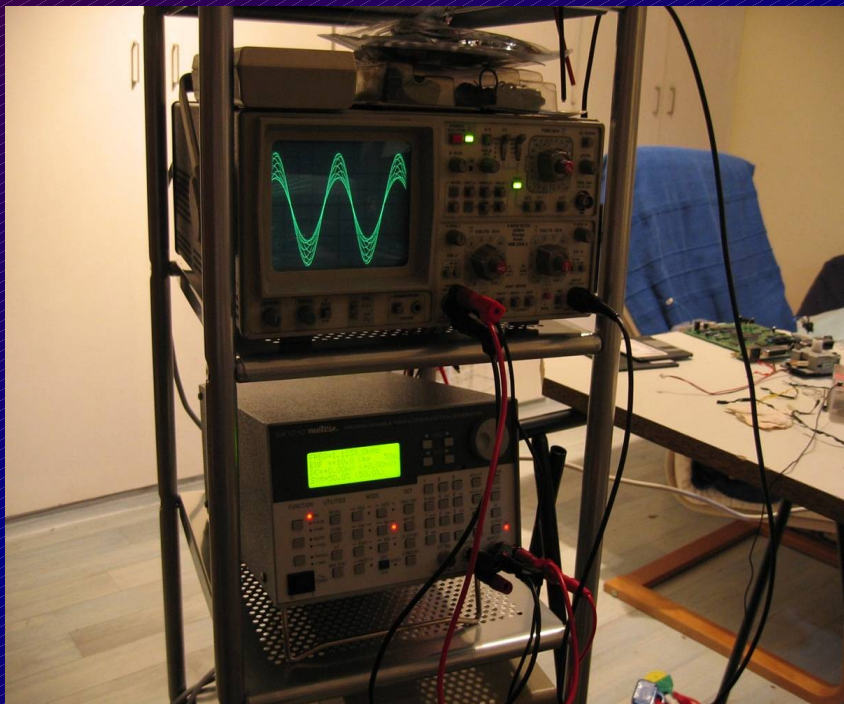
# Contexte

Vis-à-vis de l'activité de l'entreprise :

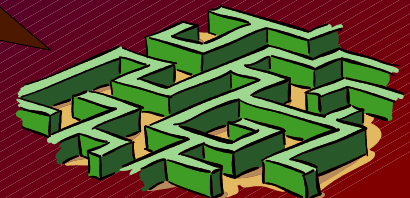
Un plan de secours informatique, pourquoi ?

La réplication à chaud de l'informatique, pourquoi ?

La virtualisation, pourquoi ?



PSI =  
L'usine à gaz ?

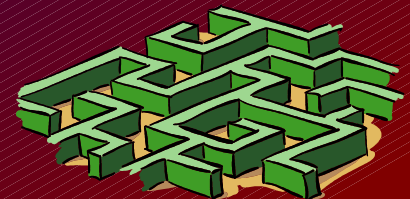




# Recette d'un *PSI* réussi

## Ingrédients :

- ➔ 2 sites informatiques
- ➔ 2 liaisons réseaux haut débit redondées
- ➔ 2 commutateurs niveau 3 de qualité
- ➔ Quelques serveurs physiques assez mûrs
- ➔ Une poignée de Vlans, et un gros trunk
- ➔ Un peu de Vmware ou équivalent
- ➔ Une pincée d'expertise Linux
- ➔ Un brin de connaissances réseaux
- ➔ De la « tchatche » pour vendre le tout à la DG, et un penchant suicidaire ;)

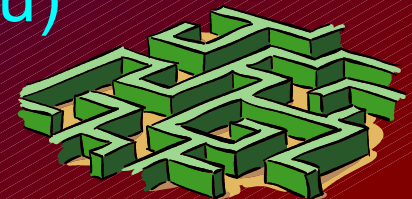




# Recette d'un PSI réussi

## Préparation :

1. Etudier l'architecture en l'état
2. Préparer la seconde salle informatique
3. Implémenter une liaison intersite fiable
4. Préparer les nouveaux serveurs physiques
5. Mettre en place la supervision et le contrôle
6. Segmenter le réseau en Vlan
7. Virtualiser quelques serveurs physiques
8. Concevoir le mécanisme de synchronisation
9. Tester et corriger si nécessaire
10. Virtualiser l'ensemble des serveurs
11. Répartir la charge intersite en fonction des besoins
12. Tester le plan de secours (à chaud bien entendu)
13. Recueillir l'avis des utilisateurs
14. Sabrer le champagne !





# Choisir les sites serveurs

Stratégie adoptée :

➔ Répartition de charge et des ressources entre les deux sites.

La liaison réseau intersite doit être

- Redondante
- Fiable
- Rapide
- Sécurisée



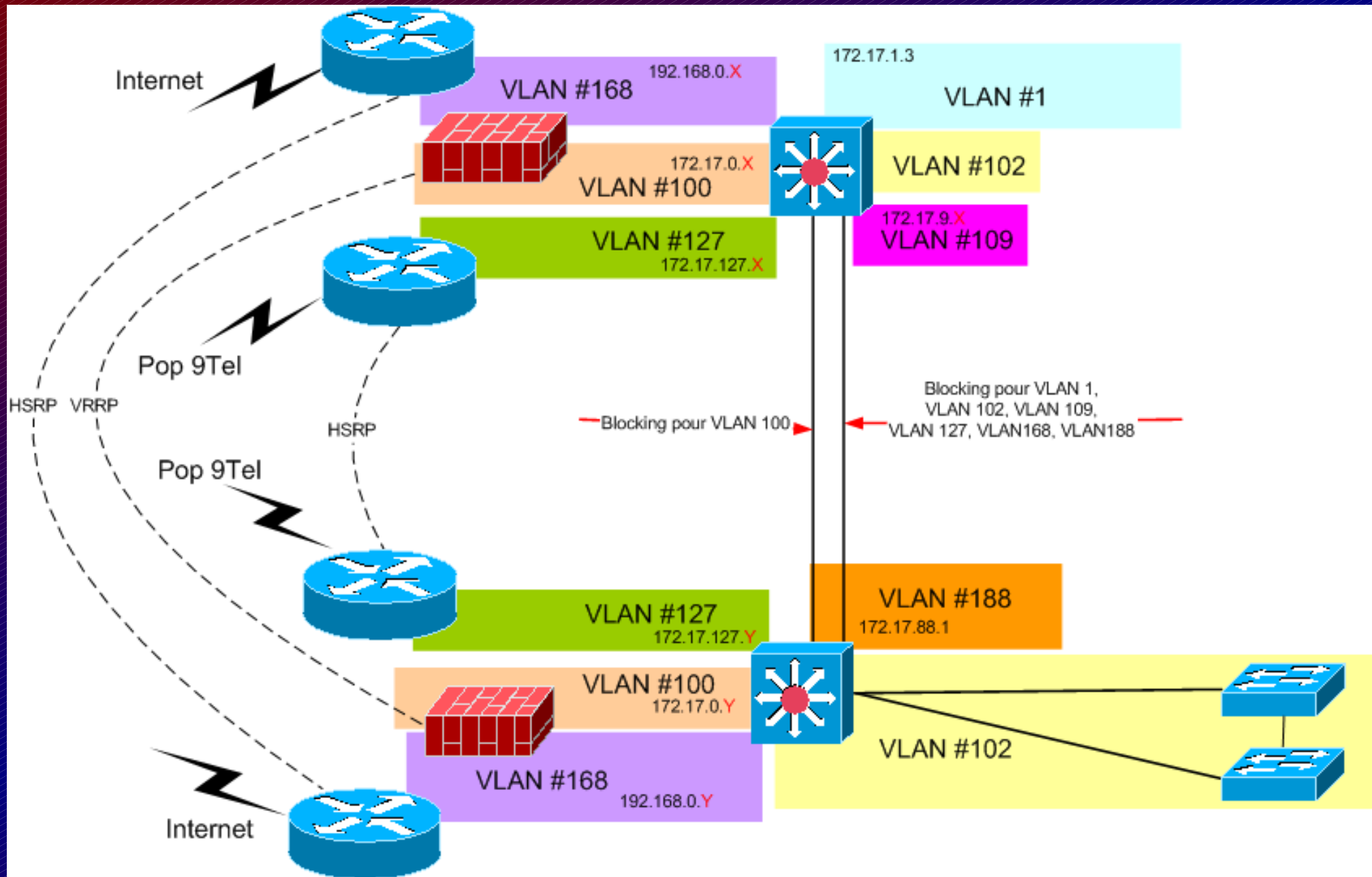
Single  
Point  
of Failure

Les 2 sites doivent héberger approximativement les mêmes serveurs et avoir les mêmes capacités

Prévoir et dimensionner air conditionné, onduleurs, protection périmétrique, etc.



# Définir l'architecture réseau





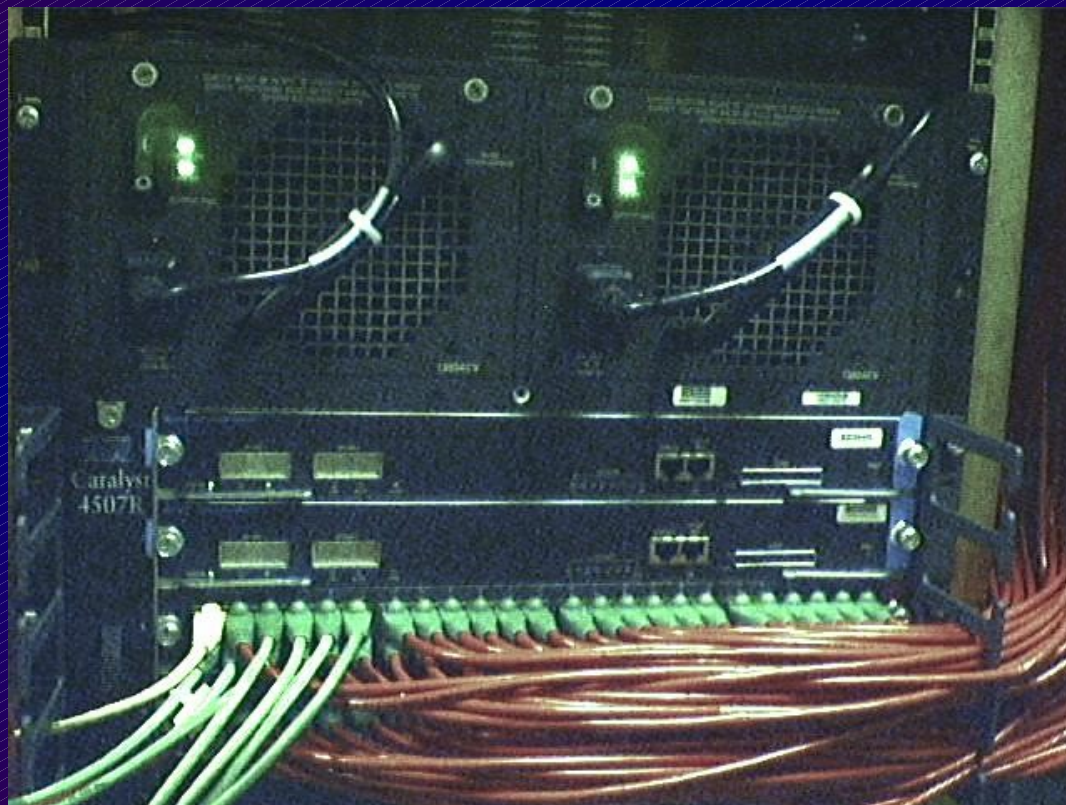
# Préparer le réseau

## Commutateurs Niveau 3 ( Routage / Vlans)

### Redondance totale :

- Alimentations
- Cartes contrôleur
- Connexions serveurs

Configuration quasiment identique sur les deux sites = simplicité.



### Points importants :

- Réseau d'administration dédié
- Utilisation des VLANs et trunk 802.1q intersite

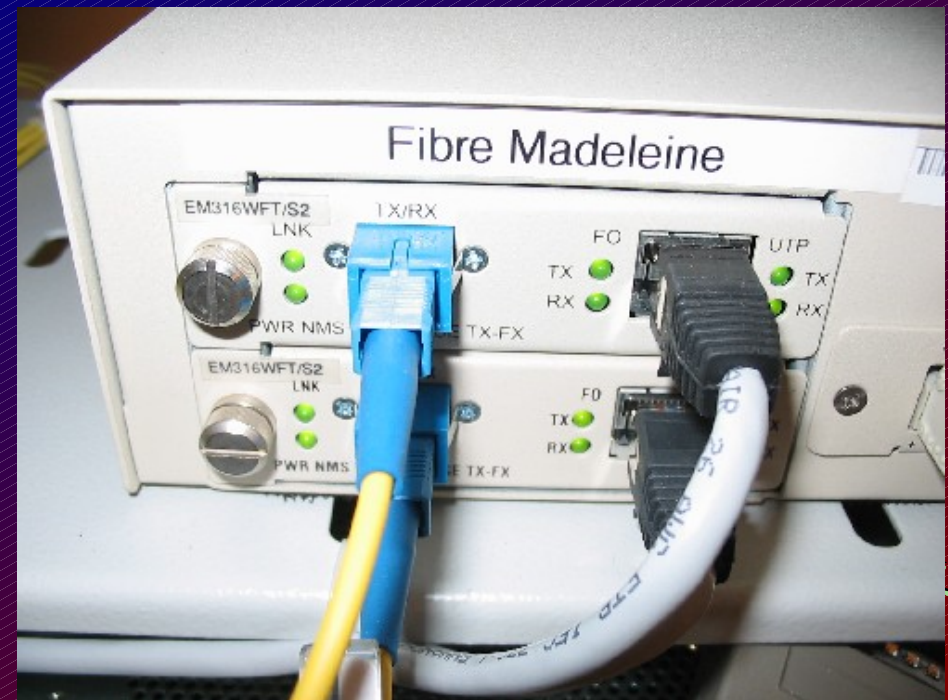
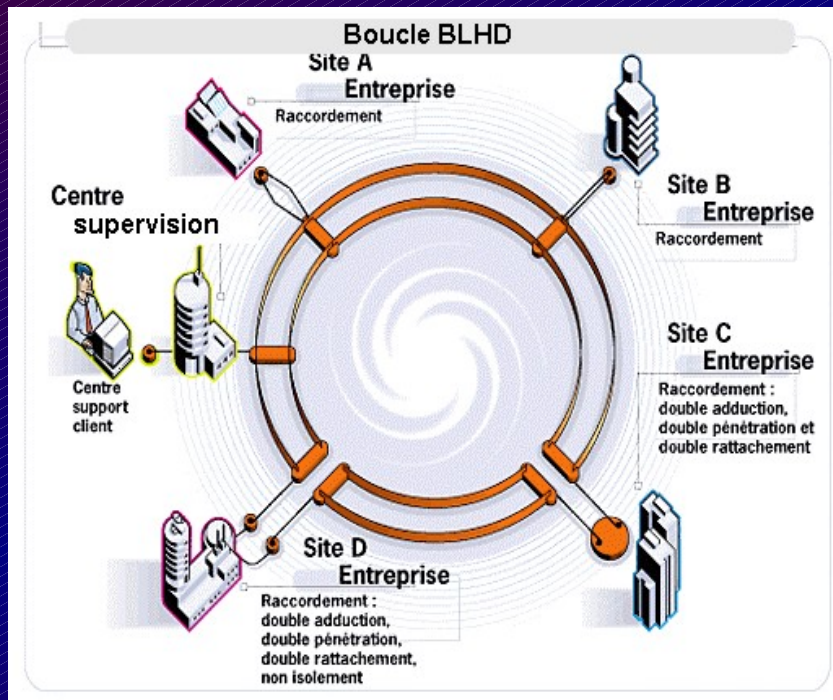




# Fiabiliser la liaison intersite

Doubler les équipements et les fibres optiques

- ➔ Utilisation d'HSRP (High Standby Redundancy Protocol) et VRRP
- ➔ Encapsulation des VLANs compartimentés dans un trunk 802.1q
- ➔ Boucle SDH (Synchronous Digital Hierarchy) du côté fournisseur
- ➔ Liaison de secours dédiée pour le réseau d'administration
- ➔ Contrats de qualité de service, SLA, et supervision.





# *Installer les serveurs physiques*

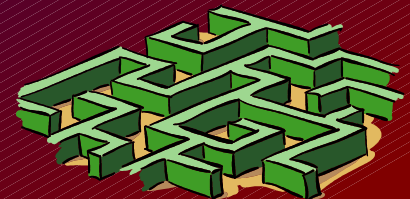


## ⇒ 12 Compaq DL-380

- bi-processeur + hyperthreading actif
- de 160 à 480Go de disque en Raid-5 par serveur
- 2 à 6 Go de RAM par serveur
- 2 cartes réseau Gigabit + 1 carte réseau de supervision (iLO)

## ⇒ VMware ESX Server 2.0

- Basé sur Linux, totalement modifié !



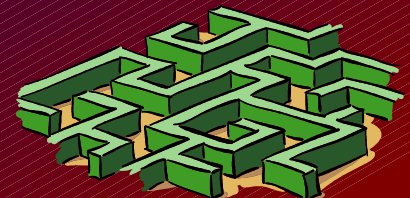


# *Paramétrer les réseaux des serveurs ESX*

Utilisation du port de supervision des Compaq DL-380 (iLO) :  
Démarrage, suivi, arrêt des serveurs à distance (suppression  
des clavier/écran/souris autrefois nécessaire, possibilité de  
« monter » une image CD-Rom à distance via le réseau et de  
démarrer dessus = **Installation de nouveaux serveurs ESX  
possible à distance**

Utilisation d'un réseau séparé dédié pour l'accès aux ressources  
Vmware sur les serveurs, et pour la synchronisation intersite.

Utilisation massive des VLANs pour segmenter le tout,  
ainsi que les différents réseaux « utilisateurs ».  
Encapsulation via un Trunk 802.1q (natif sous ESX).





# *Virtualiser les serveurs*

- ➔ Dans la majorité des cas, création d'une nouvelle machine virtuelle « neuve » et paramétrage à l'identique du serveur à virtualiser : plus propre.
- ➔ Sinon, utilisation d'un logiciel dédié : P2V (quelques déboires notamment avec NT4)
- ➔ Cas du dongle de protection matériel : résolu !
- ➔ Isolation réseau via VLAN dédié à chaque service ou métier





# Superviser les serveurs physiques

The screenshot displays the VMware VirtualCenter interface. The title bar shows the IP address 172.17.0.37 and the application name VMware VirtualCenter. The menu bar includes File, Edit, VM, View, and Help. The toolbar contains icons for Inventory, Scheduled Tasks, Templates, and Events. The left sidebar shows a tree view of Server Farms, with 'ClearChannel France' expanded to show several ESX servers, including '33par-esx3.milan.clearchannel.fr'. The main pane displays the details for this selected server, including a summary of hardware and configuration, a list of commands, and various resource utilization metrics.

172.17.0.37 - VMware VirtualCenter

File Edit VM View Help

Inventory Scheduled Tasks Templates Events

33par-esx3.milan.clearchannel.fr VMware ESX Server, 2.1.0, build-7728

Summary Virtual Machines Performance Tasks Events Alarms

Manufacturer: **HP**  
Model: **ProLiant DL380 G3**  
Total Memory: **4786MB**  
Processor: **Intel(R) Xeon(TM) CPU 2.40GHz, Hyper-threading enabled**

VMotion Enabled: **No**  
Virtual Machines: **13**  
Number of Processors: **2**  
Number of Nics: **2**  
Active Tasks: **Yes**

**Commands**

- Manage Virtual Machine Resources
- Edit Properties
- Edit Host Configuration
- Shut Down

**CPU Utilization (%)**

Virtual Machines	52	<div style="width: 52%;"></div>
Other	0	<div style="width: 0%;"></div>
System Total	52	<div style="width: 52%;"></div>

**Available Resources**

Available Disk Space: **108115 MB**  
Memory Available to New VMs: **2560 MB**

**Memory Utilization (%)**

Virtual Machines	10	<div style="width: 10%;"></div>
Other	0	<div style="width: 0%;"></div>
System Total	10	<div style="width: 10%;"></div>

**Networks**

Internal Network  
VLAN1  
VLAN200  
VLAN202  
Adapter0 Network

**Datstores**

VMFS01	329984 MB (93417 MB available)
ISOFS	15375 MB (14698 MB available)

Show active tasks

Connected as dauphin\_fr\bkero050



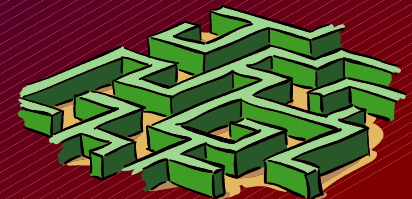
# *Mettre en place les sauvegardes*

Trois niveaux de sauvegarde !

- 1. Sauvegardes classiques avec agent sur chaque machine virtuelle (restauration de fichiers utilisateurs)
- 2. Sauvegardes de chaque machine virtuelle avec agent sur chaque machine physique (restauration de machines si nécessaire)
- 3. Réplication intersite des serveurs virtuels à chaud



*Flexibilité maximale !*





# Répartir les ressources serveur

172.17.0.37 - VMware VirtualCenter

File Edit VM View Help

Inventory Scheduled Tasks Templates Events

33par-esx3.milan.clearchannel.fr VMware ESX Server, 2.1.0, build-7728

Summary Virtual Machines Performance Tasks Events Alarms

Name, State, Host, or Guest OS contains:  Clear

Name	State	Status	% CPU	% Memory
33par-sus - Serveur W2k3 SUS [!! PRODUCTION !!]	Powered off	○○○		
33par-proxy - Squid ancien [ !! PRODUCTION !! ]	Suspended	○○○		
Clone of 33par-sus - Serveur W2k3 SUS [!! PRODUCTION !!]	Creating...	○○○		
33par-idauphin - Serveur intranet Denis [!! PRODUCTION !! ]	Powered on	○○●	2	7
33par-odb - W2Kpro Orange Bureau LAN [!! PRODUCTION !!]	Powered on	○○●	3	4
33par-pgpadmin - Console administration PGP	Powered on	○○●	3	18
33par-pgpserver - Serveur de clefs PGP [!! PRODUCTION !!]	Powered on	○○●	3	9
33par-nettools - Administration reseaux [ !! PRODUCTION !! ]	Powered on	○○●	3	2
33par-intrais - Serveur intranet IIS6 Groupe [!! PRODUCTION !!]	Powered on	○○●	8	4
33par-sql - Serveur W2k3 SQL2000 Groupe [!! PRODUCTION !!]	Powered on	○○●	9	5
33par-cisco - Supervision Reseaux [!! PRODUCTION !!]	Powered on	○○●	13	3
33par-files1 - Serveur de Fichiers Com/Mark [!! PRODUCTION !!]	Powered on	○○●	14	6
33par-proxy2 - Proxy Internet Squid [ !! PRODUCTION !! ]	Powered on	○○●	25	32

Show active tasks

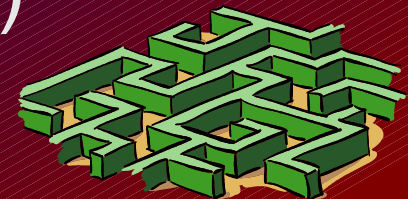
Connected as dauphin\_fr\bkero050



# *Mettre en place la réplication*

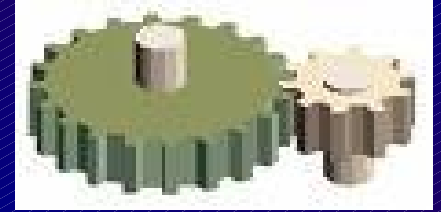
## Un VRAI Challenge :

- ➔ 35 serveurs à répliquer à chaud, 24h/24
- ➔ Pas d'interruption de service, utilisateurs connectés.
- ➔ Environ 800 Go à synchroniser entre les deux sites.
- ➔ Ne doit pas ralentir le service, ni planter.
- ➔ Les machines répliquées doivent être utilisables et redémarrables immédiatement.
- ➔ Solution Vmware proposée non envisageable ! (aurait nécessité un SAN)

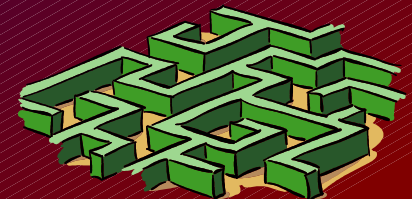




# *Création du mécanisme de réplique intersite à chaud*



- ➔ Etude du noyau Linux de VMware ESX par une société spécialisée,
- ➔ Développement de scripts et recompilation d'outils libres après adaptation nécessaire,
- ➔ Utilisation notable de l'outil rsync et conception d'un mécanisme sophistiqué de réplique différentielle unique,
- ➔ Développement d'un hyperviseur d'auto-supervision et d'auto-correction embarqué dans le mécanisme de réplique.
- ➔ En moyenne par serveur : 30mn d'analyse différentielle, de 1 à 10mn de réplique effective



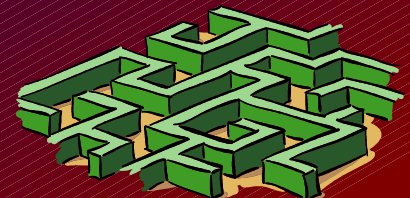


# *Limiter les pannes matérielles*

- ➔ Mathématiquement, moins de serveurs physiques = moins de pannes matérielles.

Simplicité pour la maintenance :

- Tous les serveurs physiques sont identiques
- Tous les serveurs virtuels sont transférables sur n'importe quel serveur physique sans interruption de production
- Logiciel de supervision très efficace : prévention des pannes





# *Avoir une « belle » salle machine*

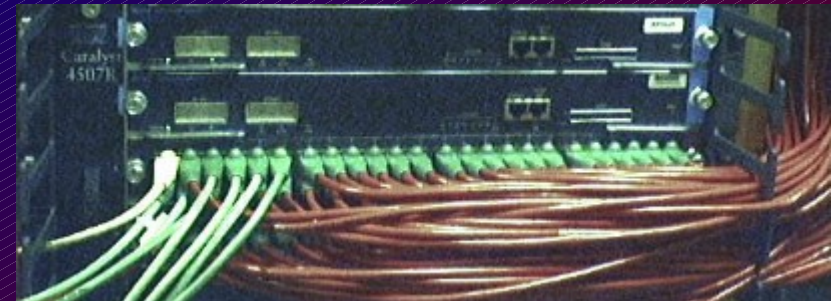
Avant :

35 serveurs physiques =  
~70 cables réseaux  
~70 cables alimentation  
~90 cables écran clavier souris



Après :

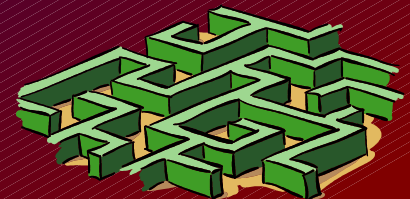
10 serveurs physiques =  
30 cables réseau  
20 cables d'alimentation  
6 cables écran clavier souris





# Remerciements

- ➔ Mes collègues de CCF qui ont :
  - subi tout cela en se demandant si le pire adviendrait
  - aidé à mettre en place le tout, courageusement
  - et qui m'ont fait confiance dans cette aventure
- ➔ Je remercie également les sociétés :
  - NSO pour l'architecture réseaux
  - Alcôve pour l'expertise Linux
  - Vmware pour leurs sympathiques logiciels



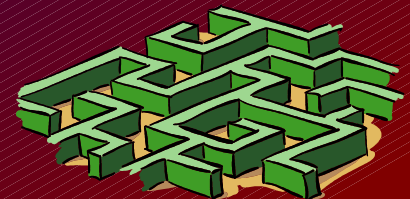


# Conclusion

- ➔ Ca marche (depuis près de 2 ans déjà)
- ➔ C'est passionnant à construire

**Tout le monde est content :**

- DSI (efficace, « scalable »)
- Directeur financier (rentable)
- Administrateurs (facile)
- RSSI (sécurisé et redondant)
- Utilisateurs (moins de problèmes)
- Direction générale (qui peut dormir tranquille)





***Merci pour votre attention***

Contact:

bruno @ kerouanton.net

<http://bruno.kerouanton.net/blog>

