

11^e salon des Solutions pour la Qualité dans l'entreprise

SisQual 2004



Association pour la maîtrise des systèmes d'information

Pour une gestion performante d'une infrastructure informatique en phase d'exploitation

Robert Lemay

Consultant Numeral Advance et Directeur Qualité FLE

Améliorer la PERFORMANCE d'un SI

La formalisation

(terminologie, concepts, inter relations...)

La gestion des compétences

La gestion des interfaces

- **Un organigramme Qualité et des responsables Qualité**
- **Des objectifs Qualité (ou de Performances)**
- **La mise en œuvre des moyens de la Qualité (référentiels, manuel qualité)**
- **Le contrôle (comparaison des résultats aux objectifs)**
- **Une communication permanente (objectifs, résultats, motivations)**

Disponibilité

Fiabilité

Extensibilité

Maintenabilité

Récupération

Testabilité

Sécurité

Intégrité

Confidentialité

Portabilité

Robustesse

Efficacité

Adaptabilité

« Defendability »

Interchangeabilité

Stabilité

Conformité

Maturité

Exactitude

Facilité d'utilisation

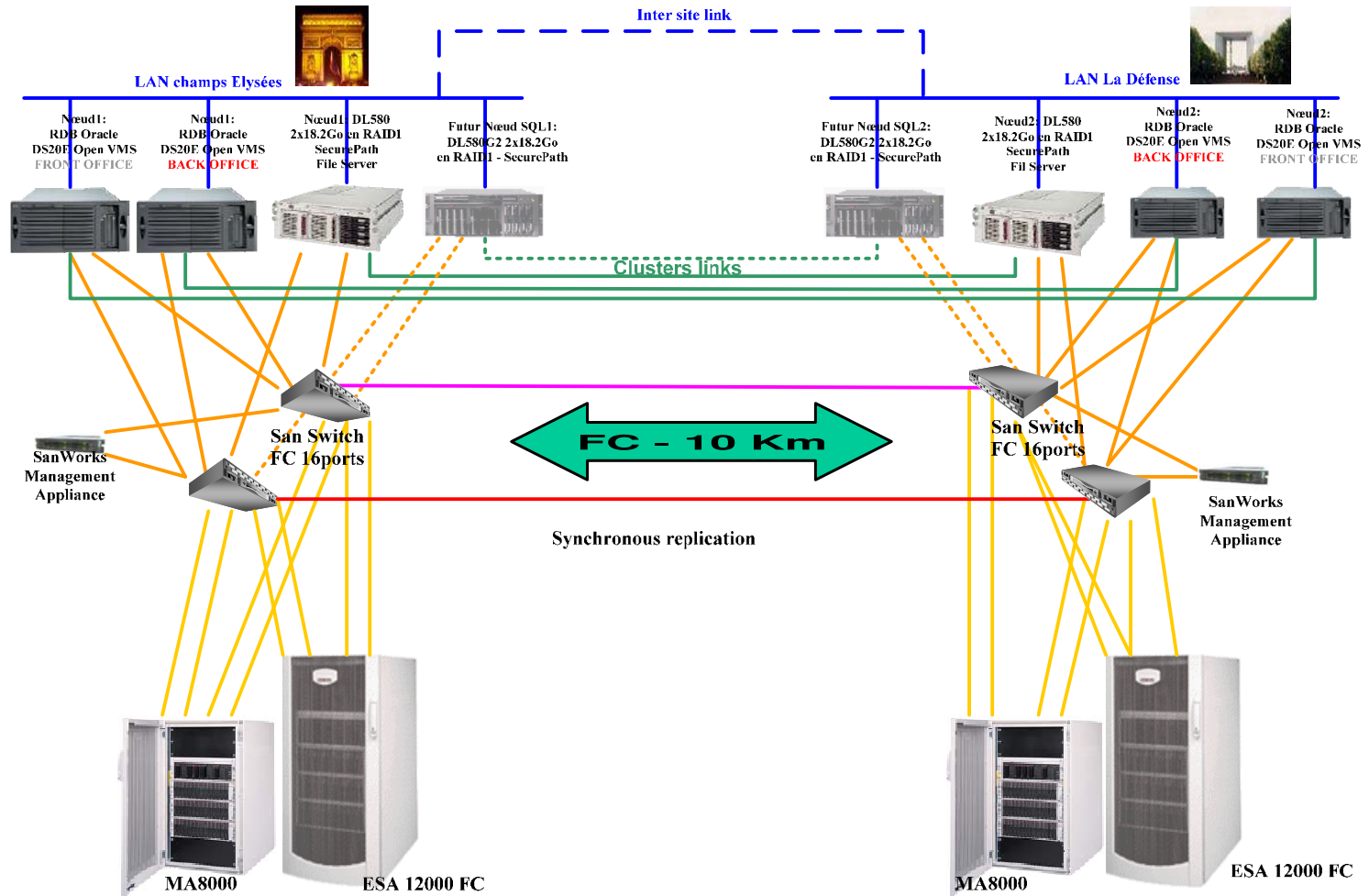
**ISO 9126 – ISO 17799 – CC – ISO 9000-3 – ISO 12207 –
Microsoft – ITIL – BS15000 – CobiT – DoD 5200.28 sdt**

- **La duplication des rôles**
- **Un organigramme figé**
- **L'effet « parapluie »**
- **Commencer la démarche qualité par la Certification**
- **Un audit Qualité orienté Conformité et non pas Amélioration (ISO 9004/2000)**
- **Présenter la Qualité comme « une obligation ».**
Il faut en permanence la « vendre », expliquer son intérêt « Business »

- **Un suivi des incidents et un processus de résolution**
- **Une bonne synchronisation entre les services**
- **Une gestion des compétences**
- **Une conduite de projet**

Traduits dans les conditions d'achats et les AOP

- **La disponibilité des ressources**
- **La fiabilité**
- **La capacité à montée en charge**
- **La répartition dynamique des charges**
- **La reprise à chaud après incidents**
- **La tolérance aux pannes**
- **La sécurisation des données et des accès**
- **La protection face aux agressions (virus...)**
- **La reprise d'activités après désastre (incendie...)**
- **L'intégrité et la confidentialité des données**
- **La maintenance sans arrêt système...**



Le « Pair et Spare »

La double alimentation

Le « Hot Swap »

Le « Dual Access »

Le Raid et le Miroir

Le Snapshot

Le Clone et le Snapclone

La Réplication de données (synchrone)

Le Cluster (applicatif, BdD, système, matériel)

Le point de reprise

Le Fault Tolerant

La Sauvegarde disque

La Sauvegarde bande

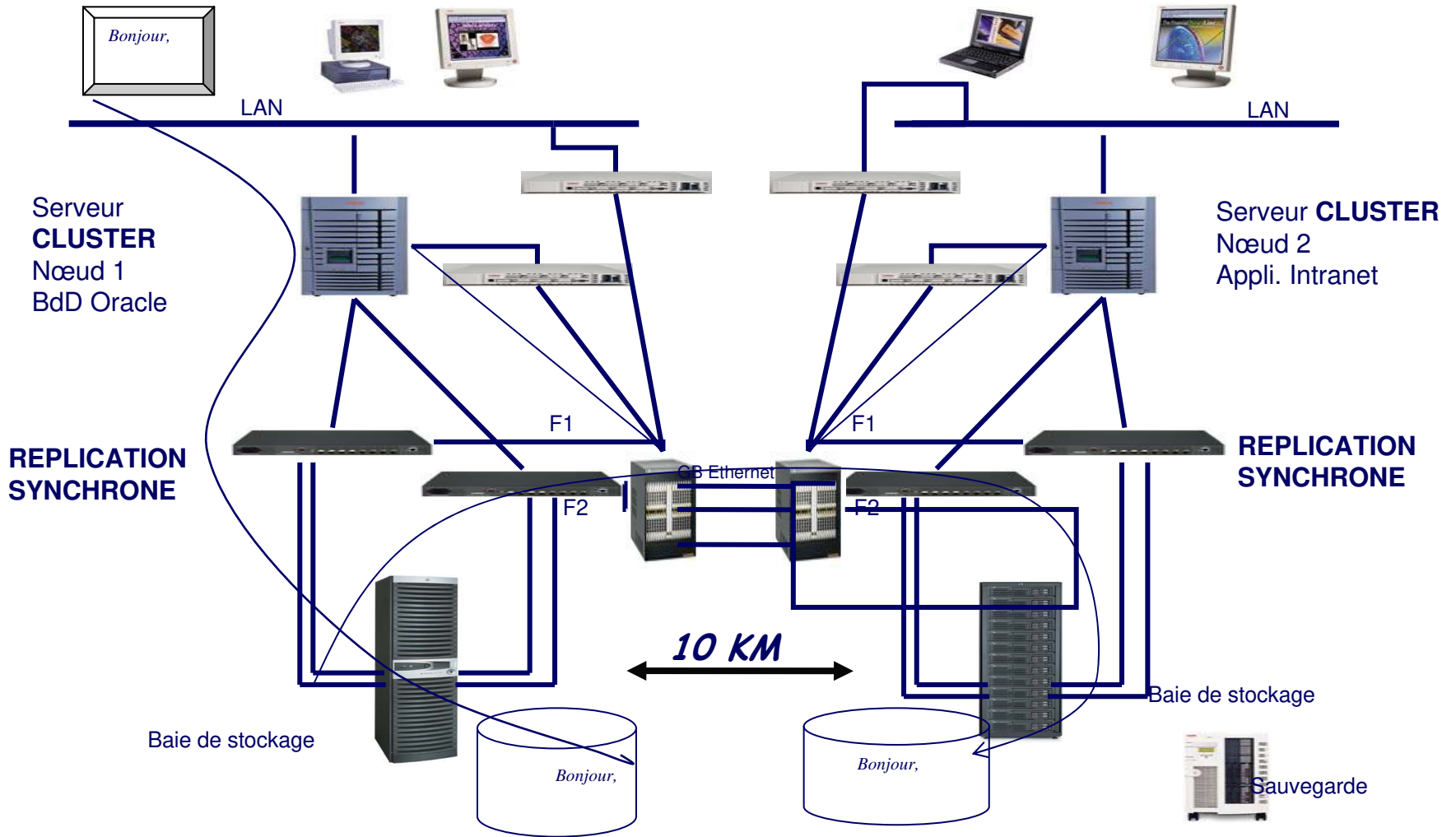
DISPONIBILITÉ : aptitude d'un système

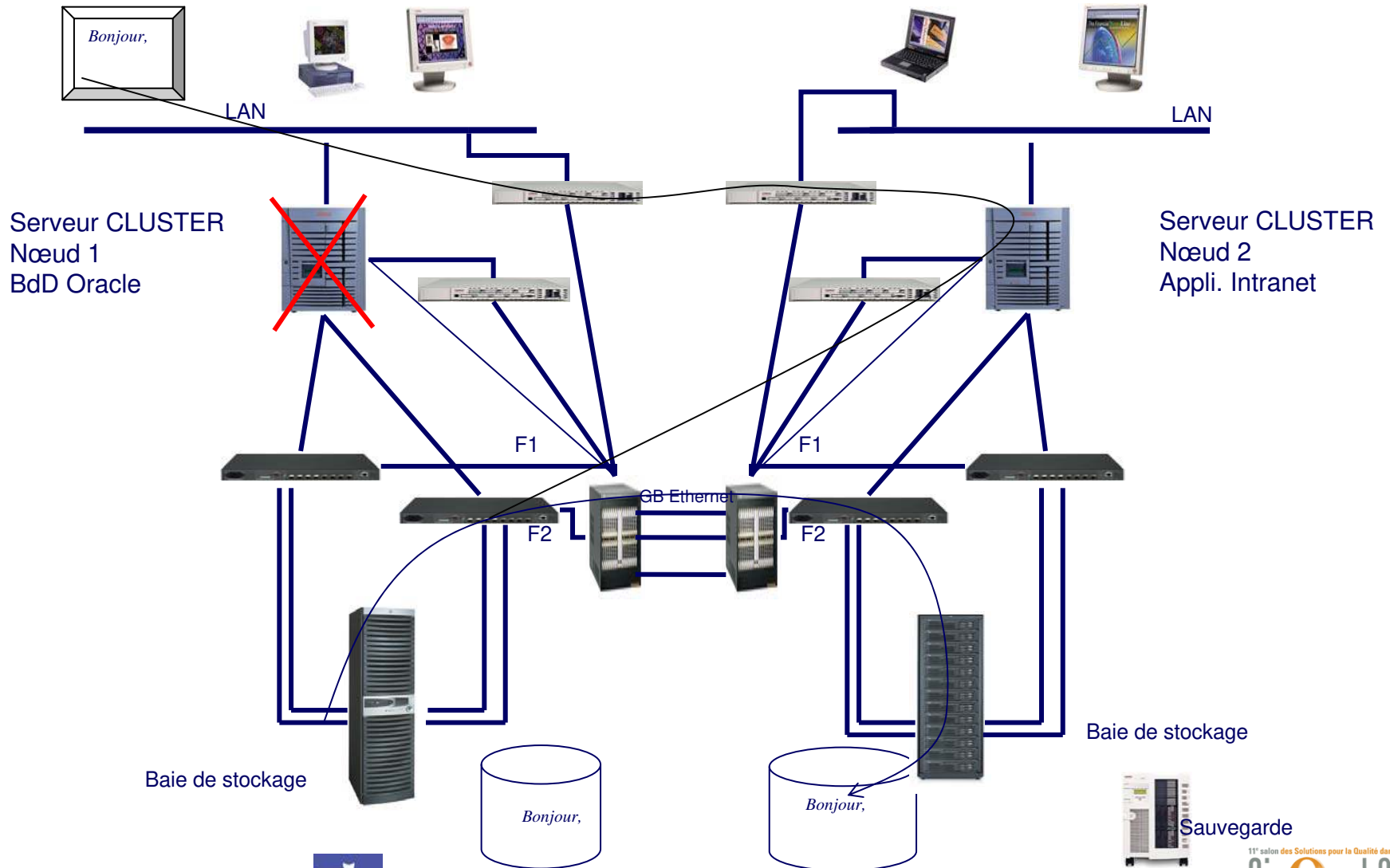
- à accomplir une fonction requise
- dans des conditions données
- à l'instant où on en a besoin
- pendant le temps prévu

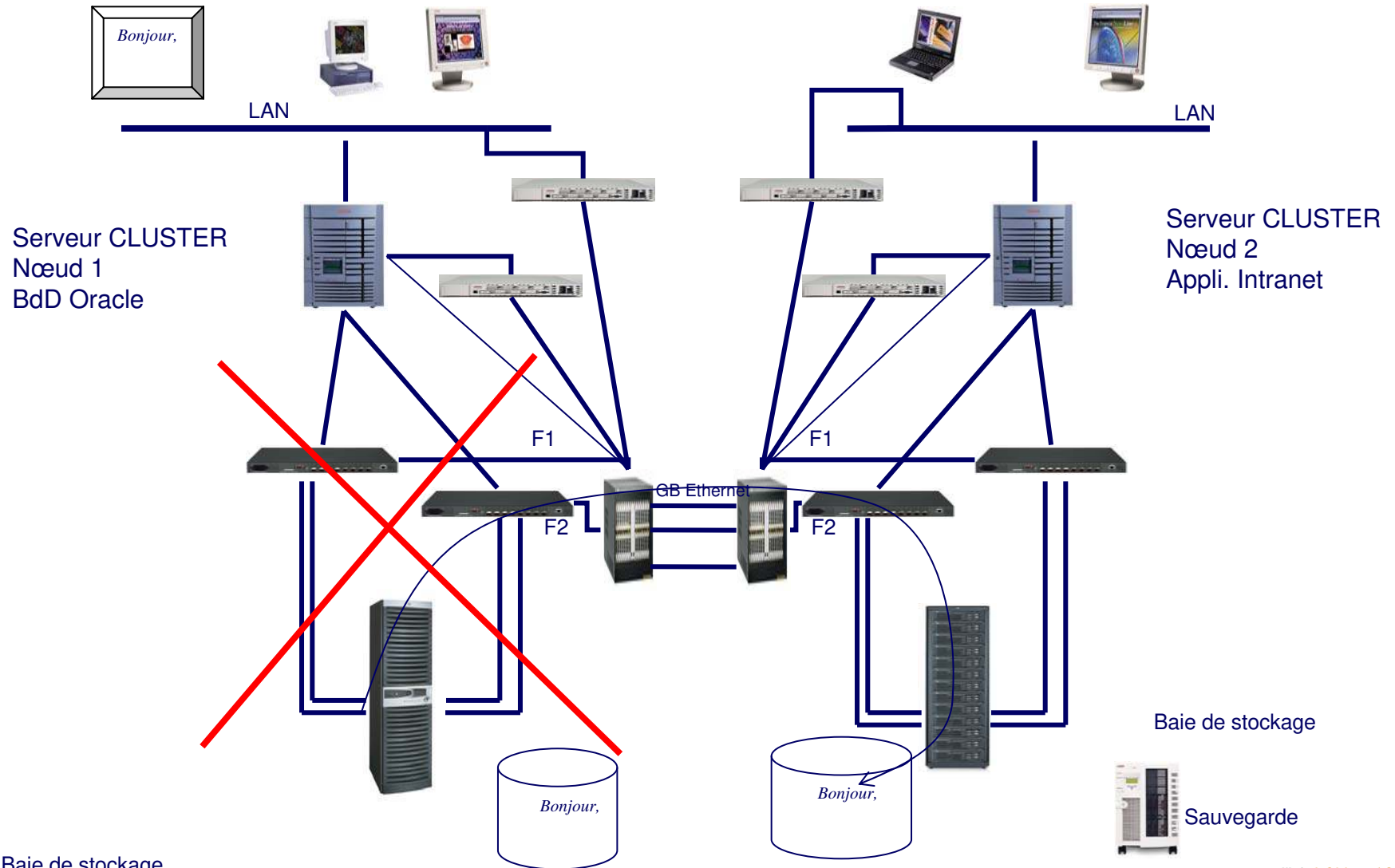
Indisponibilité mn/an	Disponibilité %
526	99,9
53	99,99
5	99,999

Disponibilité ↔ Fiabilité ↔ Extensibilité ↔ Maintenabilité

SÉCURITÉ DES DONNÉES par la réplication synchrone







Baie de stockage

Reprise après une panne système

- **bascule du système sur le site distant
(technologie cluster)**

Reprise du service après environ une minute d'arrêt

Reprise après un désastre

- **bascule des données (technologie de réplication)**
- **bascule des systèmes (technologie cluster)**

Reprise du fonctionnement normal après quelques dizaines de minutes d'arrêt

Ultérieurement, reconstitution de l'état initial (récupération)

Sans baisse de performance notable pour les utilisateurs

***La garantie est toujours soumise
à l'aléa de la panne ou de l'incident.***

Coût système sécurisé : $(100 \times 2) + 25\%$

La maîtrise d'ouvrage

Le contrôle interne

Le responsable sécurité

L'architecte systèmes et stockage

Les chefs de projets applicatifs

L'administrateur base de données

Le responsable micro et postes mobiles

Le responsable exploitation

Le responsable réseau local (LAN)

Le responsable réseau longue distance (WAN)

Le responsable stockage et sauvegarde

Le responsable du plan de reprise d'activités

Cultures, langages et pratiques différentes à faire coordonner !

TENDANCE à voir se dégrader, au cours de l'exploitation dans le temps, les performances d'un SI suite à :

- La montée en charge
- Les opérations préventives des différents intervenants
- Les mises à jour des patches, firmwares et versions d'OS
- L'absence de coordination entre différents intervenants
- Les fonctionnalités implémentées dans des composants technologiques multiples et qui évoluent à des rythmes différents

Il y a donc une difficulté importante à maintenir la cohérence de l'ensemble, et donc son niveau de performance.

- L'exploitation quotidienne doit prendre en compte les scénarios de reprise (Exemple : batch)
- Opérations préventives sans arrêt système
- Coordination entre les responsables applications et le responsable « Business Continuity »
- Gestion des fournisseurs de « Business Continuity » (application, SGBD, OS, Systèmes, Réseaux)
- L'organisation de l'exploitation va dépendre de la stratégie de « Business Continuity » retenue
- La séparation entre l'environnement de production, de qualification et de développement

Normes ou standards de nature organisationnelle :

- ITIL et BS15000
- ISO 17799
- Autres...

Normes ou standards techniques :

- Interopérabilité via SMI de l'association SNIA
- ISO 12207
- ISO 15288
- ISO 9126
- Autres...

Mais ne couvriraient pas les points de difficultés soulevés

Recherche d'un comportement commun

Création du groupe de travail AFNOR sur le thème :

**« Pour une gestion performance d'un SI
en phase d'exploitation »**

6 réunions (mai - décembre 2004) pour établir le cahier des charges

- analyse des bonnes pratiques existantes**
- panorama des normes et standards sur ce sujet**
- points à améliorer**
- plan du futur guide de Bonnes Pratiques**

jean-francois.legendre@afnor.fr