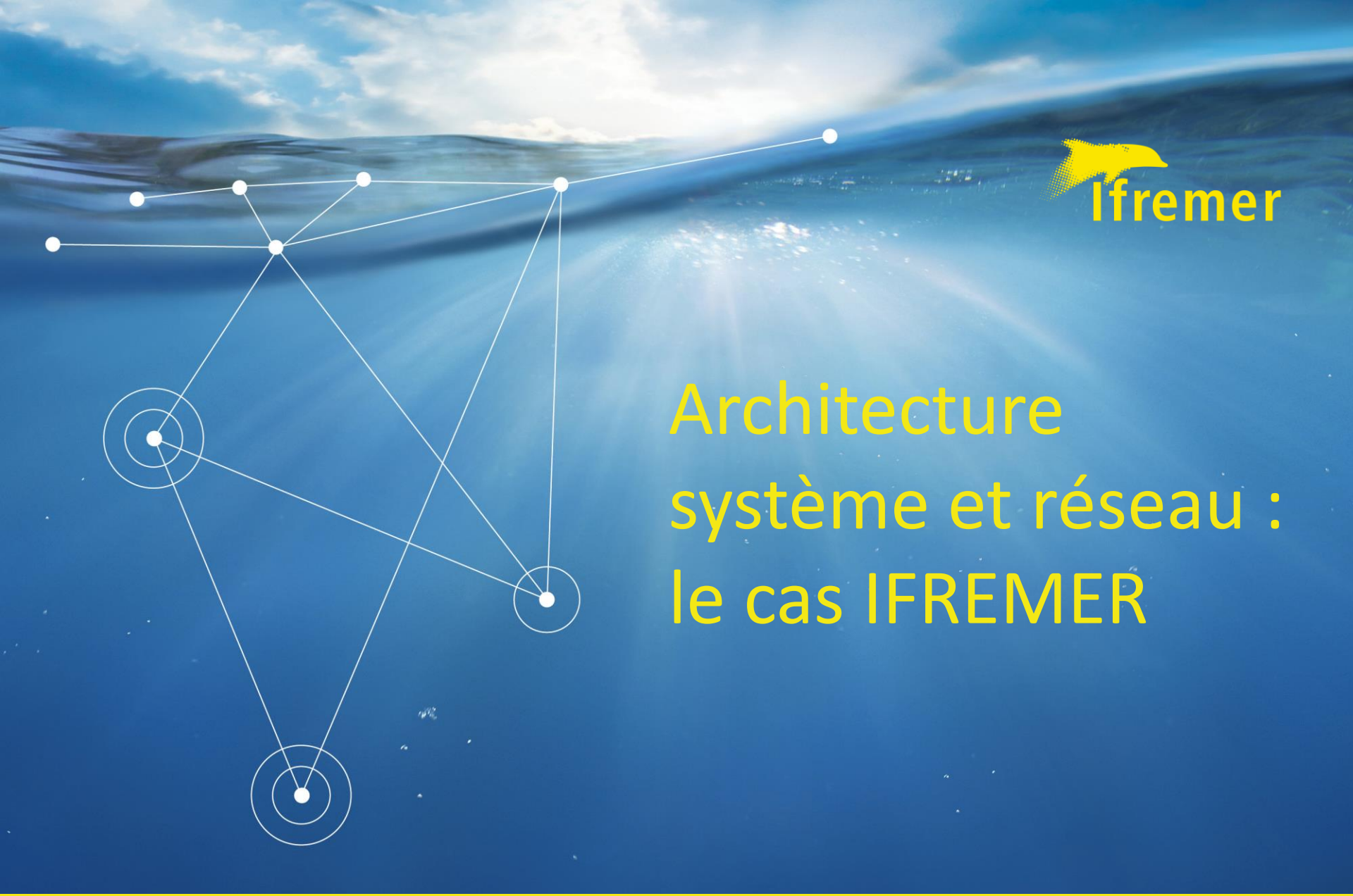


Architecture système et réseau : le cas IFREMER

PRÉSENTATION DU 07/11/2018 – IMT ATLANTIQUE
MICKAËL DEQUIDT – IMN/IDM/RIC – MICKAEL.DEQUIDT@IFREMER.FR

Ifremer

OBJECTIFS :

- Présenter les métiers de l'administration système et réseaux à travers l'exemple d'IFREMER

- Proposer une réflexion sur les spécificités de ces activités

PLAN

1. Présentation Ifremer
2. Contexte informatique
3. Environnement utilisateur
4. Architecture systèmes et réseau
5. Mobilité
6. Organisation et sécurité
7. Clés et réflexions

Présentation générale

- Institut Français de Recherche pour l'Exploitation de la Mer
- 1984 : Fusion CNEXO + ISTPM → IFREMER
- EPIC (établissement public à caractère industriel et commercial) sous tutelle de la Recherche & de l'Ecologie
- 1500 personnes (2000 avec filiales et labos associés)
- Budget annuel : 200M €

Les missions d'IFREMER

- Recherche appliquée – domaine maritime :
  - **Ressources Biologiques et Environnement**

    halieutique, écotoxicologie, biotechnologies, géochimie
  - **Ressources physiques et Ecosystèmes de fond de Mer**

    géologie, environnements profonds, géophysique, hydrocarbures
  - **Océanographie et Dynamique des Ecosystèmes**

    dynamique des habitats, étude du climat

- Missions pour le public :
  - **Expertise et suivi des ressources**
  - **Qualité des eaux et du milieu marin littoral**

Les missions d'IFREMER

- Constructeur et fournisseur de moyens :
  - **Flotte océanographique -> navires et submersibles**
  - **Systèmes de mesure, d'acquisition, de conservation et de restitution de données**
  - **Moyens d'essai**
  - **Valorisation des entreprises françaises dans le domaine maritime**

Particularité : la diversité

- Diversité thématique :
  - **De la recherche un peu partout**
  - **MAIS forte compétence technique**
  - **Couple chercheur/ingénieur**

- Diversité géographique :
  - **Dispersion des implantations dans le monde entier**
  - **Objectif : être au plus proche des sujets de recherche**


CENTRE MANCHE-MER DU NORD
Boulogne-sur-mer
Port-en-Bessin
Dinard
CENTRE BRETAGNE
Argenton
Plouzané
Concarneau
Lorient
La Trinité-sur-mer
Nantes
Bouin
L'Houmeau
CENTRE ATLANTIQUE
La Tremblade
Arcachon
Anglet
Siège social
Issy-les-Moulineaux
CENTRE PACIFIQUE
Tahiti
St-Pierre-et-Miquelon
Martinique
Guyane française
Nouvelle-Calédonie
La Réunion
Montpellier
Palavas
Sète
La Seyne-sur-mer
CENTRE MÉDITERRANÉE
Bastia
CARTE DES IMPLANTATIONS

CONTEXTE INFORMATIQUE

Les deux contextes informatiques

- Informatique au sein d'un projet
  - **Intégré dans la gestion du projet**
  - **Développements spécifiques, prestations**
  - **Produit pérenne ?**

- Infrastructures mutualisées
  - **Les ressources communes à tous**
  - **Centralisées financièrement et en termes de compétences**

Ce dont on va surtout parler

Situation générale

- Architecture serveur LINUX – sauf cas particulier

- Postes de travail :
  - **Windows en grande majorité**
  - **Linux pour utilisateurs spécialisés**
  - **Mac OS sans support**
- Si possible, suivi des standards (RFC, normes…)

- Travail dans le « monde libre », mais nécessité de composants propriétaires
  - **Mixité réfléchie**

Une équipe : le service RIC

- Ressources Informatiques et Communication
- 3M€ - 22 CDI – plusieurs CDD

- Tâche principale : administration des infrastructures
  - **Réseaux : local, accès internet, intersite**
  - **Serveurs et stockage (sites web, SGBD, calcul, espaces disques)**
  - **Services communs (comptes personnels, mail, agenda, support, sauvegarde, archivage, annuaire…)**
  - **Téléphonie et PC (fixe et mobile)**
  - **Sécurité**

- Le tout centralisé à Brest

Une équipe : le service RIC

- Concrètement, deux facettes à nos missions

- Maintenir l'infra existante
  - **Offrir le meilleur en performances**
  - **Permettre un accès continu et une disponibilité maximum aux outils de travail, pour tout le monde**
  - **Accompagner les utilisateurs et répondre à leurs demandes (assistance)**

Une équipe : le service RIC

- Concrètement, deux facettes à nos missions

- Faire évoluer l'infrastructure et les services proposés
  - **Répondre aux besoins des projets, anciens ET nouveaux**
  - **Suivre et implémenter les évolutions techniques des outils**
  - **Imaginer et concevoir de nouveaux outils**
  - **Prendre en compte**
    - les attentes utilisateur
    - les moyens à disposition (humain, financier)
    - les besoins en sécurité

ENVIRONNEMENT ET SERVICES

Les postes de travail supportés

- Windows
  - **Vista, 7, 8, 10**
  - **Cas particulier de XP : arrêt du support, mais maintien historique**
- Linux
  - **Fedora & Ubuntu (privilégié), Debian, RedHat, CentOS**
- MacOS X
  - **autorisé sans support (mais ça va changer)**

Sur Windows

- Procédure de login en réseau
  - **Exécution de programmes, installation de l'environnement**

- Package logiciel standardisé :
  - **Kaspersky Antivirus**
  - **Couple Firefox/Thunderbird**
  - **LibreOffice**
  - **Owncloud**
  - **VLC**
  - **VNC, prise de main à distance**

Compte informatique

- Un par utilisateur : couple login/passwd sur l'intranet
- Boîte de messagerie associée
- Gestion centralisée par annuaire LDAP
- Droits d'accès variés, gérés à granularité variable
- Pour chaque utilisateur, deux disques réseau sauvegardés :
  - **Un disque personnel**
  - **Un disque « groupe »**

Environnement PC

- Disques réseaux personnalisés
  - **P: disque des logiciels et utilitaires Ifremer**
  - **Q: disque personnel, un par utilisateur**
  - **N: disque commun à un service/groupe UNIX**

- Environnement Firefox/Thunderbird sur le Q: de chaque utilisateur → indépendant du PC

- Montage automatique P: Q: N: à l'ouverture de session

Sur le réseau

- Réseau local intranet
  - **Ethernet 100/1000 base T**
  - **WiFi**
  - **DHCP Ifremer**
  - **Découpage en VLAN**
- Depuis l'extérieur
  - **Portail extranet**
  - **Accès VPN**
- Imprimantes
  - **HP, pilotes PCL**
  - **Installation via serveurs intranet**

Assistance utilisateurs

- Chaque jour, deux personnes assignées
  - **Niveau 1 : interlocuteur principal, traite le classique/ordinaire**
  - **Niveau 2 : prise en charge des questions complexes**
  - **« Niveau 3 » : potentiellement tout le monde, question métier**

- Deux canaux : mail/téléphone

- Entre 50 et 100 demandes / jour.

ARCHITECTURES SYSTEME ET RESEAU

Configuration réseau

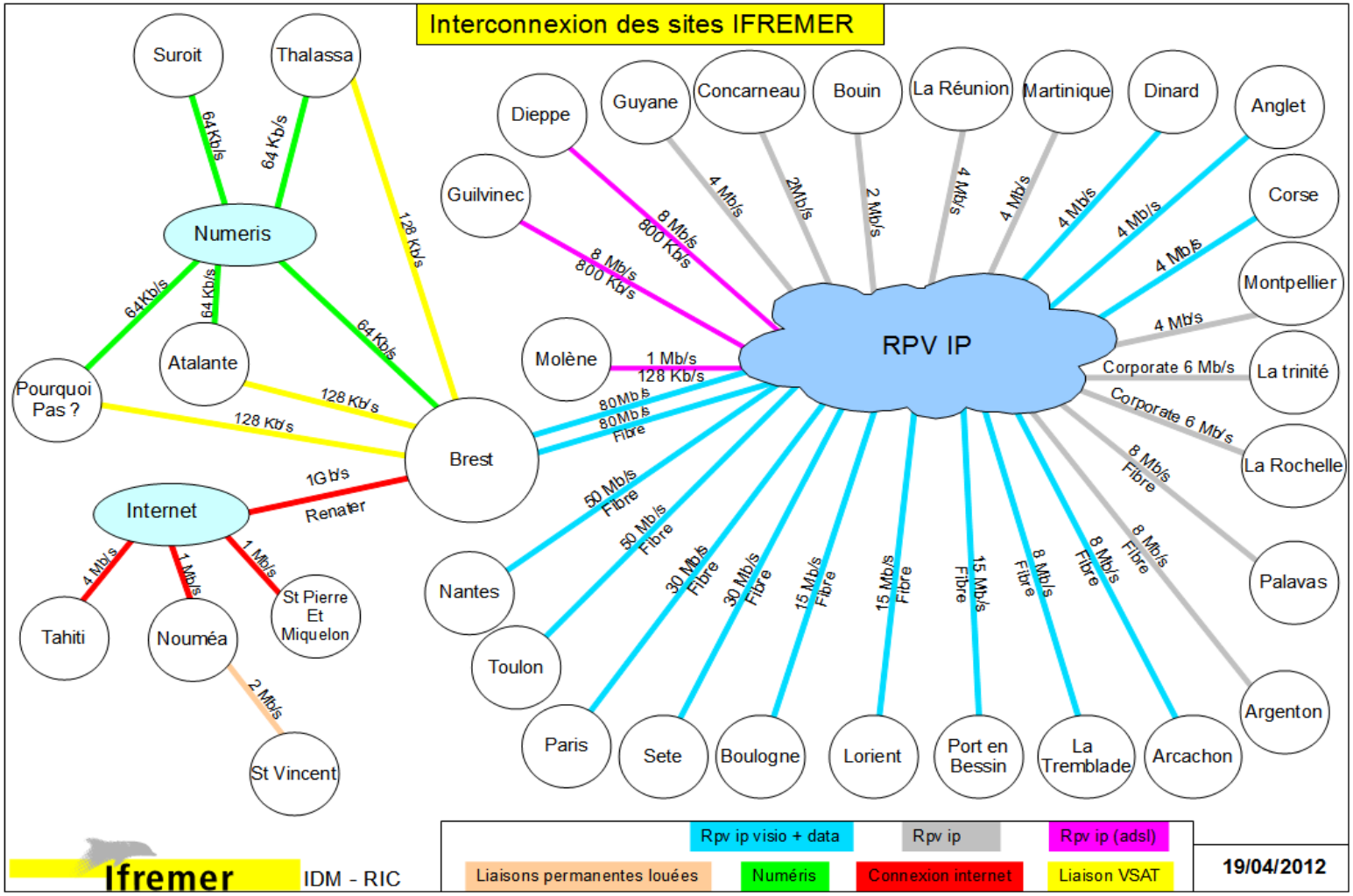
- Réseau Privé Virtuel IP : Orange
- 4 classes de services :
  - **Vidéoconférence**
  - **Flux critiques (sans volume) et téléphonie**
  - **Informatique interactive/prioritaire**
  - **Best Effort**
- Liaison intersites : VOIP
- Engagement de service contractualisé

Configuration réseau

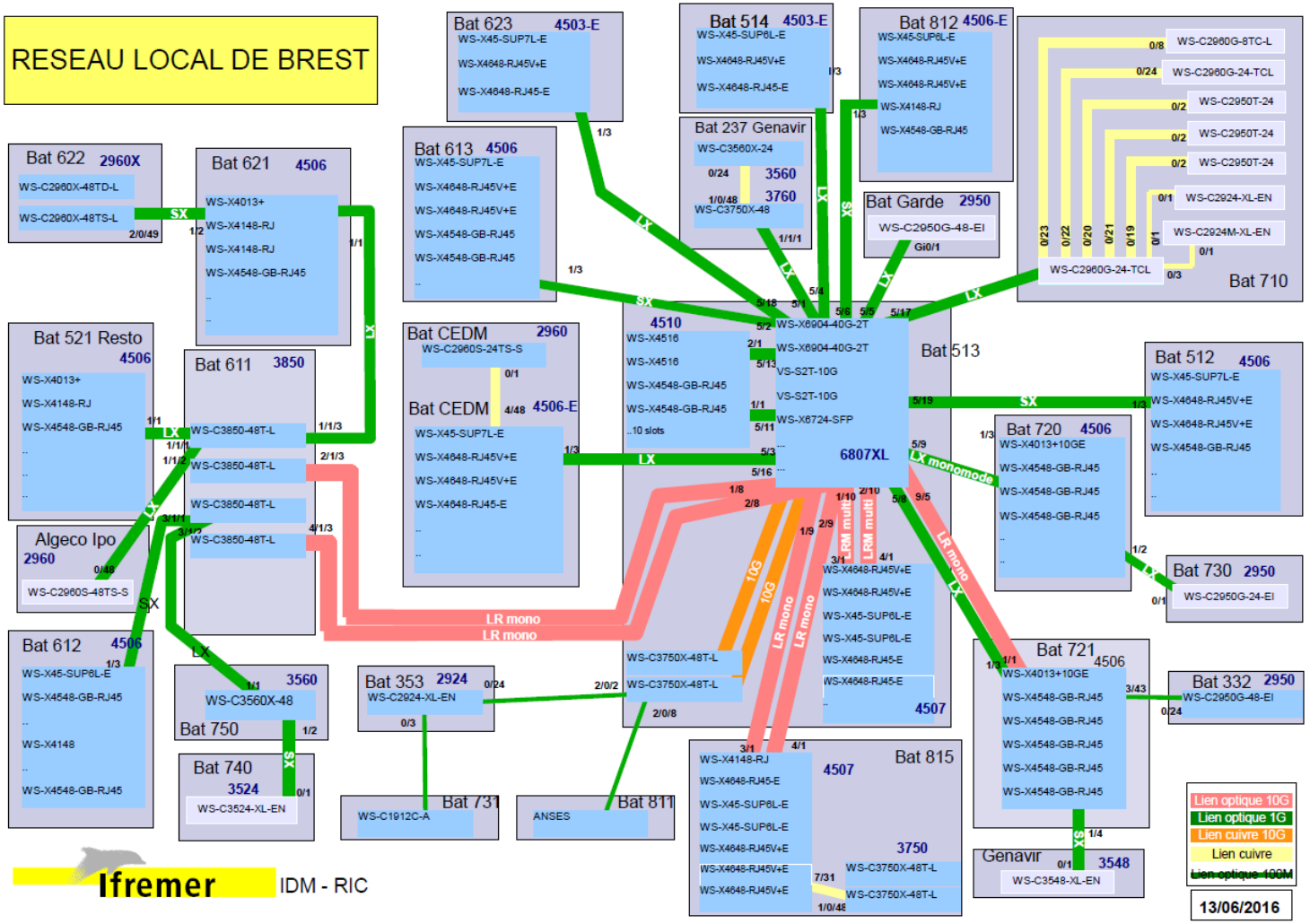
- Multiples synoptiques
  - **Réseau et organisations logiques**
  - **Intranet multisite**
  - **Réseaux locaux pour chaque site**
  - **Raccordement internet autour du firewall**
  - **Maillage physique**

- Facilite la lisibilité des architectures
- Fluidifie les évolutions

Configuration réseau



Configuration réseau



Téléphonie

- Passage en téléphonie IP
- Convergence Téléphonie Informatique – CTI
  - **Passerelle messagerie vocale → Mail**
  - **Passerelle Fax entrée/sortie → Mail**
  - **Passerelle Mail → SMS**

  - **Interface web de configuration téléphone**

La visioconférence

- ~20 salles de réunion avec système de visio
- Systèmes portatifs pour l'Outre-mer

- Fonctionnement :
  - **Ponts privés pour les connexions internes**
  - **Visio multisite (>5) : utilisation des ponts RENATER**

- Fort taux d'occupation (agenda, réservations)
- Nouvelles salles possibles
  - **Objectif : éviter le matériel perso, ingérable**

LDAP

- Standard d'annuaire informatique
- Permet de définir
  - **Le protocole d'accès à l'information**
  - **L'organisation interne et les formats des données de l'annuaire**
  - **Leur sécurité et leur répartition physique**
- A Ifremer : annuaire OpenLDAP de référence
  - **Rempli par la DRH, géré par RIC**
  - **Priorité absolue : la cohérence des données**

LDAP

- Tout découle de l'annuaire LDAP :
  - **Comptes informatiques**
  - **Contrôle d'accès**
  - **Paie**
  - **Carrière**
  - **Congés**
- Workflow ininterrompu
- Rigueur de l'actualisation des données :
  - **Retraites, démissions, décès, promotion**
  - **Nécessité d'identifier les responsables**

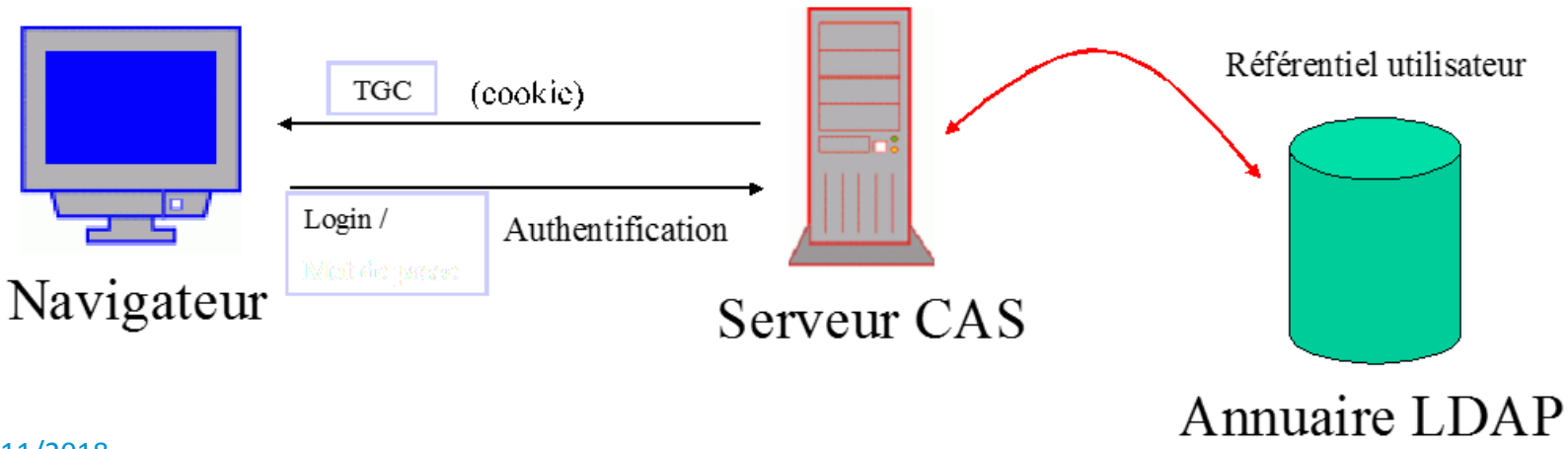
LDAP

- D’autres annuaires existent
- TOUS doivent se synchroniser sur le LDAP

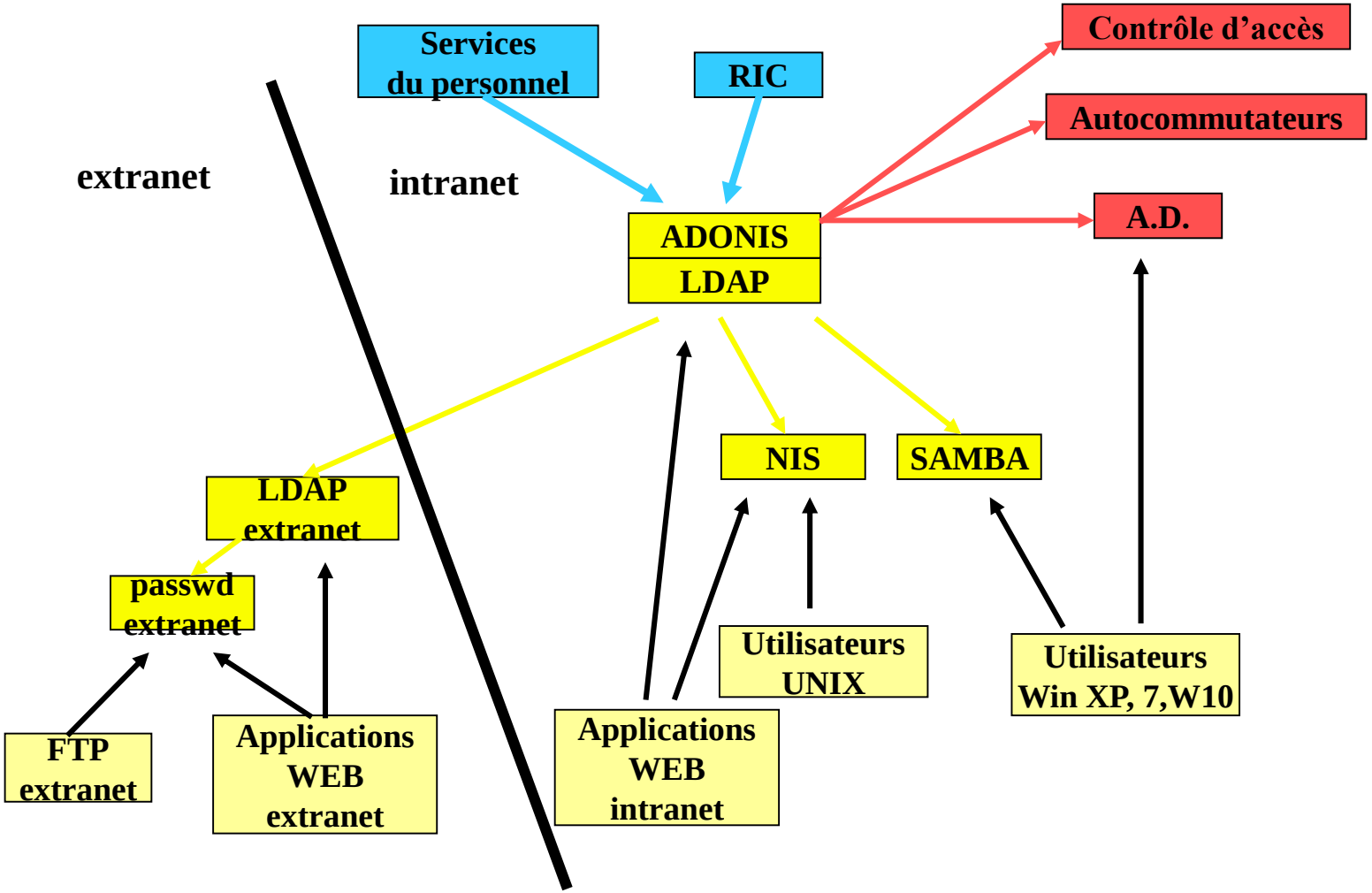
LDAP : le cas de l'authentification

- Beaucoup d'applications nécessitent de s'authentifier
  - **Certaines se branchent sur LDAP directement : Apache, Alfresco**
  - **D'autres synchronisent leur annuaire avec LDAP : NIS, SAMBA, AD…**

- Dans le cas du web : SSO (Single Sign On) CAS



LDAP : interconnexion



Système : serveurs de site

- Ifremer fortement décentralisé → coordination vitale
- Chaque site dispose d'une infra locale
- Diffusion des infos via ADONIS
  - **« Hosts » : NIS, AD, DNS, netgroup, DHCP, GLPI, Kaspersky…**
  - **« Users » : passwd, samba, alias, LDAP, group…**

Système : serveurs de site

- Au moins un serveur Debian par implantation géographique
- Relais « physique » pour :
  - **La messagerie**
  - **Les fichiers communs**
  - **Les fonctions « hosts »**
- Alimentés par CFEngine et Ansible, depuis Brest, en push
- Hébergement disques users & commun

Système : serveurs de site

- Un serveur Windows (le plus à jour possible) pour
  - **Login Active Directory**
  - **Gestion des imprimantes réseau**

- Un serveur de sauvegarde
  - **Linux**
  - **Avec robot**

- Bilan : au moins trois serveurs, dont minimum deux physiques (virtualisation windows)

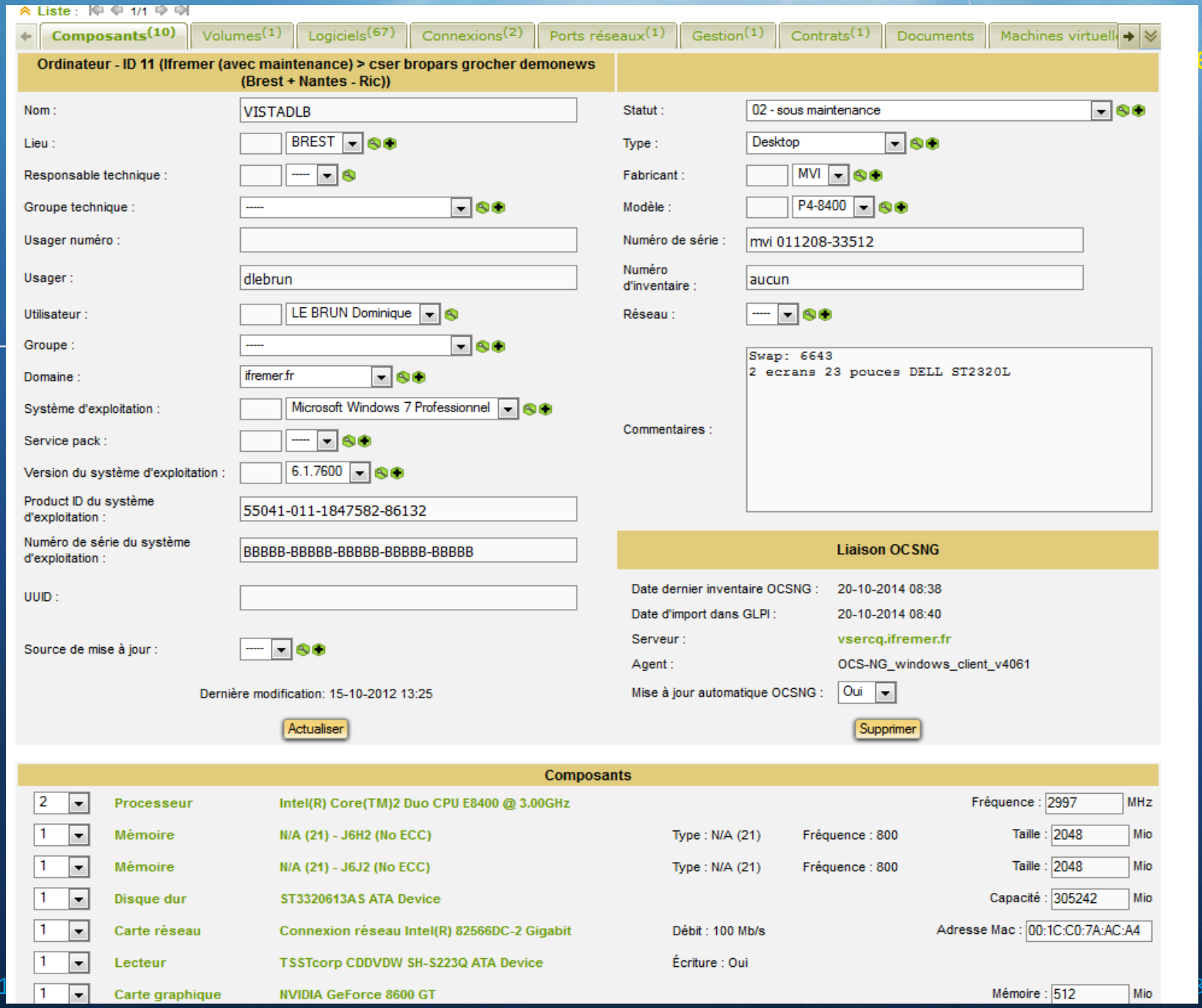
Le parc informatique

- Nécessité d'un recensement exhaustif des PC : garanties, maintenance, obsolescence…

- Difficultés : standards limités, éloignement, peu de maîtrise des achats

- **OCS** : Open Computer inventory System
- **GLPI** : Gestion Libre du Parc Informatique

- Gestion par zone (correspondants)


Liste : 1/1
Composants(10)
Volumes(1)
Logiciels(67)
Connexions(2)
Ports réseaux(1)
Gestion(1)
Contrats(1)
Documents
Machines virtuell
Ordinateur - ID 11 (Ifremer (avec maintenance) > cser bropars grocher demonews (Brest + Nantes - Ric))
Nom : VISTADLB
Lieu : BREST
Responsable technique : ----
Groupe technique : ----
Usager numéro :
Usager : dlebrun
Utilisateur : LE BRUN Dominique
Groupe : ----
Domaine : ifremer.fr
Système d'exploitation : Microsoft Windows 7 Professionnel
Service pack : ----
Version du système d'exploitation : 6.1.7600
Product ID du système d'exploitation : 55041-011-1847582-86132
Numéro de série du système d'exploitation : BBBBB-BBBBB-BBBBB-BBBBB-BBBBB
UUID :
Source de mise à jour : ----
Dernière modification: 15-10-2012 13:25
Actualiser
Statut : 02 - sous maintenance
Type : Desktop
Fabricant : MVI
Modèle : P4-8400
Numéro de série : mvi 011208-33512
Numéro d'inventaire : aucun
Réseau : ----
Commentaires : Swap: 6643
2 ecrans 23 pouces DELL ST2320L
Liaison OCSNG
Date dernier inventaire OCSNG : 20-10-2014 08:38
Date d'import dans GLPI : 20-10-2014 08:40
Serveur : vsercq.ifremer.fr
Agent : OCS-NG_windows_client_v4061
Mise à jour automatique OCSNG : Oui
Supprimer
Composants
2 Processeur Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz Fréquence : 2997 MHz
1 Mémoire N/A (21) - J6H2 (No ECC) Type : N/A (21) Fréquence : 800 Taille : 2048 Mio
1 Mémoire N/A (21) - J6J2 (No ECC) Type : N/A (21) Fréquence : 800 Taille : 2048 Mio
1 Disque dur ST3320613AS ATA Device Capacité : 305242 Mio
1 Carte réseau Connexion réseau Intel(R) 82566DC-2 Gigabit Débit : 100 Mb/s Adresse Mac : 00:1C:C0:7A:AC:A4
1 Lecteur TSSTcorp CDDVDW SH-S223Q ATA Device Écriture : Oui
1 Carte graphique NVIDIA GeForce 8600 GT Mémoire : 512 Mio

Système : la messagerie

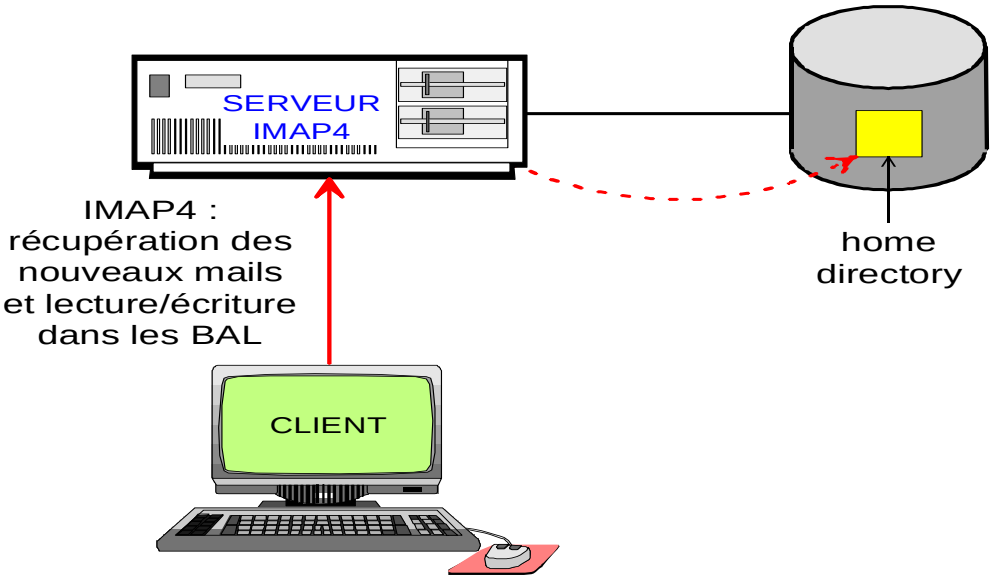
- Tous les utilisateurs ont un compte mail
- Comptes virtuels : projet, groupe, fonction…

- Côté client : Thunderbird
- Côté serveur : Postfix pour SMTP, Dovecot pour IMAP

- Systèmes de forward et de gestion d'absence - SIEVE
- Listes de diffusion :
  - **SYMPA (SYstème de Multi-Postage Automatique)**
  - **Listes dynamiques avec LDAP**

Système : la messagerie

- Consultation des mails par IMAP uniquement



AVEC IMAP4

- Pourquoi ?
  - **Concurrence d'accès**
  - **Souplesse de transit**
  - **Intégrité de la donnée**
  - **Pérennité de la donnée : stockage serveur vs stockage client**

Système : la messagerie

- Avant : stockage sur serveur de site, dans les Homedir
- Aujourd'hui : stockage centralisé sur Brest à 99%
  - **Cas de Nouméa**

- Pourquoi ?
  - **Un serveur IMAP au lieu de plusieurs dizaines**
  - **Updates, sauvegardes et transferts faciles**
  - **Gain d'espace et de sécurité utilisateur**
  - **« Serveurisation » des traitements**
  - **Ouverture IMAP vers l'extérieur**

- Limitation : le réseau

Système : la messagerie

- Au total :
  - **3 900 comptes**
  - **9 To de données, en croissance constante**
  - **~0,3 mail/s, plus de 24 000 mails reçus par jour, autant d'envoyés**

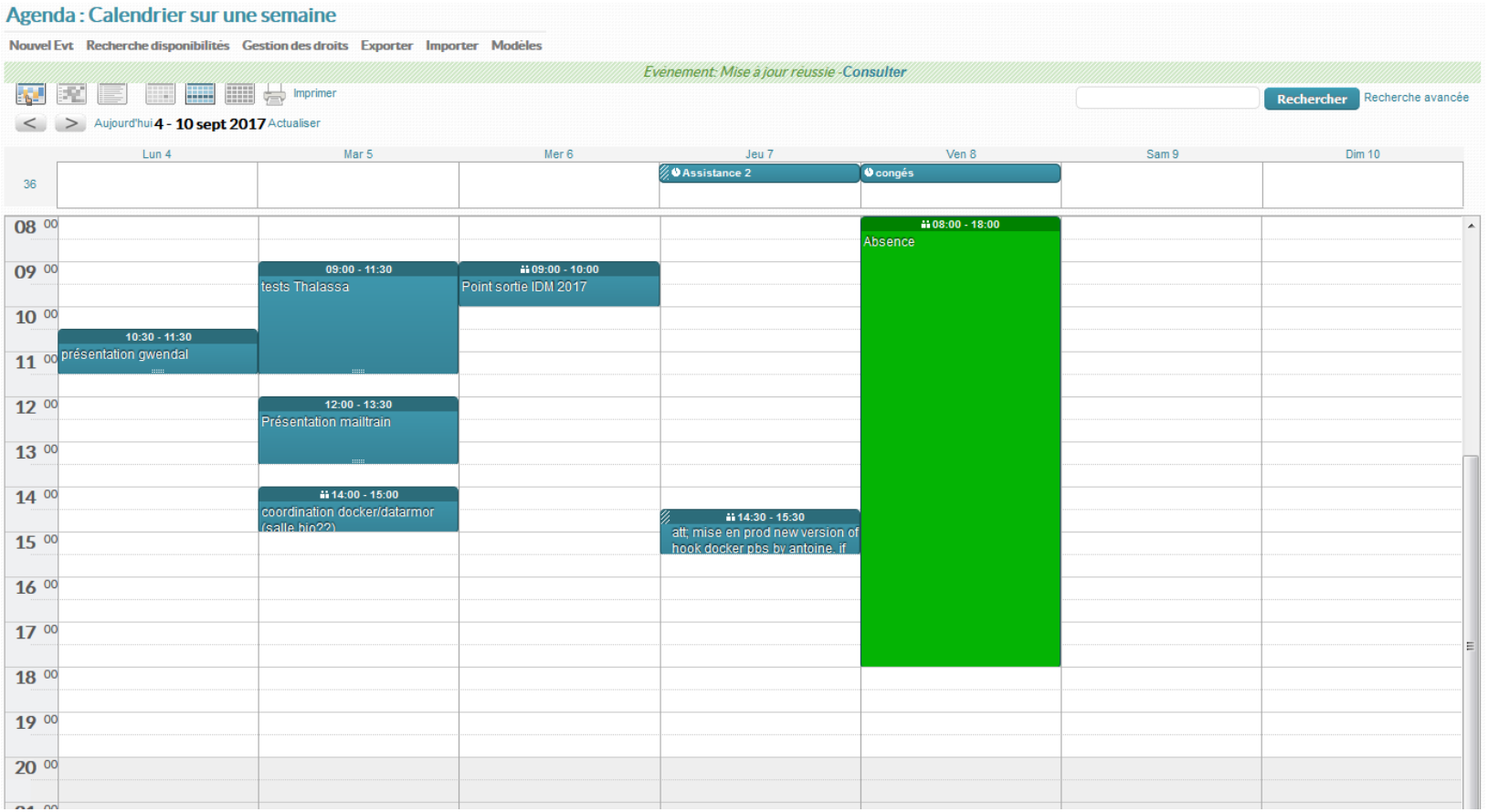
- Service sensible, à surveiller

Le travail collaboratif

- ALFRESCO : Gestionnaire libre de contenu en ligne
  - **Arborescence de répertoire avec droits d'accès de fine granularité**
- Mantis : Gestion de projet
  - **Dépôts de versionning**
- Owncloud : Solution libre pour le cloud Ifremer ~ dropbox
- Filesender : Partage de fichier, par Renater
- FTP : anonyme ou non, plusieurs serveurs

Le travail collaboratif

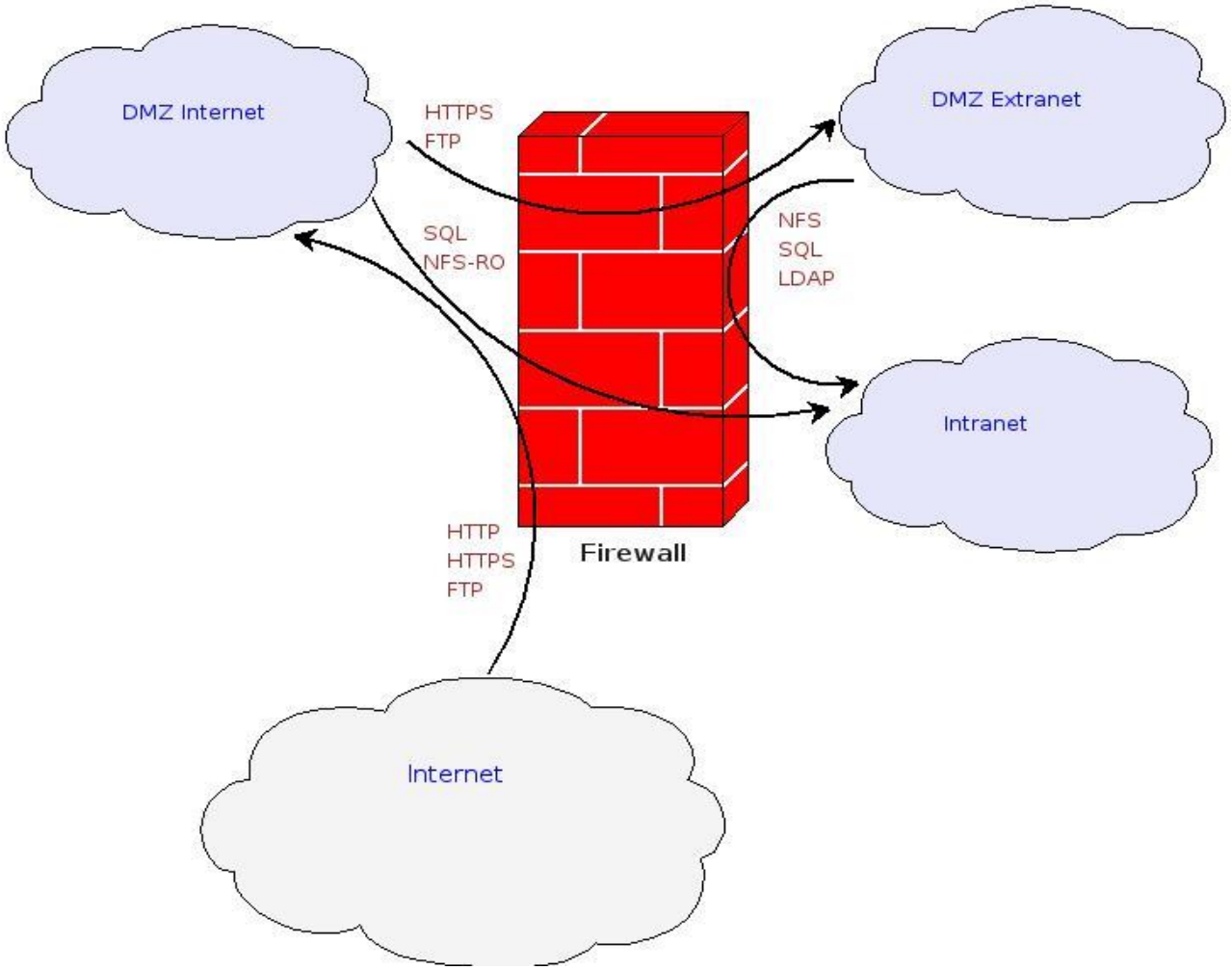
- L'agenda OBM – Open Business Management



Services Web

- Richesse du domaine ifremer.fr
- 3 zones d'hébergement : **Internet/Extranet/Intranet**
- Technologies :
  - **HTTPS (serveurs Apache sur Linux)**
  - **CMS EZPublish pour la production utilisateur**
  - **Applications métier développées : Tomcat, Jboss, PHP, PERL**
  - **Bases de données MySQL, Postgres, Oracle**
  - **LDAP, le plus souvent par SSO CAS**
  - **De plus en plus de technos différentes : attention !**

Services Web : structure



Services Web : J2EE

- Spécification Java pour applications d'entreprise
- Plusieurs applis J2EE hébergées sur serveur Tomcat (v6/v7)
  - **Dans les trois zones**
  - **Instances applicatives indépendantes**
  - **Suivi automatisé**
- Projets européens : besoin de stabilité

La donnée : serveurs SGBD

- 3 systèmes en place : Oracle, MySQL, PostgreSQL
- Objectif : Offrir des alternatives selon les besoins
  - **Chaque projet 'donnée' = étude du meilleur stockage, fonction de l'appli**
- Oracle très robuste et étendu, mais coûteux
  - **Mutualisation des licences par processeur**
- PostgreSQL : solution libre, alternative avantageuse

La donnée : serveurs SGBD

- Virtualisation = souplesse et dynamisme
  - **Maintenance, dimensionnement**
  - **Possible pour MySQL et Postgre, pas Oracle**

- Evolution de l'infra
  - **Nécessité : sécurité, support, nouveautés fonctionnelles**
  - **Gestion du portage : implication des devs**
  - **Oracle = raccourcir le temps, coût de licence**

La donnée : gestion des ressources

- Partage complexe des capacités machine (CPU, Mem, IO)

- La question de la PERFORMANCE
  - ***Parfois*** **le dimensionnement n'est pas adéquat**
  - ***Souvent*** **soucis de conception applicative – peu ou pas d'indexation, requêtes longues, mauvais design de la base, plan d'exécution…**

- Peu importe le matériel, les temps de réponse peuvent devenir ingérable
  - **Accompagner les projets et le développement**

La donnée : vers le « Big Data »

- Constat : les volumes de données ne cessent d'augmenter
- Le paradigme « BDD relationnelle » ne convient plus forcément
- Suivant les applis, passage au NoSQL
- Expérimentations en cours

La donnée : vers le « Big Data »

- Cluster ElasticSearch :
  - **Stockage de données distribué, très forte scalabilité**
  - **Multiplicité des formats et des usages**
  - **Haute disponibilité**
- Usages envisagés :
  - **Datamining de logs divers**
  - **Accès rapide à de grands volumes (données satellites)**
- Evolutions architecturales nécessaires

Virtualisation

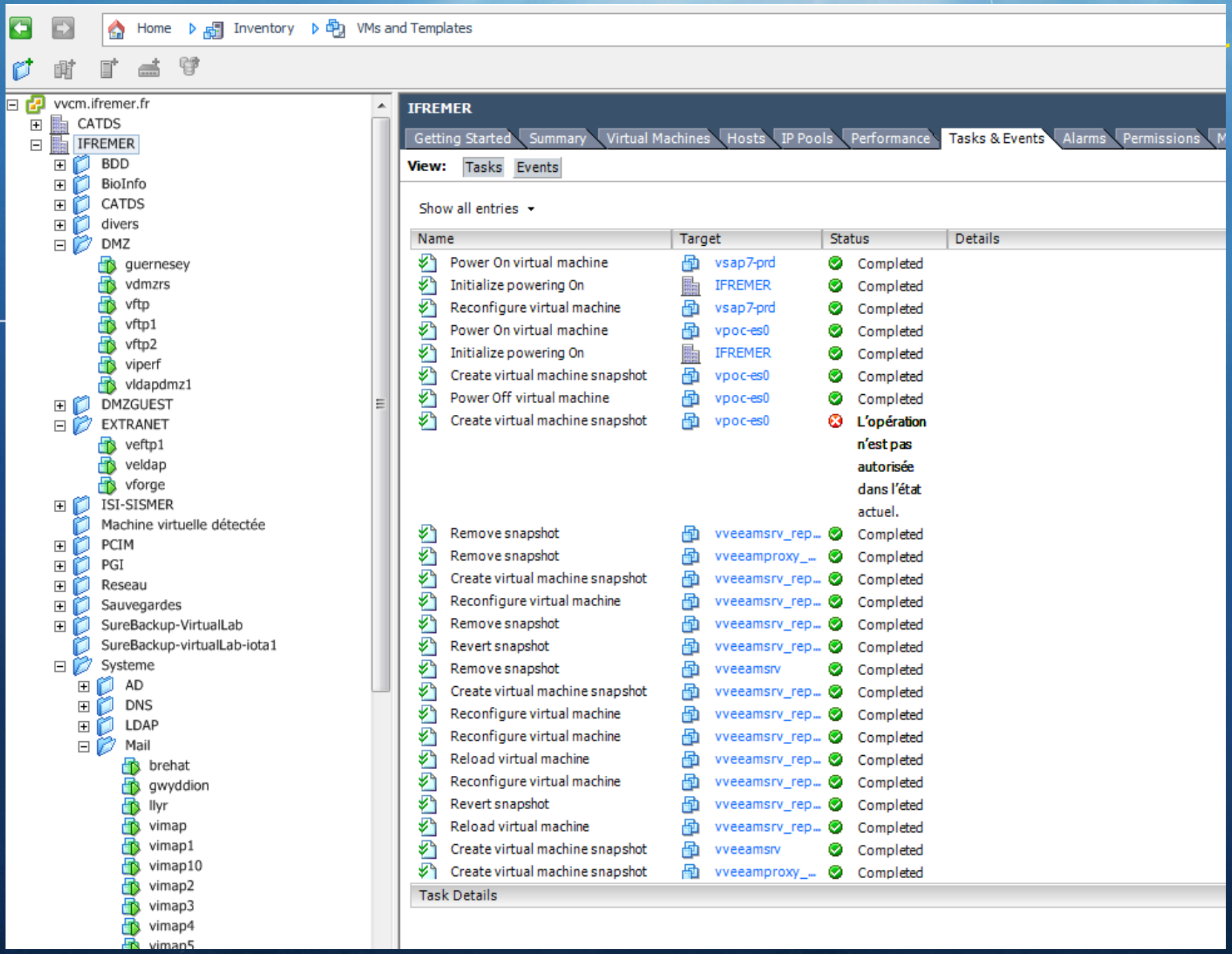
- Il y a dix ans : un serveur = une machine
  - **Coûteux, encombrant**
  - **Complexité d'administration et de renouvellement**

- Aujourd'hui : serveurs virtualisés : techno VMWare
  - **Une quinzaines de hosts physiques, les ESX**
  - **Gestion d'un pool de ressources CPU et mémoire**
  - **~360 machines virtuelles**
  - **Evolution progressive (homedir, Oracle)**

- A surveiller : I/O entre stockage et VMs

Virtualisation

- Mécanismes de backup & sauvegarde :
  - **VEEAM : sauvegarde du système de chaque VM, à chaud chaque nuit**
  - **Sauvegarde des espaces de stockage, différentes technos**
  - **Mécanismes de snapshot VMWare**
- On peut rétablir les données, les configurations systèmes, la RAM
- Objectif : PCS et PRA


Home
Inventory
VMs and Templates
vvcm.ifremer.fr
CATDS
IFREMER
BDD
BioInfo
CATDS
divers
DMZ
guernesey
vdmzrs
vftp
vftp1
vftp2
viperf
vldapdmz1
DMZGUEST
EXTRANET
veftp1
veldap
vforge
ISI-SISMER
Machine virtuelle détectée
PCIM
PGI
Reseau
Sauvegardes
SureBackup-VirtualLab
SureBackup-virtualLab-iota1
Systeme
AD
DNS
LDAP
Mail
brehat
gwyddion
llyr
vimap
vimap1
vimap10
vimap2
vimap3
vimap4
vimap5
IFREMER
Getting Started
Summary
Virtual Machines
Hosts
IP Pools
Performance
Tasks & Events
Alarms
Permissions
View:
Tasks
Events
Show all entries
Name
Target
Status
Details
Power On virtual machine
vsap7-prd
Completed
Initialize powering On
IFREMER
Completed
Reconfigure virtual machine
vsap7-prd
Completed
Power On virtual machine
vpoc-es0
Completed
Initialize powering On
IFREMER
Completed
Create virtual machine snapshot
vpoc-es0
Completed
Power Off virtual machine
vpoc-es0
Completed
Create virtual machine snapshot
vpoc-es0
L'opération n'est pas autorisée dans l'état actuel.
Remove snapshot
vveeamsrv_rep...
Completed
Remove snapshot
vveeamproxy_...
Completed
Create virtual machine snapshot
vveeamsrv_rep...
Completed
Reconfigure virtual machine
vveeamsrv_rep...
Completed
Remove snapshot
vveeamsrv_rep...
Completed
Revert snapshot
vveeamsrv_rep...
Completed
Remove snapshot
vveeamsrv
Completed
Create virtual machine snapshot
vveeamsrv_rep...
Completed
Reconfigure virtual machine
vveeamsrv_rep...
Completed
Reconfigure virtual machine
vveeamsrv_rep...
Completed
Reload virtual machine
vveeamsrv_rep...
Completed
Reconfigure virtual machine
vveeamsrv_rep...
Completed
Revert snapshot
vveeamsrv_rep...
Completed
Reload virtual machine
vveeamsrv_rep...
Completed
Create virtual machine snapshot
vveeamsrv
Completed
Create virtual machine snapshot
vveeamproxy_...
Completed
Task Details

Calcul scientifique

- Nombreuses activités requérant une forte puissance de calcul :
  - **Physique des océans, calcul de marées**
  - **Océanospatial**
  - **Bioinformatique**

- Grands besoins matériels et logiciels :
  - **Architecture dédiée**
  - **Compilateurs spécifiques, parallélisation, optimisation, compétence développement**

Calcul scientifique

- A Ifremer, plusieurs générations de calculateurs :
  - **1993 – 1998 : ATLANTIS**
  - **1998 – 2001 : ANTINEA**
  - **2001 – 2007 : NYMPHEA**
  - **2007 – 2016 : CAPARMOR**
  - ***2016 – ? : DATARMOR***

Calcul scientifique

- DATARMOR matériel :
  - **11K cœurs de calcul, 128Go de RAM / noeud**
  - **426 TFLOPS**
  - **6,5 Po de stockage**

- DATARMOR réseau :
  - **Infiniband – 20Go/s vers le stockage (pic à 30)**
  - **10Go/s en liaison avec réseau Ifremer**

Calcul scientifique

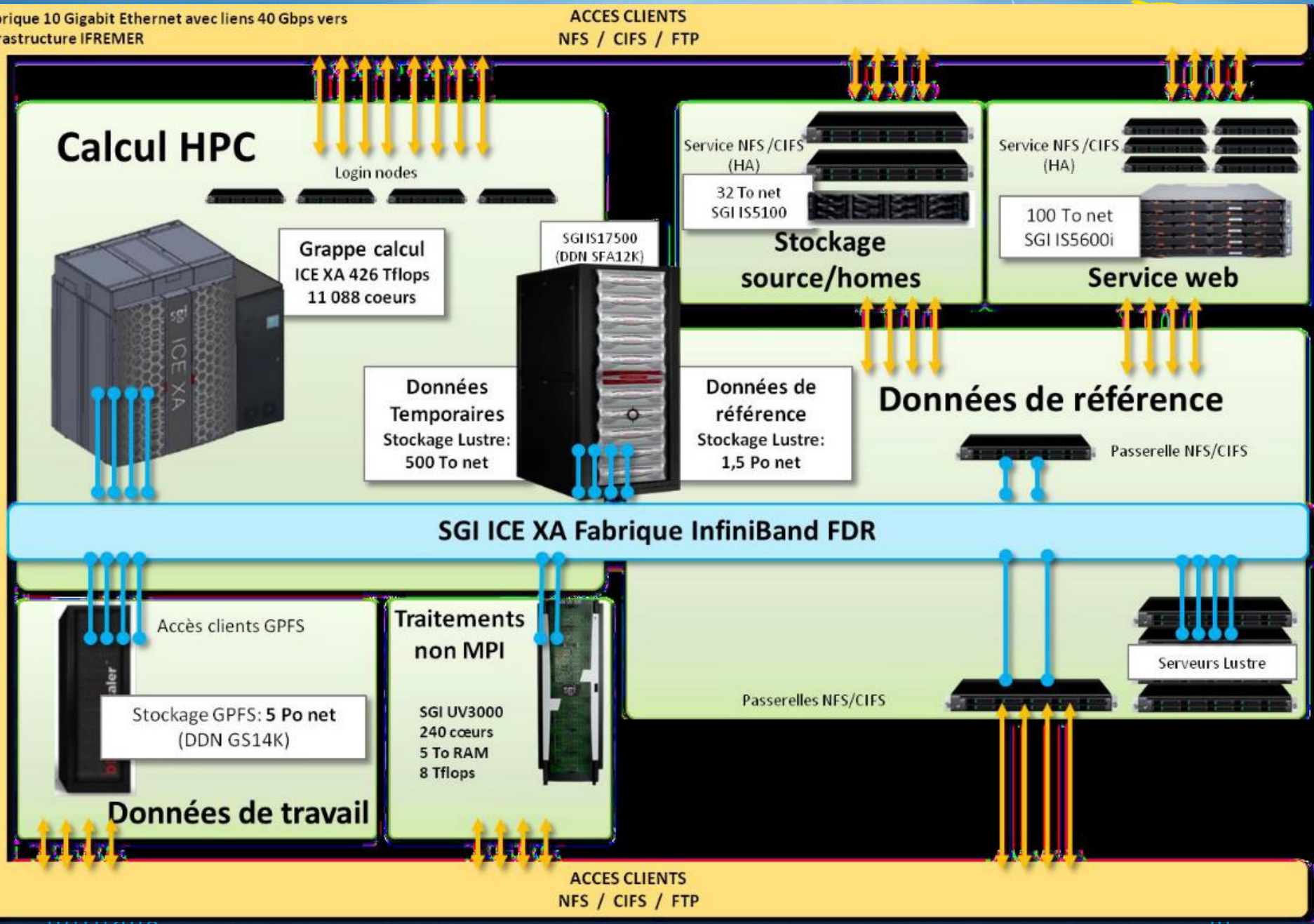
- DATARMOR fonctionnel :
  - **Cluster ICE XA, nœuds de calcul hyperthread**
  - **Cluster SMP, mémoire partagée**
  - **Ordonnanceur PBS**
  - **Environnements logiciels : Conda, Docker**

- DATARMOR stockage :
  - **Plusieurs filesystem : NFS, GPFS, Lustre**
  - **Définition d'espaces fonctionnels : travail, données de référence…**

Calcul scientifique

- Gestion de l'infrastructure :
  - **Partage équitable des ressources**
  - **Evolution des besoins, nouvelles technologies**

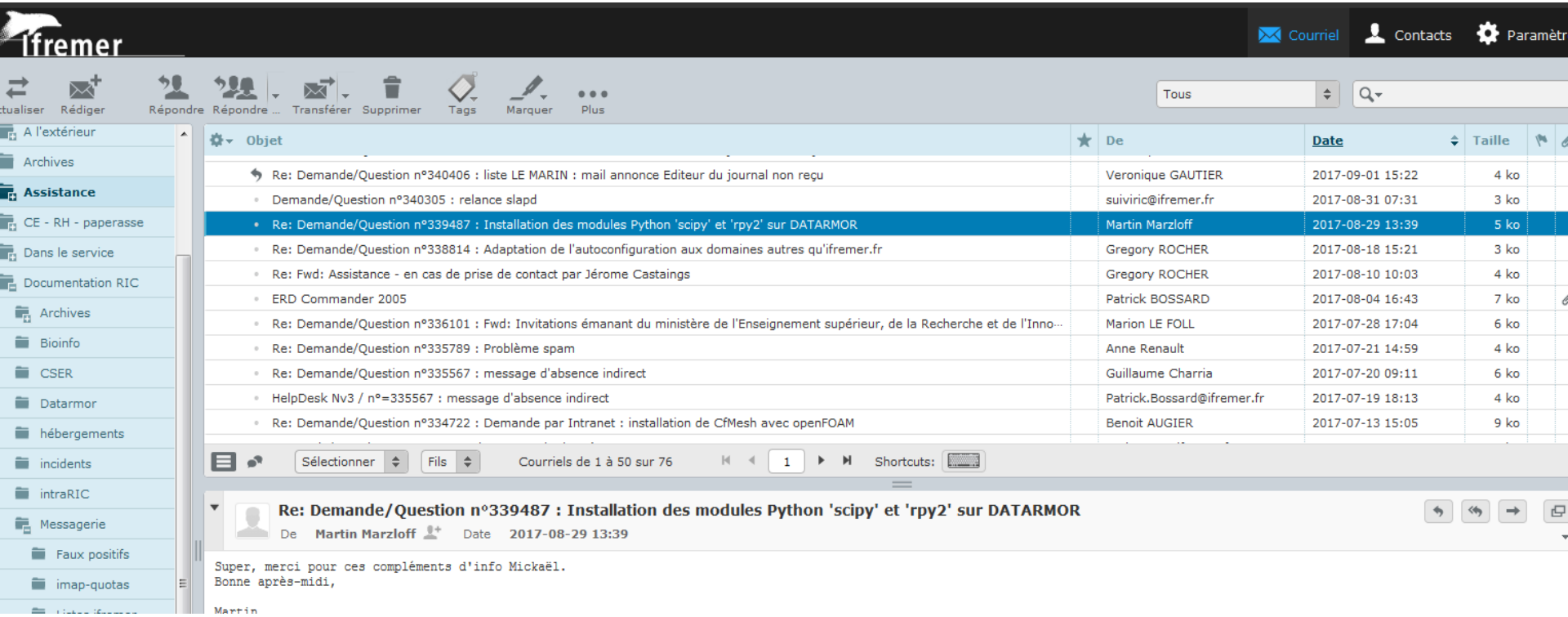
- Les problématiques :
  - **Big Data sur espace non-infini**
  - **Projets de plus en plus immenses : services de tuilages, applications synchrones**
  - **Ouverture vers l'internet ? Tout un débat.**


Fabrique 10 Gigabit Ethernet avec liens 40 Gbps vers Infrastructure IFREMER
ACCES CLIENTS
NFS / CIFS / FTP
Calcul HPC
Login nodes
Grappe calcul
ICE XA 426 Tflops
11 088 coeurs
SGI IS17500
(DDN SFA12K)
Service NFS /CIFS
(HA)
32 To net
SGI IS5100
Stockage
source/homes
Service NFS /CIFS
(HA)
100 To net
SGI IS5600i
Service web
Données
Temporaires
Stockage Lustre:
500 To net
Données de
référence
Stockage Lustre:
1,5 Po net
Données de référence
Passerelle NFS/CIFS
SGI ICE XA Fabrique InfiniBand FDR
Accès clients GPFS
Stockage GPFS: 5 Po net
(DDN GS14K)
Données de travail
Traitements
non MPI
SGI UV3000
240 cœurs
5 To RAM
8 Tflops
Passerelles NFS/CIFS
Serveurs Lustre
ACCES CLIENTS
NFS / CIFS / FTP

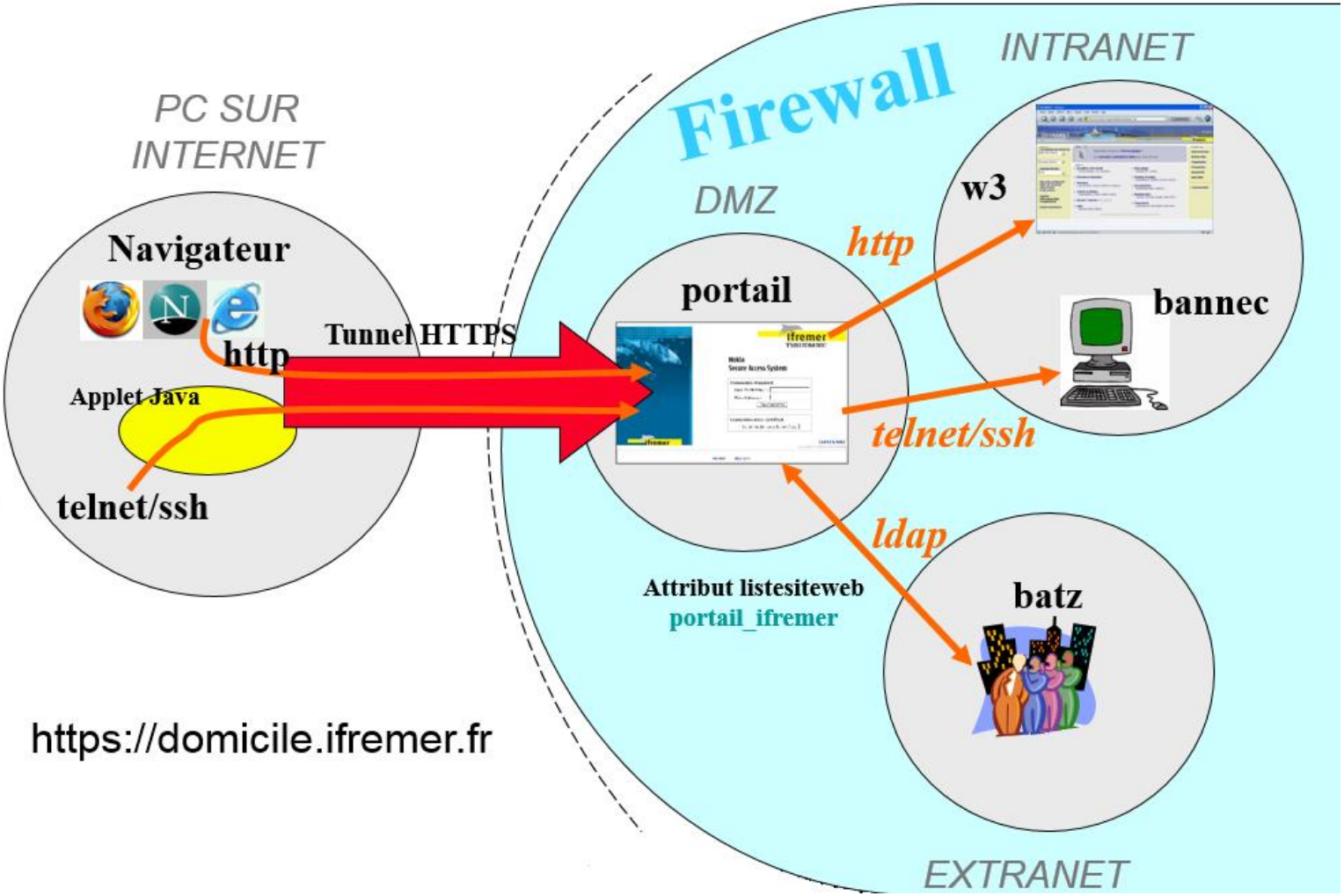
MOBILITÉ

Messagerie en extérieur

- Webmail Roundcube, grâce à la centralisation IMAP



Portail d'accès Juniper



Messagerie en mer

- Lien réseau amélioré au fil des ans, mais coupures toujours présentes
  - **INMARSAT-B à 64kbit/s ou VSAT 128kbit/s**

- Pour la messagerie, files d'attente spécifiques à terre
- Gestion des embarquements
  - **Adresses de bord temporaires et vacations**

- Cas général : cycles de communication terre-mer de 5mn
- En cas de perte du réseau :
  - **données conservées, procédure de récupération auto**

Le WiFi Ifremer

ssid **Portail Captif**
accès Internet uniquement

Identification au choix
(réseaux sociaux, google…)

ssid **INTRAIFR**
accès Intranet, montage des disques

EAP/TTLS
LDAP

Diffusion limitée aux salles de réunion, mais élargissement progressif du périmètre

Téléphonie mobile

- Smartphones fournis par RIC
  - **Pour la hiérarchie**
  - **Pour les agents aux tâches spécifiques**
- Pool commun voix et data
- Solution Business Everywhere
  - **Accès intranet depuis smartphone**
- Sécurité : Pradeo
  - **Gestion à distance**

ORGANISATION ET SÉCURITÉ

Trois visions à avoir

- Court, moyen et long terme
- Court terme : l'opérationnel
  - **Assistance, services existants. Prioritaire et volumineux**
- Moyen terme : extension de l'opérationnel
  - **Qualité et quantité, automatisation**
- Long terme : évolutions et pérennisation
  - **Anticiper les besoins, suivre les changements techniques**

Trois visions à avoir

- Toujours conserver un **équilibre** entre les trois
- Sans opérationnel, pas de service, **pas de crédibilité**, **pas de budget**
- Sans ajustements, pas d'amélioration, pas de satisfaction, **pas de crédibilité**, **pas de budget**
- Sans nouveautés techniques, péremption des services, pas d'écoute utilisateur, **pas de crédibilité**, **pas de budget**

Démarche Qualité

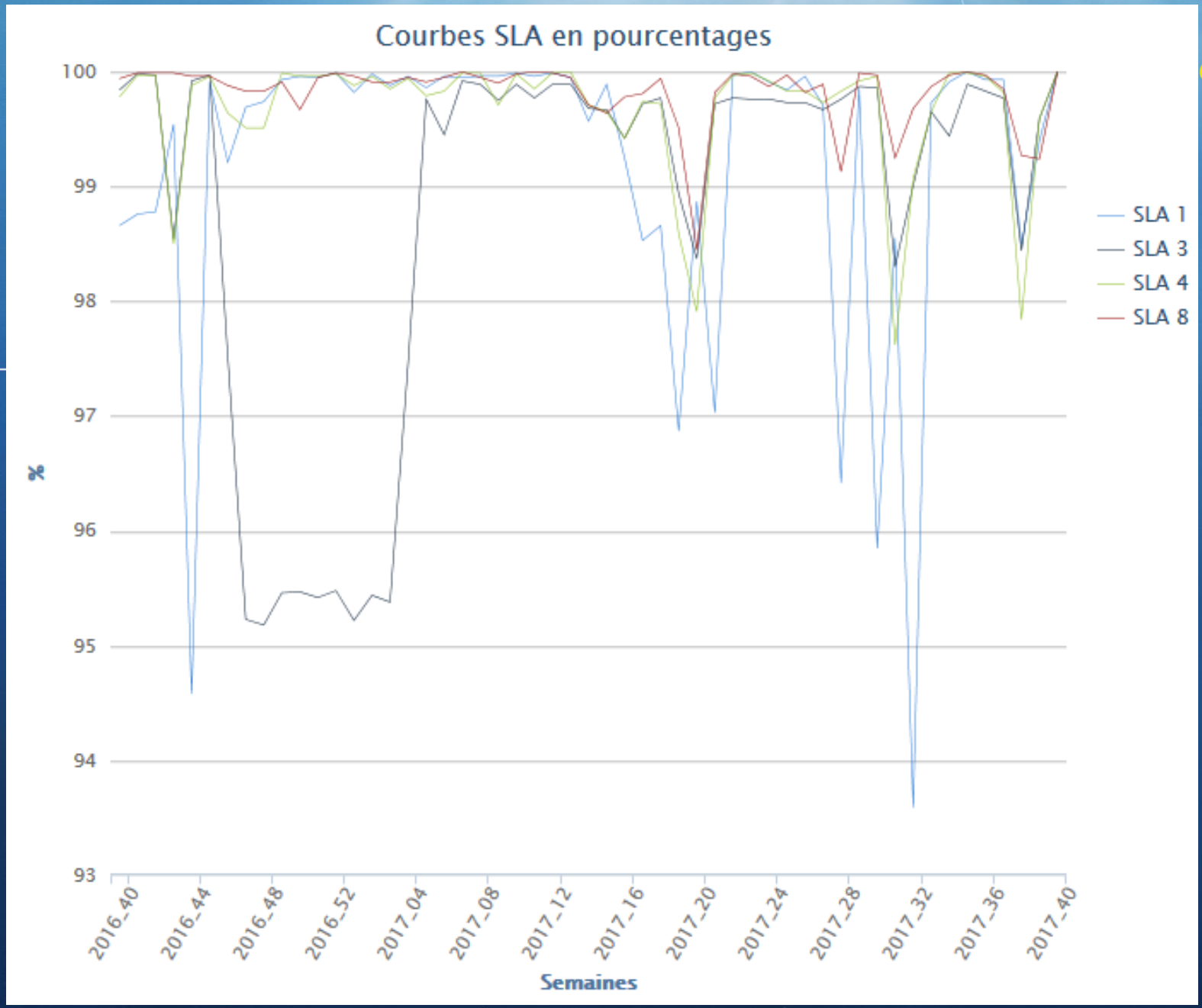
- Utilisation (souple) du référentiel ITIL
  - **Information Technology Infrastructure Library**
  - **Modélisation des techniques de gestion de l'infrastructure IT**
  - **Unité : le processus**

- Définition des services rendus et des relations
  - **Avec les décideurs, les utilisateurs, les fournisseurs**

- Contrats de service (SLA) entre RIC et le reste du monde
  - **Niveaux d'engagement**
  - **Dépendances, ressources mises en œuvre**

Démarche Qualité

- Les engagements de service :
  - **SLA « services communs » : tous les services en ligne par intranet**
  - **SLA « Postes de travail Windows » : Configuration et gestion du parc**
  - **SLA « Autres postes de travail » : la même chose pour Linux et MacOS**
  - **SLA « Hébergement d'applications » : Mise à disposition hard/software pour des SI tiers hébergés à Ifremer**


Courbes SLA en pourcentages
100
99
98
97
96
95
94
93
%
SLA 1
SLA 3
SLA 4
SLA 8
2016_40
2016_44
2016_48
2016_52
2017_04
2017_08
2017_12
2017_16
2017_20
2017_24
2017_28
2017_32
2017_36
2017_40
Semaines

Démarche Qualité

- En accord avec la norme ISO-9001
- Des outils de suivi indispensables :
  - **Relations utilisateurs : Helpdesk**
  - **Relations fournisseurs : Sigma SAP**
- Monitoring constant des activités, statistiques temps réel :
  - **ICINGA**
  - **Grafana**

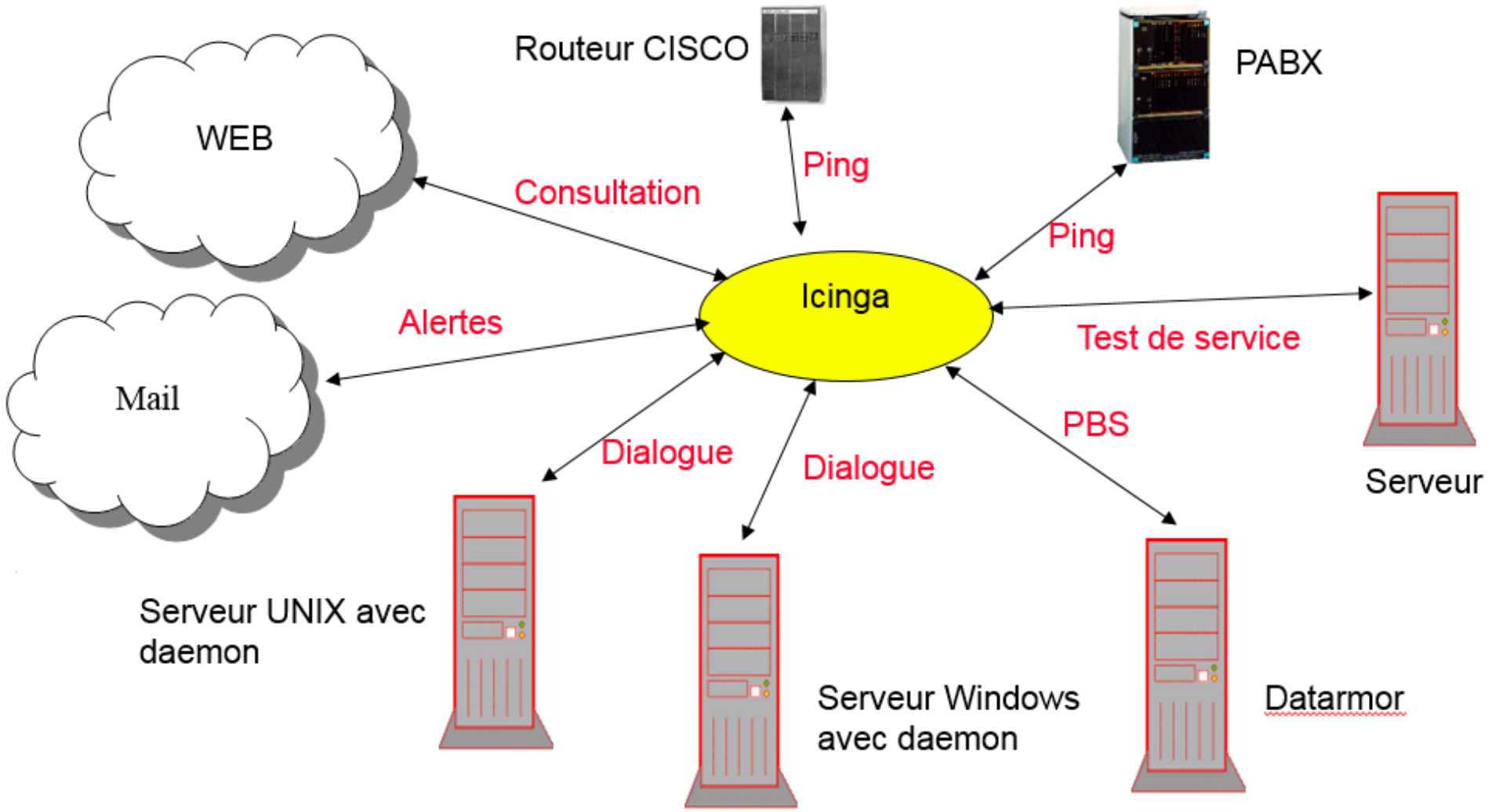
Surveillance et administration

- Monitoring et alertes automatiques par Icinga
- Statistiques temps réel, outil Grafana

- Routeurs et commutateurs Cisco : contrôle charge et traffic
- Suivi de l'occupation des liens téléphoniques

- Administration web des salles de visioconférence

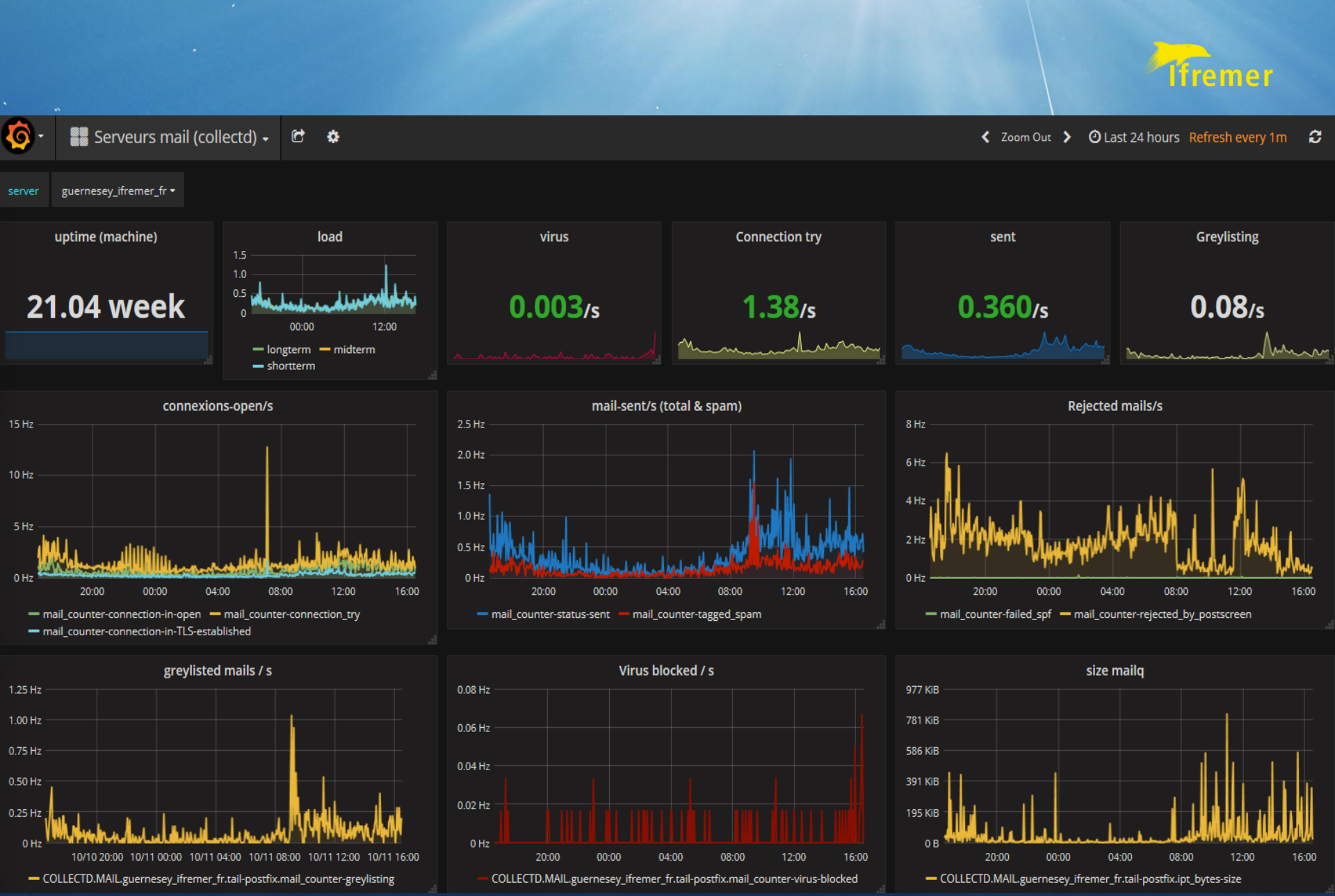
- Logiciel de supervision (machines, services, réseaux)
  - **OpenSource**
  - **Héritier de Nagios**
- Daemons déportés sur les équipements, vérifiant le bon fonctionnement des choses à intervalles réguliers
- Problème détecté : alerte mail, SMS, Web
- Interface web dédiée, statistiques sur la durée


Routeur CISCO
PABX
WEB
Ping
Consultation
Ping
Icinga
Alertes
Test de service
Mail
Serveur
PBS
Dialogue
Dialogue
Serveur UNIX avec daemon
Serveur Windows avec daemon
Datarmor

- 559 Hosts, 2847 services testés toutes les 5 à 10mn

- Exemples de test :
  - **HTTP, HTTPS pour les serveurs web**
  - **SMTP, MAILQ pour les serveurs mail**
  - **LDAP**
  - **FTP, DNS, SAMBA…**

- Interface web de statistiques
- Présente dans le temps les métriques remontées par des agents locaux, comme Graphite
- Gestion des données par tranches temporelles
- Exemple : agent graphite sur serveur mail
  - **Lecture des logs en temps réel**
  - **Formatage et remontée des chiffres significatifs**


Ifremer
Serveurs mail (collectd)
Zoom Out
Last 24 hours
Refresh every 1m
server
guernesey_ifremer_fr
uptime (machine)
21.04 week
load
1.5
1.0
0.5
0
00:00
12:00
longterm
midterm
shortterm
virus
0.003/s
Connection try
1.38/s
sent
0.360/s
Greylisting
0.08/s
connexions-open/s
15 Hz
10 Hz
5 Hz
0 Hz
20:00
00:00
04:00
08:00
12:00
16:00
mail_counter-connection-in-open
mail_counter-connection_try
mail_counter-connection-in-TLS-established
mail-sent/s (total & spam)
2.5 Hz
2.0 Hz
1.5 Hz
1.0 Hz
0.5 Hz
0 Hz
mail_counter-status-sent
mail_counter-tagged_spam
Rejected mails/s
8 Hz
6 Hz
4 Hz
2 Hz
0 Hz
mail_counter-failed_spf
mail_counter-rejected_by_postscreen
greylisted mails / s
1.25 Hz
1.00 Hz
0.75 Hz
0.50 Hz
0.25 Hz
0 Hz
10/10 20:00
10/11 00:00
10/11 04:00
10/11 08:00
10/11 12:00
10/11 16:00
COLLECTD.MAIL.guernesey_ifremer_fr.tail-postfix.mail_counter-greylisting
Virus blocked / s
0.08 Hz
0.06 Hz
0.04 Hz
0.02 Hz
0 Hz
COLLECTD.MAIL.guernesey_ifremer_fr.tail-postfix.mail_counter-virus-blocked
size mailq
977 KiB
781 KiB
586 KiB
391 KiB
195 KiB
0 B
COLLECTD.MAIL.guernesey_ifremer_fr.tail-postfix.ipt_bytes-size

La sécurité : vue d'ensemble

- Anti-intrusion : firewall, OS à jour
- Contre les virus : Kaspersky à jour sur les PC
- Protection mail : spam, phishing

- Sauvegarde et archivage des données
- Droits d'accès des comptes

- Sensibilisation des utilisateurs

La sécurité anti-intrusion

- Firewall sur les 4 zones – Internet, DMZ, Extranet, Intranet
- Un frontal unique pour le web
- Filtrage selon (IP appelée, IP appelante, port)
- « Tout ce qui n'est pas explicitement autorisé est considéré interdit »
- Souplesse imposée par les partenariats et les usages

Contre les virus

- Tout est géré centralement.

- Trois outils principaux :
  - **Antivirus sous forme de client lourd sur tous les PC – Kaspersky. Géré à partir d'un serveur contrôlant les MaJ et les routines**
  - **Antivirus filtrant les mails entrants – ClamAV. Procédures de quarantaine, types de pièces jointes…**
  - **Antivirus de nettoyage – Sophos. Balaie les disques réseaux à intervalles réguliers**

Sécurité et messagerie

- Traitement entrant :
  - **Rejet si RFC non-respectés**
  - **Greylisting**
  - **Filtre SPF**
  - **Filtre Antispam**
  - **Gestion des exceptions au cas par cas**

- Traitement sortant :
  - **Signature DKIM**
  - **Règles SPF publiées**
  - **Vérification du domaine**

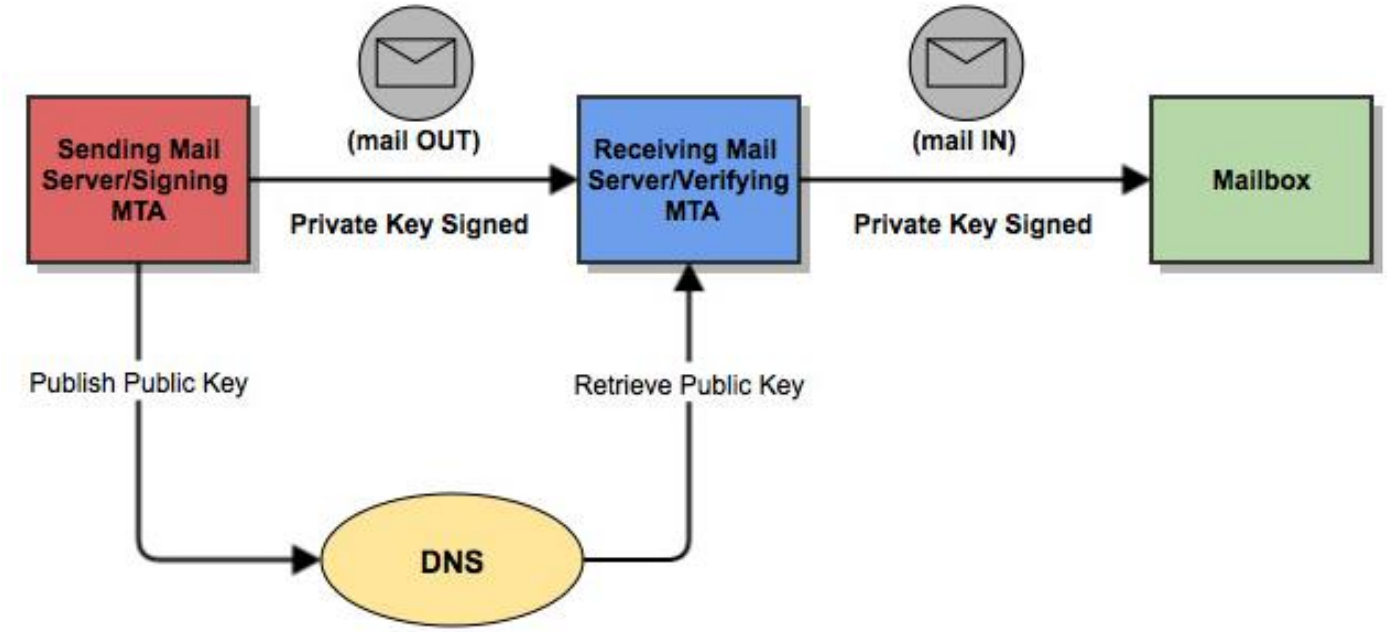
Sécurité et messagerie

- Le greylisting :
  - **Conservation {IP source, FROM, TO}. Si inconnu, rejet temporaire**
  - **Un constat : les spammeurs se fichent des réponses**
  - **Si réexpédition, OK**

- SPF : Sender Policy Framework
  - **Dans le DNS, liste des IPs autorisées à envoyer du mail**
  - **Rejet si SPF Fail**
  - **"v=spf1 a:brest.ifremer.fr a:gwyddion.ifremer.fr -all«**

Sécurité et messagerie

- DKIM : DomainKey Identified Mail
  - **Signature chiffrée, corps et plusieurs en-têtes du mail**
  - **Le mail provient du bon endroit, n'a pas été modifié**



Sécurité et messagerie

- Antispam : j-chkmail, Mines de Paris
  - **Implémentation greylisting, recherche textuelle, heuristiques, URLBL…**
  - **Technique participative : le filtre bayésien**

- Principe : IA statistique, apprentissage supervisé
  - **Les utilisateurs envoient les messages mal classés**
  - **Ceux-ci nourrissent le filtre, qui produit des tokens à matcher**
  - **Décision : comparaison score – seuil**
  - **Effet : tag SPAM**

- Que faire avec ?

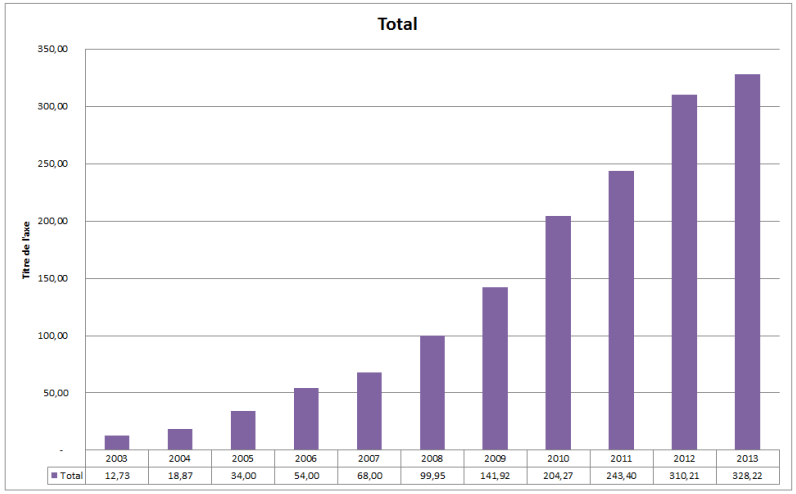
La sauvegarde

- La donnée doit être sécurisée (26 sites)

- **Erreurs humaines**
- **Pannes matérielles**

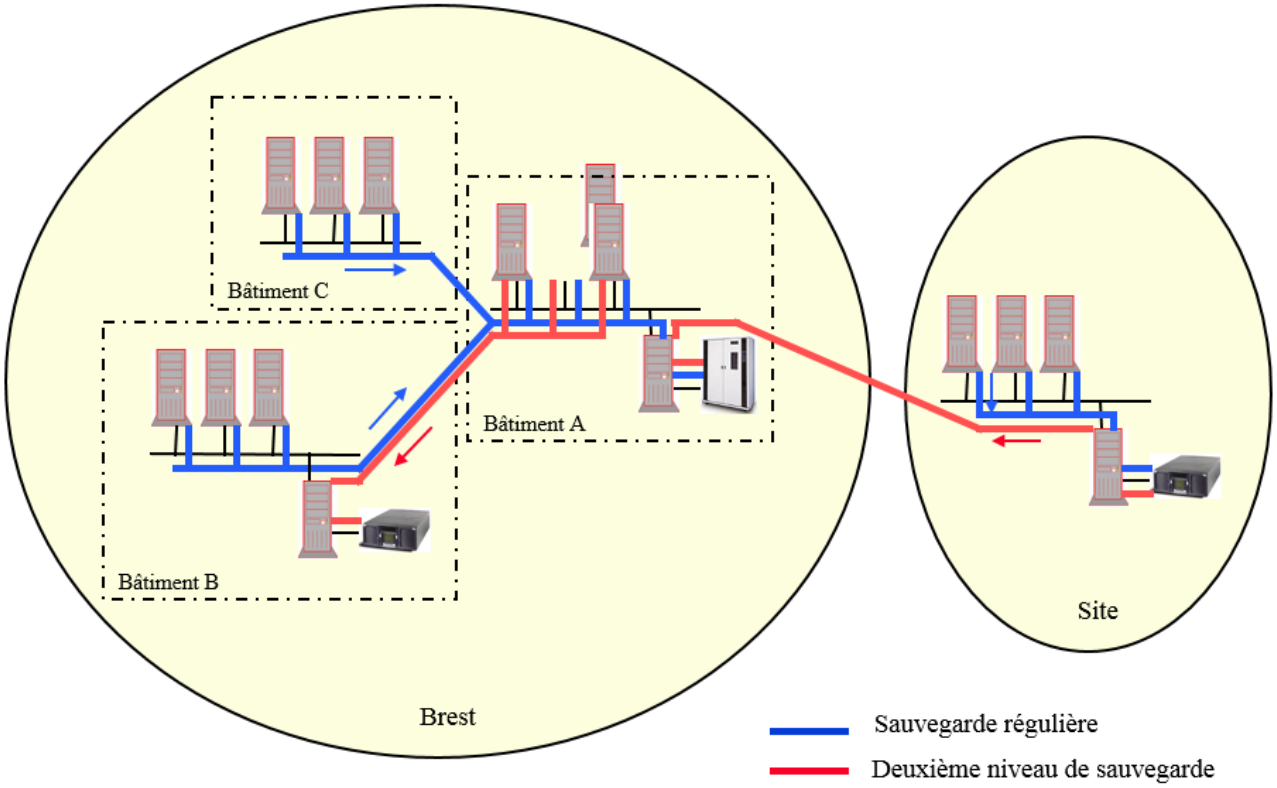
→ **Sauvegardes régulières**

- **Accident majeur** → **Délocalisation donnée/sauvegarde**



La sauvegarde

- Réplication intra et intersite



La sauvegarde

- Plusieurs outils :
  - **TimeNavigator – à la demande sur de nombreux serveurs**
  - **VeeamBackup – sur les VMs**
  - **Snapshots – sur certains stockages**

- Administration centralisée sur Brest, réseau SAN dédié
- Engagements :
  - **Sauvegarde quotidienne, jusqu'à horaire**
  - **Deux mois de rétention minimum**
  - **Interface utilisateur de restitution**

- Important : ne rien stocker en local !

L’archivage

- Données pérennes immobiles
  - **Copie – et recopie - de la donnée par des robots**
  - **Accessibilité continue**

- Solution en place :
  - **Espace tampon SamFS**
  - **Object Archive**
  - **2 librairies Overland (800To) avec lecteurs LT06**
  - **Aujourd’hui : 530 To**

- Tout le monde peut archiver

La communication

- Population d'usagers très divers
  - **Compétences et connaissances IT variables**
  - **Nécessité de communiquer par différents canaux**

- La charte informatique
  - **Validée par le CE**
  - **Cadrage du bon usage, des réflexes à acquérir, des possibilités offertes**
  - **Idéal : que tout le monde lise et retienne**

- Le mail d'accueil
  - **Détaille la charte et ouvre sur l'échange avec RIC**
  - **Tous les nouveaux arrivants**

La communication

- La RICNews :
  - **Newsletter bimensuelle, éditée par le service**
  - **Depuis 2015, en inscription libre**
  - **Diffusion nouveautés techniques et services proposés**
  - **Ouverture vers la culture générale**
  - **Avec concision et humour !**

La communication

- Les CSER – un réseau de correspondants
  - **Constat : infra décentralisée, gestion complexe**
  - **Sur tous les sites distants, volontaires pour relayer l'information**
  - **Interface RIC/utilisateur → utilisateurs eux-mêmes !**
  - **Réunions régulières d'échange entre eux et nous.**
- Maillon essentiel pour le fonctionnement de l'infra

CLÉS ET RÉFLEXIONS

Que faut-il retenir ?

La cohérence technique et l'évolutivité de l'architecture

- Suivre les besoins tout en mutualisant
  - **Différentes versions apache, oracle, php, python → DANGER**
- Attention aux montées de version :
  - **Identifier les responsables applicatifs (pas d'applis orphelines)**
  - **Imposer et maîtriser le processus**
- Montée de version d'un module = projet en soi
  - **Impliquer toutes les parties prenantes**

Que faut-il retenir ?

Définition formelle du périmètre supporté

- Matériel admissible sur le réseau, type d'OS, applications
  - **Gain : Sécurité et efficacité**
  - **Coût : standardisation**
- Surveillance : Bornes Wifi pirates, stockage « clandestin », PC personnel
- Maîtriser le périmètre = optimiser les processus

Que faut-il retenir ?

Optimisation des coûts et des ressources

- Anticiper les besoins futurs, les répercuter
  - **En termes d'investissements**
  - **En termes de ressources humaines**
- Ecoute utilisateur sur la durée
  - **Retours de l'assistance**
  - **Amender l'organisation technique « en souplesse »**
- Conserver les acquis de la mutualisation

Que faut-il retenir ?

Accessibilité et uniformité des services

- Disponibilité pour tout le monde, tout le temps
- Documenter, communiquer vers tous
- Eviter le déploiement en local
  - **Lourd en volume, lourd en support**
  - **Créations de spécificités**
- Pour des services mutualisés, cas particulier = danger

Que faut-il retenir ?

Accessibilité et uniformité des services

- Effort de communication : aucun service n'est pérenne
  - **Sensibiliser à la stabilité temporelle *RELATIVE* des outils**
  - **Difficile à admettre pour une certaine population**
  - **Accompagner le changement**

- A garder en tête : le but des outils
  - **Faciliter les activités métiers de l'entreprise (organisation, communication, production…)**
  - **PAS de nous faire plaisir**

Que faut-il retenir ?

Accessibilité et uniformité des services

- A garder en tête : différences de paradigme
  - **RIC gère l'existant, son évolution et sa relative pérennité**
  - **Les développeurs gèrent la nouveauté, l'innovation**

- Concilier les deux paradigmes pour une architecture harmonieuse

Que faut-il retenir ?

Décloisonner les compétences

- Dans le service, de nombreux métiers différents
  - **Activité riche, métier très évolutif**
  - **Nécessité d'ouverture et de vigilance**
  - **Tendance naturelle : expertise et spécialisation**

- Attention, SPOF : Single Point Of Failure
  - **Redonder les compétences dans l'équipe**
  - **Communication dans le service**

Que faut-il retenir ?

Travailler la qualité

- Améliorer la perception du service rendu
  - **Du point de vue des agents**
  - **Du point de vue de l'administration**
- Penser l'architecture et sensibiliser la direction
  - **Au Plan de Continuité de Service**
  - **Au Plan de Reprise d'Activité**
- Entretenir la confiance des fournisseurs

Administrer des services informatiques

Au-delà de la maîtrise technique :

- Organiser et communiquer
- Concevoir, repenser, remettre en question
- Maîtriser les changements
- Optimiser les coûts
- Décloisonner, se concerter

Et tout ira bien ! (on l'espère)