Des JI08 aux JI10

Bilan du groupe de travail Active Directory

Cédric MULLER – Journées Informatiques IN2P3/IRFU – Aussois Mai 2010

Agenda

- Situation actuelle de la forêt IN2P3
- Deux nouveaux domaines: Edd et Lnca
- Monitoring
  - Résumé des épisodes précédents
  - Monitoring / ACS
- Divers
  - Catia/Smarteam
  - Modification de l'architecture
  - Déploiement Windows 2008 dans les laboratoires

Active Directory IN2P3

- Projet commencé en 2001:
  - mutualiser les efforts pour la gestion de parc de machines Windows (postes de travail)
  - fédérer l'ensemble des postes dans une architecture unique et sécurisée

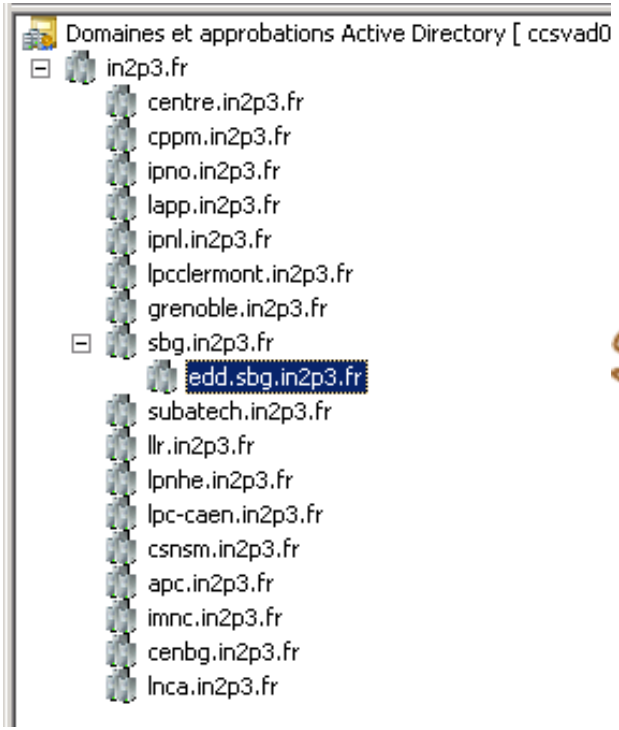
- Forêt Active Directory IN2P3 nationale.
  Annuaire LDAP, Kerberos
  19 laboratoires participants

Active Directory IN2P3

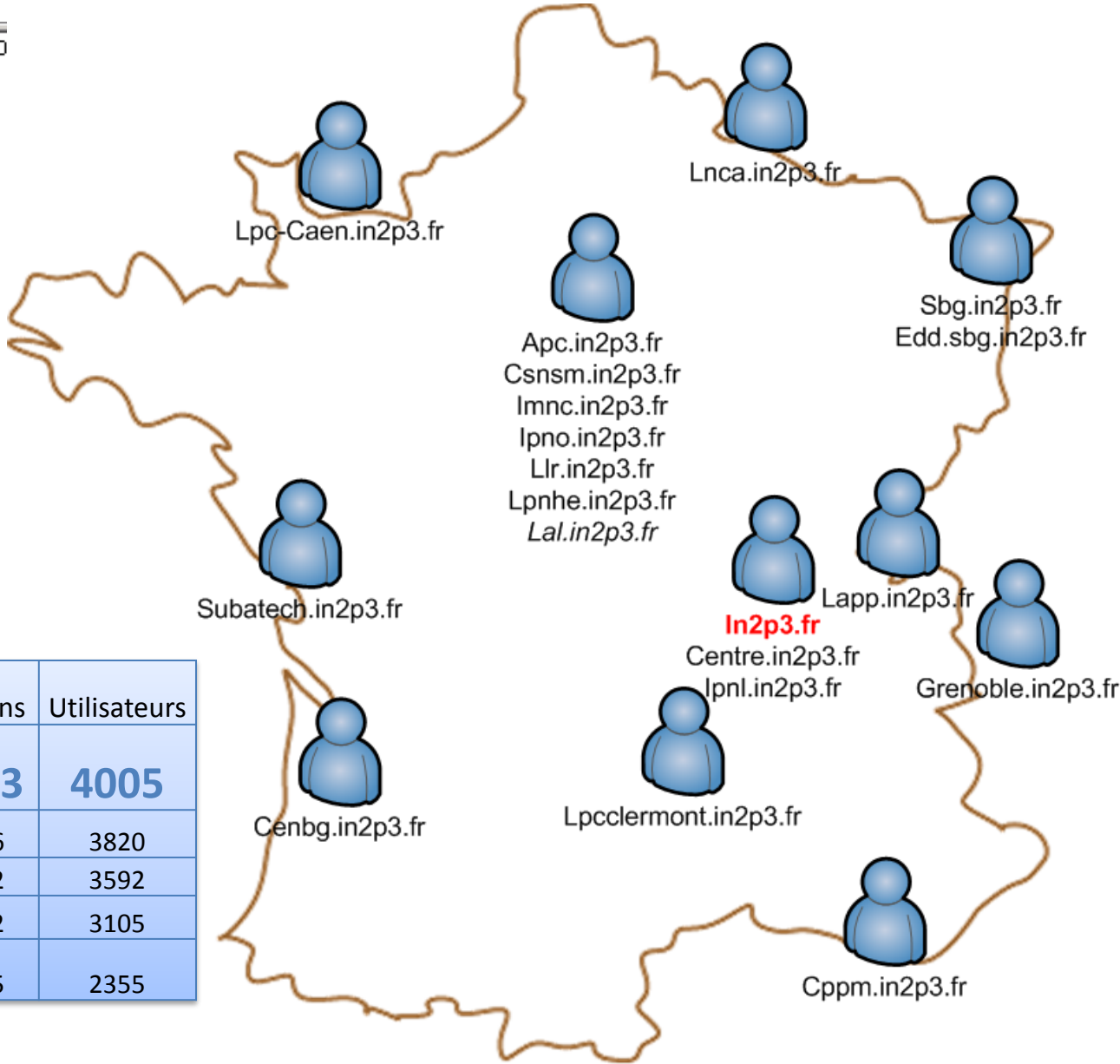
Bénéfices de l'architecture:

- Architecture répartie, tous liés mais chacun reste maître dans son laboratoire
- Périmètre de sécurité (Kerberos)
- Un compte unique par utilisateur,
- Authentification unique (Unix, Wifi, Vpn…)
- Facilité d'accès aux ressources (partages réseau (\\in2p3.fr\dfs\Partage) , application Catia/Smarteam pour les BE de mécaniciens)
- Compétences partagées entre les administrateurs : wiki, mailing-list, réunions…
- Besoins des laboratoires (Autorité de certification, Exchange,..)
- ….

Active Directory IN2P3

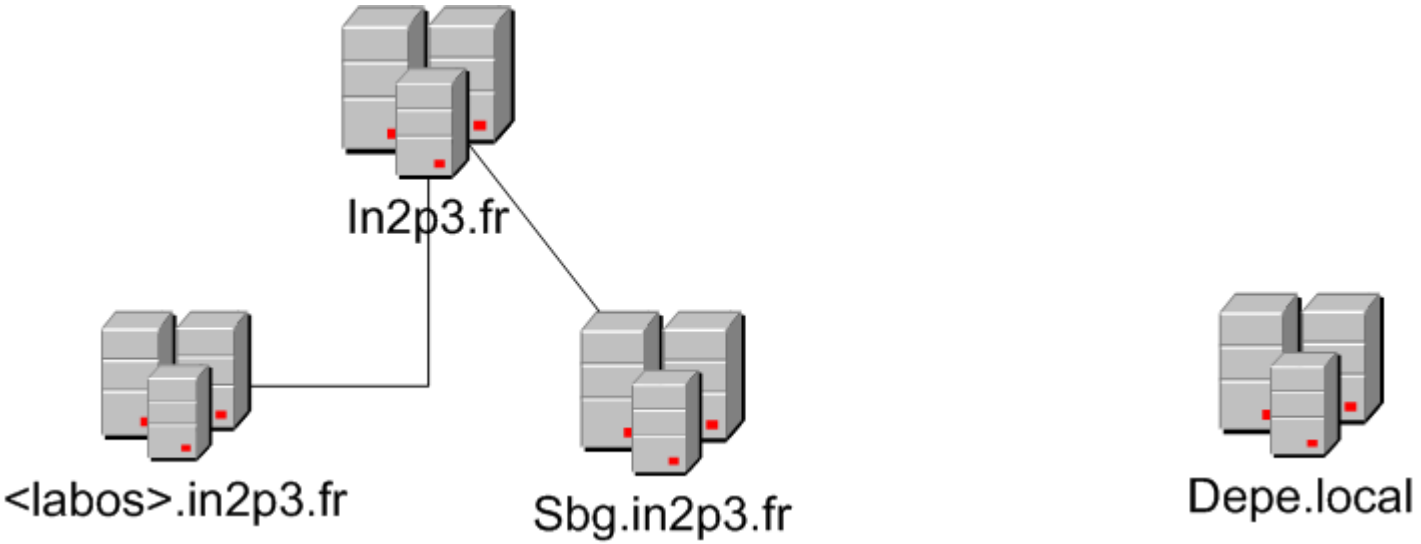


	Laboratoires	Serveurs	Stations	Utilisateurs
2010	**19**	**278**	**3373**	**4005**
2009	18	221	3076	3820
2008	17	196	2762	3592
2007	15	157	2332	3105
2006	14	135	2035	2355



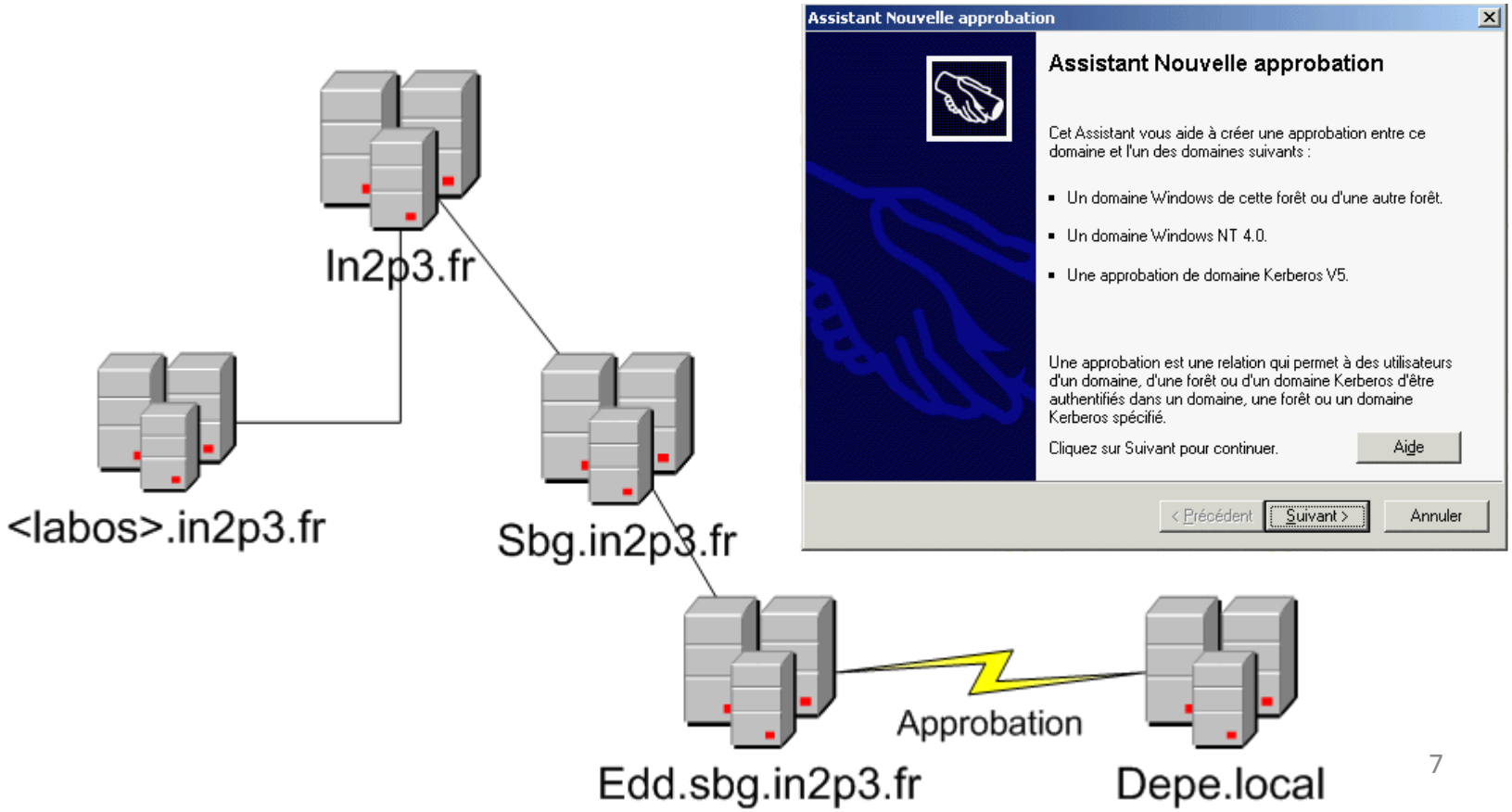
Edd.sbg.in2p3.fr

- 2006 à Strasbourg, l'IReS est devenu l'IPHC avec le rassemblement de 3 laboratoires.
- Le Depe, demandeur de rejoindre la structure IN2P3. (début 2009)



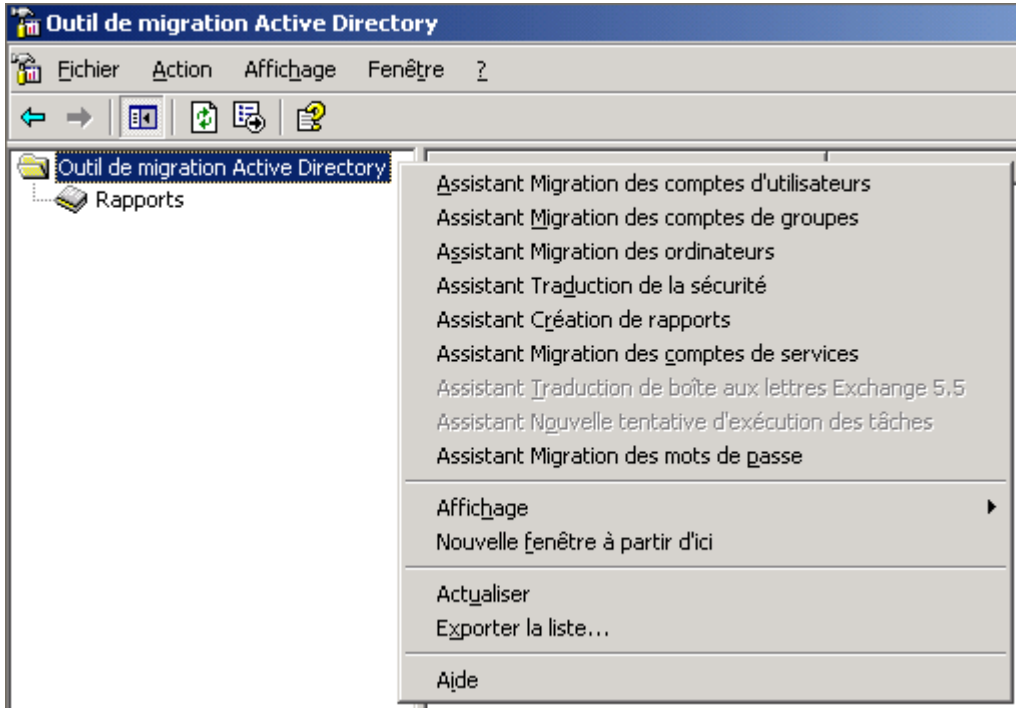
Edd.sbg.in2p3.fr

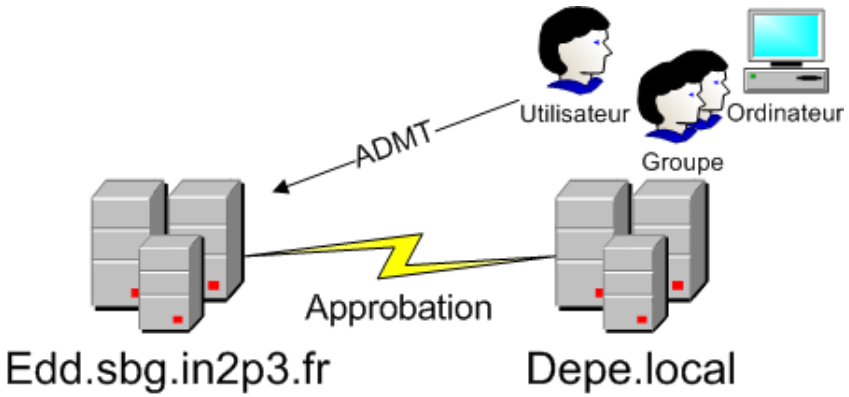
- Création d'un domaine **edd** enfant à **sbg**. Relation approbation entre edd et depe.



Edd.sbg.in2p3.fr

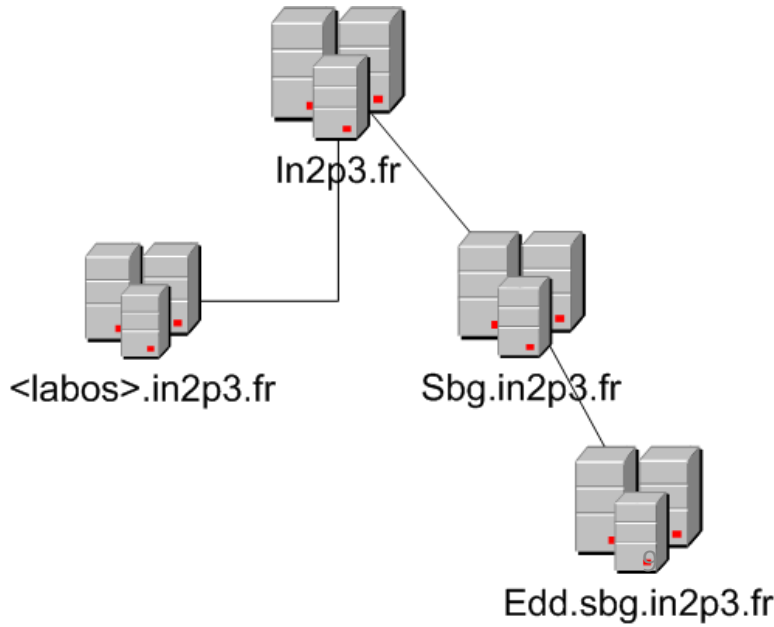
- Outil ADMT : Active Directory Migration Tools Migration des comptes utilisateurs, machines, mot de passes,…





Edd.sbg.in2p3.fr

- Passer chaque poste dans le nouveau domaine, les utilisateurs se connectent sous le nouveau domaine, récupérer les profils , …
- Pour terminer supprimer l'approbation, arrêter les contrôleurs de l'ancien domaine.
- Opération au fil du temps



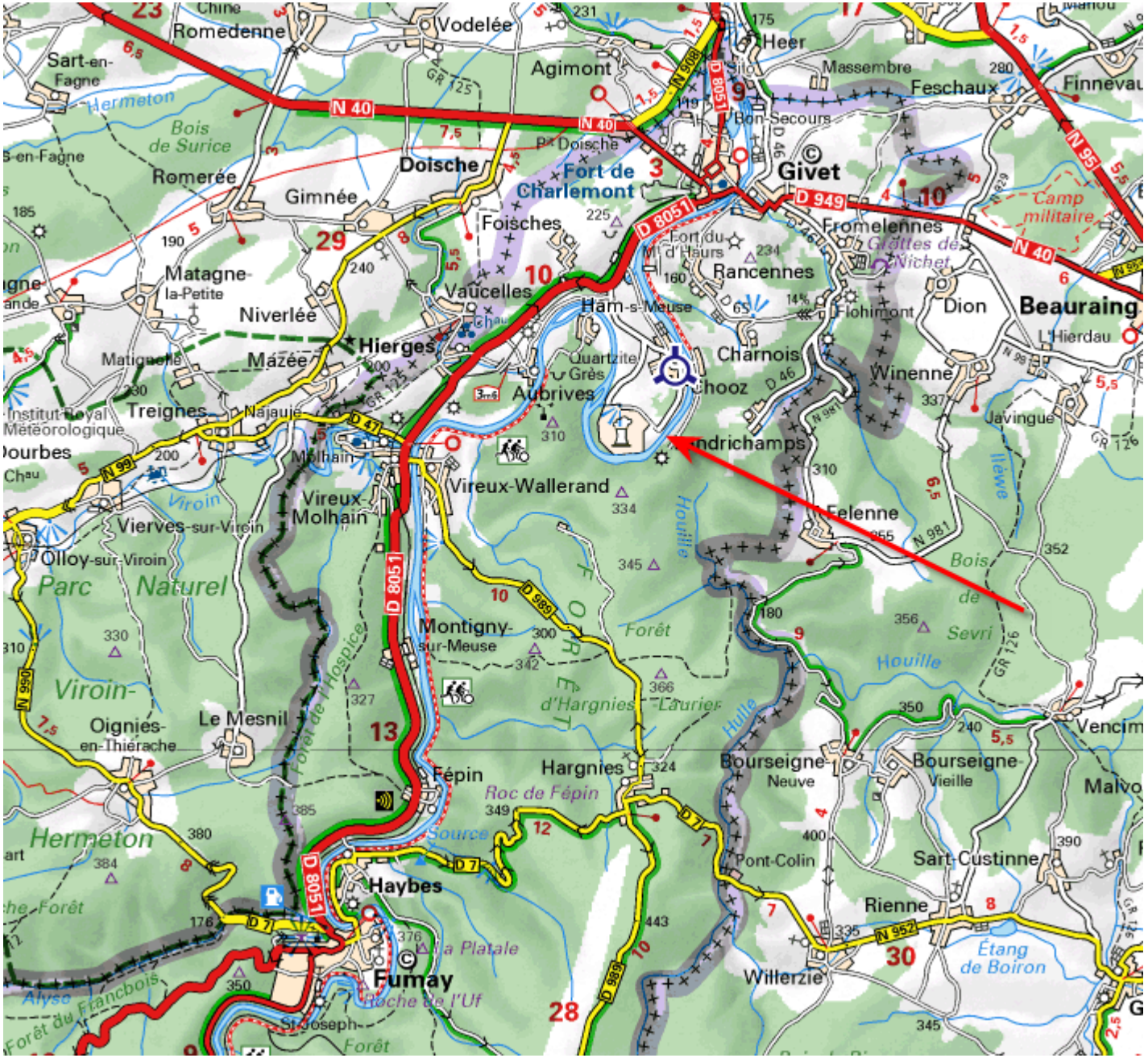
Nouveau domaine LNCA début 2010

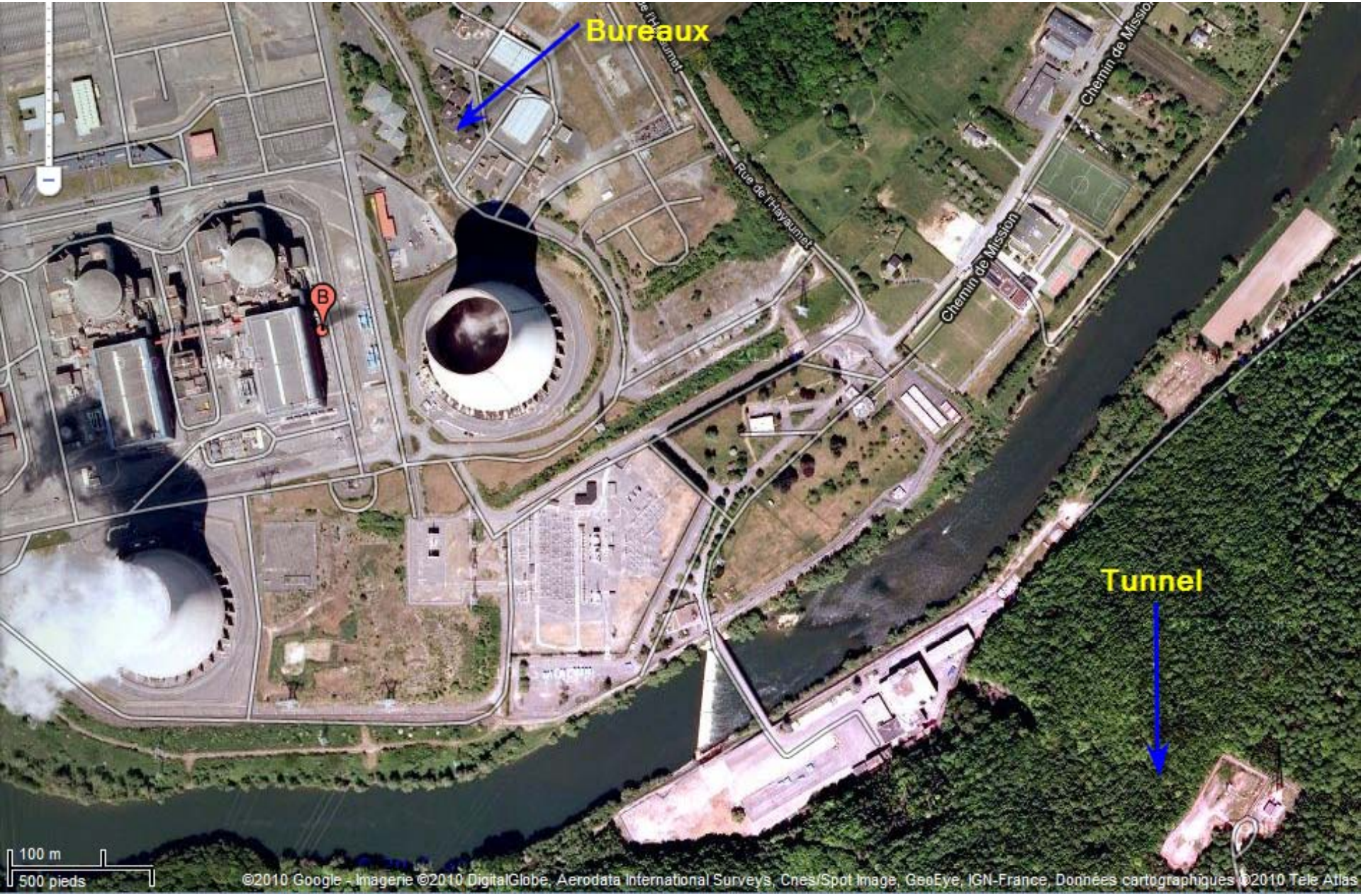
- **L**aboratoire **N**eutrino de **C**hampagne **A**rdennes, Centrale Nucléaire de Chooz (UMS 3263 créé en 2009).

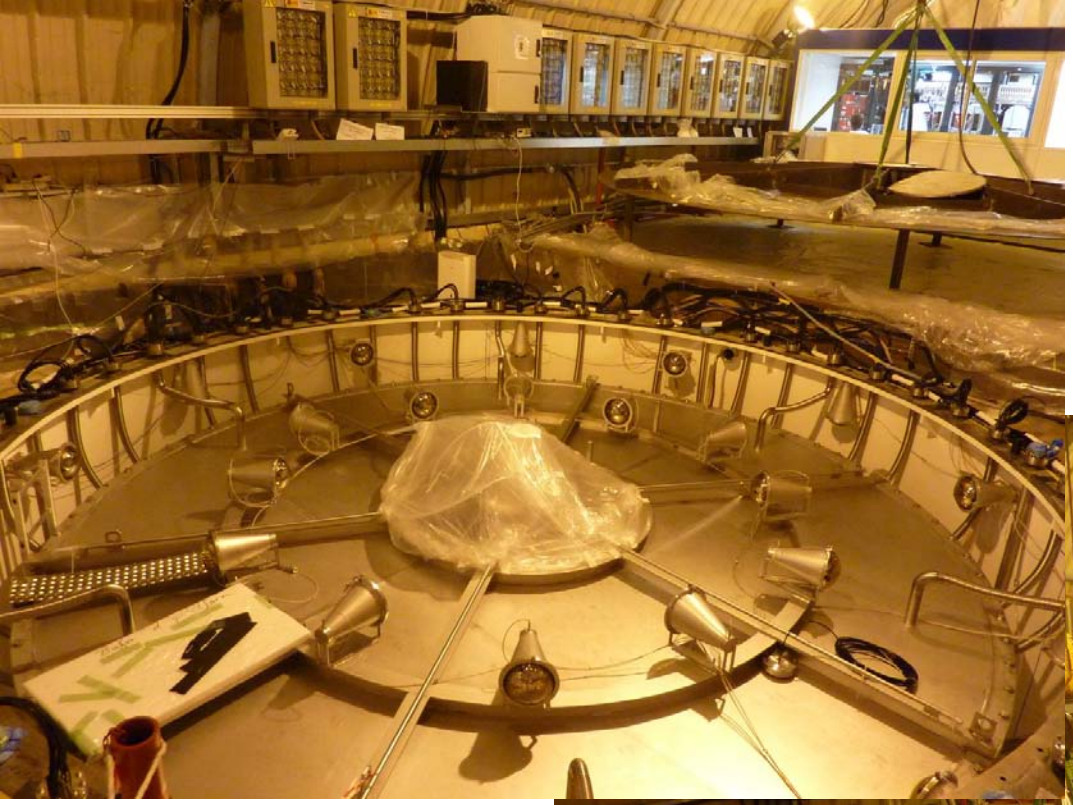
- Deux sites techniques : tunnel, bureaux

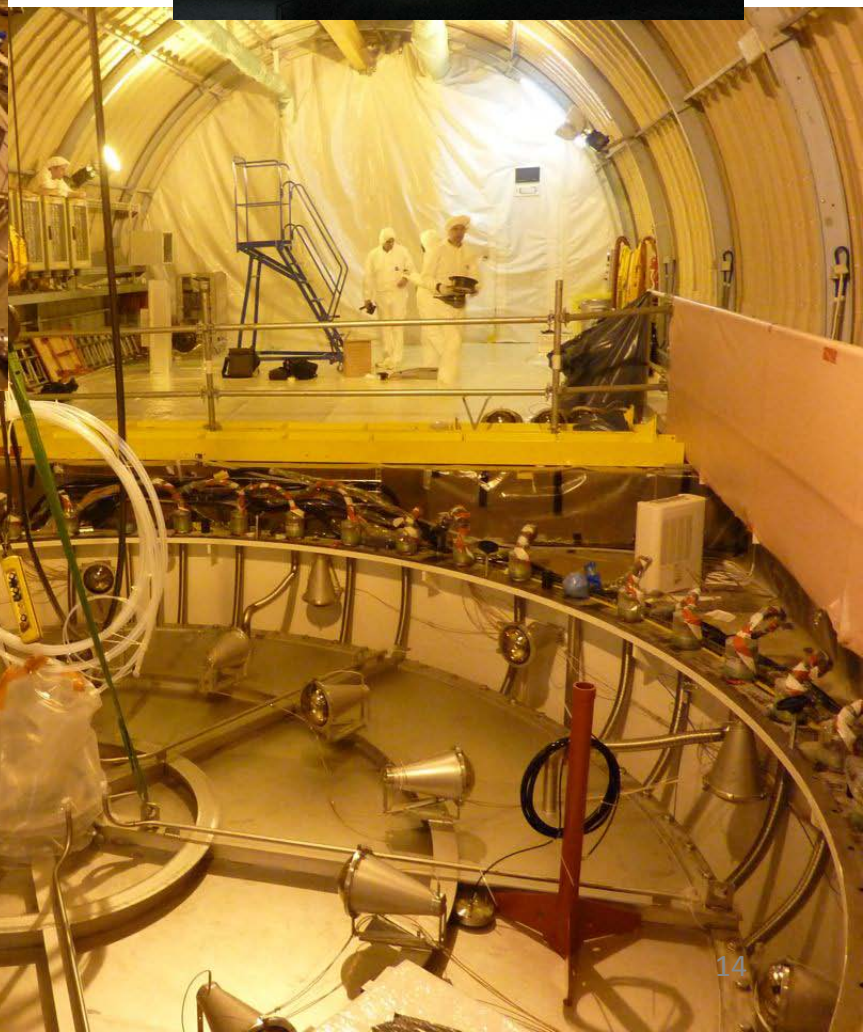
- Architecture entièrement virtualisée

Chooz dans les Ardennes


Romedenne
Vodelée
Sart-en-Fagne
Hermeton
Bois de Surice
Agimont
Heer
Massembre
Feschaux
Finnevau
Bon-Secours
Doische
Fort de Charlemont
Givet
Romerée
Gimnée
Foisches
Fromelennes
Grottes de Nichet
Camp militaire
Matagne-la-Petite
Vaucelles
Rancennes
Niverlée
Ham-s-Meuse
Flohimont
Dion
Beauraing
L'Hierdau
Hierges
Mazée
Charnois
Quartzite Grès
Aubrives
Winenne
Treignes
Najaujé
Javingue
Molhain
Vireux-Wallerand
Vireux-Molhain
Vierves-sur-Viroin
Felenne
Olloy-sur-Viroin
Parc Naturel
Bois de Sevri
Montigny-sur-Meuse
Forêt d'Hargnies
Laurier
Viroin-
Oignies-en-Thiérache
Le Mesnil
Fépin
Hargnies
Bourseigne-Neuve
Bourseigne-Vieille
Roc de Fépin
Source
Hermeton
Pont-Colin
Sart-Custinne
Haybes
Rienne
Fumay
Willerzie
Étang de Boiron
Roche de l'Uf
St-Joseph
Forêt du Francbois
Forêt de l'Hospice
Houille
Hulle
Ilèwe
N 40
N 95
N 99
N 990
N 952
N 908
D 8051
D 949
D 47
D 989
D 7
D 46
D 46
GR 125
GR 126


Bureaux
Tunnel
Rue de l'Hayaumet
Chemin de Mission
100 m
500 pieds
©2010 Google - Imagerie ©2010 DigitalGlobe, Aerodata International Surveys, Cnes/Spot Image, GeoEye, IGN-France, Données cartographiques ©2010 Tele Atlas





L'expérience Double Chooz a pour but de mesurer le troisième angle de mélange des neutrinos, θ_{13}
http://doublechooz.in2p3.fr

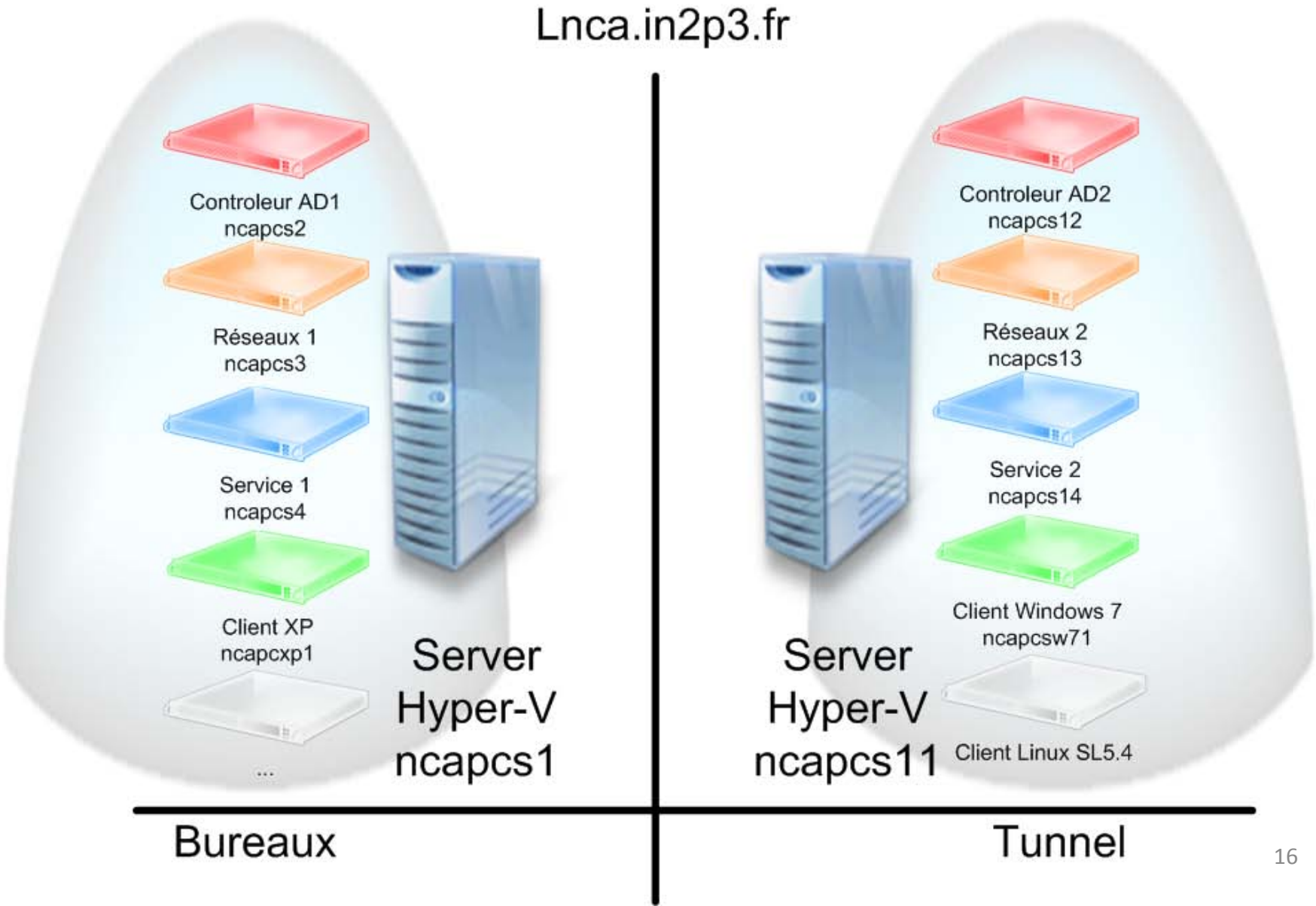
Architecture Chooz

- Windows server 2008 R2 Enterprise
  (4 licences pour les vms) Hyper-V v2

- Sur chaque serveur :
  - Vm contrôleur de domaines
  - Vm services réseau: dhcp, dns, radius (vpn, wifi)
  - Vm services: serveur impression, création utilisateur et changement de mot de passe via un site Web
  - Vm clientes : Linux, Windows XP et Windows 7

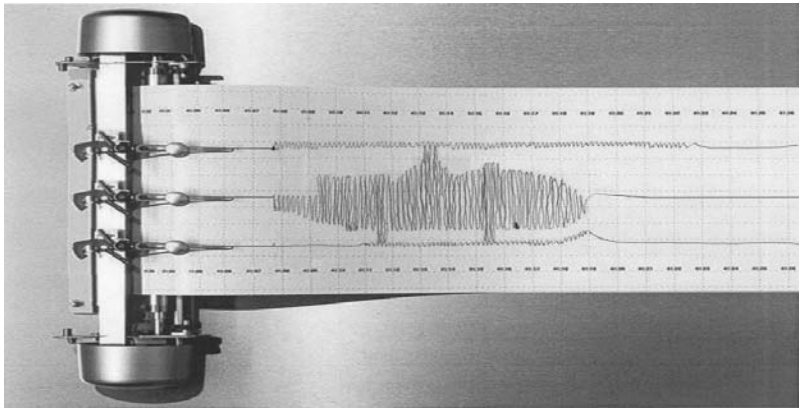
Authentification centralisée
(Identity Manager for Unix => NIS et Kerberos)

Architecture Chooz



Monitoring

- <u>Forêt Active Directory, une architecture complexe, fortement répartie</u>
  nécessité d'avoir un outil pour superviser l'ensemble de la plate-forme (santé des contrôleurs de domaines, réplications entre domaines, sécurité des comptes,…), pour avoir une vision globale.



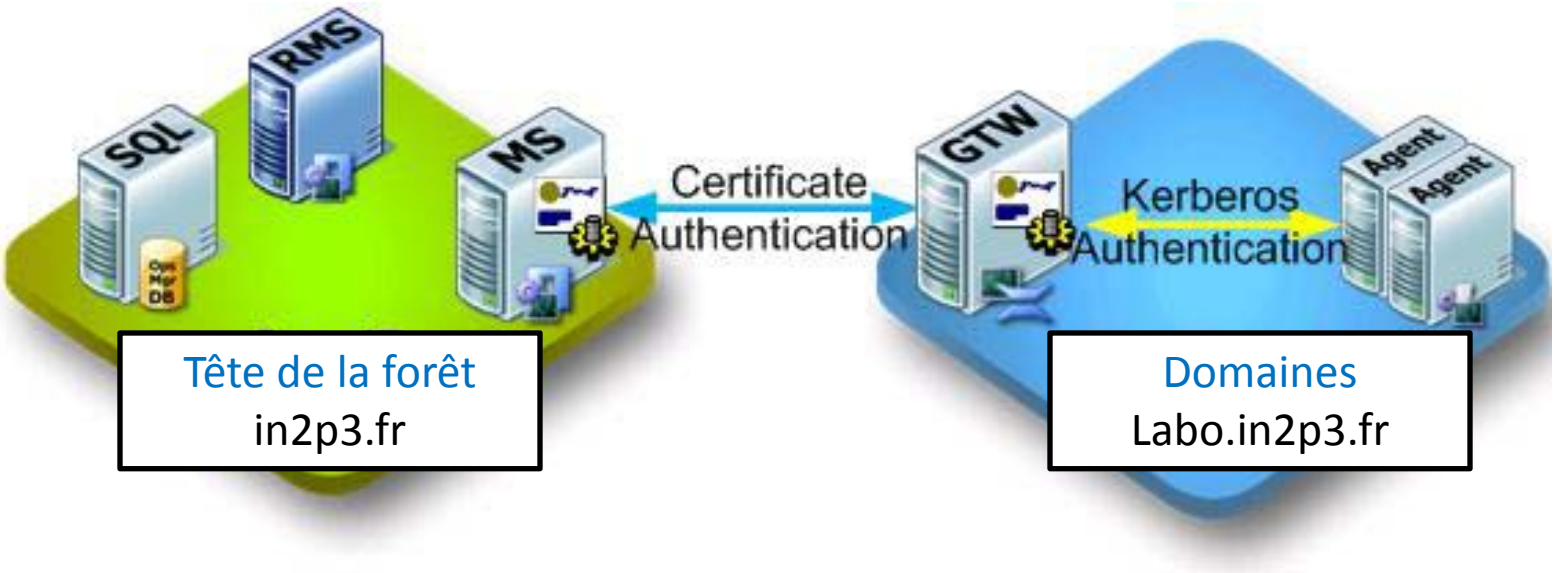
Monitoring

Choix de l'outil

- SCOM2007 (System Center Operation Manager) :
  - Répond le mieux en terme d'architecture répartie
  - Utilise les mécanismes de sécurité Windows intégrés à la Forêt Active Directory.
  - Grande diversité des objets supervisés
  - Temps de mise en œuvre et d'apprentissage
  - Grande échelle (scalable)…

- Déployé depuis 2007,
- Mise à jour version SCOM 2007 *R2*, décembre 2009

Communication



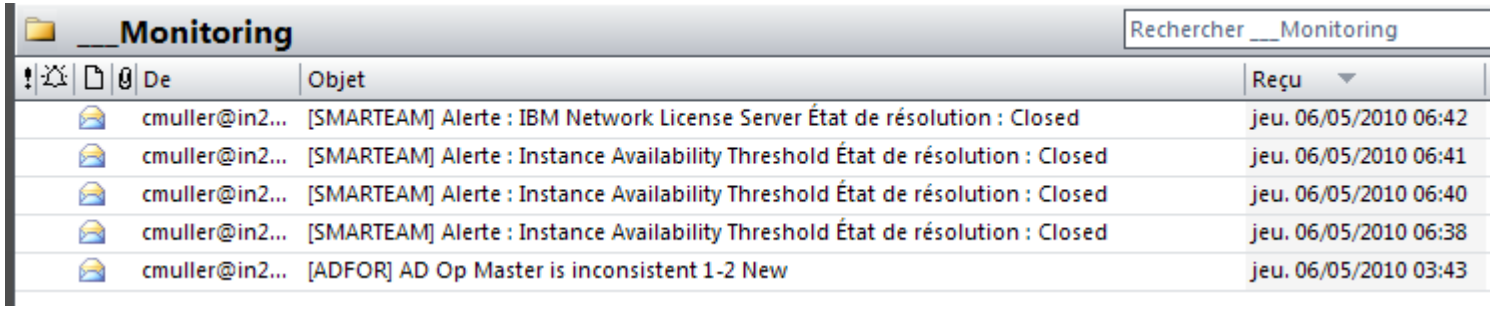
- Mise en place d'un agent passerelle (**GTW**) dans les laboratoires pour centraliser les remontées des autres agents.
  un seul port ouvert : la passerelle vers le port TCP 5723 du serveur de monitoring
- Authentification de l'agent avec le serveur de supervision par certificat x509 CNRS2.
- Authentification de l'agent proxy avec les autres agents du domaine se fait par Kerberos.

Actuellement

- 64 serveurs sont supervisés:
  - L'ensemble des contrôleurs de domaines des laboratoires (44 serveurs)
  - L'ensemble de la plate-forme Smarteam (9 serveurs)
  - Des serveurs dans des laboratoires (11 serveurs)
- 3 statuts de santé des machines: Critique, Avertissement, Sain
- La base de données contient environ 8 Go de données.

Pour les administrateurs

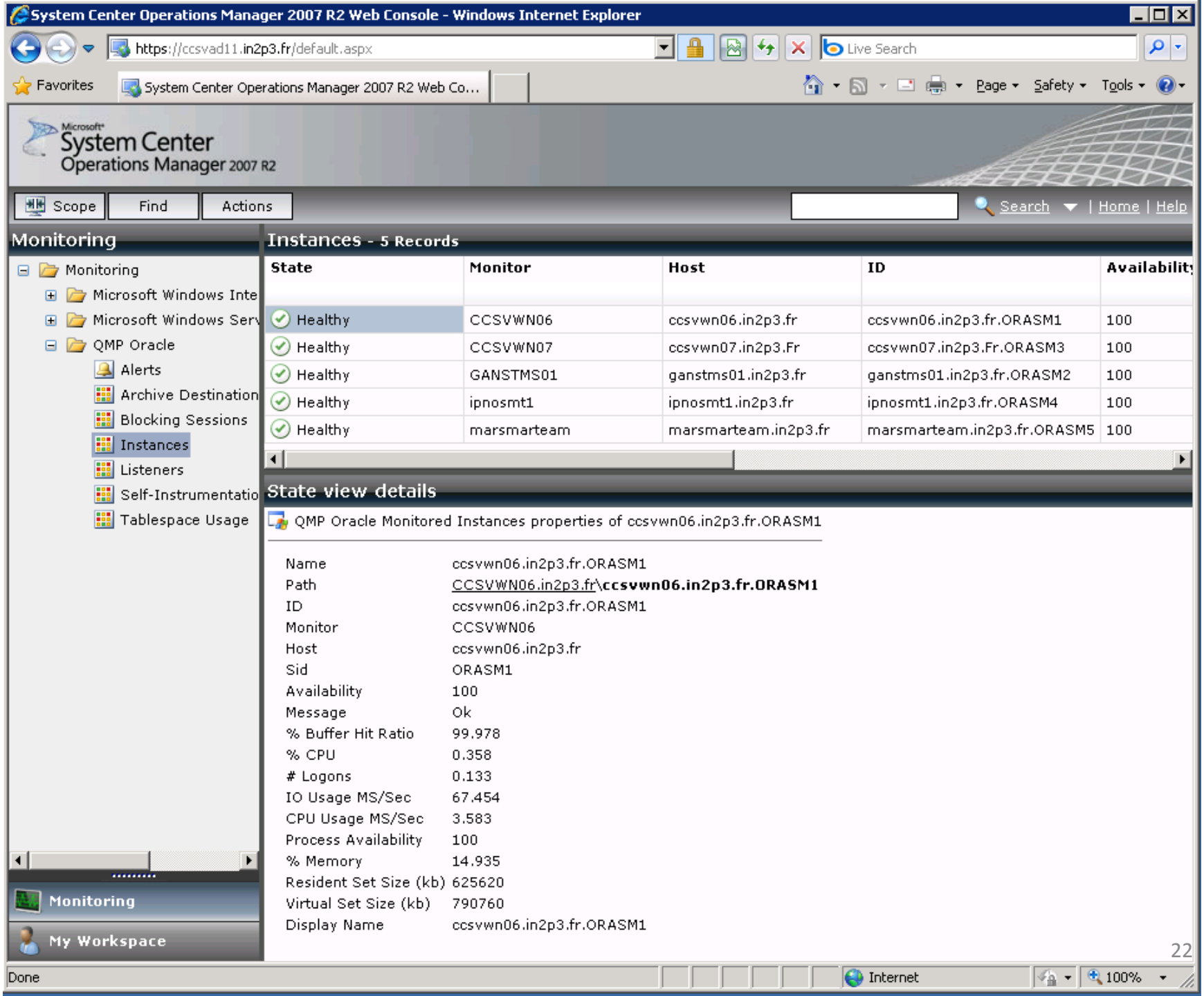
- Envoi d'emails lors d'alertes critiques:
  (retardées, si résolution dans les 10 minutes pas de mail)



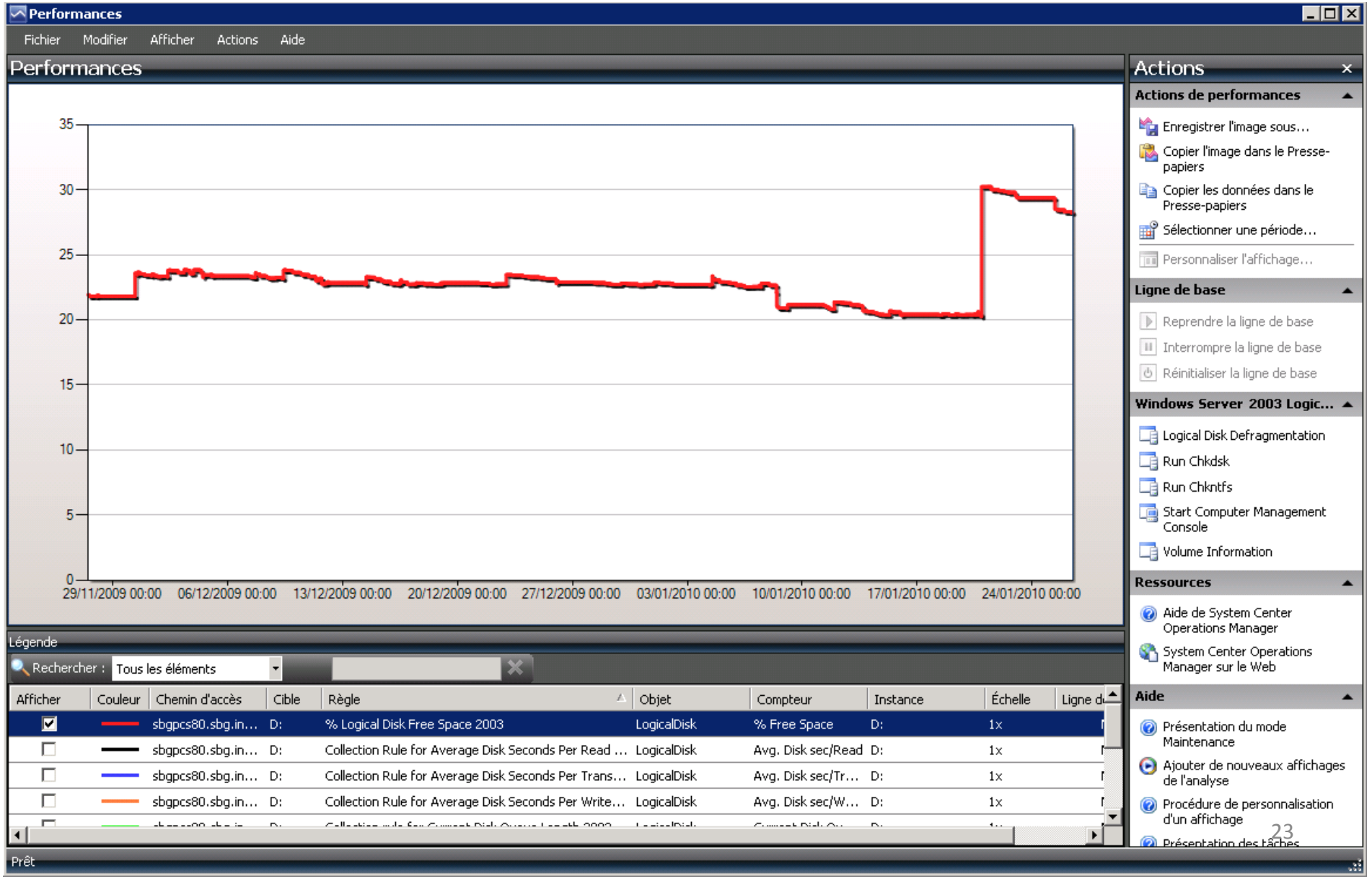
___Monitoring — Rechercher ___Monitoring

De	Objet	Reçu
cmuller@in2...	[SMARTEAM] Alerte : IBM Network License Server État de résolution : Closed	jeu. 06/05/2010 06:42
cmuller@in2...	[SMARTEAM] Alerte : Instance Availability Threshold État de résolution : Closed	jeu. 06/05/2010 06:41
cmuller@in2...	[SMARTEAM] Alerte : Instance Availability Threshold État de résolution : Closed	jeu. 06/05/2010 06:40
cmuller@in2...	[SMARTEAM] Alerte : Instance Availability Threshold État de résolution : Closed	jeu. 06/05/2010 06:38
cmuller@in2...	[ADFOR] AD Op Master is inconsistent 1-2 New	jeu. 06/05/2010 03:43

- Console Web
  Pour voir plus en détail les informations,
  accéder à l'état de santé d'un serveur,
  moniteurs de performances,…

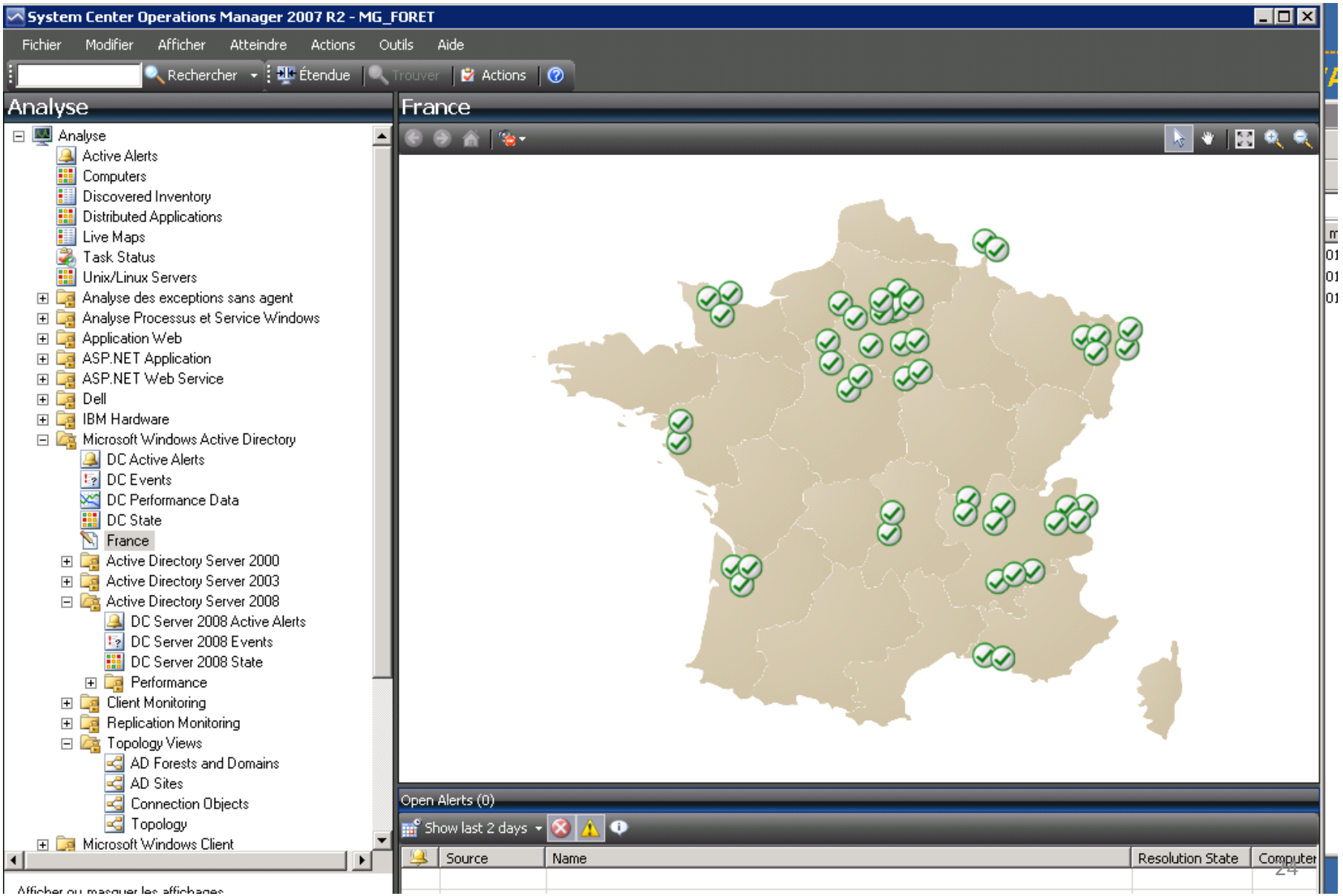

System Center Operations Manager 2007 R2 Web Console - Windows Internet Explorer
https://ccsvad11.in2p3.fr/default.aspx
Live Search
Favorites
System Center Operations Manager 2007 R2 Web Co...
Page
Safety
Tools
Microsoft System Center Operations Manager 2007 R2
Scope
Find
Actions
Search
Home
Help
Monitoring
Monitoring
Microsoft Windows Inte
Microsoft Windows Serv
QMP Oracle
Alerts
Archive Destination
Blocking Sessions
Instances
Listeners
Self-Instrumentatio
Tablespace Usage
Monitoring
My Workspace
Instances - 5 Records
State
Monitor
Host
ID
Availabilit
Healthy
CCSVWN06
ccsvwn06.in2p3.fr
ccsvwn06.in2p3.fr.ORASM1
100
Healthy
CCSVWN07
ccsvwn07.in2p3.Fr
ccsvwn07.in2p3.Fr.ORASM3
100
Healthy
GANSTMS01
ganstms01.in2p3.fr
ganstms01.in2p3.fr.ORASM2
100
Healthy
ipnosmt1
ipnosmt1.in2p3.fr
ipnosmt1.in2p3.fr.ORASM4
100
Healthy
marsmarteam
marsmarteam.in2p3.fr
marsmarteam.in2p3.fr.ORASM5
100
State view details
QMP Oracle Monitored Instances properties of ccsvwn06.in2p3.fr.ORASM1
Name ccsvwn06.in2p3.fr.ORASM1
Path CCSVWN06.in2p3.fr\ccsvwn06.in2p3.fr.ORASM1
ID ccsvwn06.in2p3.fr.ORASM1
Monitor CCSVWN06
Host ccsvwn06.in2p3.fr
Sid ORASM1
Availability 100
Message Ok
% Buffer Hit Ratio 99.978
% CPU 0.358
# Logons 0.133
IO Usage MS/Sec 67.454
CPU Usage MS/Sec 3.583
Process Availability 100
% Memory 14.935
Resident Set Size (kb) 625620
Virtual Set Size (kb) 790760
Display Name ccsvwn06.in2p3.fr.ORASM1
22
Done
Internet
100%

Moniteurs de performance : garder de l'information pour suivre les évolutions (historique de 2 mois)



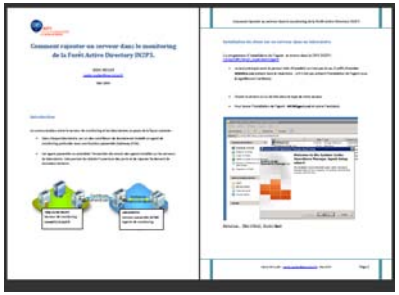
LiveMaps (Savision)

Mise à disposition sur la console Web



Remarques

- Pour les administrateurs qui le souhaitent, il est possible d'ajouter des serveurs de leur domaine.



- Redirection des alertes vers Nagios.

- Entièrement personnalisable, scriptable (PowerShell). Création des règles de supervisions pour tous type de services (Smarteam, serveurs de licences FlexLM, etc..)

- Coût en terme de licences :
  - SCOM 2007 R2 avec SQL Server : 320 Euros
  - Par agent : 37 Euros

Quelques exemples d'alertes

Dell OMSA Power supply detected a failure sensor

Alert Description Source: sbgpcs115.sbg.in2p3.fr

Power supply detected a failure

Sensor location: PS 1 Status

Chassis location: Main System Chassis

Previous state was: OK (Normal)

Power Supply type: AC

Power Supply state: Presence detected, Failure detected, AC lost

Alert: Total CPU Utilization Percentage is too high

Source: Microsoft(R) Windows(R) Server 2003, Standard Edition

Path: marw2k.cppm.in2p3.fr

Last modified by: System

Last modified time: 25/09/2009 09:27:33

Alert description: The threshold for the Processor\% Processor Time_Total performance counter has been exceeded. The values that exceeded the threshold are: 100.% CPU and a processor queue length of 16.

Alert: AD Replication is occurring slowly

Source: CLRPC38

Path: clrpc38.lpcclermont.in2p3.fr

Last modified time: 24/07/2009 15:43:27

Alert description: AD Replication Monitoring : The following DCs took more than three times the expected replication time to replicate.

Format: DC, Naming Context, Calculated Replication Time (in minutes)

Site name: Clermont

(Intrasite, expected replication time is 5 minutes)

clrw2k01, NDNC:DC=ForestDnsZones,DC=in2p3,DC=fr, 156

Monitoring et ACS (Audit Collection Service)

Fonctionnalité non implémentée par défaut dans SCOM 2007

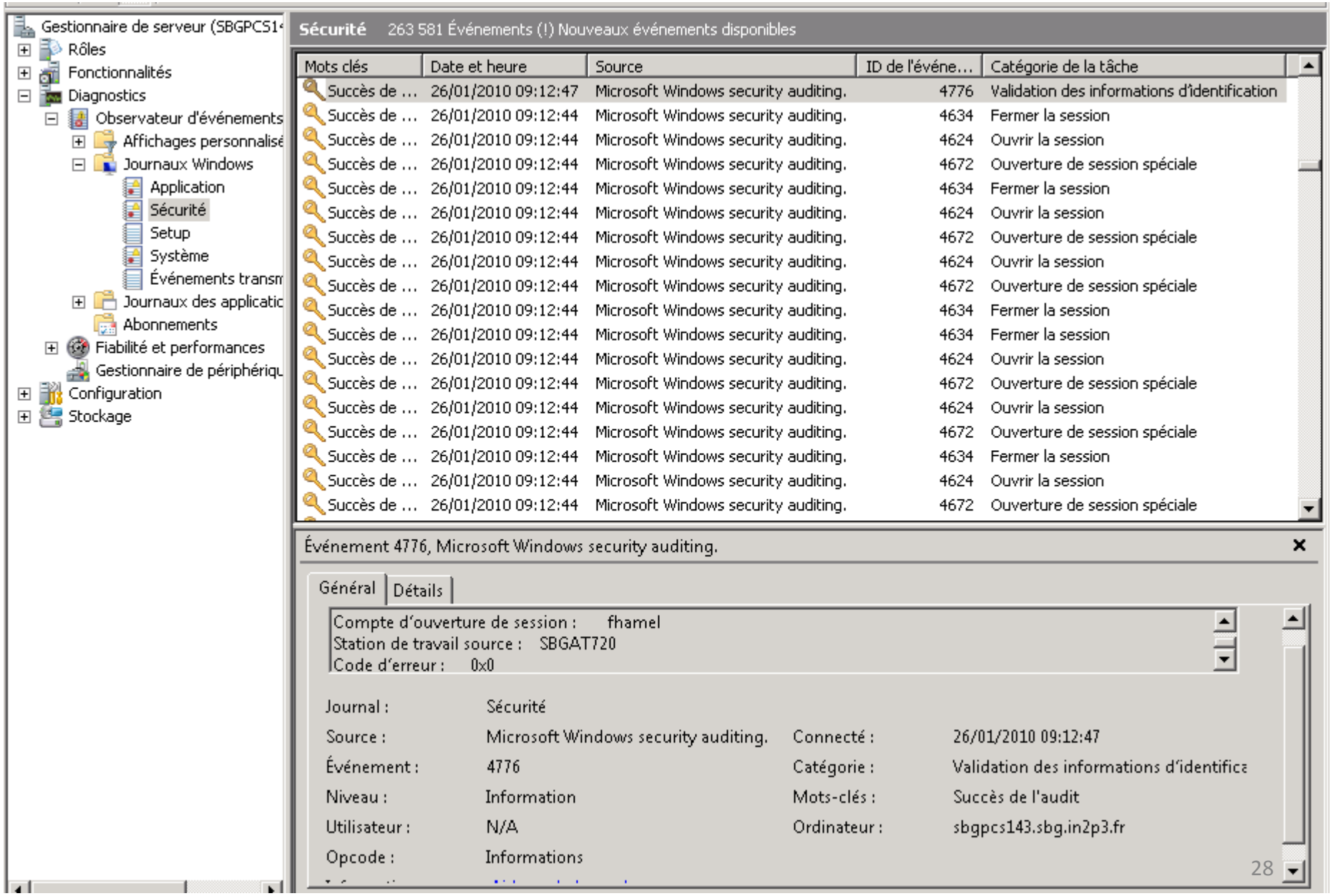
Collecte des journaux de sécurité des contrôleurs de domaine.

- **Obligations**
  Centraliser, monitorer, archiver les événements de sécurité.

- **Audit**
  Sécurité interne, qui à fait quoi, échecs sur les mots de passe,..

- **Sécurité**
  Garantir la disponibilité des logs en temps réels en les exportant du serveur.

Journal de sécurité Windows Server



ACS / Principe

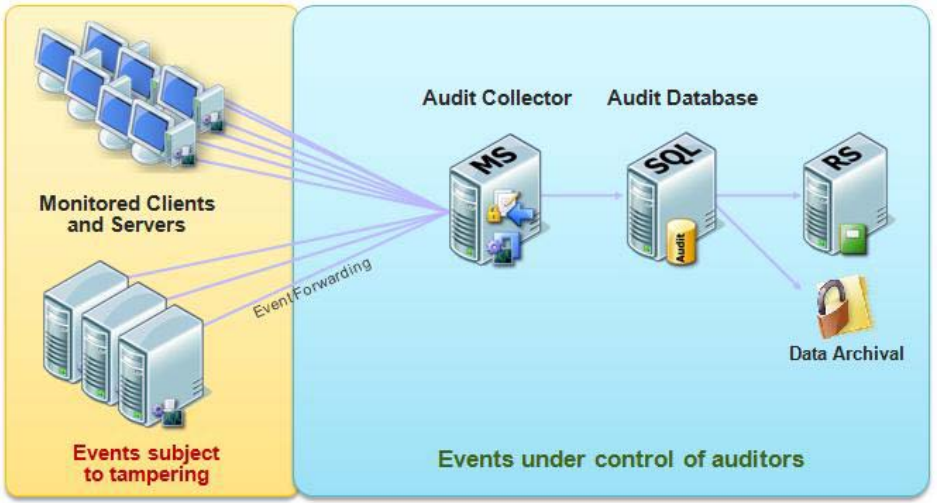
Inclus dans SCOM2007, pas de surcoût de licence

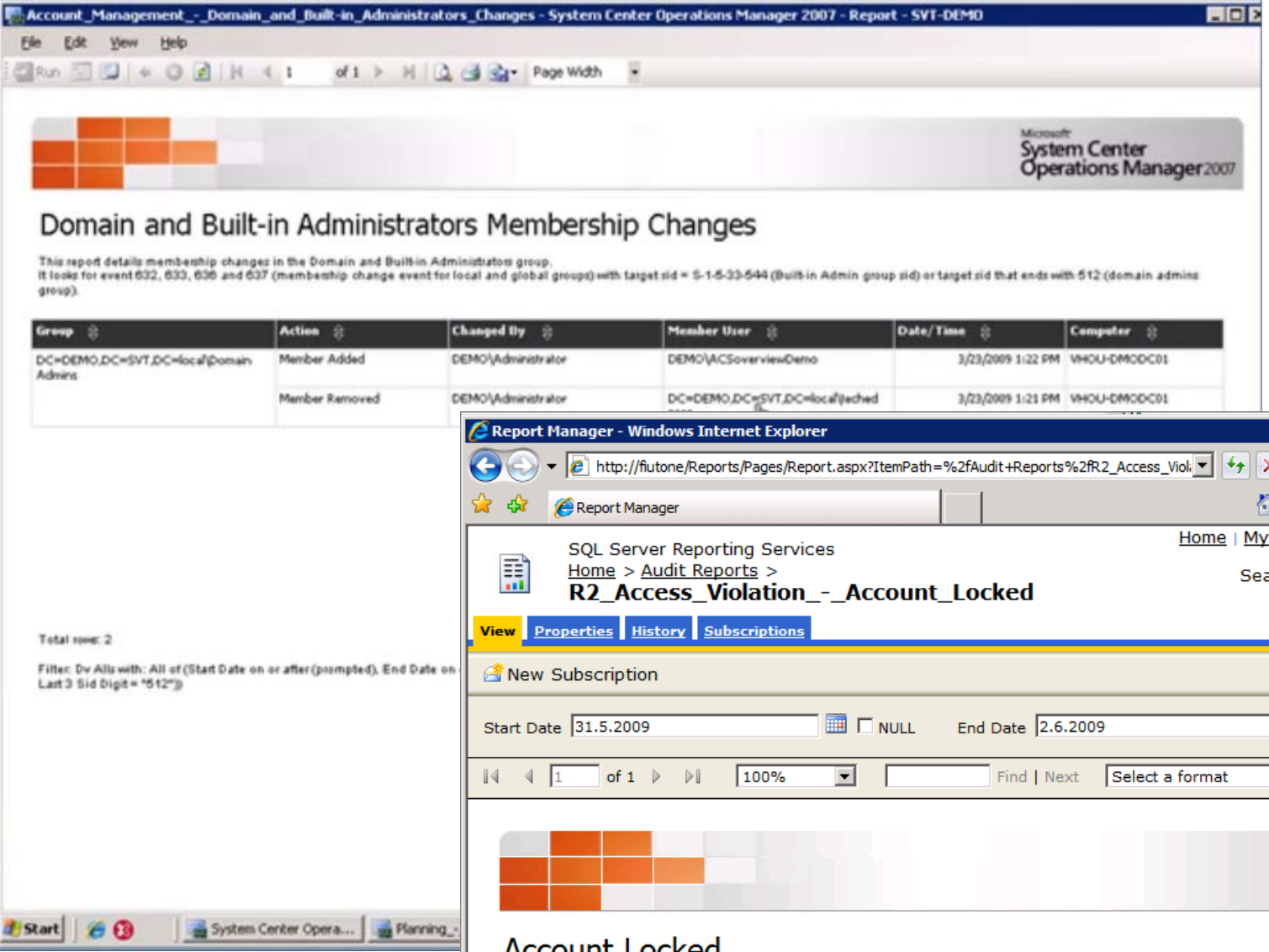
- Renvoi en quasi temps réel les évènements du journal de sécurité vers un serveur de collecte
- Modifications impossibles, *tamper resilient*
- Assurance que tous les évènements sont bien transmis
- Chiffrement et compression du trafic réseau
- Rapports prédéfinis :
  - création suppression d'utilisateurs et d'ordinateurs
  - changement de membres de groupe (administrateurs,..)
  - changement de mot de passe 'extérieur'
  - accès non autorisés
  - changement dans les stratégies de groupes
  - effacement log,…

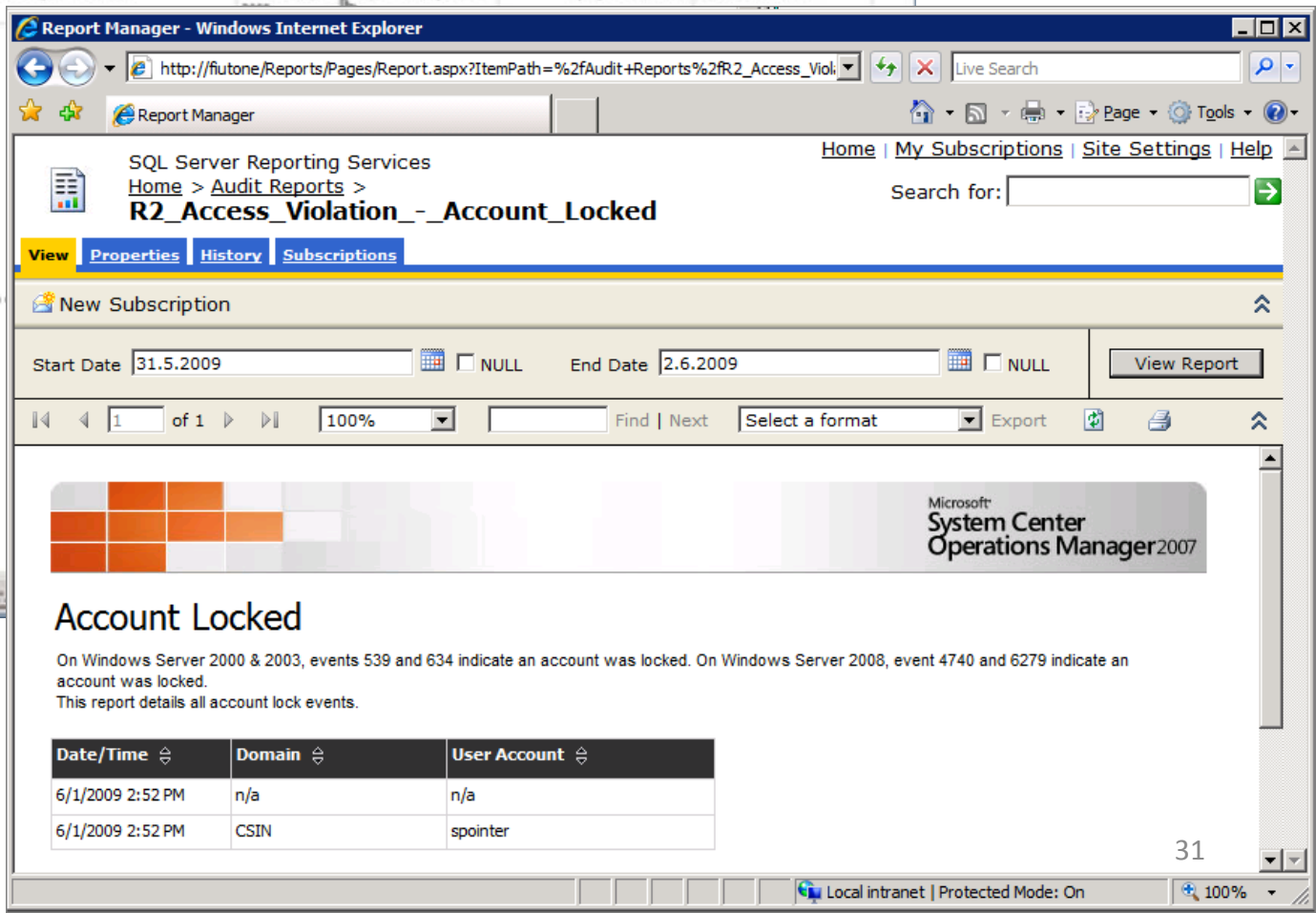
ACS Architecture

Nécessite :

- un serveur de collecte pour recevoir les différents évènements (**Audit Collector**)
- un serveur de base de données spécifique, grande volumétrie de données. (50 Go/an) rapide en I/O disque. (**Audit Database**)
- un serveur pour les rapports (**Report Server**)
- Une sauvegarde régulière




Account_Management_-_Domain_and_Built-in_Administrators_Changes - System Center Operations Manager 2007 - Report - SVT-DEMO
File Edit View Help
Page Width
Microsoft System Center Operations Manager 2007
Domain and Built-in Administrators Membership Changes
This report details membership changes in the Domain and Built-in Administrators group.
It looks for event 632, 633, 636 and 637 (membership change event for local and global groups) with target sid = S-1-5-32-544 (Built-in Admin group sid) or target sid that ends with 512 (domain admins group).
Group
Action
Changed By
Member User
Date/Time
Computer
DC=DEMO,DC=SVT,DC=local\Domain Admins
Member Added
DEMO\Administrator
DEMO\ACSoverviewDemo
3/23/2009 1:22 PM
VHOU-DMODC01
Member Removed
DEMO\Administrator
3/23/2009 1:21 PM
VHOU-DMODC01
Total rows: 2
Start
System Center Opera...
Planning_...


Report Manager - Windows Internet Explorer
http://fiutone/Reports/Pages/Report.aspx?ItemPath=%2fAudit+Reports%2fR2_Access_Viol
Live Search
Report Manager
Page Tools
Home | My Subscriptions | Site Settings | Help
SQL Server Reporting Services
Home > Audit Reports >
R2_Access_Violation_-_Account_Locked
Search for:
View Properties History Subscriptions
New Subscription
Start Date 31.5.2009 NULL
End Date 2.6.2009 NULL
View Report
1 of 1
100%
Find | Next
Select a format
Export
Microsoft System Center Operations Manager 2007
Account Locked
On Windows Server 2000 & 2003, events 539 and 634 indicate an account was locked. On Windows Server 2008, event 4740 and 6279 indicate an account was locked.
This report details all account lock events.
Date/Time
Domain
User Account
6/1/2009 2:52 PM
n/a
n/a
6/1/2009 2:52 PM
CSIN
spointer
Local intranet | Protected Mode: On
100%

ACS / Remarques…

- Intégration des remontées des syslog Unix.
- Remontée les informations sur les comptes des domaine, pas des comptes locaux des machines.
- Impossible d'utiliser les agents proxy de la supervision.
- Ouverture d'un port de chaque DC vers le serveur de collecte
- Génération d'un certificat pour chaque DC.
- Faut-il mettre en place la solution,
  à qui donner accès, …

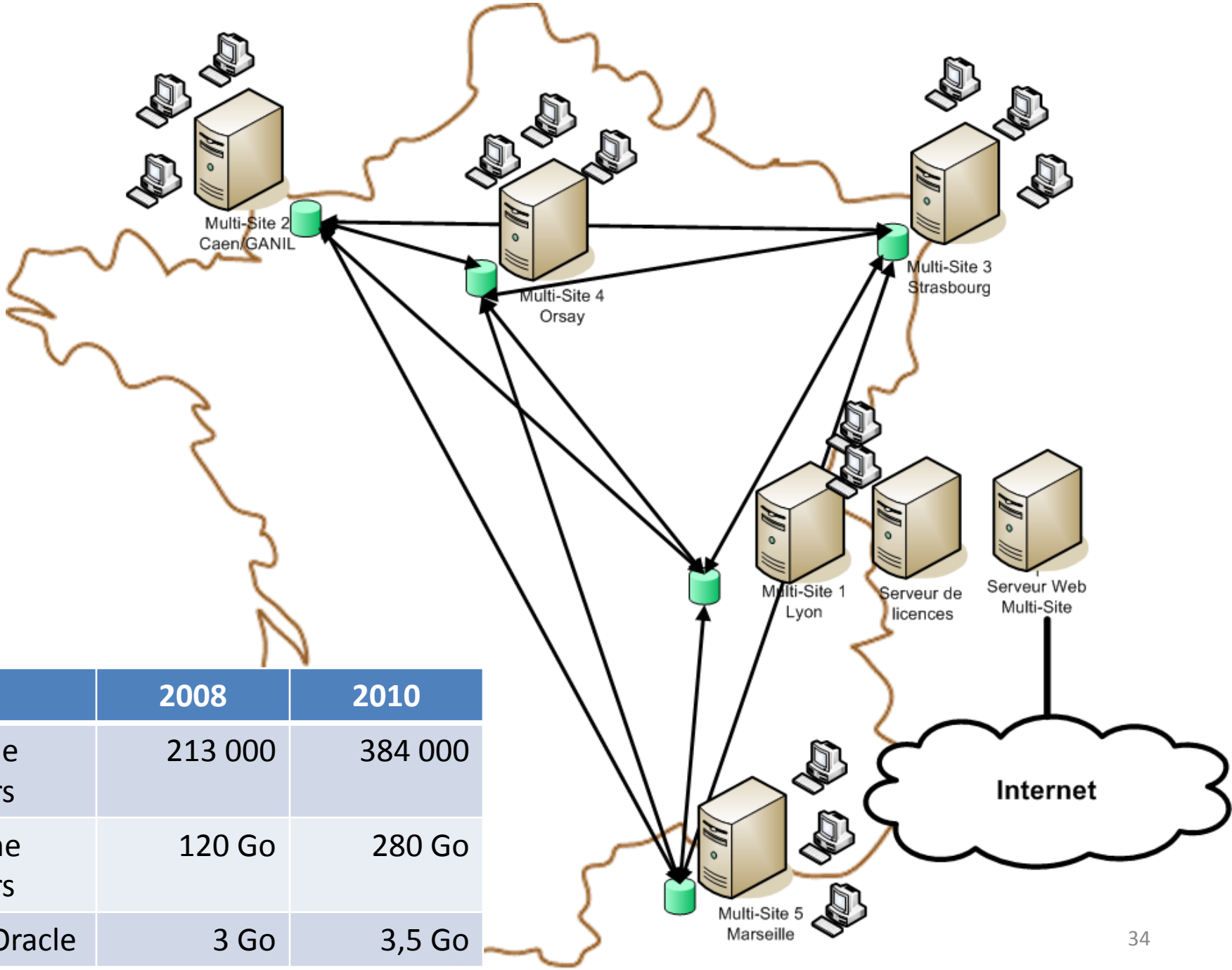
Catia/Smarteam

- Catia : CAO conception 3D Bureau d'études

- Smarteam (PLM : Gestion cycle de vie, gestion de version, travail en équipe,…)
  - Services Smarteam
  - Base Oracle (métadonnées)
  - Coffres (Vaults)

- Environnement distribué sur 5 sites (Spiral2), accès par navigateur internet avec visualiseur 3D.

- Plus de 200 Pcs Clients Catia, 100 Smarteam.



	2008	2010
Nbs de fichiers	213 000	384 000
Volume fichiers	120 Go	280 Go
Base Oracle	3 Go	3,5 Go

Catia/Smarteam

- Migration R19 Septembre 2009 (arrêt de 2 jours) :
  - Mise à jour des 5 serveurs d'applications
  - Mise à jour de l'accès Web
  - Mise à disposition des scripts de déploiements pour les postes clients dans les Bureaux d'Etudes

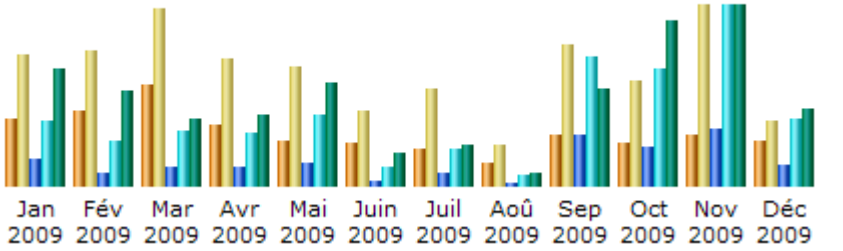
- Test de Migration R20 (Mars 2010) dans environnement virtualisé pour permettre l'installation de clients sous Windows 7 et Client Oracle 11. Version encore jeune (SP1).

- Prochaine version majeure V6, annonce de grands changements (base de données locale, Matrix)

Catia/Smarteam

- Forte montée en puissance depuis 8 mois, avec Spiral2 et de nouveaux projets (Guinevere,…)
- Forte utilisation du Web:
  pas d'installation de client lourd
  A destination des chefs de projets, validateurs,
  autres laboratoires de la collaboration

Historique mensuel



Mois	Visiteurs différents	Visites	Pages	Hits	Bande passante
Total	405	882	65414	191047	4.33 Go

Pays (Top 10) - Lis

Pays		Pages
France	fr	62005
Italy	it	1468
United States	us	968
Switzerland	ch	395
Belgium	be	220
India	in	95
Inconnu	unknown	71
Germany	de	67
Morocco	ma	37
Russian Federation	ru	31
Autres		57

Favorites | SMARTEAM - Web Editor | Page | Safety | Tools

ENOVIA

joe - PROD_SM1
Aucun objet princ...

ENOVIA SmarTeam

Tous les Projets - Vue Objets du bureau

Tous les Projets

Naviguer | Edition | Cycle de vie | Filtrer | Vues | Général

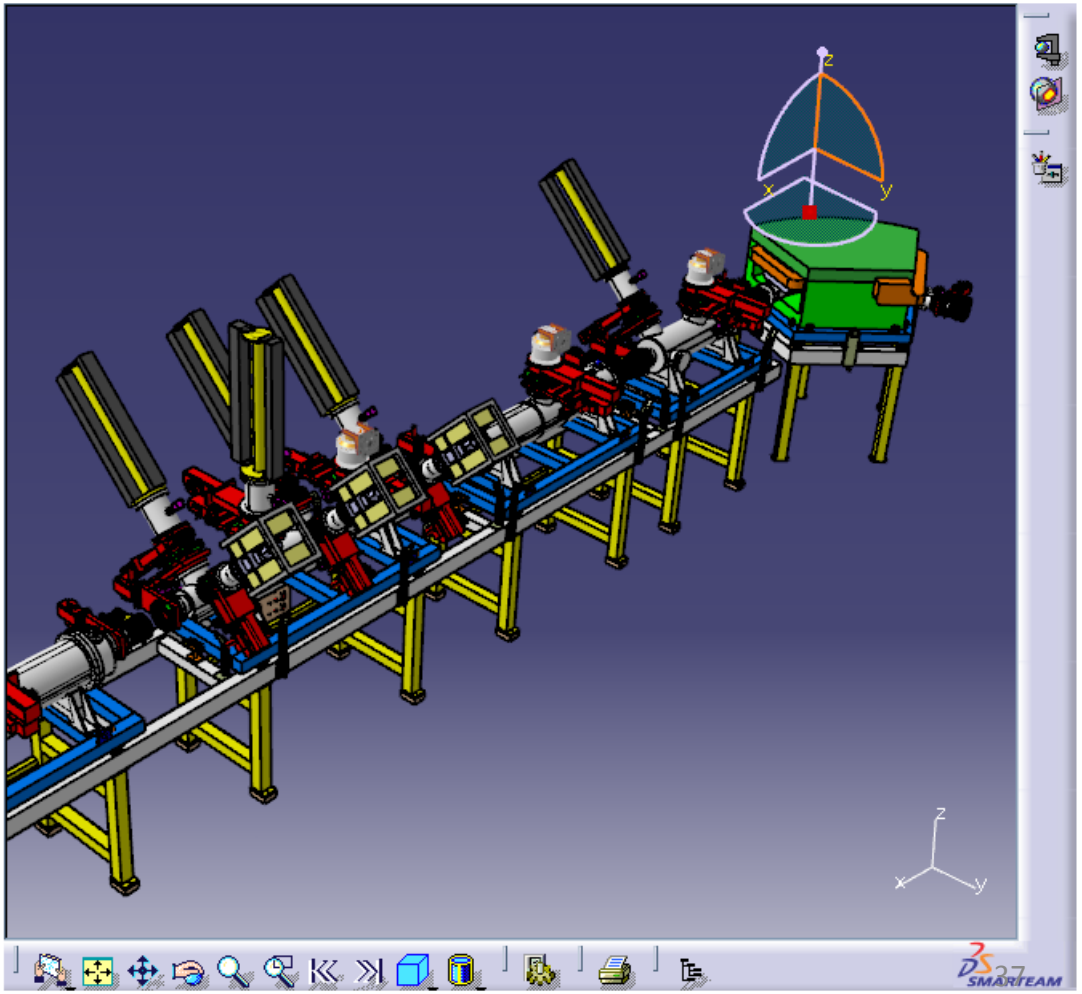
SM3_DOS30177-Integration provisoire zone transport-IPHC Strasbourg-24/02/201
SM3_PRD30257-Integration L1+ transport batiment-A.04-IPHC Strasbourg
SM3_PRD30251-Integration L1+ transport-A.08-IPHC Strasbourg-04/05/2
SM3_PRD30329-Partie mobile bender 5 10-A.03-IPHC Strasbourg-04/0
SM3_PRD30253-Chassis fixe 5 9-A.03-IPHC Strasbourg
SM3_PRD30250-Chassis fixe troncon 5-A.07-IPHC Strasbourg-06/05/2
SM3_PRD30255-Chassis fixe 7 1-A.03-IPHC Strasbourg
SM3_PRD30341-Dispositif maintenance sous modules 45-A.00-IPHC St
SM3_PRD30211-Partie mobile 5 4-A.08-IPHC Strasbourg-11/05/2010
SM3_PRD30318-Partie mobile 7 3-A.06-IPHC Strasbourg-04/05/2010
SM3_PRD30258-Partie mobile 5 11-A.07-IPHC Strasbourg-04/05/2010
SM3_PRD30249-Partie mobile 5 5-A.08-IPHC Strasbourg-04/05/2010
SM3_PRD30252-Partie mobile 5 9-A.07-IPHC Strasbourg-04/05/2010
SM3_PRD30254-Partie mobile 7 1-A.06-IPHC Strasbourg-04/05/2010
SM3_PRD30266-Partie mobile 5 7-A.06-IPHC Strasbourg-04/05/2010
SM3_PRD30195-Partie mobile 5 3-A.07-IPHC Strasbourg-11/05/2010
SM3_PRD30177-Partie mobile 5 2-A.07-IPHC Strasbourg-11/05/2010
SM3_PRT301219-Chariot maintenance sous modules 45-A.01-IPHC Str
SM3_PRD30330-Partie mobile 7 2-A.01-IPHC Strasbourg-07/05/2010
SM3_PRD30321-Partie mobile 5 8-A.02-IPHC Strasbourg-29/04/2010
SM3_PRD30320-Partie mobile 5 1-A.03-IPHC Strasbourg-29/04/2010
SM3_PRT301196-Reference Ligne Zone Jaune 50 degres-A.01-IPHC S
SM3_PRT301164-Chassis fixe aimant 90 R750-A.01-IPHC Strasbourg-
SM2_PRD20220-Reference Lignes zone jaune-A.03-SPIRAL2-27/08/20
SM2_PRD20341-MAITRE D'OEUVRE-A.00-SPIRAL2-04/06/2009 16:32

Objets associés

	Classe	Classe	Etat	ID Smarteam	Référence	Rév
				SM3_DOS30177	Integration provisoire zone transport	

Général | Détails | Composition | Remarques | Visionneuse

The object you selected is out of Vault. Showing previous revision



Done | Internet | 100%

Modifications d’architecture

- Extension du schéma Active Directory:
  - Installation de serveur Windows 2008
  - Installation d’Exchange
  - Installation de serveur Windows 2008 R2
- Ajout d’un contrôleur ccsvad05 en Windows 2008 x64
- Arrêt du serveur historique ccsvad01 (PIII, 800 mhz, 256 mo)

Déploiement Windows 7 et 2008

		2008/R2	2008		DC 2008	Niveau Fonct.		Vista	W 7
1	apc	0	2			2003		1	13
2	cenbg	0	0			2003		0	4
3	centre	0	0			2003		0	0
4	Cppm	3	0		2	2003		4	9
5	csnsm	0	0			2003		0	2
6	edd	0	0			2003		0	5
7	grenoble	0	2		1	2003		1	0
8	imnc	0	0			2003		0	0
9	in2p3	0	3		1	2003		0	0
10	ipnl	0	0			2003		0	16
11	lpno	7	5		1	2003		51	34
12	lapp	12	0		1	2003		1	25
13	llr	4	1		3	2003		0	2
14	lnca	2	0		2	**2008**		0	1
15	lpc-caen	4	6		4	**2008**		1	18
16	Lpcclermont	0	1			2003		1	0
17	lpnhe	0	3			2003		17	3
18	sbg	1	3		1	2003		2	6
19	subatech	0	0			2003		0	2
	Total	33	26		16			79	148

Octobre 2009 / Réunions des Administrateurs des domaines

- Réunion au Centre de Calcul,
  16 laboratoires participants + visioconférence

- Présentations:
  - Nouveaux systèmes d'exploitations
    Windows 7 / Windows 2008 R2
  - Déploiement d'Exchange au LAPP
  - System Center Essentials – outil d'administration (<300 postes)
  - Ajout d'un contrôleur Windows 2008
  - Présentation de WDS – déploiement d'images

- Tour des laboratoires, échanges sur nos sujets de préoccupation du moment.

- Formation avec Travaux Pratiques autour de Powershell
  Mise à disposition de machines virtuelles.

..Perspectives..

- Continuer la migration des contrôleurs de domaines de tête de forêt, Windows 2008 R2.

- Test sur la partie ACS de l'outil monitoring, remontée des journaux de sécurités dans un laboratoire.

- Support aux laboratoires pour les migrations.

Merci de votre attention