GPO Windows : notions de base et paramétrages pour Win10
Problématique de migration de PDC de Samba3 NT4-like vers AD

Journées Mathrice
Montpellier
27 - 29 mars 2018

Didier Depoisier

Institut Fourier - UMR 5582 - Grenoble

INSTITUT FOURIER

Plan

Préambule

1/ GPO : Définition et notions de base

2/ Paramètres pour Win10

3/ Migration Samba3 NT4-like vers AD

1 – GPO : Définition et notions de base

GPO : Group Policy Object – Stratégies de groupe

Outil qui permet de

- centraliser, regrouper, modéliser la configuration de paramètres
- déployer sur les serveurs et postes clients des configurations
- outil de gestion de configurations

Sont apparues dans les **années 2000** avec la mise sur le marché de Windows 2000 Server.
=> il n'y a pas de GPO pour NT

Quelques exemples de fonctionnalités :

- Installer des logiciels automatiquement en fonction de groupes d'utilisateurs ou profils d'utilisation (administratifs, enseignants...)
- s'appliquent au système ou a un utilisateur - permet de gérer des règles sur les comptes utilisateurs – règles sur les mots de passe
- paramétrer le bureau - le menu - les préférences d'affichage des dossiers - forcer un proxy sortant - bloquer l'accès au panneau de configuration - bloquer certains exécutables
- s'appliquent ou se ré-appliquent périodiquement 60 – 90 - 120 mn

1 – GPO : Définition et notions de base

GPO locales => **gestion et approche unitaire** du poste
GPO de domaine => **gestion globale / par groupes** de postes

Des centaines de paramètres !

Plus de 3600 paramètres configurables toutes versions de Windows Server et Windows clients confondus (jusqu'à Win2012 Srv)

Un paramètre de stratégie de groupe appliqué à un ordinateur qui ne peut pas le traiter, est tout simplement ignoré.

La plupart des paramètres de stratégie ont trois états :

- **Non configuré** : pas de modification de la configuration existante pour ce paramètre.
- **Activé** : le paramètre de stratégie est appliqué.
- **Désactivé** : le paramètre de stratégie est spécifiquement inversé.

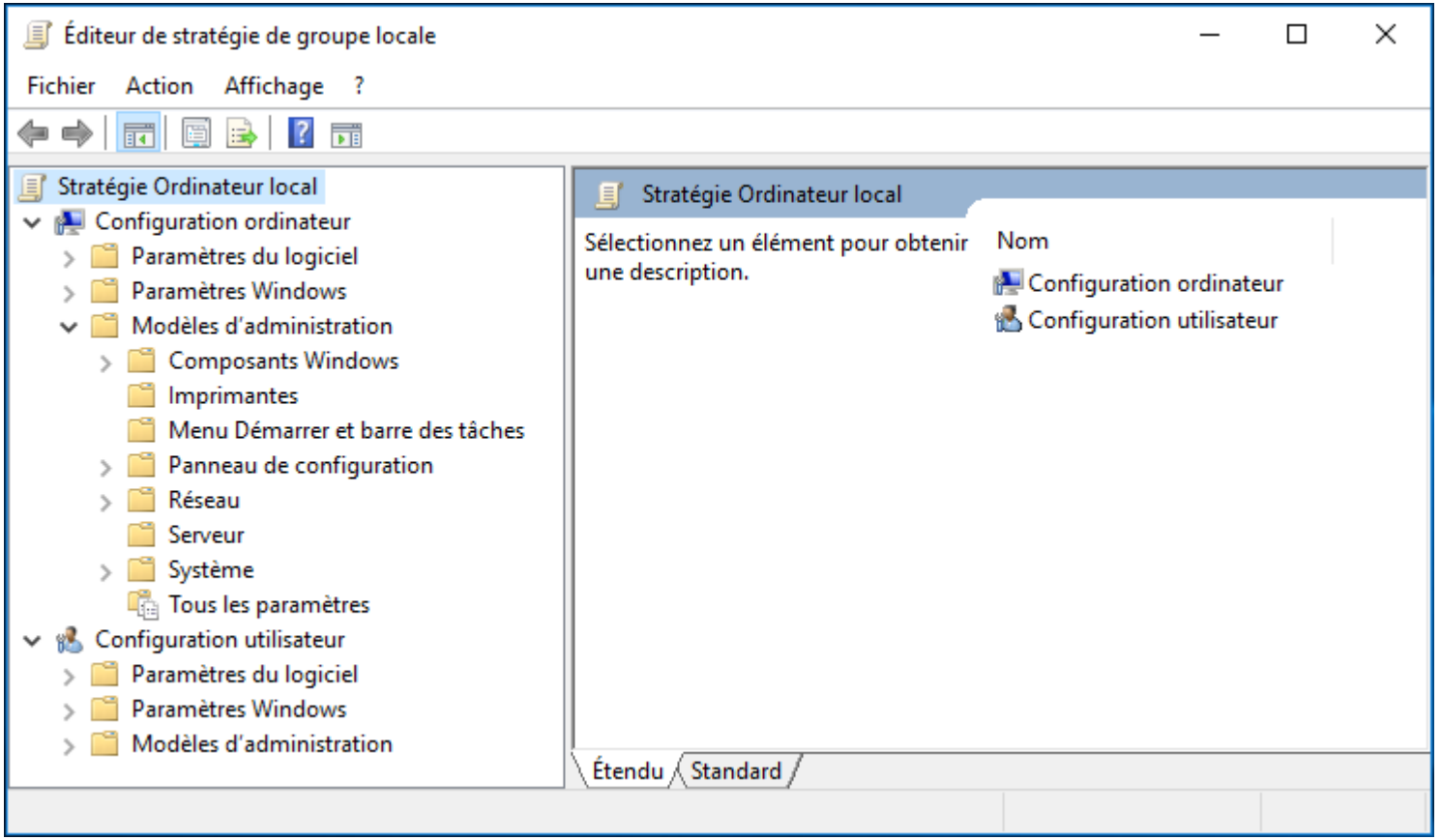
Par défaut, Non configuré affecté à la plupart des paramètres.

Modification d'un paramètre => Modification de la base de registre.

1 – GPO : Définition et notions de base

Stratégie locale

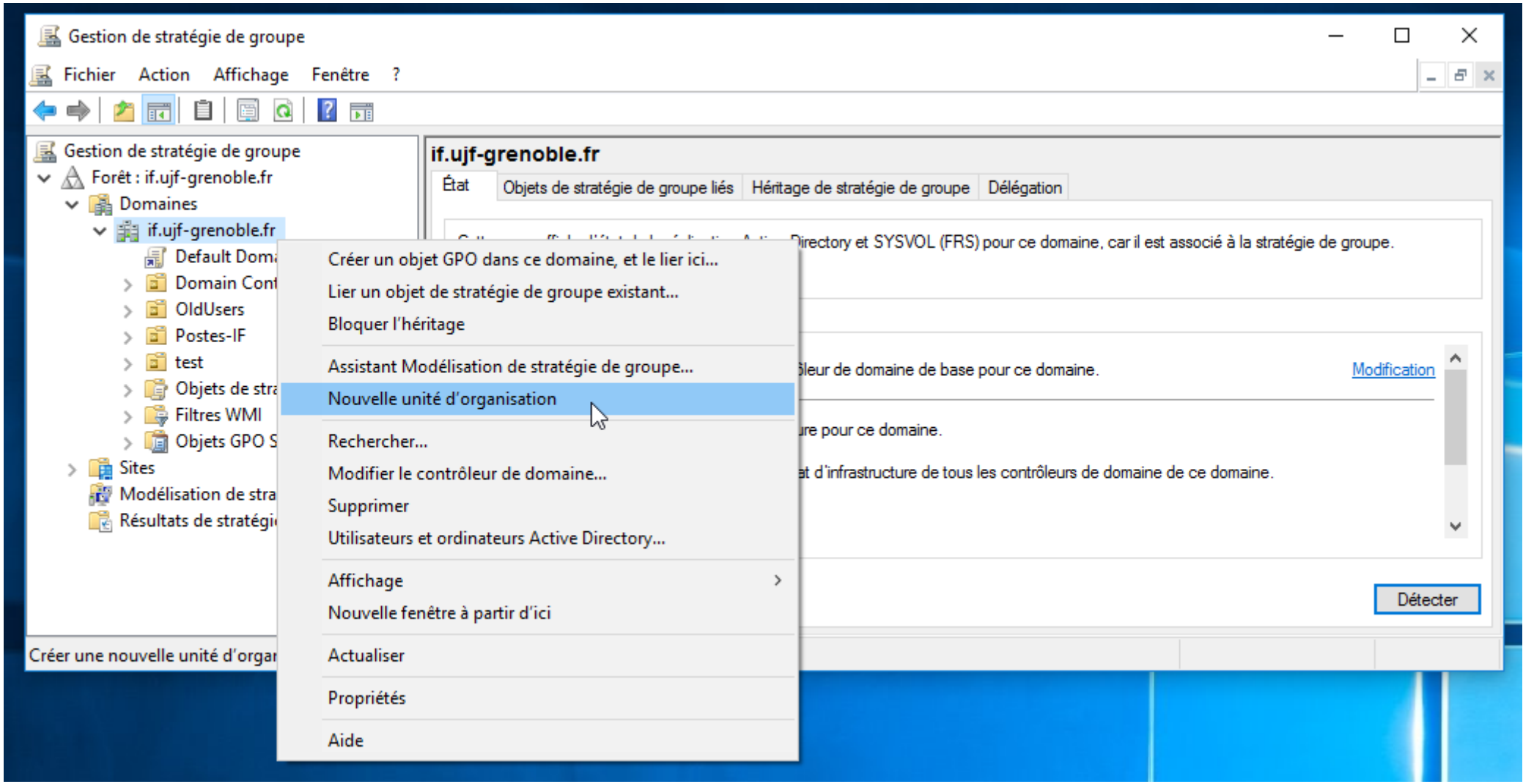
Démarrer / exécuter : **gpedit.msc**



1 – GPO : Définition et notions de base

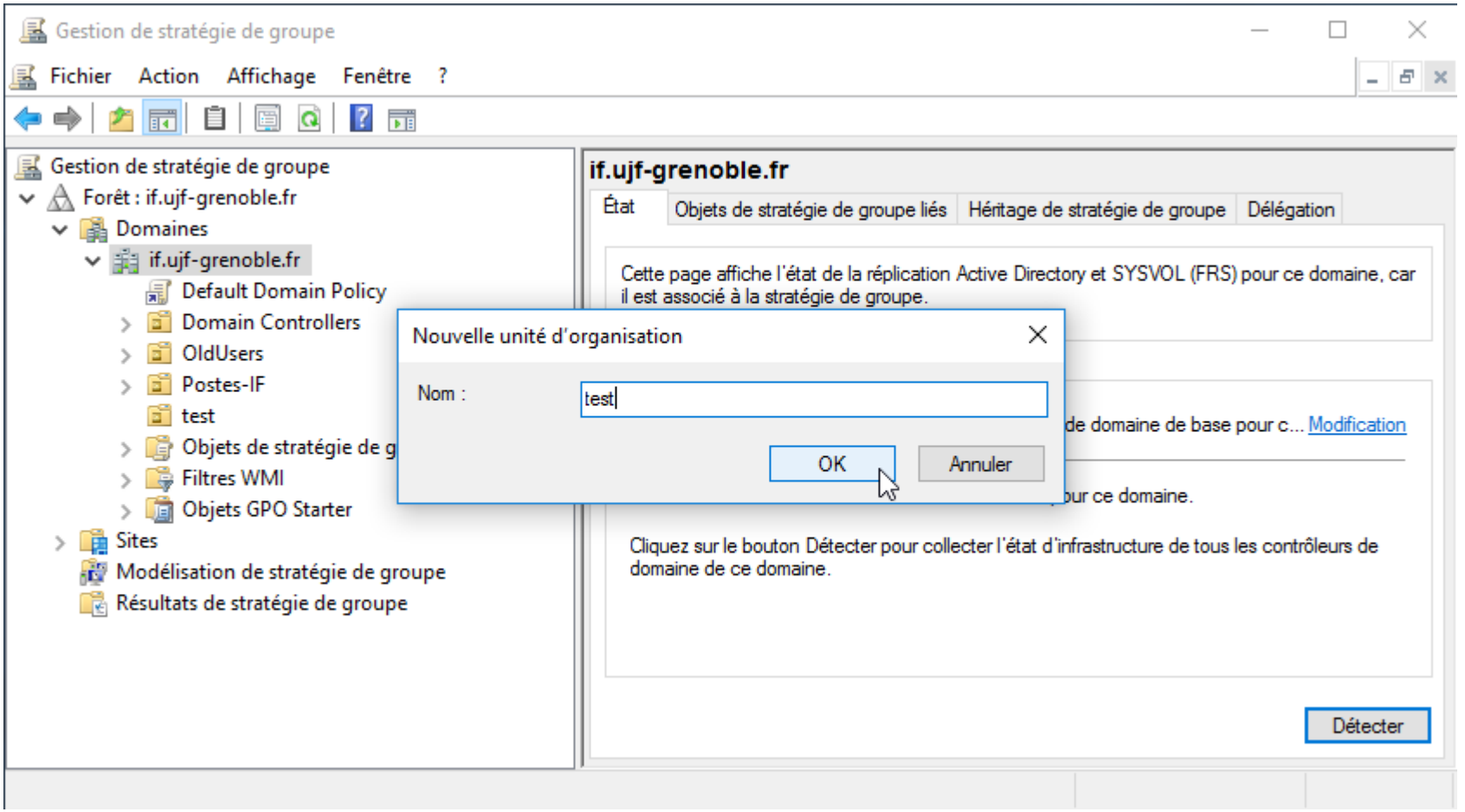
Stratégie du domaine

Depuis une console d'administration : Outils d'administration Windows / Gestion des stratégies de groupe



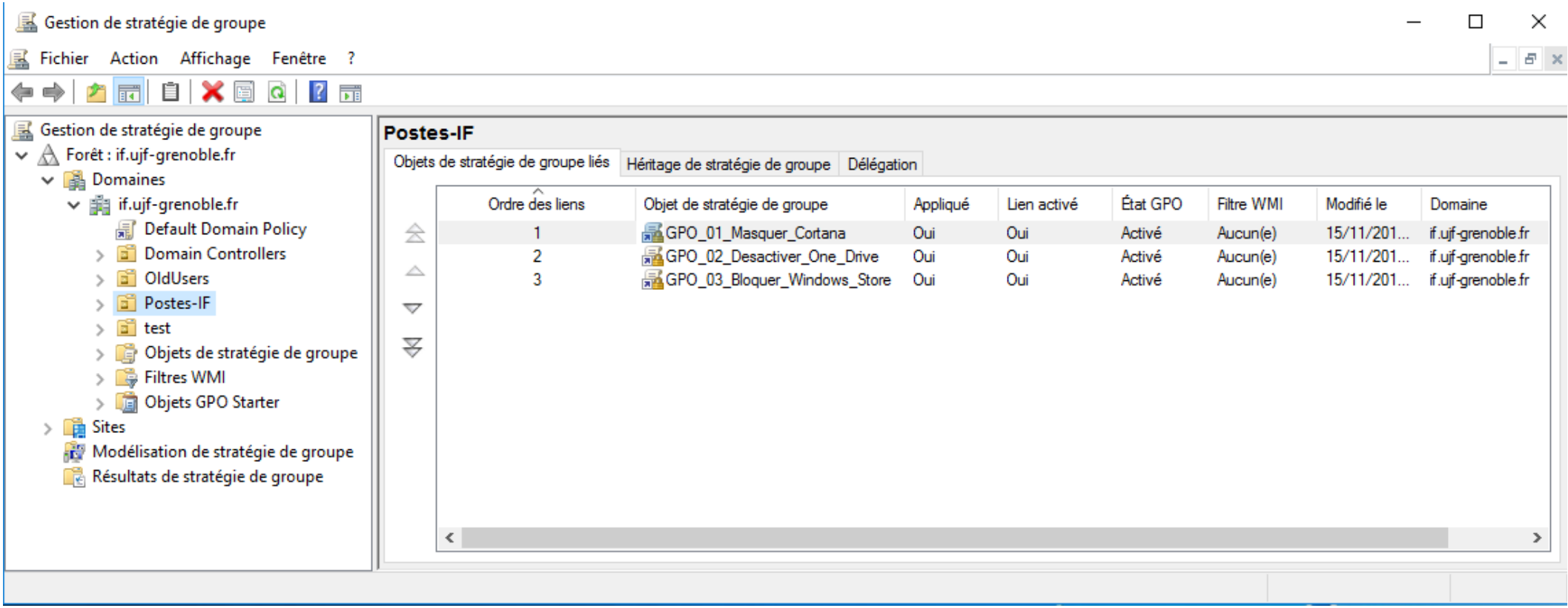
1 – GPO : Définition et notions de base

Stratégie du domaine



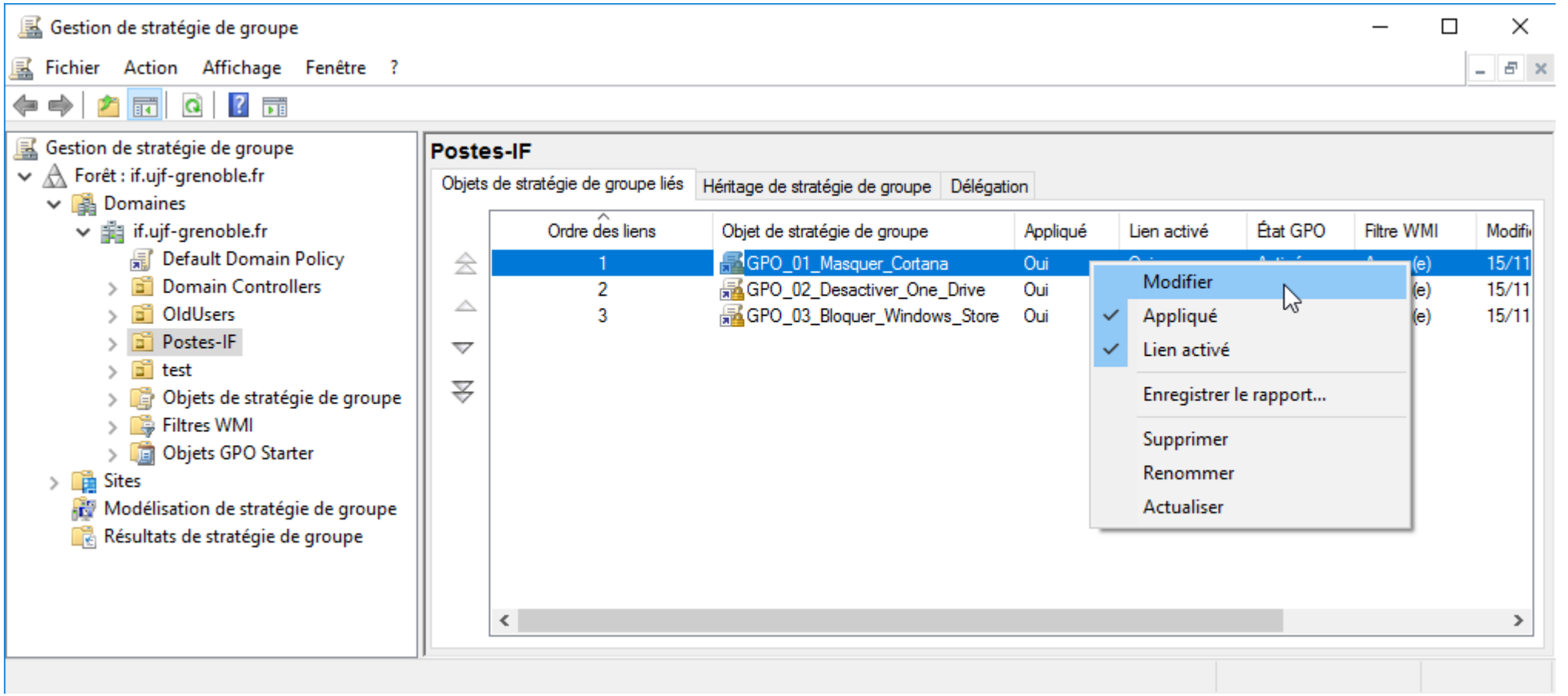
1 – GPO : Définition et notions de base

Stratégie du domaine



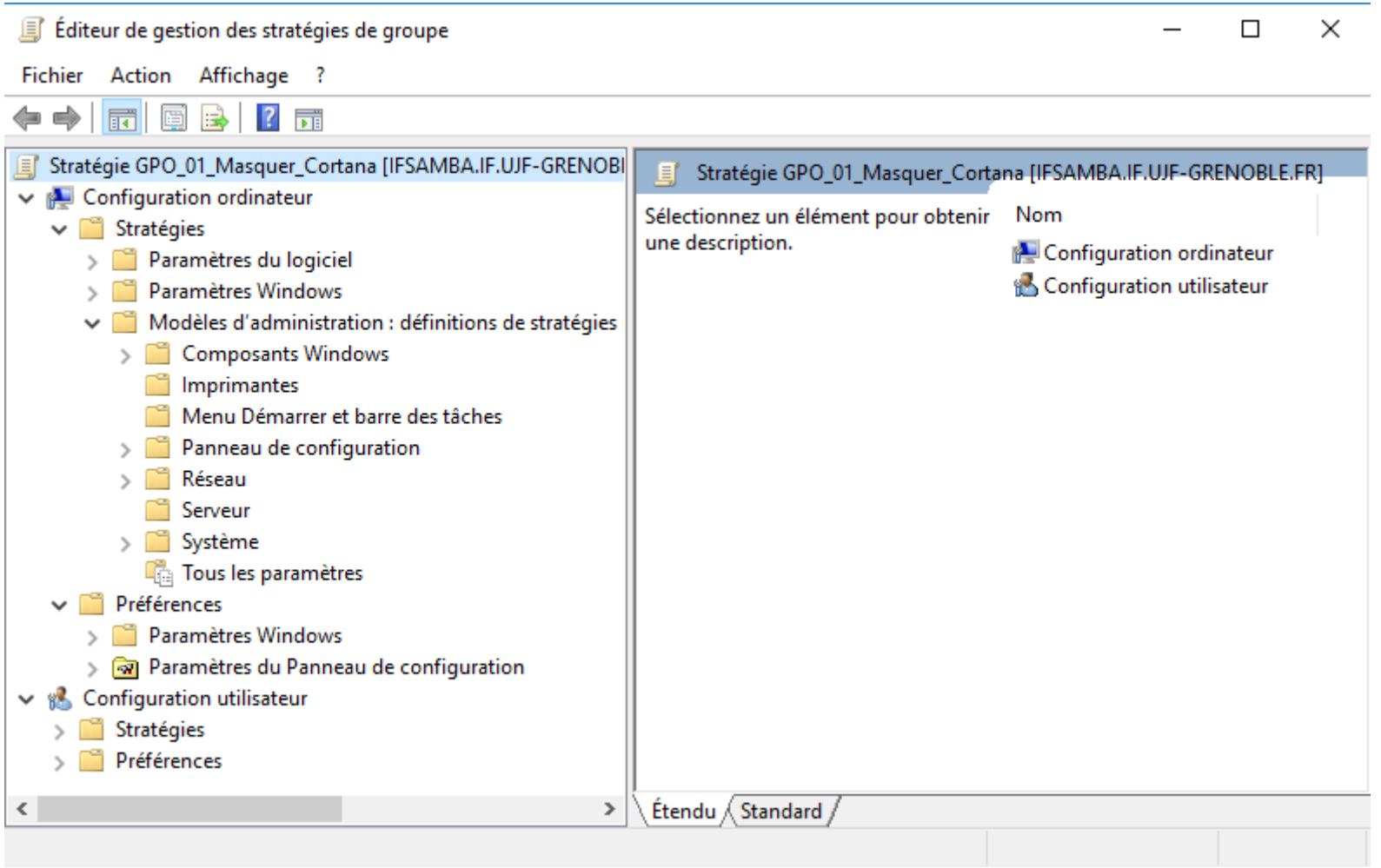
1 – GPO : Définition et notions de base

Stratégie du domaine



1 – GPO : Définition et notions de base

Stratégie du domaine



2 – Paramètres pour Win10

Win10

- Nouvelles fonctionnalités de collecte d'informations personnelles
- Envoi et usage des données chez Microsoft ou des tiers

La méthode d'installation rapide active par défaut ces fonctionnalités (Cortana - identifiant publicitaire...)

Contrat de Service Microsoft :

- Lorsque l'identifiant publicitaire est activé dans Windows 10 dans vos paramètres de confidentialité, **les applications Microsoft peuvent accéder et utiliser l'identifiant publicitaire** (de la même manière que les sites Web peuvent accéder et utiliser un identifiant unique stocké dans un cookie) **pour sélectionner et diffuser des annonces**.
- **Nous recueillons** des données sur les fonctionnalités que vous utilisez, les articles que vous achetez et les pages Web que vous visitez. Ces données incluent **vos requêtes ou commandes de recherche vocale et textuelle vers Bing, Cortana et nos robots de discussion**. Cela inclut également les paramètres que vous sélectionnez et les configurations logicielles que vous utilisez le plus.

2 – Paramètres pour Win10

Paramètre / fonctionnalité	Chemin d'accès – nom paramètre - valeur
Désactiver l'identifiant de publicité	Configuration ordinateur > Modèles d'administration > Système > Profils utilisateur > Désactiver l'identifiant de publicité => Activé
Désactiver le filtre SmartScreen	Configuration ordinateur > Modèles d'administration > Composants Windows > Microsoft Edge > Désactiver le filtre SmartScreen => Activé
Emplacement de cet appareil	Configuration ordinateur > Modèles d'administration > Composants Windows > Emplacement et capteurs > Désactiver l'emplacement. => Activé
Localisation	Configuration ordinateur > Modèles d'administration > Composants Windows > Confidentialité de l'application > Permettre aux applications Windows d'accéder à l'emplacement - Forcer le refus => Activé
Autoriser les applications à accéder à mon nom, à mon avatar et à d'autres informations sur le compte	Configuration ordinateur > Modèles d'administration > Composants Windows > Confidentialité de l'application > Permettre aux applications Windows d'accéder aux informations de compte - forcer le refus => Activé - Force Allow

2 – Paramètres pour Win10

Paramètre / fonctionnalité	Chemin d'accès – nom paramètre - valeur
Voix, entrée manuscrite et frappe - Arrêter de me connaître	Configuration ordinateur > Modèles d'administration > Panneau de configuration > Options régionales et linguistiques > Personnalisation de l'écriture manuscrite > Désactiver l'apprentissage automatique => Activé
Commentaires et diagnostic Windows demande à recevoir mes commentaires	Configuration de l'ordinateur > Modèles d'administration > Composants Windows > Collecte des données et versions d'aperçu > Ne pas afficher les notifications de commentaires. => Activé
Envoyer les données de l'appareil à Microsoft (télémétrie)	Configuration ordinateur > Modèles d'administration > Composants Windows > Collecte des données et versions d'aperçu > Autoriser la télémétrie => Activé Option 0 "Désactivé" [Enterprise uniquement] => nécessite une licence Win Enterprise ou Educ
Autoriser les applications à lire ou envoyer des e-mails	Configuration ordinateur > Modèles d'administration > Composants Windows > Confidentialité de l'application > Permettre aux applications Windows d'accéder aux e-mails => Forcer le refus => A partir de Win10 Pro build 1703

2 – Paramètres pour Win10

Paramètre / fonctionnalité	Chemin d'accès – nom paramètre - valeur
Autoriser les applications à utiliser ma caméra	Configuration ordinateur > Modèles d'administration > Composants Windows > Confidentialité de l'application > Permettre aux applications Windows d'accéder à la caméra => Forcer le refus
Autoriser les applications à utiliser mon microphone	Configuration ordinateur > Modèles d'administration > Composants Windows > Confidentialité de l'application > Permettre aux applications Windows d'accéder au microphone => Forcer le refus
Masquer Cortana	Configuration ordinateur > Modèles d'administration > Composants Windows > Rechercher > Autoriser Cortana => Désactivé
Bloquer OneDrive	Configuration ordinateur > Modèles d'administration > Composants Windows > OneDrive > Empêcher l'utilisation de OneDrive pour le stockage de fichiers => Activé

2 – Paramètres pour Win10

Paramètre / fonctionnalité	Chemin d'accès – nom paramètre - valeur
Bloquer le Windows Store	Configuration ordinateur > Modèles d'administration > Composants Windows > Windows Store > Désactiver l'application du Windows Store => Activé => nécessite licence Win Enterprise ou Educ

Contournement possible pour Win 10 Pro : établir une stratégie qui bloque l'exécution de certaines applications

Configuration d'ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégie de restriction logicielle > Au besoin click droit puis New - > Puis Règle supplémentaire > Click droit – Nouvelle règle de chemin d'accès > Dans le chemin d'accès :

%programfiles%\WindowsApps\Microsoft.WindowsStore*
Niveau de sécurité : non autorisé.
Rmq : il faut bien mettre * à la fin !

2 – Paramètres pour Win10

Beaucoup d’autres paramètres plus courants ou communs :

- Désactivation CMD utilisateur
- Désactivation REGEDIT utilisateur
- Désactivation Modification Proxy IE
- Configuration de Edge
- Gestion plus fine de Windows Update

…/… la liste est longue !

2 – Paramètres pour Win10

Remarques :

On cherche beaucoup - passe beaucoup de temps surtout pour la mise au point.

Pas de référence propre exhaustive et concise si ce n'est build par build
mais pas W7 / W10 Pro / W10 Educ

Grosse masse d'information **ET** diffuse

Préconisation : Licence Enterprise ou Educ !

Tarifs :

Win 10 Educ : 135 + 1,25 / mois => 210 pour 5 ans (groupe logiciel)
Win 10 Pro : 101 (marché Dell)

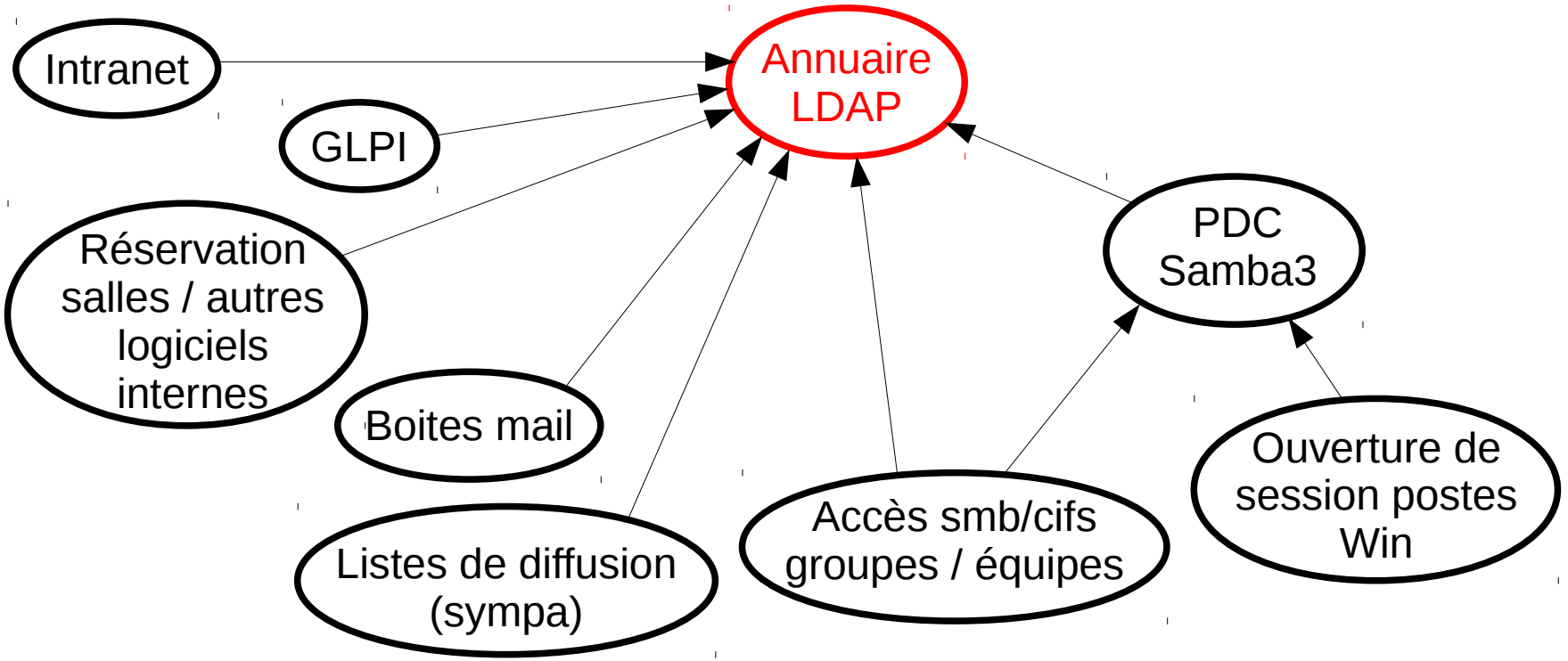
UGA prépare le déploiement Win 10 à priori en licence PRO
à partir d'un build particulier

3 – Migration Samba3 NT4-like vers AD

Situation historique

- Contrôleur de domaine Samba 3
- Utilise les Wins / noms netbios et un **annuaire ldap interne et maîtrisé**

Une source d'authentification unique pour la gestion des comptes, mots de passe pour tous les services du SI



3 – Migration Samba3 NT4-like vers AD

Situation historique

… qui peut perdurer dans le temps

Intégration d'un poste Win 7

* Modifier le registre : rendez-vous dans la clef suivante
HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters

Ajouter les valeurs suivantes (qui à priori n'existent pas):
DWORD DomainCompatibilityMode = 1
DWORD DNSNameResolutionRequired = 0

* Vérifier les clés suivantes spécifiées comme suit (valeurs par défaut) :
HKLM\System\CurrentControlSet\Services\Netlogon\Parameters
DWORD RequireSignOrSeal = 1
DWORD RequireStrongKey = 1

3 – Migration Samba3 NT4-like vers AD

Intégration d'un poste Win 10

- Mêmes clés à modifier que pour un Win 7
- Quelques ajouts : bloque l'accès au netlogon du PDC

  gpedit.msc

  Configuration ordinateur > Modèles d'administration > Réseau >
  Fournisseur réseau > Chemins d'accès UNC renforcés >
  Spécifier « Activé »
  Options - On ajoute un nouveau paramètre :
  - "Nom de la valeur", spécifier : \\my_srv_pdc\netlogon (ou *\netlogon)
  - "Valeur" : RequireMutualAuthentication=0, RequireIntegrity=0

L'intégration fonctionne toujours

+ On gère au moins une authentification du user
- On perd le bénéfice de la puissance des GPO

L'arrivée d'un Win 10 intrusif est peut être l'occasion de moderniser l'infra ?

3 – Migration Samba3 NT4-like vers AD

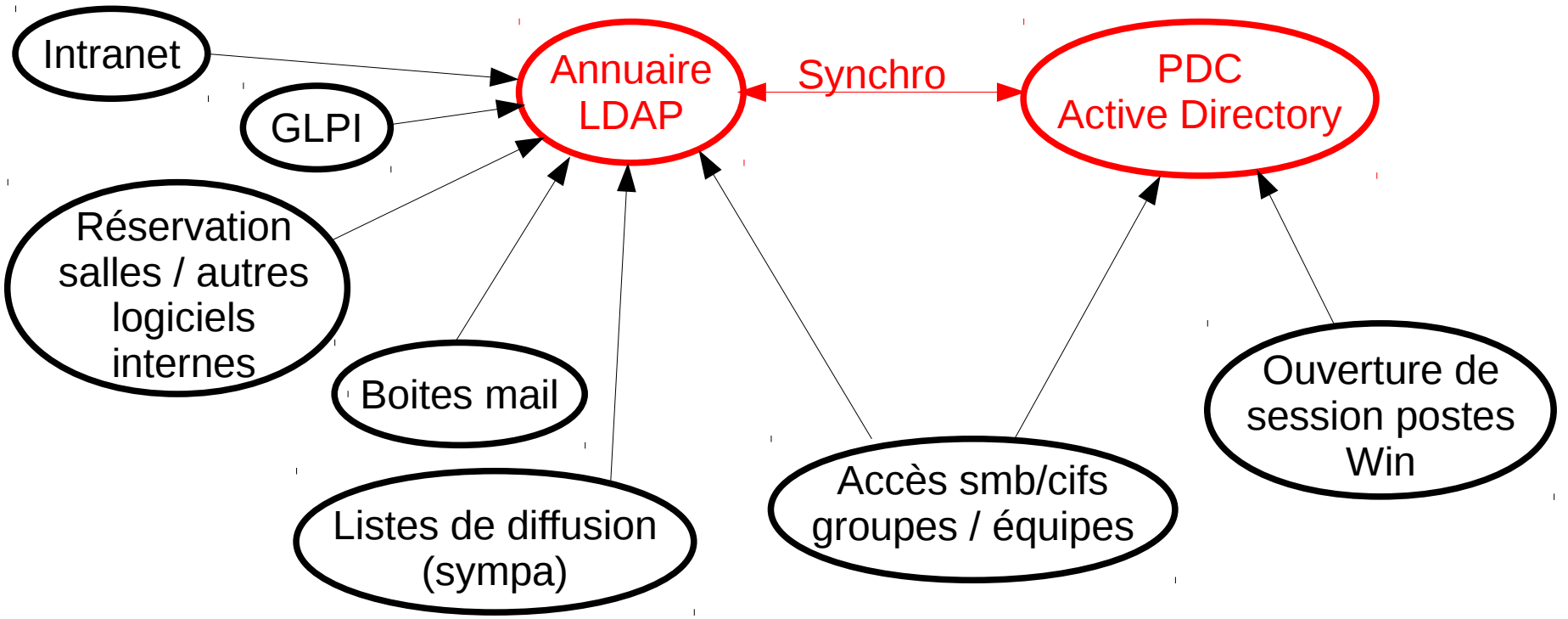
Mise en place d'un contrôleur de domaine AD

- **Ne peut pas déléguer l'authentification à une autre source.**
- Il doit lui même authentifier les utilisateurs, les accès, etc...

Implique :

- Instaurer une nouvelle source d'authentification dans le SI.
- Double gestion des comptes, des mots de passe, des groupes, dates de début et fin de contrats, dates d'expiration des mots de passe, etc...
- Établir une synchronisation entre la base LDAP et AD
- Définir le périmètre d'usage / utilisation de AD
  - Ouverture de session des postes clients
  - Un utilisateur peut se connecter aussi bien à des postes Win et Linux ?
  - Gestion des accès pour d'autres services du SI ?

3 – Migration Samba3 NT4-like vers AD



=> Une infrastructure qui se complique

3 – Migration Samba3 NT4-like vers AD

Deux technologies possibles

- Microsoft Active Directory
  Solution propriétaire- Win2012 ou Win2016 srv
- Contrôleur Samba4
  Basé sur LDAP – ldap intégré – **Schéma non extensible**
  Outil en mode commande : samba-tools
  Mode graphique : console RSAT depuis un poste Win client

Importance du DNS

Licences

- Microsoft Active Directory
  Srv : 200 + Cal client 5,76 par device ou user
  Cal client : pour la durée d'utilisation du serveur (environ 5 ans)
- Contrôleur Samba4
  Licence gratuites : 0

Quid du TCO ?

3 – Migration Samba3 NT4-like vers AD

Outils / modalités de synchronisation

- 389 Directory Server (anciennement Fedora Directory Services FDS)
  Possibilité d'interfacer AD avec 389 DS et 389 DS avec OpenLdap avec synchro bidirectionnelle des mots de passe
  => A actualiser / valider avec des contrôleurs récents ?

- Scripts personnalisés qui poussent le mdp dans AD et LDAP

- LSC-Project

  La principale difficulté réside dans la synchronisation du mot de passe utilisateur

Outils à évaluer ? Rex ?

- Solution Microsoft : ADFS (Active Directory Federation Services)
  Module d'interopérabilité entre Active Directory et une fédération d'identités permet d'authentifier des comptes stockés dans un annuaire LDAP v3

- Solution Microsoft : Microsoft Identity Manager un connecteur LDAP
  Connecteur LDAP qui gère **certaines fonctionnalités** de gestion des mots de passe avec AD - Serveur d'annuaire 389 - Apache Directory Server - IBM Tivoli DS - Open DS - OpenLDAP

3 – Migration Samba3 NT4-like vers AD

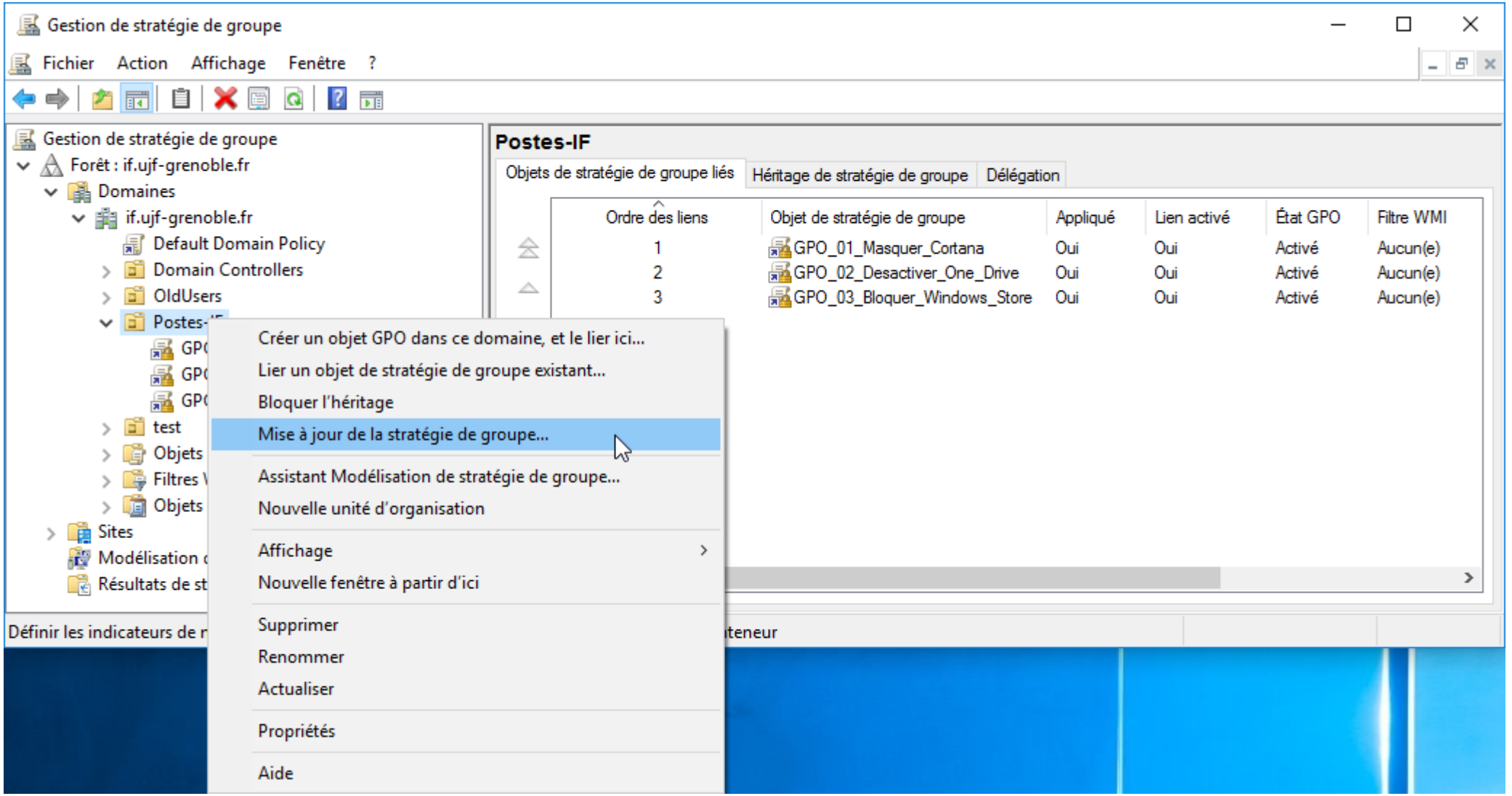
Migration des postes clients / profils utilisateurs

- 2h par poste (maxi). Impact utilisateur limité pour **UN** utilisateur
- Impact pour l'équipe info : x nb de postes
- Avec Samba migration de Samba3 à Samba4 one shot possible pour tout le parc ! Risque accru mais gain de temps énorme - Pas de possibilité de retour en arrière !
- Migration au fil de l'eau lors du renouvellement des postes

Questions ?

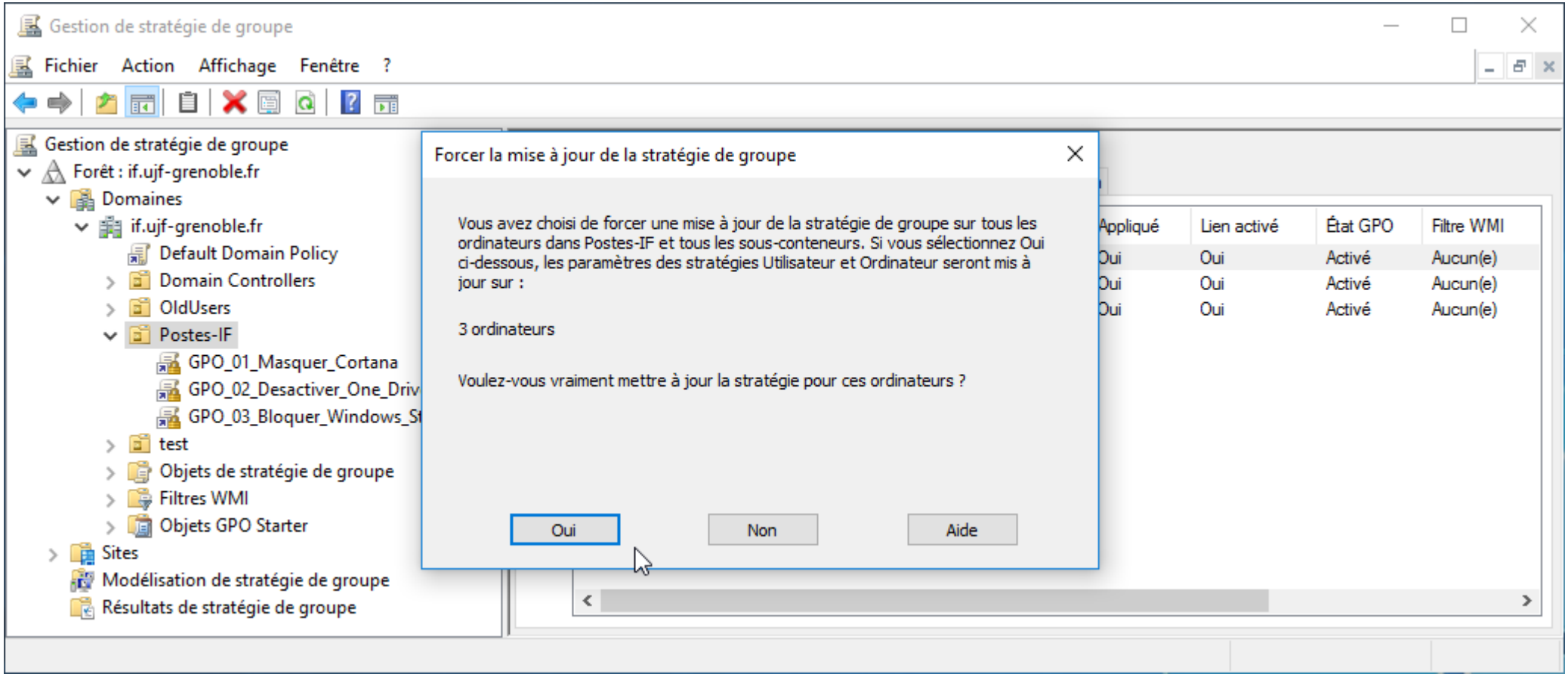
Compléments – GPO debug

Forcer l'application des GPO + debug



Compléments – GPO debug

Forcer l'application des GPO + debug



On obtient la liste poste par poste des messages d'erreur et de ce qui se passe.

Poste xxxx - Erreur 8007071a => il faut activer la licence !

Le serveur RPC n'est pas disponible

Compléments – Migration S3 S4 One shot

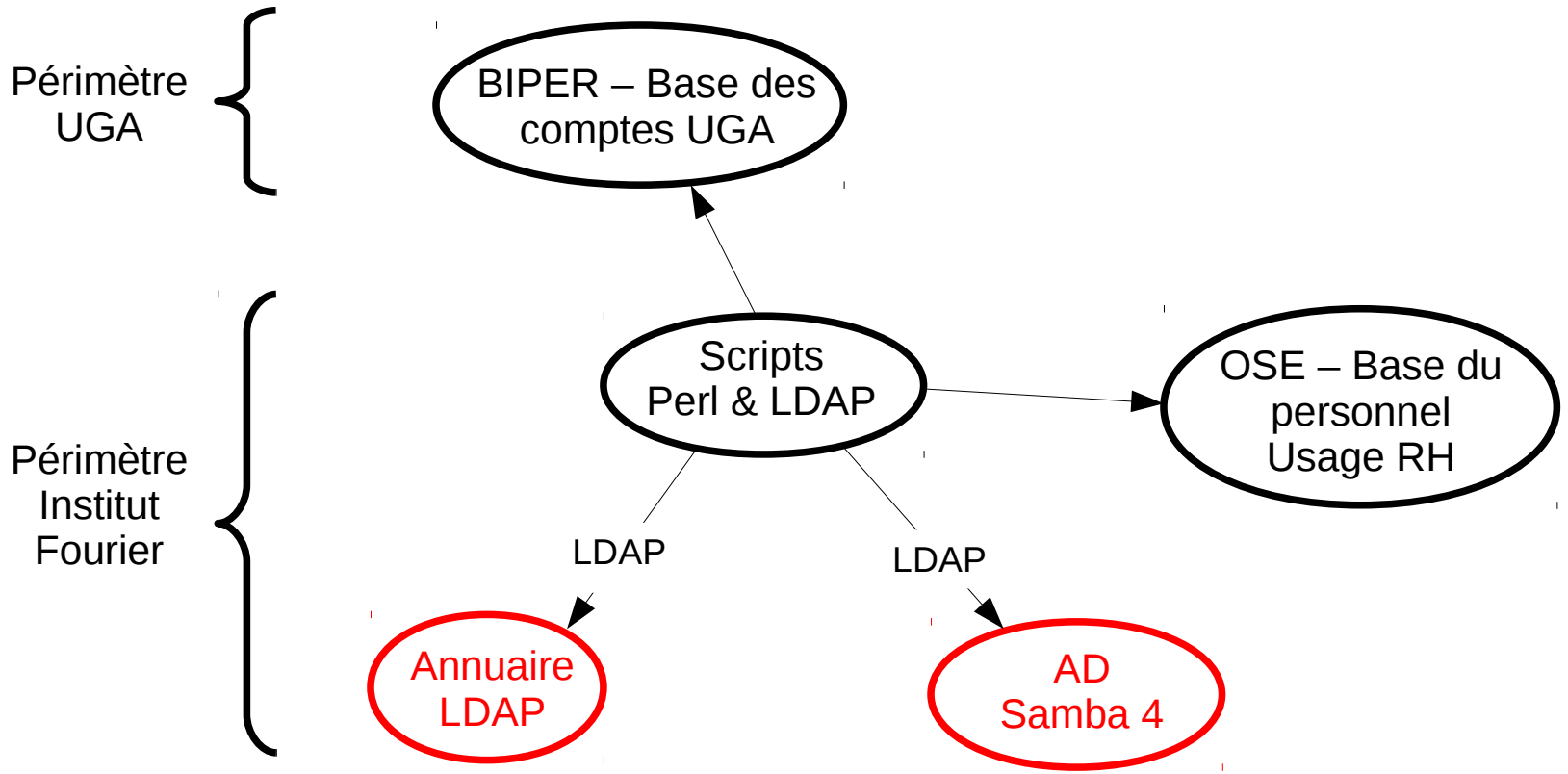
Migration de Samba3 à Samba4 one shot !

Migration réalisée à l'Institut de Physique et Chimie des Matériaux de Strasbourg
Unité CNRS / Université de Strasbourg

http://xstra.u-strasbg.fr/lib/exe/fetch.php?media=doc:2016-06-03-samba4.pdf

Présentation très détaillée

Compléments – IF : Gestion des comptes

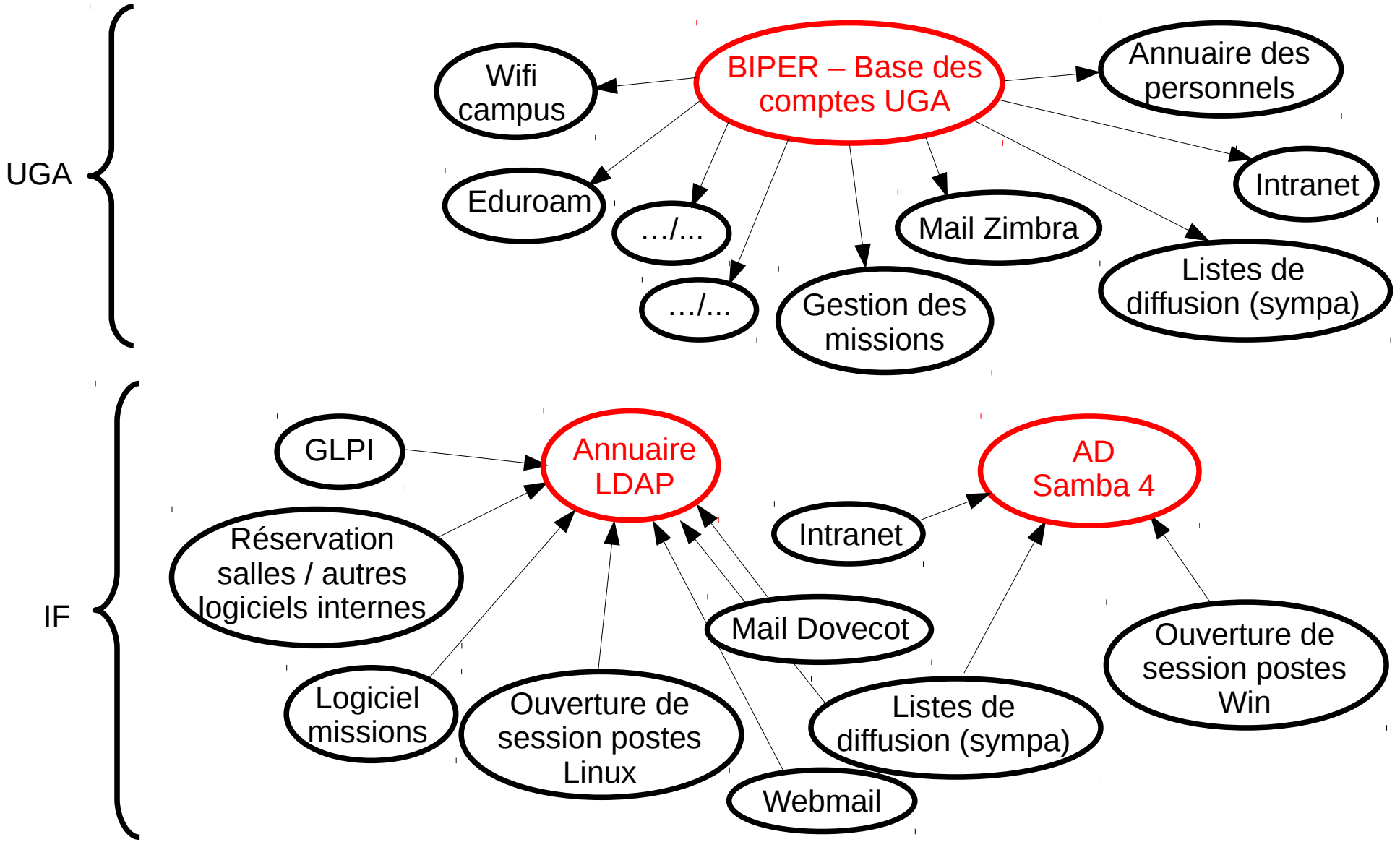


Pas de synchro des mots de passe

Difficultés pour faire correspondre les uidnumber

Dates d'expiration des comptes et mots de passe qui ne sont pas forcément strictement identiques entre base LDAP et AD S4

Compléments – IF : Périmètres des services



Un utilisateur parfois un peu perdu...