JEOLE 2016

Active Directory aux MEEM/MLHD

Emmanuel Ihry

Pole National d'Expertise

Serveurs et Réseaux

MINISTÈRE DE L'ENVIRONNEMENT,
DE L'ÉNERGIE ET DE LA MER
www.developpement-durable.gouv.fr

MINISTÈRE DU LOGEMENT,
ET DE L'HABITAT DURABLE
www.logement.gouv.fr

Contexte global du projet

- Une architecture bureautique en fin de vie
  - fonctionnant en mode NT
  - dysfonctionnements avec des équipements récents
- Volonté de la DSI de déployer au plus tôt la technologie Active Directory et grande attente des services
  - **Samba 4 est privilégié sauf à démontrer une impossibilité technique**
- Projet piloté par le PNE Serveurs et Réseaux:
  - Volets technique / fonctionnel / accompagnement

Principaux besoins services

Disposer d'une solution :

- qui fonctionne bien et tout le temps !
- qui permette l'utilisation de tout type de serveurs et services (serveurs Windows, watchdoc, tout type d'imprimante..)
- qui permette de déployer des GPO locales
- qui permette de partager des ressources entre services distincts
- qui leur laisse l'autonomie de gestion suffisante pour prendre en charge les tâches quotidiennes inhérentes à l'infrastructure bureautique sur leur périmètre
  - **Ne sont pas forcément attachés à leur rôle d'administrateur du domaine**
  - **Ne sont pas à priori opposés à la mise en place d'une forêt mono-domaine à conditions que les droits de gestions soient encadrés**

Principales attentes nationales

- Accompagner l'avancée technique d'un bond fonctionnel
  - partages inter services
  - faciliter la mobilité
- ***Dans la mesure du possible***, le système doit être évolutif pour s’adapter à des restructurations de services
- Mettre en place une architecture uniforme - cadre national
  - comptes injectés depuis le LDAP national / Schéma AD unique…
  - condition pour bénéficier d'un support national
- Ne pas reconduire les problèmes liés à l'architecture actuelle :
  - relations d’approbation / mode local / changement de mot de passe

Exigences de sécurité

Respecter les exigences de sécurité inhérentes à la technologie AD

- Préconisations ANSSI
- Limiter les pouvoirs des comptes aux seuls besoins
- Faciliter le déploiement de règles de sécurité nationales
- Sécurité physique des contrôleurs de domaine
- Sécurité des sauvegardes
- Limitation de l’utilisation du compte « administrateur du domaine »
- Prendre en compte les différences actuelles des services dans la conception de la solution (sécurité d'accès au réseau..)

Analyse des domaines bureautiques

- Actuellement 188 domaines bureautiques dont
  - **MEEM/MLHD 61**
    - **Après fusion des régions, reste 46 domaines**
  - **DDI 95**
  - Hors périmètre
    - Cerema 11 → migration vers Windows AD
    - VNF 5 → migration vers Windows AD
    - Divers en cours de suppression

Analyse relations d'approbation existantes périmètre MEEM et DDT

- 79 relations d'approbation **identifiées** entre domaines, **cependant** :
  - **La majorité va disparaître naturellement, resterait à traiter :**
    - **3 entre services du MEEM**
    - **cas des écoles administratif / stagiaires**
    - 2 entre DDT et Service du MEEM
    - 3 entre DDI
    - 1 entre DDI et DRAAF

→ **Attention au réflexe consistant à reconduire l'existant !!**

→ **Faire autrement pour partager certaines ressources ?**

sites MEEM/MLHD et population

- AC : 1 site regroupant environ 5000 personnes
- Services Déconcentrés : 499 sites regroupant environ 12500 personnes
  - **33 sites de plus de 100 personnes**
  - 20 sites de 50 à moins de 100 personnes
  - 68 sites de 20 à moins de 50 personnes

→ recommandations ANSSI : un ensemble de 33 contrôleurs pourrait être suffisant en cas de foret mono-domaine !!

Lien avec l'architecture du RIE

- « Étanchéité » entre certaines VRF
- Une logique de positionner les ressources nationales ou interministérielles en Data center :
  - Vers un partage de ressources fichiers entre communautés positionnées en Data Center ?
  - **les relations d'approbation entre certaines communautés n'ont pas forcément de raison d'être**
- Deux solutions distinctes doivent être proposées pour réponde à ces deux cas :
  - Partages au sein d'une communauté
  - Partages entre communautés

Étude en cours : expertise AD

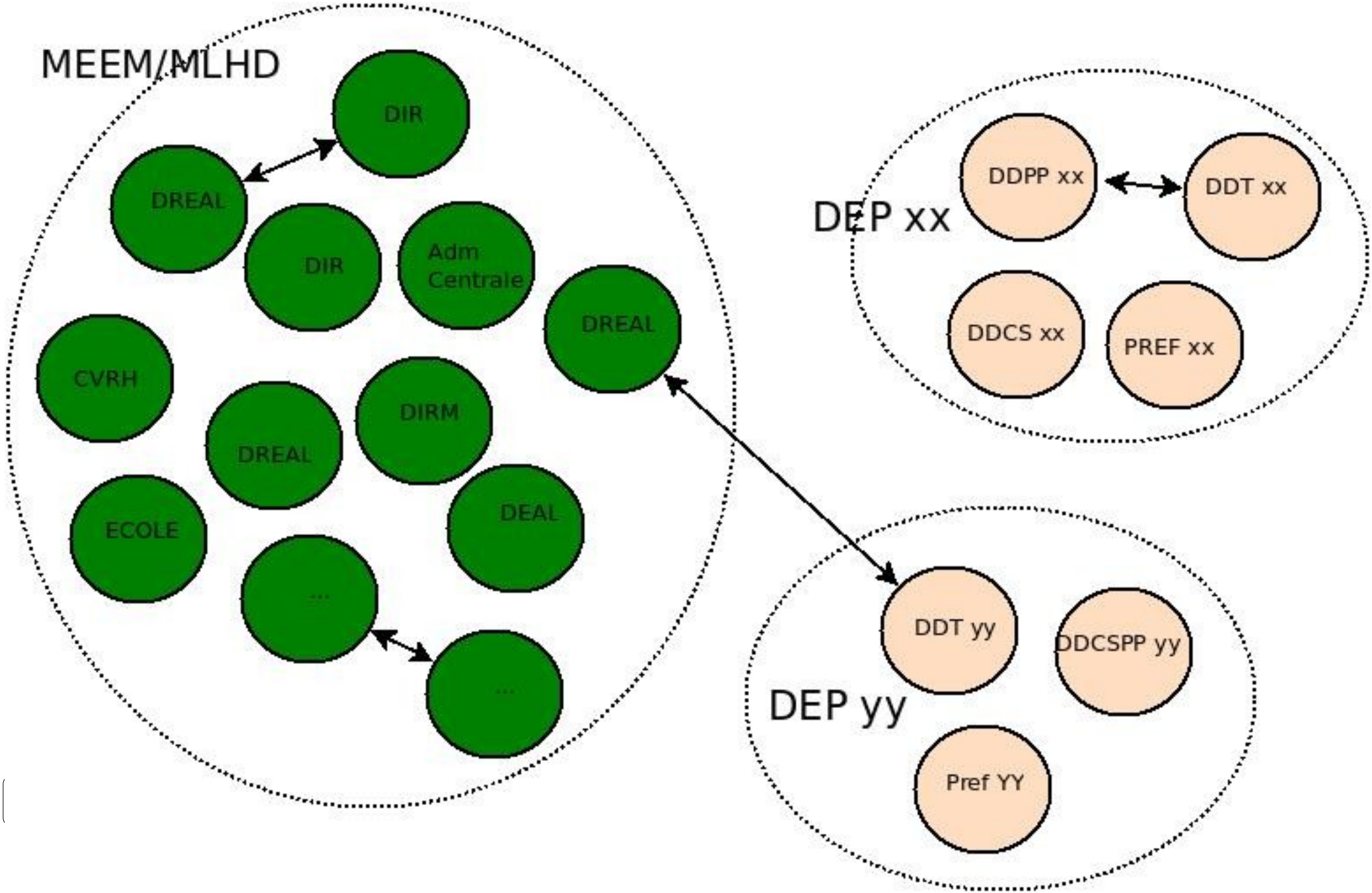
- Phase 1 : prise de connaissance
- **Phase 2 (en cours) : architecture idéale Active Directory**
  - Structuration de l'Active Directory optimale selon les règles de l'art actuelles et tenant compte du contexte
  - Stratégie pour l'administration des serveurs
  - Architectures bureautiques types pour des types de services
  - GPO minimales à mettre en place
  - Processus de déploiement
- Phase 3
  - Adapter la stratégie à l'environnement SAMBA 4
- Phase 4
  - Identifier des solutions d'interfaçage avec l'annuaire LDAP central

Structuration de l’AD
architecture et périmètre de l'étude

Le périmètre de l'étude pour la structuration de l'AD

- Étude de l'architecture AD pour les besoins du MEEM/MLHD
- Étude séparée pour les DDI, projet porté par la DINSIC en cours
- Pas de relations d'approbations entre MEEM et DDI
- Alimentation des comptes (et groupes?) depuis le LDAP

Périmètre de l'étude



Forets / Domaines 1/2

- Avantages / inconvénients Mono forêt avec un seul Domaine
  - Facilité de gestion
  - Facilité de mobilité et de collaboration
  - Une erreur est répliquée partout
  - Nécessaire de bien séparer les droits
- Avantages / inconvénients Mono forêt plusieurs Domaines
  - Seuls les comptes du domaine sont présents sur le DC
  - Facilité de mobilité et de collaboration (Relation d'approbation implicite)
  - Problème de perméabilité des droits admins
  - Duplication de certaines tâches d'administration
  - N'est plus recommandé par Microsoft
  - N'est pas supporté par Samba4

Forets / Domaines 2/2

- Avantages / inconvénients plusieurs « forêt mono Domaine »
  - séparation des droits admins
  - isolation des problèmes / erreurs
  - duplication de certaines tâches d'administration
  - Ne répond pas aux besoins de partages et de mobilité

- Scénarios à l'étude
  - Une mono foret mono-domaine
  - Plusieurs forets mono-domaine

Gestion AD : Qui / Quels outils ?

- Taches d’administration AD quotidienne
  - Gestion des utilisateurs (création / modification / suppression)
  - Création de comptes machine et jonction des ordinateurs au domaine
  - Gestion des postes locaux
  - Gestions de GPO locales
  - Création des ressources bureautiques
- Taches d’administration AD technique
  - mise en place de la VM (installation OS, configuration IP, configuration FTP, etc.)
  - connexion entre Amédée et les contrôleurs AD
  - maintenance technique des contrôleurs AD :
    - jonction d'un nouveau contrôleur de domaine,
    - gestion des sites / rôles FSMO ;
    - gestion des sauvegardes

Samba4

- principaux moins de SaMBa4-AD
  - absence des relations d’approbation inter-forêt2
  - absence de RODC3
  - aucun exemple d’un réseau SaMBa4-AD d’ampleur équivalente
  - coût des évolutions nécessaires pour les ministères : 6000 heures
    - Support 100k objects (inclus les améliorations sur la réplication) : ~1320 h
    - Support trusted domains : ~960 h
    - High load support in Samba AD DC (dont le multi Threading) : ~600.00 h
    - Windows 2012 functional level support : ~480 h
    - Tooling improvements (Outils de réplications) : ~180 h
    - Logon Audit logging : ~180h

Architecture optimale

- Concentrer les domaines
  - **aller (progressivement?) vers un (?) seul domaine**
- Définir quelles applications seront utilisées pour la gestion de l'AD
  - Gestion l'unicité de gestion des comptes
  - Faut il conserver des données bureautiques dans le LDAP ?
  - extensions Amédée ? autre outil ? autre application ?
- Déterminer le nombre de contrôleurs et positionnement
- Nécessite évolutions techniques et organisationnelles
  - mise en place des délégations de droits efficaces
  - nécessité d'homogénéiser les niveaux de sécurité
  - nécessité d'homogénéiser les procédures

Architecture technique

- Maquette opérationnel EOLE AD alimentée en temps réel depuis le LDAP (30 000 comptes)
- Module EOLE AD à finaliser
  - Quelle version SAMBA utiliser ?
  - Adaptation des droits de gestion aux contraintes liées à la sécurité
    - Qui administre ces serveurs ?
  - Mise en place d'un mécanisme d’interception du changement de mot de passe par CTRL ALT SUP ?

FIN

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ENVIRONNEMENT,
DE L'ÉNERGIE ET DE LA MER
www.developpement-durable.gouv.fr

MINISTÈRE DU LOGEMENT,
ET DE L'HABITAT DURABLE
www.logement.gouv.fr