JEOLE 2017

Active Directory

aux

Ministère de la Transition écologique et solidaire (MTES)

Ministère de la Cohésion des territoires (MCT)

Pole National d'Expertise Serveurs et Réseaux

Emmanuel Ihry / Michel Bally

Le Pole National d'Expertise Serveurs et Réseaux

Une équipe de maîtrise d’œuvre, d'assistance et d’accompagnement

- 12 agents (Nantes / Lyon)
- Périmètre d'intervention :
  - Services dépendants des MTES/MCT
  - Directions départementales interministérielles
    - DDT (historique)
    - DDPP, DDCSPP (ouverture progressive)

Le Pole National d'Expertise Serveurs et Réseaux

Missions périmètre serveurs :

- MOE technique EOLE
  - partenariat avec le Pôle EOLE
  - contribution à certains développements
  - participation aux SPRINTS
  - gestion de l'infrastructure nationale (Zéphir, miroirs..)
- MOE Accompagnement des services informatiques
  - Pilotage technique national
  - Assistance de niveau 3
  - Animation de formations

PNE Serveurs et Réseaux

Missions périmètre réseaux:

- Plan d'adressage national / gestion technique des liens RIE
- Traitement des problématiques de flux : interministériels, inter VRF, internet…
- Gestion technique système national de visio-conférence
- Production de recommandations d’architectures réseaux
- Suivi technique de la plate-forme d'accès à Internet
- Études préalables à la mise en place de pare-feux
- Assistance de niveau 3 : configuration switch, expertise réseau
- Animation de formations
- ...

Contexte EOLE

2786 serveurs EOLE installés

- Modules génériques : Zephir / amon (eSSL)
- Modules spécifiques basés sur le SCRIBE :
  - eCDL contrôleurs de domaines (NT)
  - eSBL serveurs de fichiers / appli Web / Geomatique

ZEPHIR	AMON	eCDL	eSBL
4	339	602	1841

Version des serveurs :

- 75 % des serveurs en v2.5 ou supérieure
- Un objectif de 100 % du parc en version supportée à fin juin 2017
  - **Enjeu important en matière de sécurité**

V2.3	V2.4	V2.5	V2.6
527	48	2193	14

Projet Active Directory

Extrait de la présentation JEOLE 2016 :

- Volonté de la DSI de déployer au plus tôt la technologie Active Directory
  - architecture bureautique en fin de vie : mode NT
  - grande attente des services
- Expertise AD réalisée mi 2016
  - Identification d'une architecture idéale Active Directory
    - Etat de l'art
  - Capacité de déployer cette architecture avec samba 4
  - Adapter si besoin la stratégie à l’environnement SAMBA 4

Exigences

- Respecter les exigences de sécurité inhérentes à la technologie AD
  - Préconisations ANSSI
  - Limiter les pouvoirs des comptes aux seuls besoins
    - Restrictions sur compte « administrateur du domaine »
  - Faciliter le déploiement de règles de sécurité nationales
  - Sécurité physique des contrôleurs de domaine
  - Sécurité des sauvegardes
- S'interopérer avec l'existant :
  - Ldap national
  - Architecture des services (sécurité d'accès au réseau..)

Conclusions de l'expertise

- Décision du ministère d'une architecture AD / SAMBA4
- Le nouveau module EOLE SETH sera utilisé
- Architecture « idéale » = 2 forêts mono-domaine
  - forêt pour l'administration centrale (AC)
  - forêt pour les services déconcentrés (SD)
- Mais déploiement d'une architecture intermédiaire
  - maintien dans un premier temps d'une forêt par SD
  - contrainte par les limites actuelles de samba 4
  - effort « minimal » pour le déploiement initial
- Architecture technique prenant en compte les exigences de sécurité

Le déploiement de la solution

Contexte sites pilotes
architecture
outils de gestion
migration

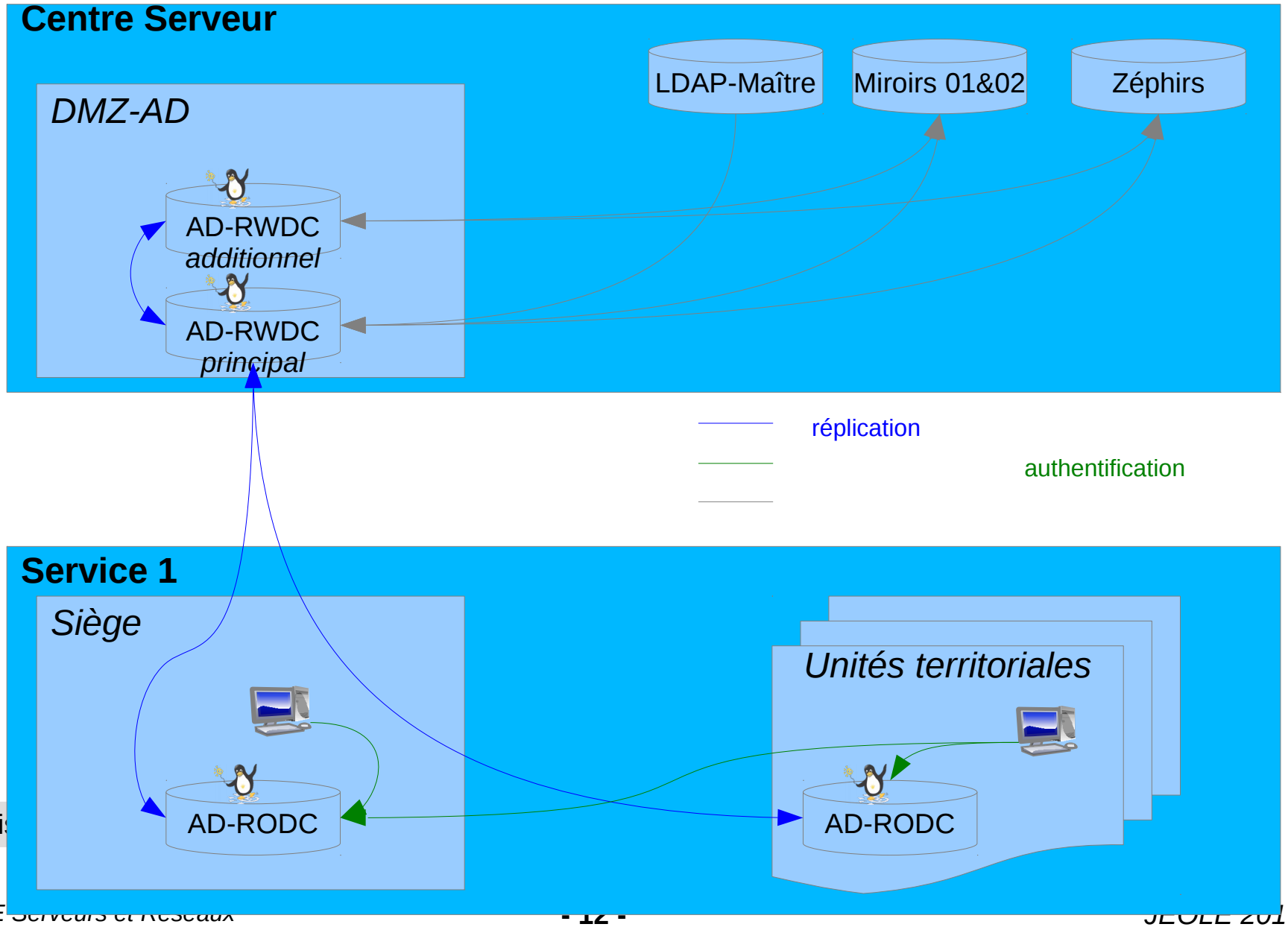
Présentation du projet

- 5 sites pilotes dont une DDT
- Déploiement des sites avec la version 2.6.1 et samba >=4.6
- Formation des sites pilotes réalisée en avril et mai
- Déploiement de l'infrastructure nationale en cours de finalisation
- Début de mise en production pour quelques sites avant fin juin

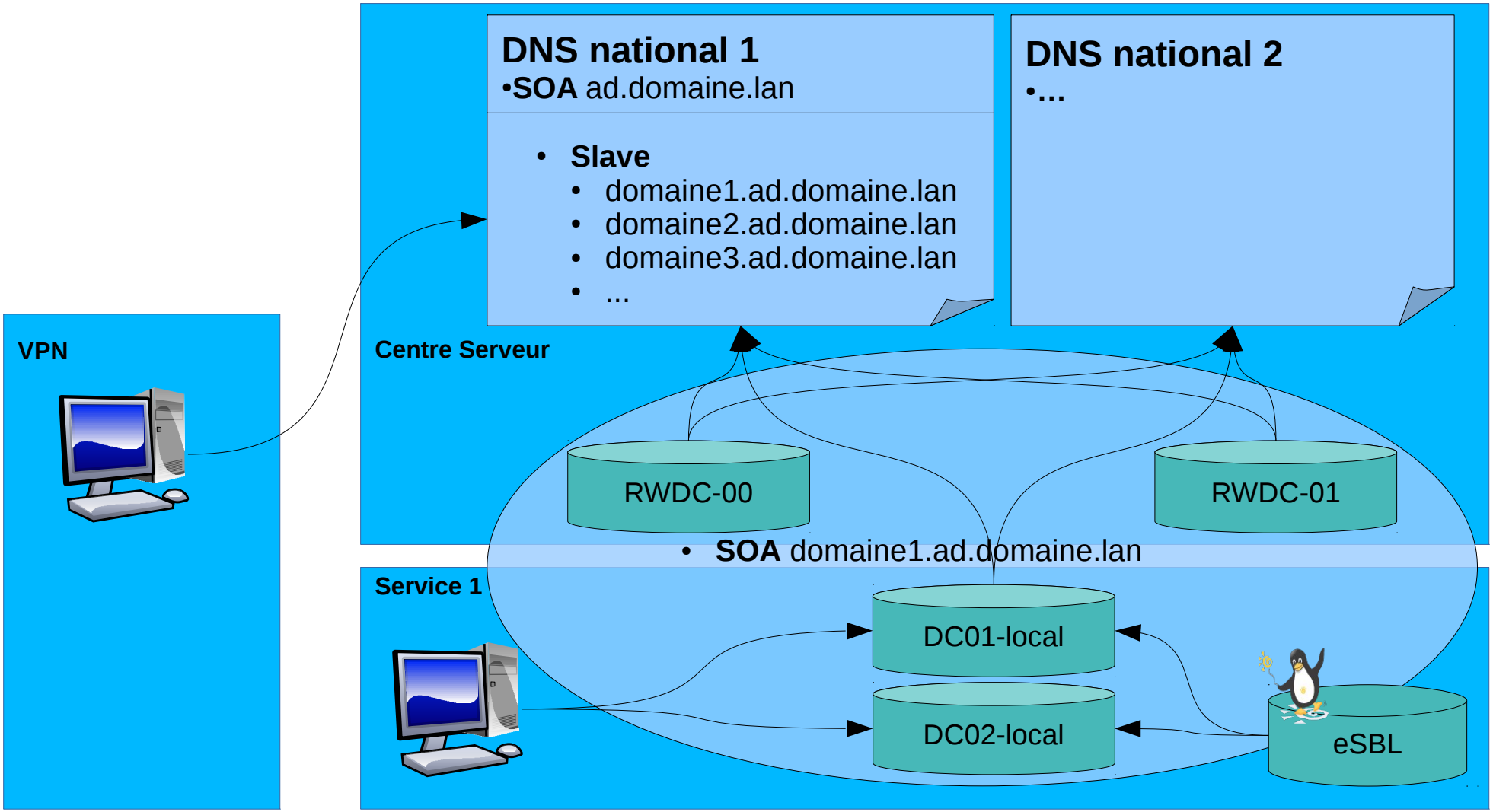
L'architecture cible

- Des contrôleurs EOLE SETH - Active Directory-Samba4
  - Des serveurs principal et secondaire (RWDC) : **remplacent les eCDL**
    - Hébergement Centre Serveur
    - Gestion par une équipe nationale
    - Alimentation des comptes USER en mode synchrone depuis le LDAP national
- Dans les services, déploiement exclusif de serveurs RODC
  - Hébergement local
  - Gestion par les services informatiques locaux
- Des serveurs bureautique intégrés à l'AD de type
  - eSBL
  - Seth en mode « serveur membre »
  - Serveurs membres Windows le cas échéant

L'architecture cible

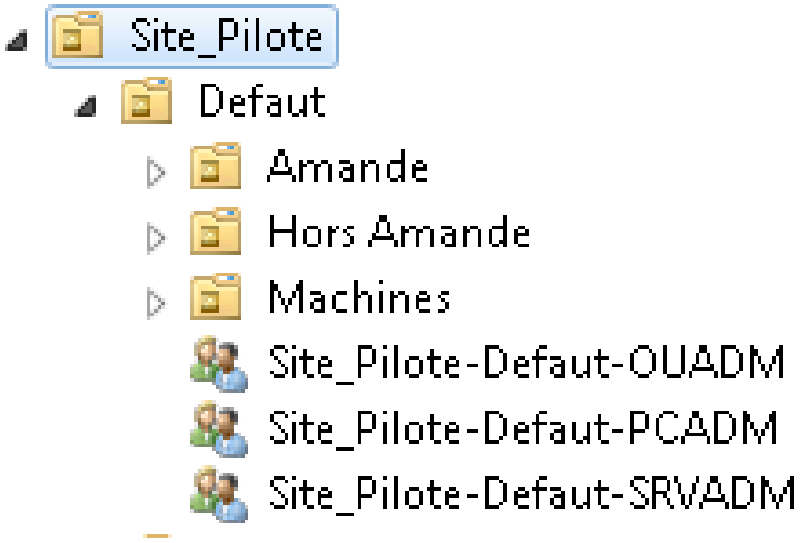


DNS


DNS national 1
•SOA ad.domaine.lan
• Slave
• domaine1.ad.domaine.lan
• domaine2.ad.domaine.lan
• domaine3.ad.domaine.lan
• ...
DNS national 2
•...
VPN
Centre Serveur
RWDC-00
RWDC-01
• SOA domaine1.ad.domaine.lan
Service 1
DC01-local
DC02-local
eSBL

La structuration de l'AD

- Chaque domaine est structuré en OU
  - des groupes pour administrer les objets



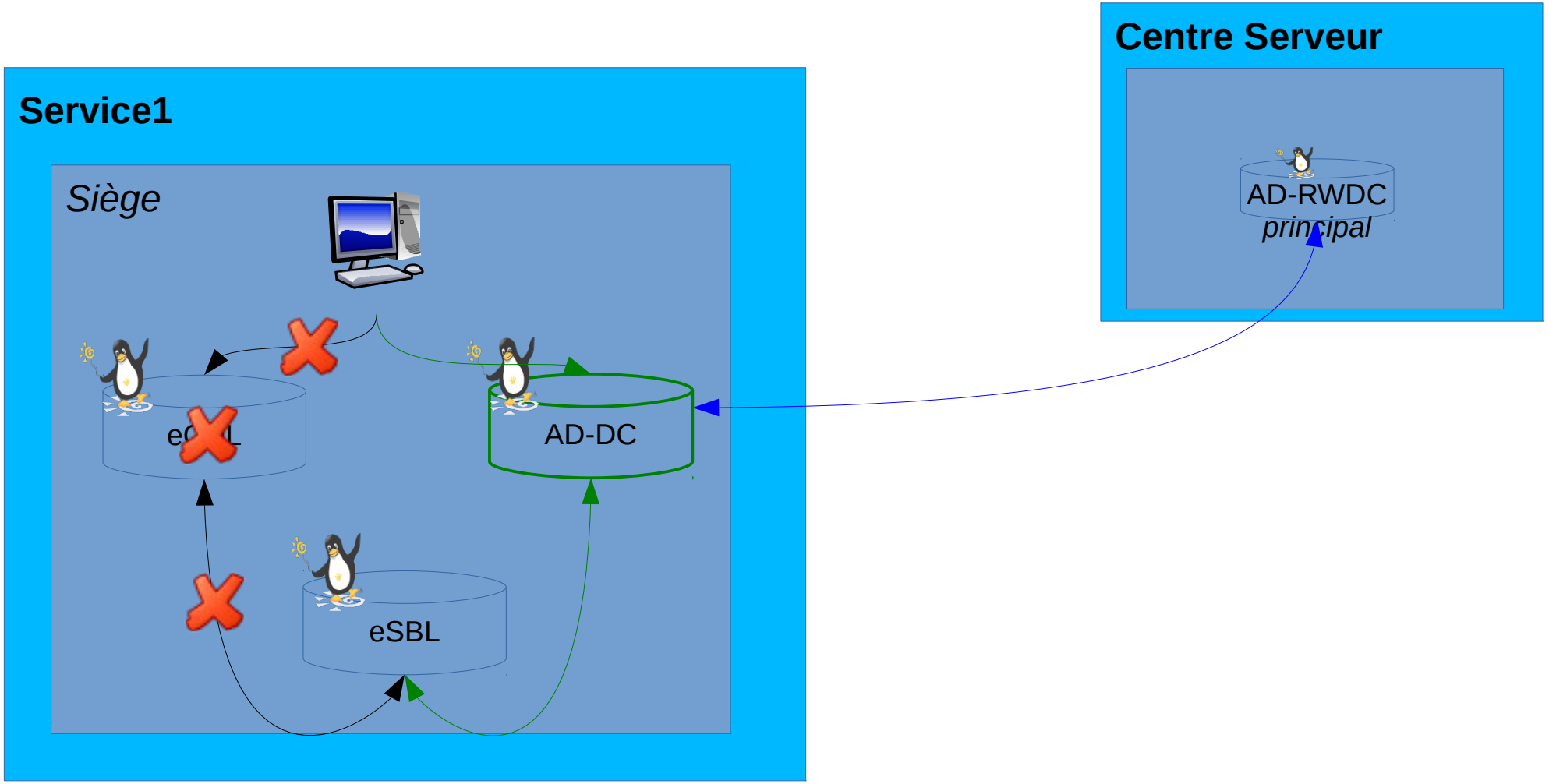
Les outils d'administration

- Utilisation d'Amédée pour la gestion des comptes
  - Script LDAP→AD (comptes)
- Outils RSAT pour autre gestion
  - OU, groupes
  - Script AD (groupes auto)
- Compte de gestion spécifiques
  - Membre du/des groupes OUADM, PCADM, SRVADM pour l'administration locale et l'intégration des postes

Les principes de la migration

- Migration à ISO domaine (même SID)
- Réinjection par scripts des comptes LDAP
  - Machines
  - User
  - Group
- Scripts de « migration » des PC
  - Passage à DHCP statique
  - Modification de clés de registre
  - Intégration dans le domaine

Le principe de la migration



Le projet AD et EOLE

Une occasion de ne plus utiliser que des modules communs avec le MEN

- Abandon à terme des eSBL et eCDL
- Meilleure contribution des MTES/MCT au projet EOLE puisque les développements financés sur les modules communs intéressent potentiellement toutes les communautés
- Amélioration du service rendu à nos « clients » :
  - Modules bénéficiant des tests d'Intégration continue
  - Simplification du Maintien en Conditions Opérationnelles (MCO)

Exemples de contributions du MTES/MCT EOLE et module SETH

Version 2.6.1

- Intégration d'une version samba plus récente que celle d'Ubuntu
- Évolution sur les règles de firewalling sur le SETH
- Intégration d'un processus de sauvegarde
- Outils de gestion des ACL et Quotas sur EAD 3
  - Nouvelle solution sur EOLE pour la gestion des partitions
- Écriture de cas de tests sur SETH, Quotas, ACL

Version 2.6.2

- Participation aux développements Zephir
- Évolutions sur SETH
  - notamment délégation de la fonction samba DNS à BIND

FIN