

# Migration de plateformes

## NIS

JIs 2016

GIVAUDAN Valérie / Rago Emiliano **IN2P3/LAL**



GAUTIER DE LAHAUT Anthony **CEA/IRFU**



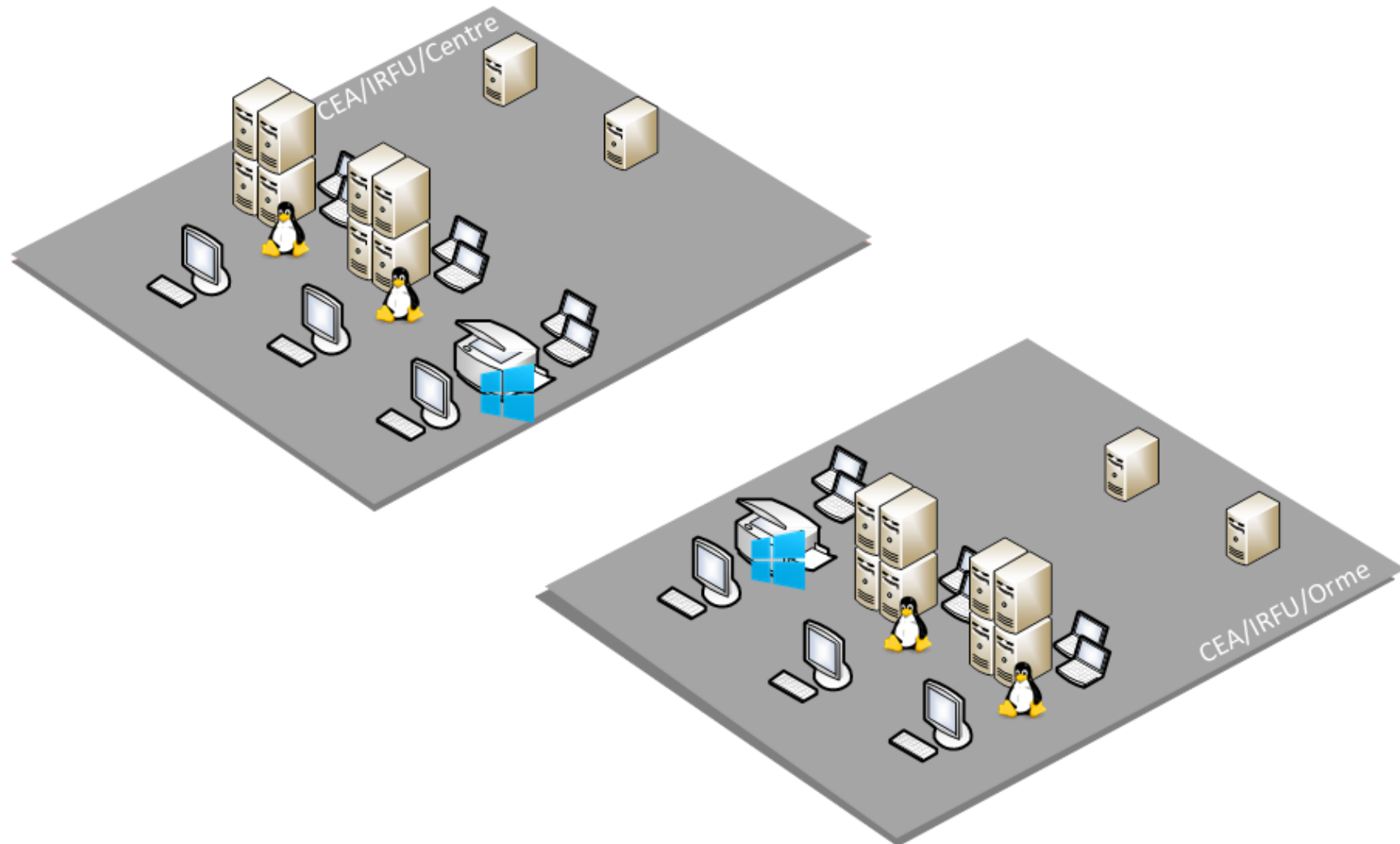
# 1 Introduction

1. L'existant
2. Les besoins
3. Les problématiques
4. Les solutions

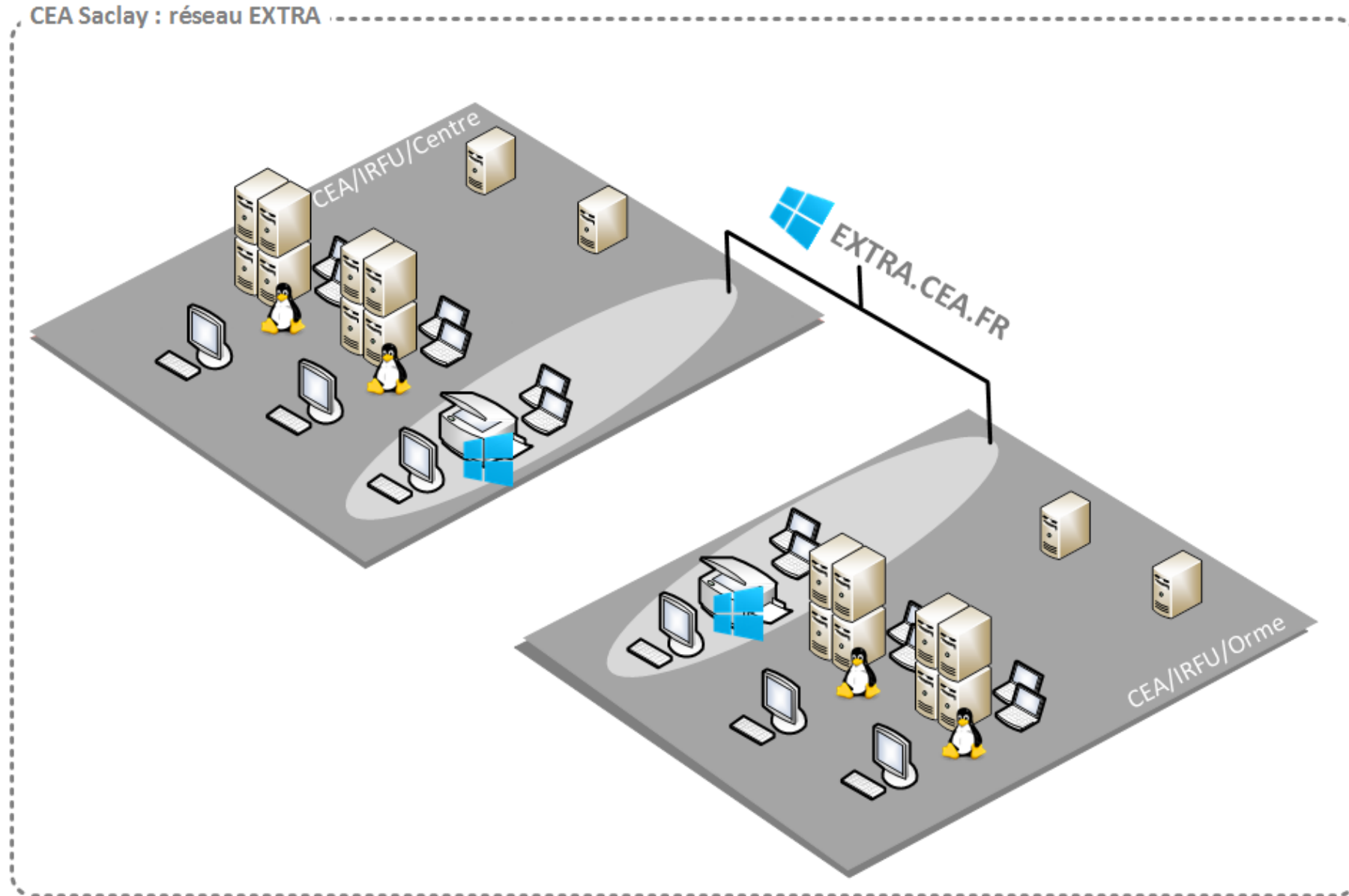


# Le parc informatique : IRFU

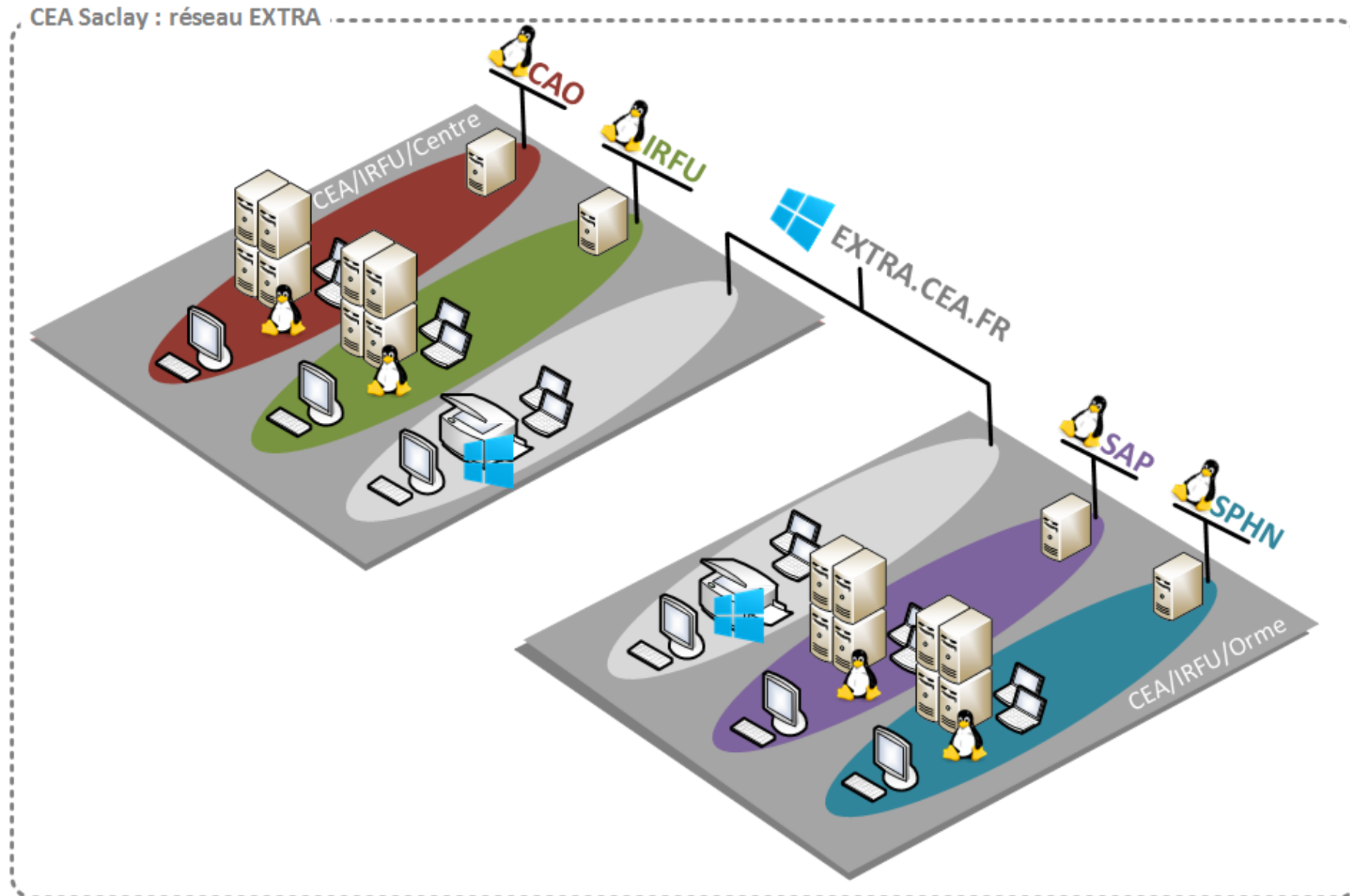
CEA Saclay : réseau EXTRA



# Le parc informatique : IRFU



# Le parc informatique : IRFU

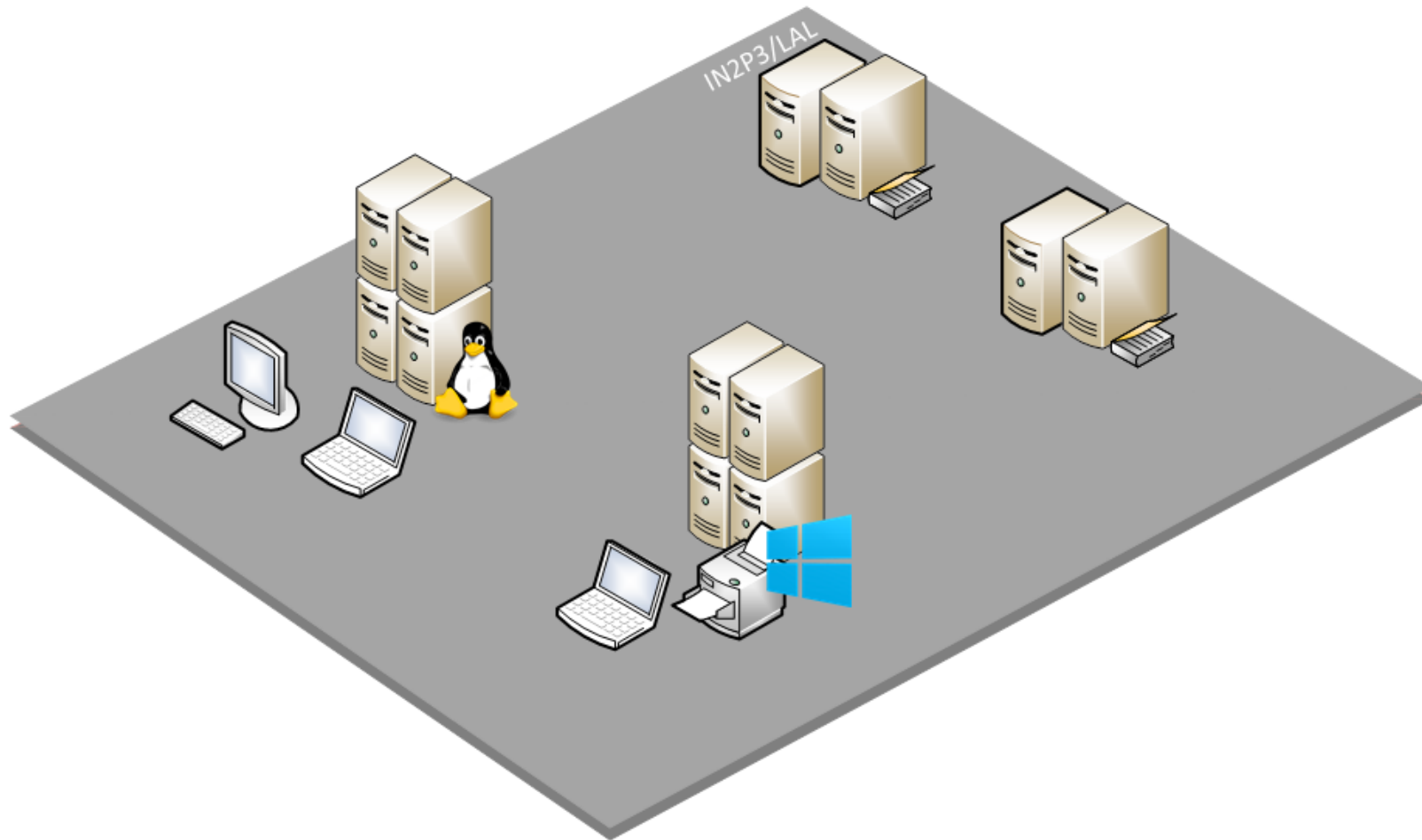


# 1

## 1. L'existant

# Le parc informatique : LAL

LAL Saclay : réseau LAL.IN2P3.FR

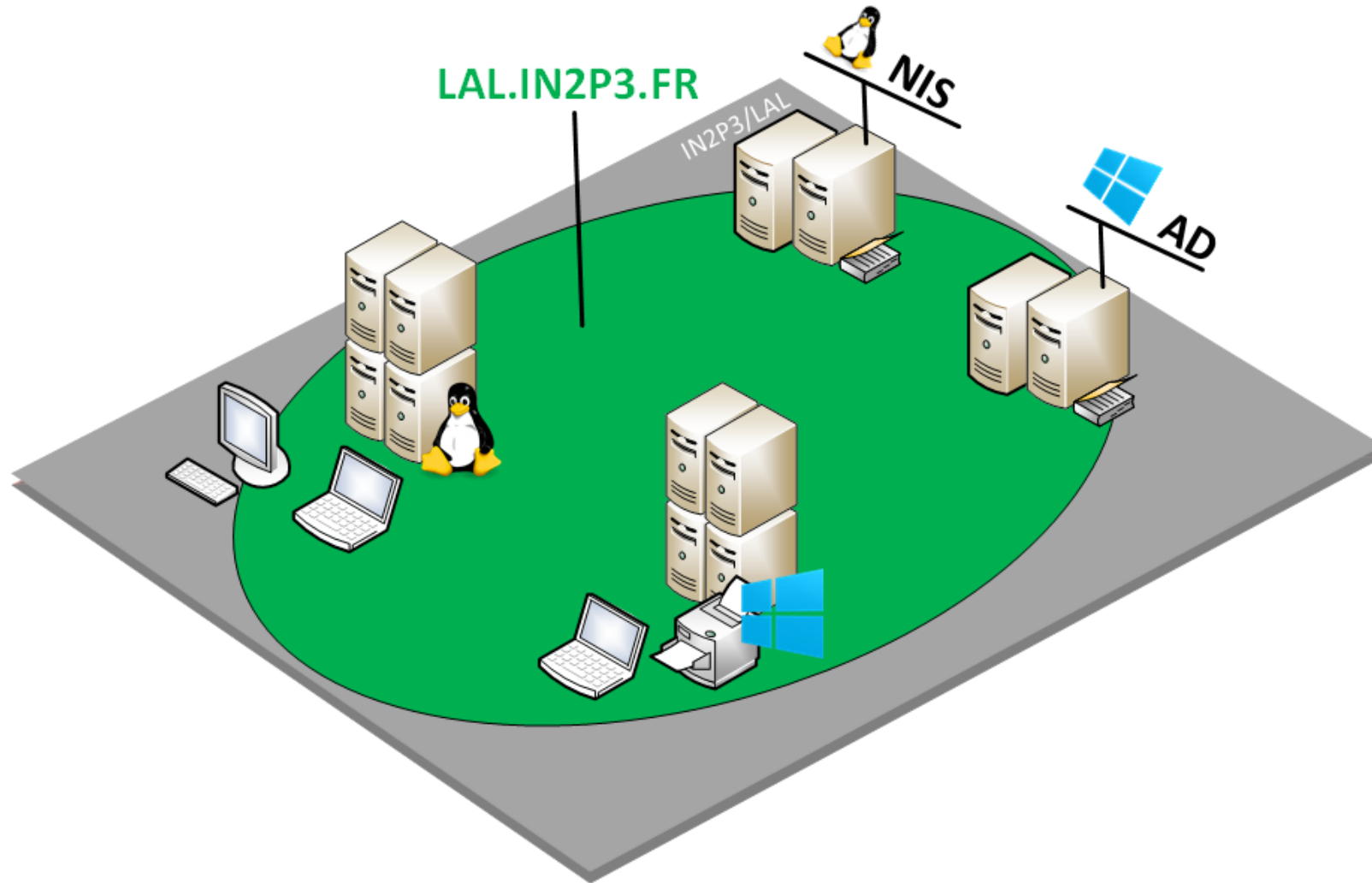


# 1

## 1. L'existant

# Le parc informatique : LAL

LAL Saclay : réseau LAL.IN2P3.FR



- Aucune centralisation des données
  - Plusieurs services de comptes non synchrones
  - Workflow compliqué
  - Différents `homedir` et `shell`
- NIS est un protocole vieillissant
  - Peu d'interopérabilité
  - Mais simple et robuste!
- Aucune redondance
- Faible en terme de sécurité.



- Un service de gestion des comptes unique, centralisé et sécurisé.
- Un seul outil : interface simple et utilisable par TOUS
- Une politique de sécurité unique et solide
- Un seul mot de passe
- Une migration la plus transparente possible pour les utilisateurs...
- Solution qui utilise des standards
- Solution pérenne qui ne réinvente pas la roue...**Et utilisable pour tous les services**
- **Postes clients : Système de cache pour le mot de passe**

# Annuaire full OpenLDAP

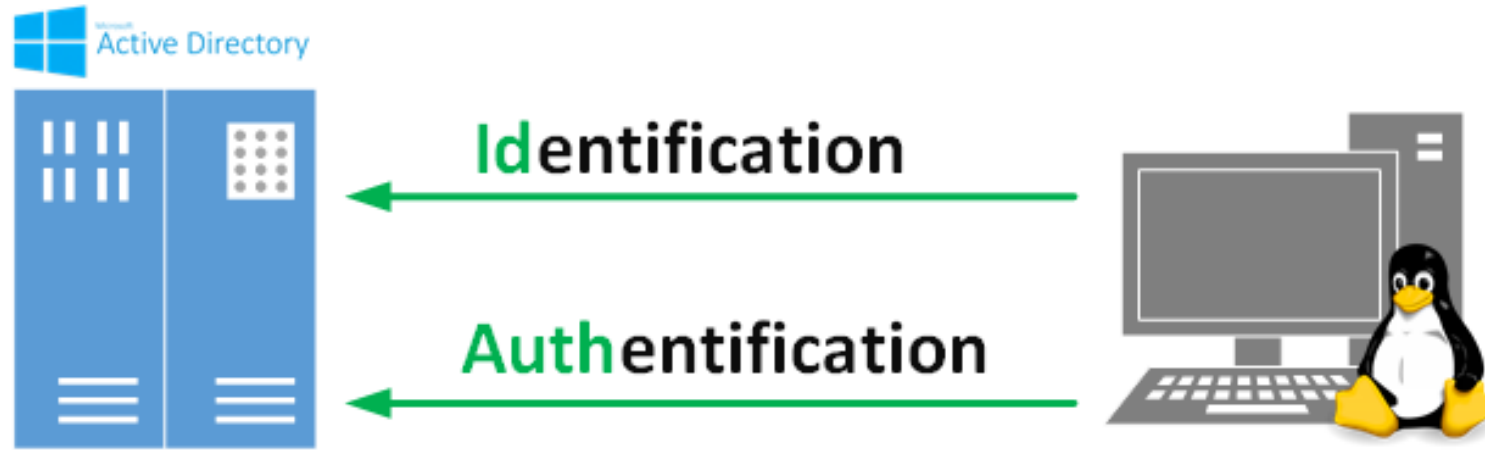


## 4. Les solutions 1/3

	Les plus	Les moins	Retenue
IRFU	<ul style="list-style-type: none"> <li>- Un seul annuaire pour Linux</li> <li>- Totalement géré par l'IRFU</li> </ul>	<ul style="list-style-type: none"> <li>- Mise en œuvre</li> <li>- 2 annuaires</li> </ul>	<b>REJECTED</b>
LAL	NC	NC	<b>REJECTED</b>

# Annuaire full Active Directory

## 4. Les solutions 2/3



	Les plus	Les moins	Retenue
<b>IRFU</b>	<ul style="list-style-type: none"> <li>- Un seul annuaire</li> <li>- Géré par les STIC</li> </ul>	<ul style="list-style-type: none"> <li>- N'est pas géré par l'IRFU</li> <li>- Deprecated</li> <li>- Migration</li> </ul>	<b>REJECTED</b>
<b>LAL</b>	<ul style="list-style-type: none"> <li>- Centralisé &amp; sécurisé</li> <li>- Service compatible (Kerberos)</li> </ul>	NC	<b>APPROVED</b>

# Annuaire OpenLDAP & AD

## 4. Les solutions 3/3



	Les plus	Les moins	Retenue
IRFU	<ul style="list-style-type: none"> <li>- Un annuaire géré par l'IRFU</li> <li>- Migration</li> </ul>	- 2 annuaires	
LAL	NC	NC	



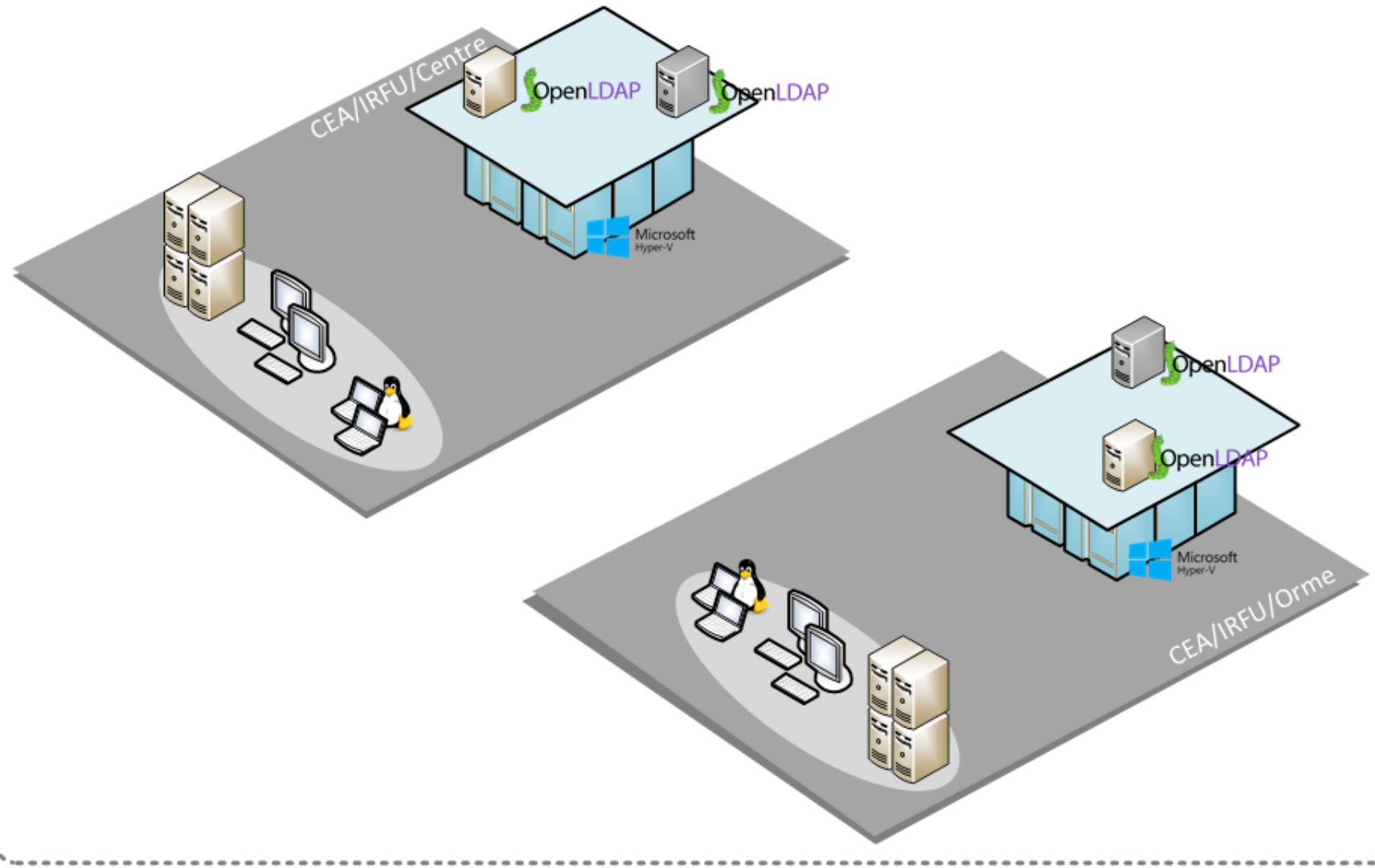
# Implémentation

Coté IRFU

1. Architecture détaillée
2. Coté machines clientes
3. Coté utilisateurs

# Infrastructure OpenLDAP

CEA Saclay : réseau EXTRA

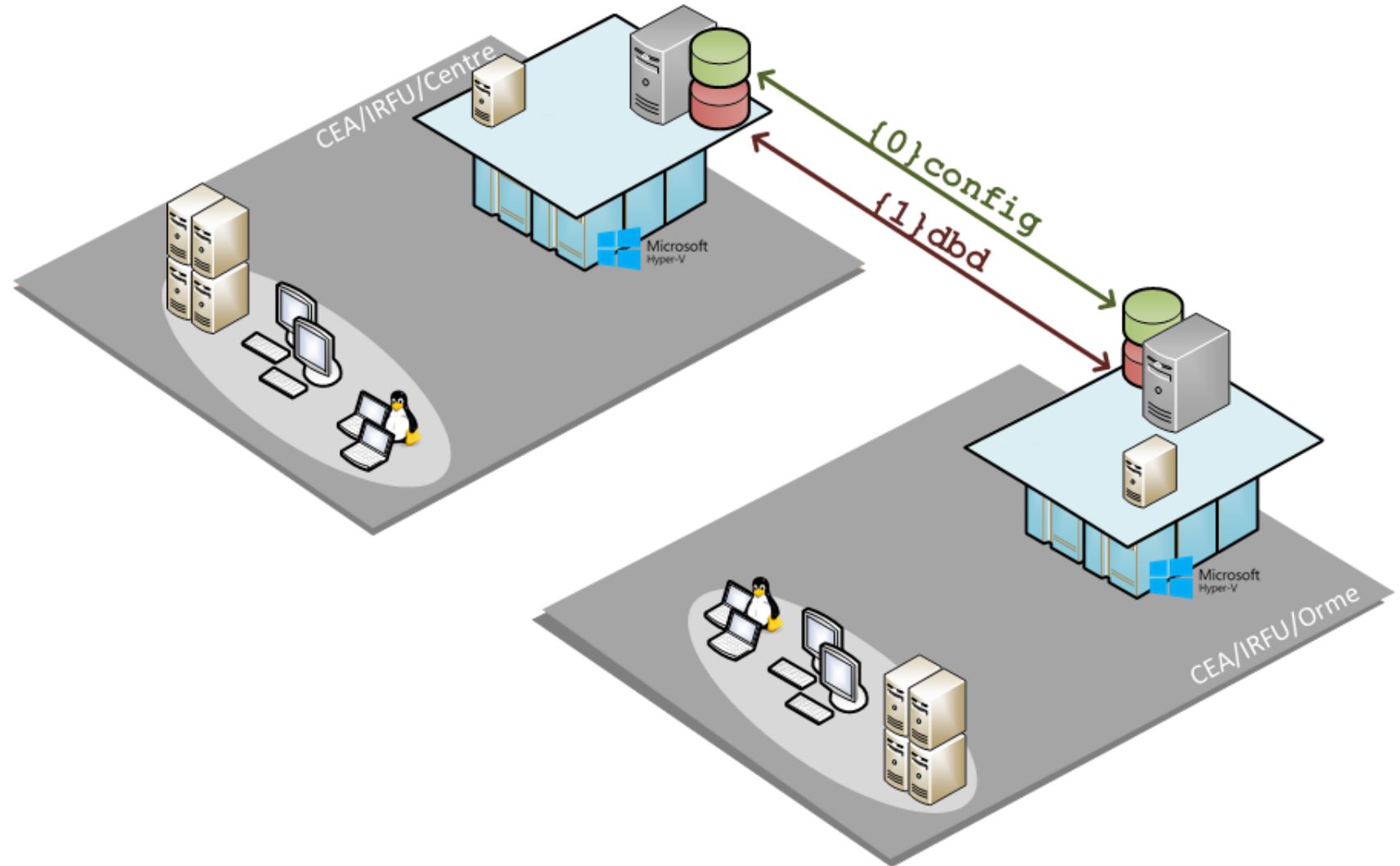


2

1. Archi' détaillée

# Réplication multi-master

CEA Saclay : réseau EXTRA

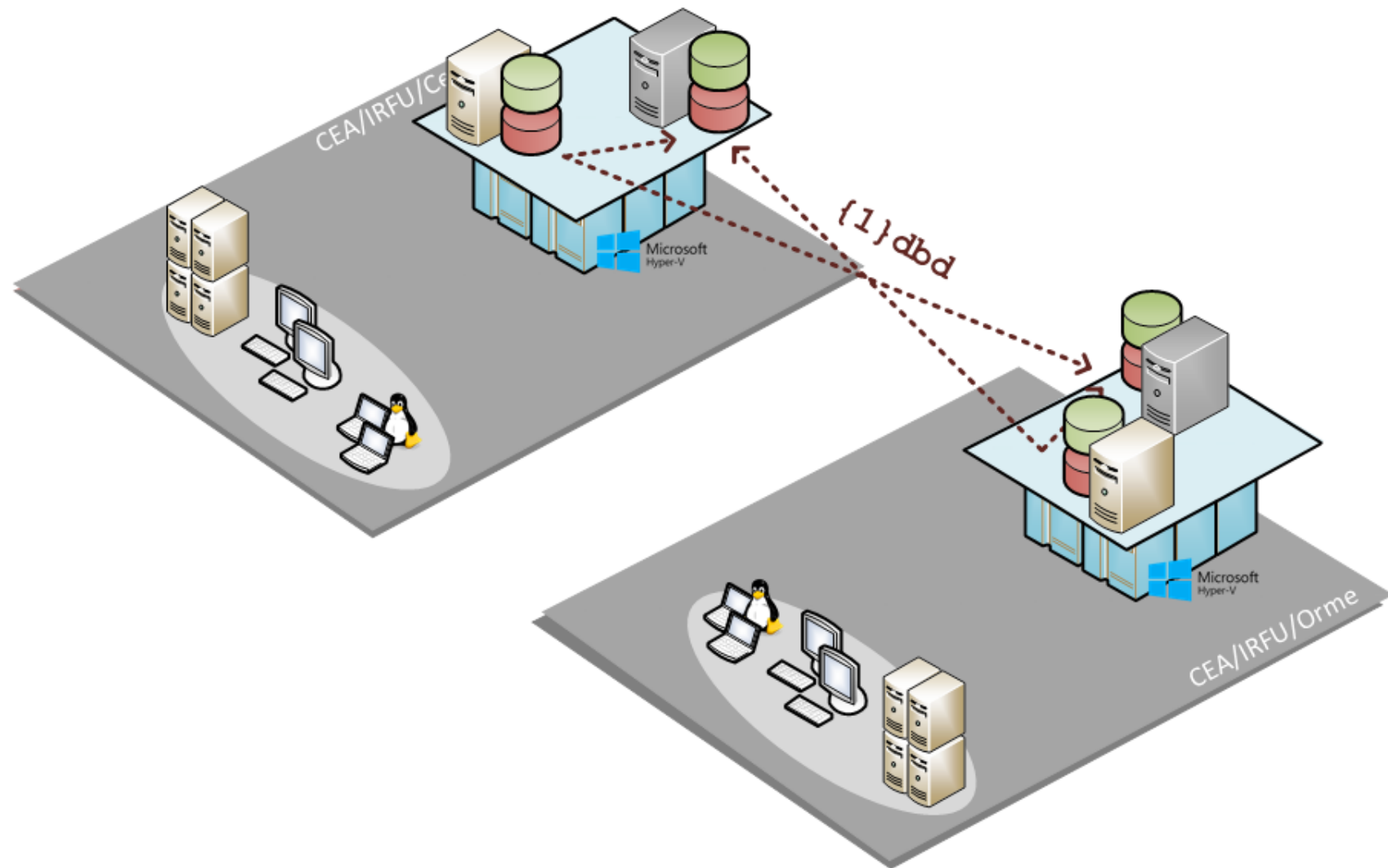


2

1. Archi' détaillée

# Réplication masters-slaves

CEA Saclay : réseau EXTRA



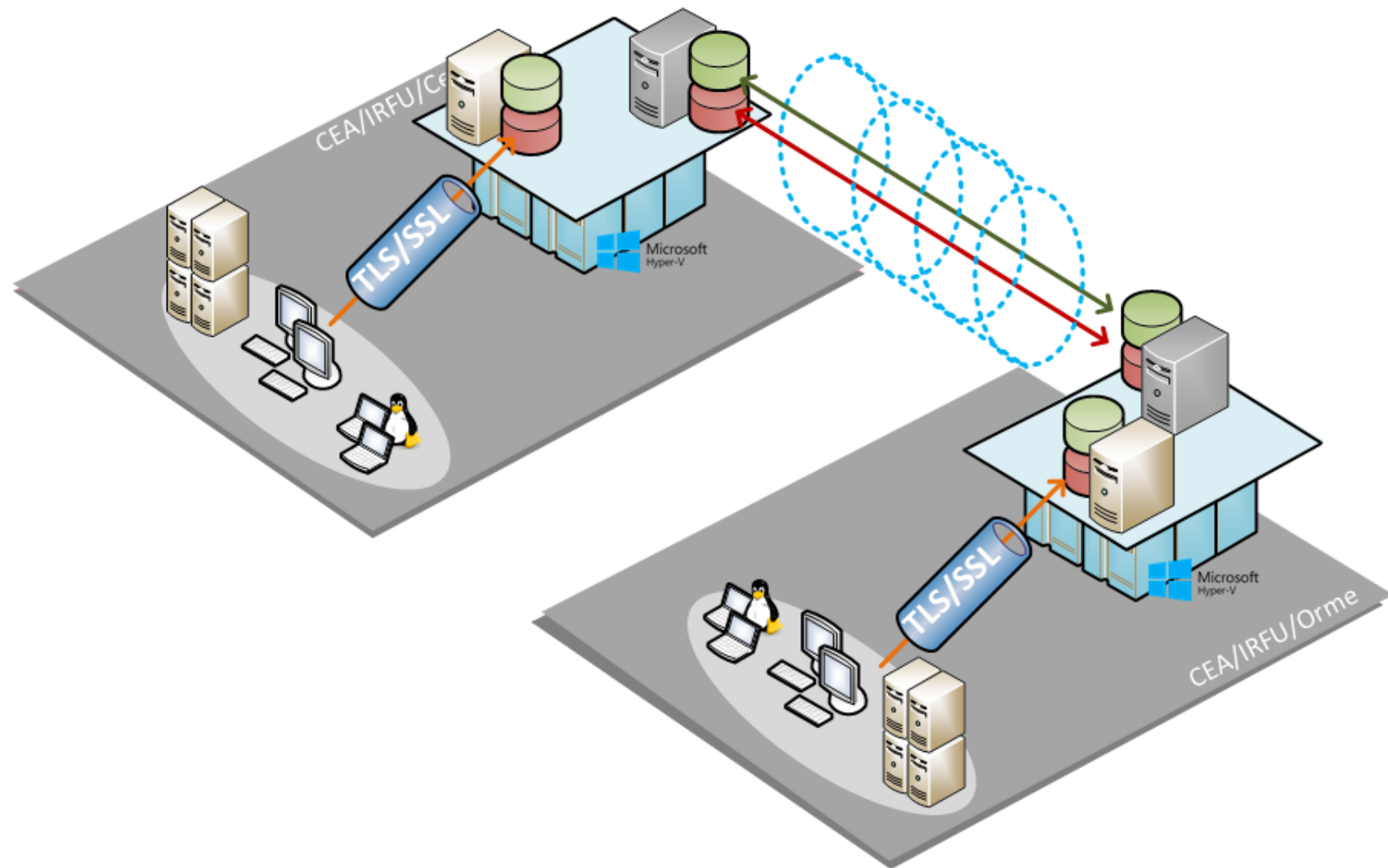
2

1. Archi' détaillée



# Sécurité

CEA Saclay : réseau EXTRA



2

1. Archi' détaillée

- Les démons
  - Local LDAP Name Service Daemon (*NSLCD*)
  - Automount File System (*AUTOFS*)
  - System Security Services Daemon (*SSSD*)

- `sssd.conf`

```
auth_provider = krb5
autofs_provider = ldap
cache_credentials = true
chpass_provider = krb5
enumerate = true
id_provider = ldap
krb5_realm = NOM.DE.DOMAINE
krb5_store_password_if_offline = true
ldap_search_base = dc=nom,dc=de,dc=domaine
ldap_uri = ldap://ldap4.nom.de.domaine/
ldap_user_home_directory = homeDirectory03
ldap_user_shell = loginShell103
```

```
dn: uid=agautier,ou=People,ou=irfu,dc=extra,dc=cea,dc=fr
uid: agautier
cn: Anthony Gautier-De-Lahaut
sn: Gautier-De-Lahaut
givenName: Anthony
mail: agautier@extra.cea.fr
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: homeSupp
objectClass: shadowAccount
objectClass: posixAccount
objectClass: top
userPassword:: {SASL}agautier@EXTRA.CEA.FR
gecos: Anthony Gautier-De-Lahaut
uidNumber: 14623
gidNumber: 1288
shadowExpire: 29584
homeDirectory: /home/agautier
loginShell: /bin/bash
homeDirectory02: /home/usr201/mnt/agautier
loginShell102: /bin/bash
```



# Implémentation

Coté LAL

- 1 – Map autofs
- 2 – Attribut Unix

# 3

## 1. Map autofs

Nom	Classe	Nom unique
CN=auto-atlas.master	nisMap	CN=auto-atlas.master,CN=AutoMountUniX,DC=lal,DC=in2p3,DC=fr
CN=auto-groups.master	nisMap	CN=auto-groups.master,CN=AutoMountUniX,DC=lal,DC=in2p3,DC=fr
CN=auto_map.data	nisMap	CN=auto_map.data,CN=AutoMountUniX,DC=lal,DC=in2p3,DC=fr
CN=auto_map.exp	nisMap	CN=auto_map.exp,CN=AutoMountUniX,DC=lal,DC=in2p3,DC=fr
CN=auto_map.indico	nisMap	CN=auto_map.indico,CN=AutoMountUniX,DC=lal,DC=in2p3,DC=fr
CN=auto_map.sps	nisMap	CN=auto_map.sps,CN=AutoMountUniX,DC=lal,DC=in2p3,DC=fr
CN=auto_map.top	nisMap	CN=auto_map.top,CN=AutoMountUniX,DC=lal,DC=in2p3,DC=fr
CN=auto_map.users	nisMap	CN=auto_map.users,CN=AutoMountUniX,DC=lal,DC=in2p3,DC=fr

Nom	Type	Description
/data	nisObject	
/exp	nisObject	
/indico	nisObject	
/sps	nisObject	
/tmp_mnt	nisObject	
/users	nisObject	

- Sur les serveurs Linux:

Fichiers `/etc/sysconfig/autofs` et  
`/etc/autofs_ldap_auth.conf` (utilisation de  
LDAP, schéma)

Fichier `/etc/nsswitch.conf` (LDAP au lieu de NIS)

3

1. Map autofs

3

## 2. Attributs Unix

The screenshot shows the Active Directory console window titled "Active Directory - [Racine de la console\Utilisateurs et ordinateurs Active Directory [LALAD1.lal.in2p3.fr]\lal.in2p3.fr\Laboratoire\services techniques\SI]". The left pane shows a tree view of the directory structure, with "services techniques" expanded to show the "SI" group. The middle pane lists users, with "Valerie Givaudan" selected. The right pane shows the "Propriétés de : Valerie Givaudan" dialog box, with the "Attributs UNIX" tab selected. The dialog contains the following fields:

- Domaine NIS : lal
- UID : 802
- Environnement de démarrage : /bin/tcsh
- Répertoire de base : /users/dsksi/givaudan
- Nom de groupe principal/GID : SI

Buttons at the bottom of the dialog include "OK", "Annuler", "Appliquer", and "Aide".

- Authentification des utilisateurs :
  - Fichier `/etc/nsswitch.conf` (ldap au lieu de NIS)
  - Fichier `/etc/nslcd.conf` (mapping name service: ex uid Unix= sAMAccountName AD)
  - Intégration dans le domaine AD `/etc/kerberos.conf` permet de faire un kinit
  - Modification de pam (autorise un user à se connecter)

**Suppose que tout user ait un compte avec les attributs Unix dans LDAP/AD**



# Conclusion



1. Migrations
2. Conclusion générale



- Avancement du projet

- Mise en place des serveurs,
- Mise en place des services,
- Mise en production.



- Bascule de la configuration clientes

- Ubuntu 12/14/15 → Ubuntu 16
- SL4/5/6/7 → CentOS7



Pré-requis: au moins SL6

AD et NIS en parallèle (~ un an): pas de synchronisation

Migration service par service

### ***1°) Passage des Maps d'automount sur AD :***

Pas de mécanisme d'authentification → simple!

Décider où les mettre dans AD...et le faire, Mais gérer les maps dans AD/LDAP plus difficile que dans les fichiers textes de NIS → Script en python

Fichiers de config → Déploiement via Quattor

## *2°) Le service de mail: le plus simple...*

Les clients besoin uniquement du mot de passe

Nécessite **pas d'information en plus** dans AD

Aucune modification de la config clients

Dovecot, et smtp utilisent Kerberos

**Impératif:** Login windows= Login Unix (y compris majuscule/minuscule)

Gros travail de « ménage » et cohérence des comptes!

Mot de passe Windows dans le client de mail le jour J

### *3°) Les serveurs Linux*

#### **Besoin attributs Unix dans AD: shell, UID, GID, home**

Configuration Nslcd: mapping attributs Unix et champs LDAP/AD

Configuration pam, kerberos

Intégration des serveurs dans le domaine avant

Scripts import des attributs Unix de NIS vers AD

Déploiement avec Quattor

### *4°) Points importants de la migration*

#### **Informez les utilisateurs !**

Mot de passe Windows

Support : site Web, mails, Comité des utilisateurs, ...

Réorganisation des comptes: grand ménage !!

Attention aux comptes « systèmes »

Groupes:

Tous les groupes unix doivent exister dans AD  
organisation AD pas la même que celle sous NIS...

Groupe primaire (linux) n'existe pas sous Windows

Kerbérisation des services possible mais travail à faire pour  
l'automatisation ...

Pré-requis: SL6 (upgrade des serveurs + pb avec la CAO...)

Création d'un compte:

Choix du uid/gid ?

Comment créer les home unix

Besoin de lancer des scripts

- Un seul système sécurisé qui gère vraiment les comptes...c'est ce qu'on voulait!
- Un seul domaine pour les 2 systèmes : EXTRA
- Un annuaire au lieu de 5
- Migration assez simple
- Versions futures de MS: suppression de la gestion des identités pour Unix...
- Comment fait-on la gestion des attributs Unix?
  - **Présentation « éclair » : utentomatic pour gérer les comptes!**