# AD Integration options for Linux Systems

## Overview

Dmitri Pal

*Developer Conference. Brno. 2013*

# Agenda

- Problem statement
- Aspects of integration
- Options
- Questions

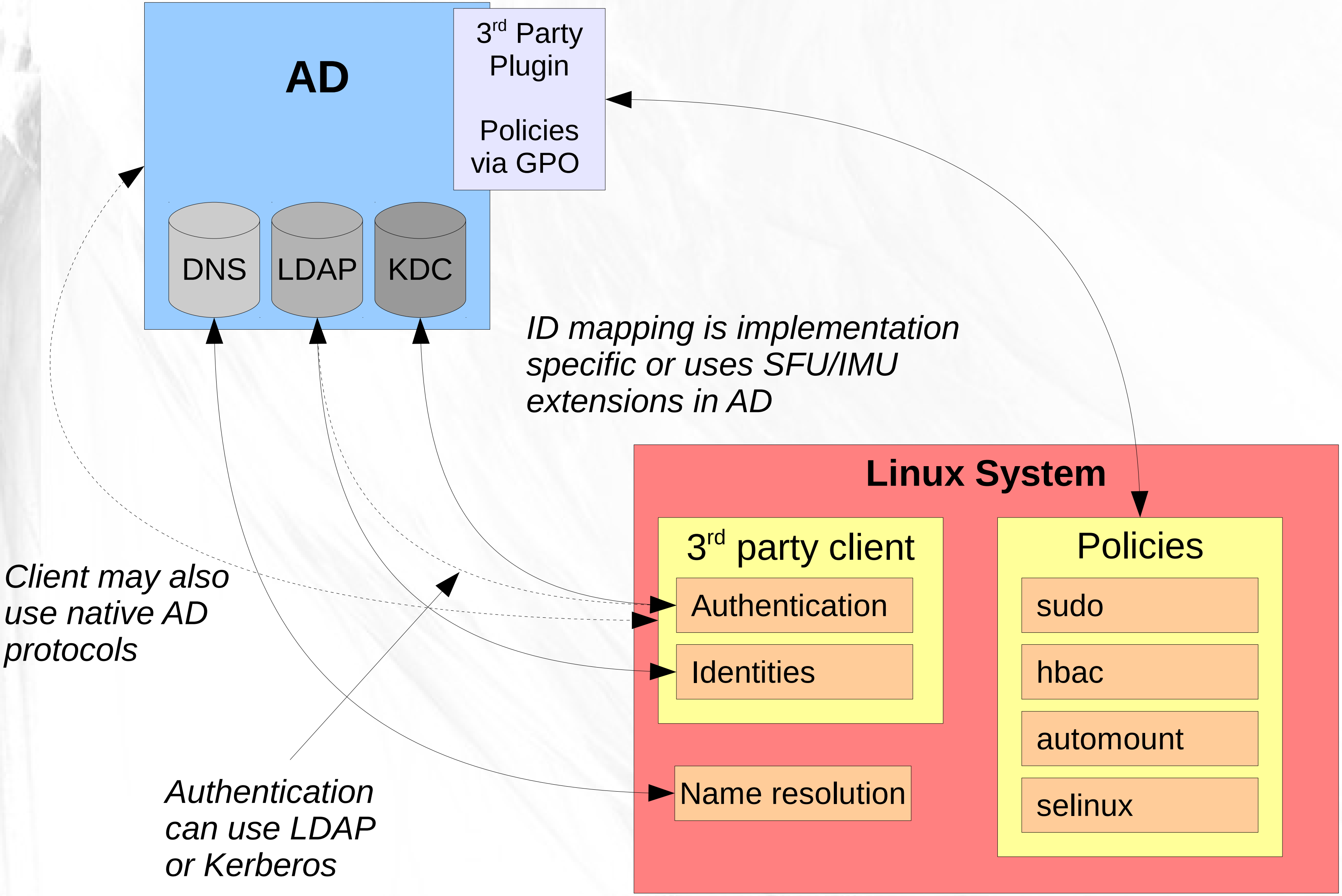
# Problem Statement

- For most companies AD is the central hub of the user identity management inside the enterprise
- All systems that AD users can access (including Linux) need (in some way, i.e. directly or indirectly) to have access to AD to perform authentication and identity lookups
- In some cases the AD is the only allowed central authentication server due to compliance requirements
- In some cases DNS is tightly controlled by the Windows side of the enterprise and non Windows systems need to adapt to this

# Aspects of integration

- Authentication
  - User logs into a Linux system, how he is authenticated?
- Identity lookup
  - How system knows about the right accounts?
  - How AD accounts are mapped to POSIX?
- Name resolution and service discovery
  - How system knows where is its authentication and identity server?
- Policy management
  - How other identity related policies are managed on the system?

# Third Party Integration Option



*ID mapping is implementation specific or uses SFU/IMU extensions in AD*

*Client may also use native AD protocols*

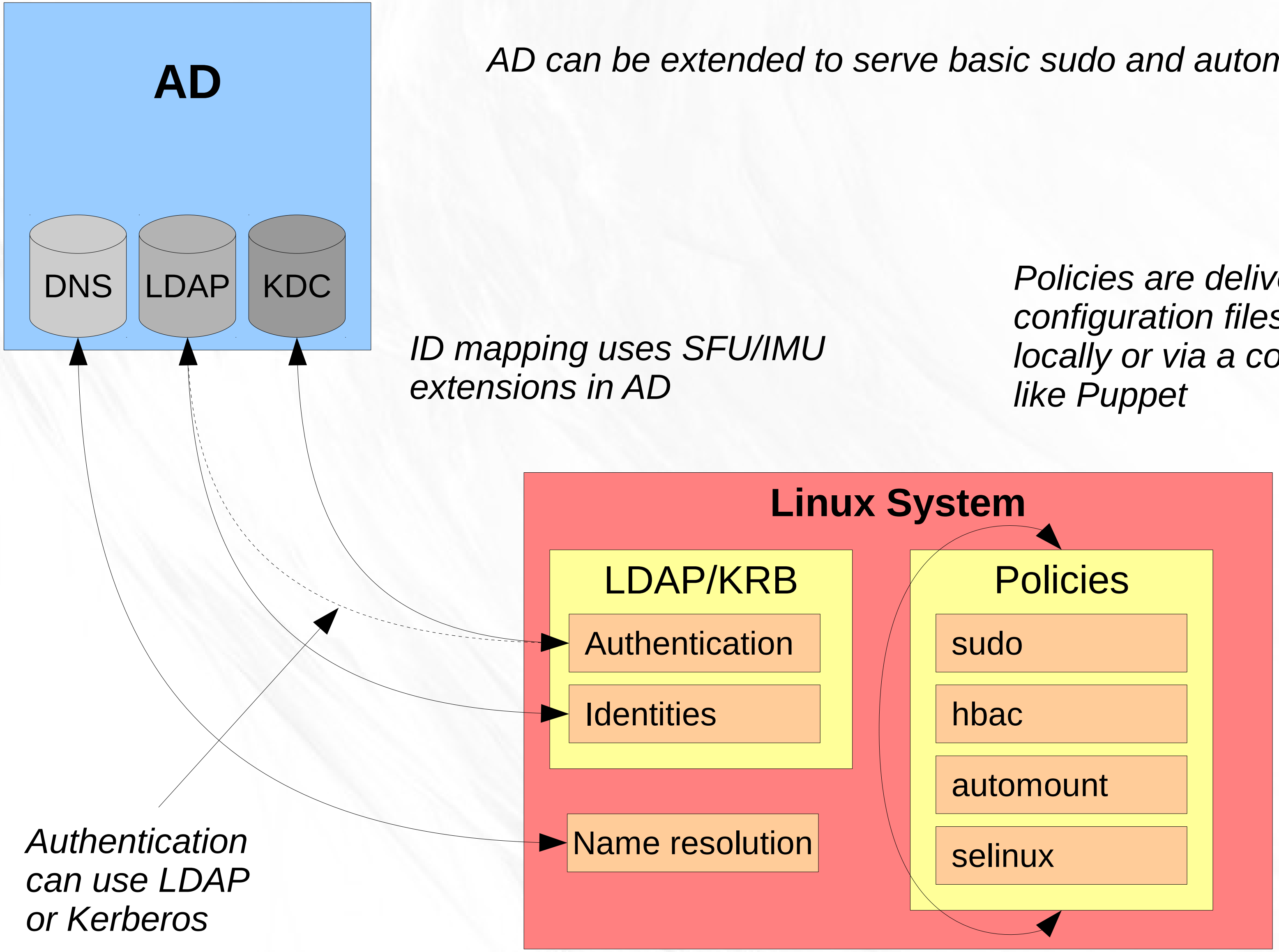
*Authentication can use LDAP or Kerberos*

# Pros and Cons of the 3rd Party Option

- Pros
  - Everything is managed in one place including policies
- Cons
  - Requires third party vendor
  - Extra cost per system (adds up)
  - Limits UNIX/Linux environment independence
  - Requires software on AD side

# Legacy Integration Option

*AD can be extended to serve basic sudo and automount*



AD

DNS

LDAP

KDC

Linux System

LDAP/KRB

Authentication

Identities

Name resolution

Policies

sudo

hbac

automount

selinux

*ID mapping uses SFU/IMU extensions in AD*

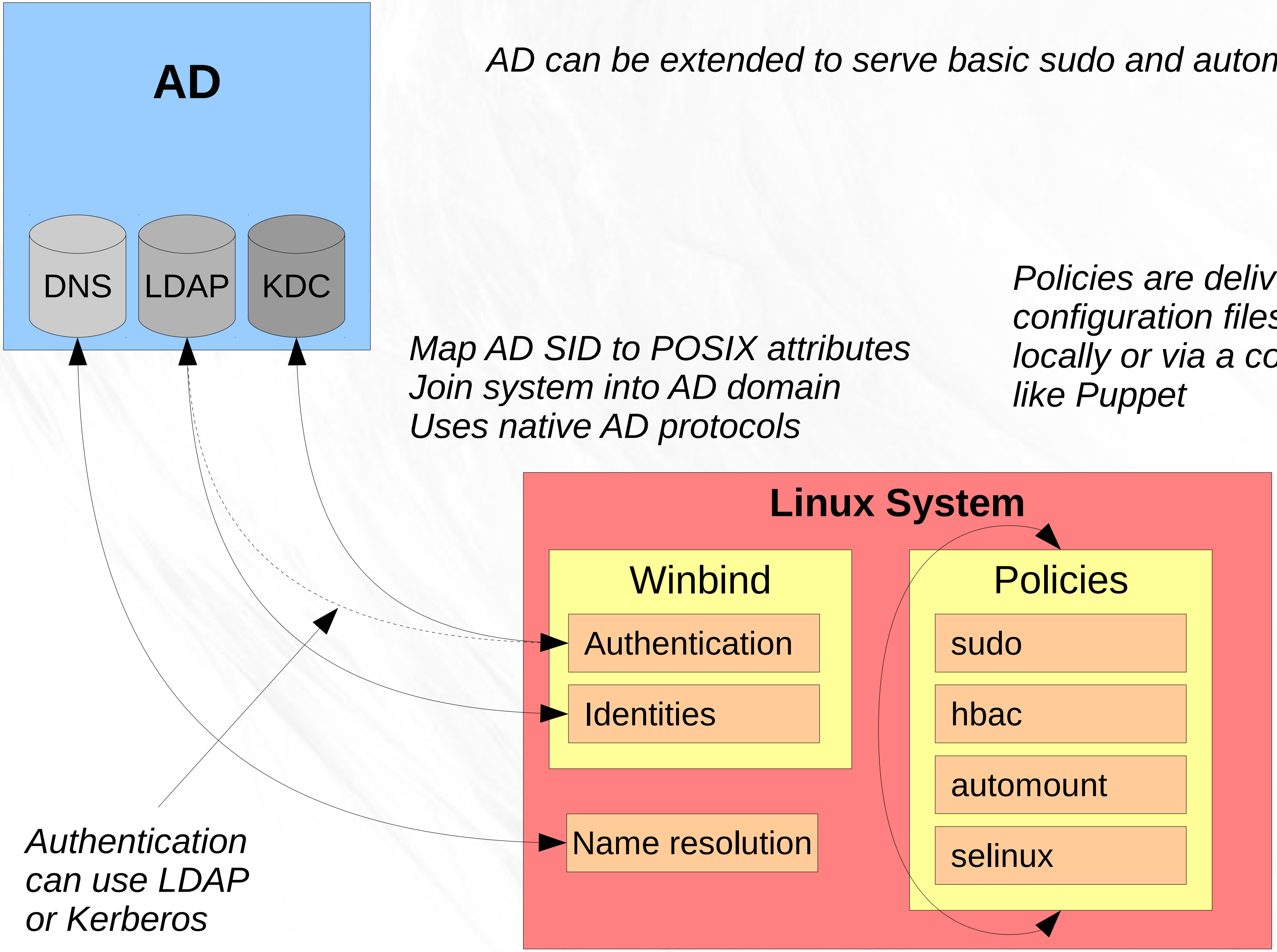
*Policies are delivered via configuration files managed locally or via a config server like Puppet*

*Authentication can use LDAP or Kerberos*

# Pros and Cons of the Legacy Option

- Pros:
  - Free
  - No third party vendor is needed
  - Intuitive
- Cons:
  - Requires SFU/IMU AD extension
  - Policies are not centrally managed
  - Hard to configure securely

# Traditional Integration Option



*AD can be extended to serve basic sudo and automount*

*Map AD SID to POSIX attributes*
*Join system into AD domain*
*Uses native AD protocols*

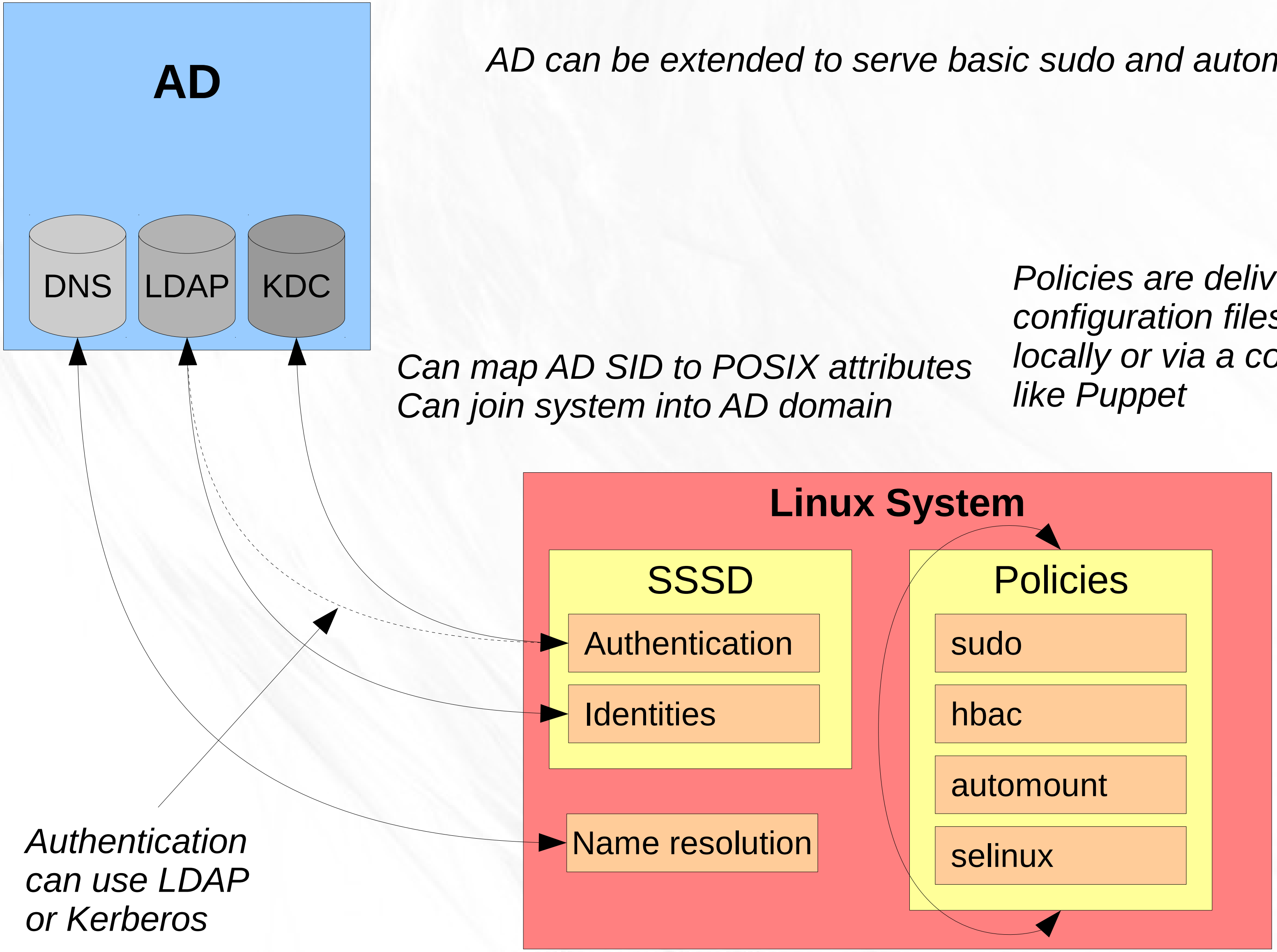
*Policies are delivered via configuration files managed locally or via a config server like Puppet*

*Authentication can use LDAP or Kerberos*

# Pros and Cons of the Traditional Option

- Pros:
  - Well known
  - Does not require third party
  - Does not require SFU/IMU
  - Supports trusted domains
- Cons:
  - Can connect only to AD and very MSFT focused
  - Has some perceived stability issues
  - Community is hard to deal with

# Contemporary Integration Option



*AD can be extended to serve basic sudo and automount*

*Policies are delivered via configuration files managed locally or via a config server like Puppet*

*Can map AD SID to POSIX attributes*
*Can join system into AD domain*

*Authentication can use LDAP or Kerberos*

# Pros and Cons of the Contemporary Option

- Pros:
  - Does not require third party
  - Does not require SFU/IMU (SSSD 1.9)
  - Supports trusted domains with FreeIPA (SSSD 1.9)
  - Supports heterogeneous environments
- Cons:
  - Does not support transitive trusts in AD domains (1.10)
  - Does not support some advance AD optimizations (1.10)

# Option Comparison

| Feature | LDAP/KRB | Winbind | SSSD |
|---|---|---|---|
| Authenticate using Kerberos or LDAP | Yes | Yes | Yes |
| Identities are looked up in AD | Yes | Yes | Yes |
| Requires SFU/IMU | Yes | No | No |
| ID mapping | None | Multiple ways | One way starting SSSD 1.9<br>Domain ranges |
| System is joined into AD | Manual | Has join utility | Samba join utility needs to be used (realmd project makes it easy) |
| Supports transitive trusts for AD domains | No | Yes | Will in SSSD 1.10 |
| Supports heterogeneous domains | No | No | Yes |
| Support advanced AD features | No | Yes | Some |

# Current Plan

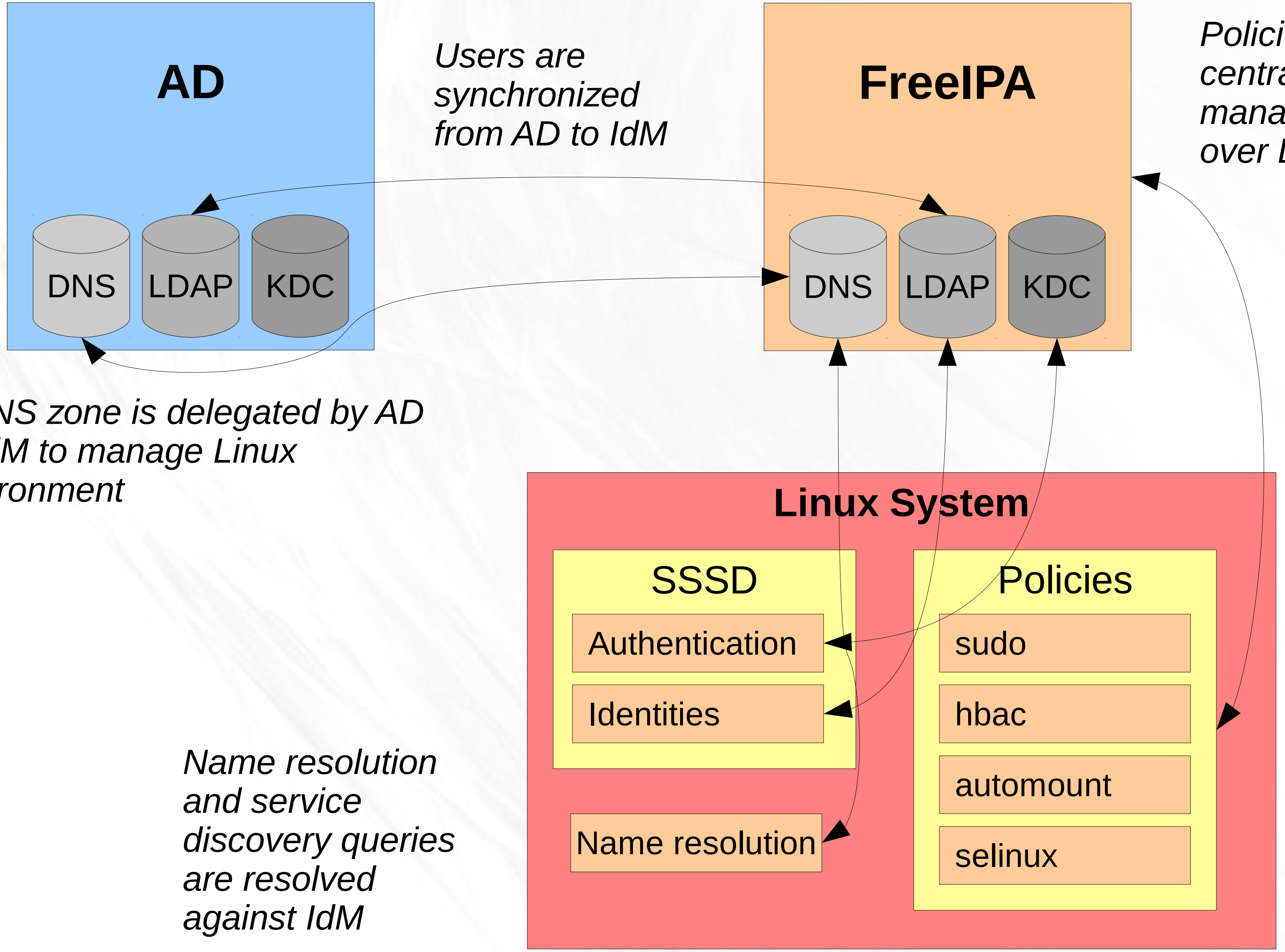
- Evolve SSSD to get in full feature parity with Winbind and bypass it in some areas (SSSD 1.10 and after)
- Do not reinvent the wheel, rather package elements of samba winbind as libraries and consume those libraries in SSSD
- Augment SSSD with realmd for easier enrollment into AD or FreeIPA (Fedora 18/19)

# Limitations of the Direct Integration Options

- Policy management is left out
- Per system CALs add to cost
- Linux/UNIX administrators do not have control of the environment

***All these limitations prevent growth of the Linux environment inside the enterprise!***

# FreeIPA Based Integration (sync)



*Users are synchronized from AD to IdM*

*Policies are centrally managed over LDAP*

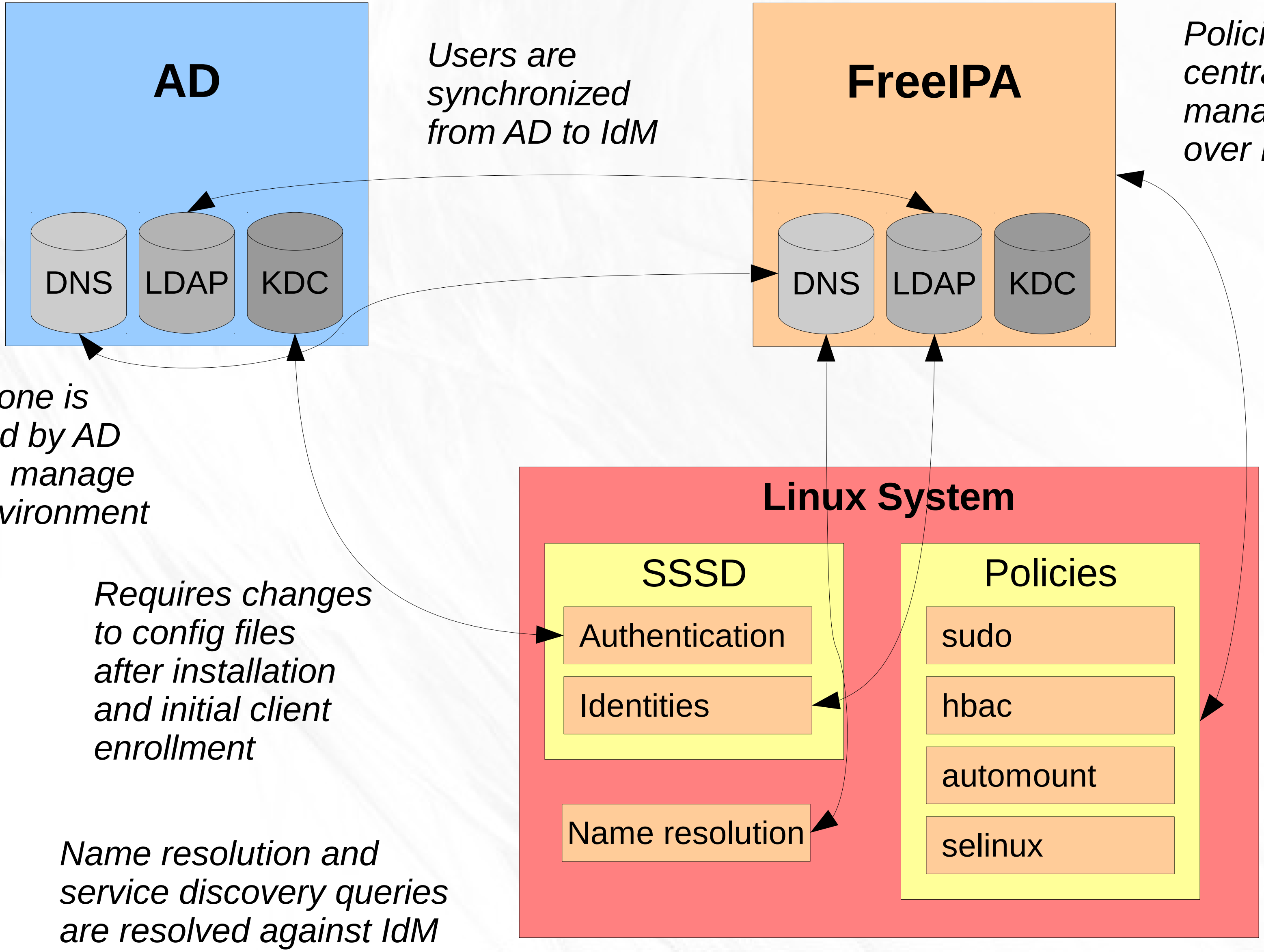
*A DNS zone is delegated by AD to IdM to manage Linux environment*

*Name resolution and service discovery queries are resolved against IdM*

# Pros and Cons of the FreeIPA Integration

- Pros:
  - Reduces cost – no CALs or 3rd party
  - Policies are centrally managed
  - Gives control to Linux admins
  - Enabled independent growth of the Linux environment
- Cons:
  - Requires user and password sync
  - Authentication does not happen in AD
  - Requires proper DNS setup

# FreeIPA Based Integration (split brain)



**AD**

DNS LDAP KDC

**FreeIPA**

DNS LDAP KDC

**Linux System**

SSSD

Authentication

Identities

Name resolution

Policies

sudo

hbac

automount

selinux

*Users are synchronized from AD to IdM*

*Policies are centrally managed over LDAP*

*A DNS zone is delegated by AD to IdM to manage Linux environment*

*Requires changes to config files after installation and initial client enrollment*

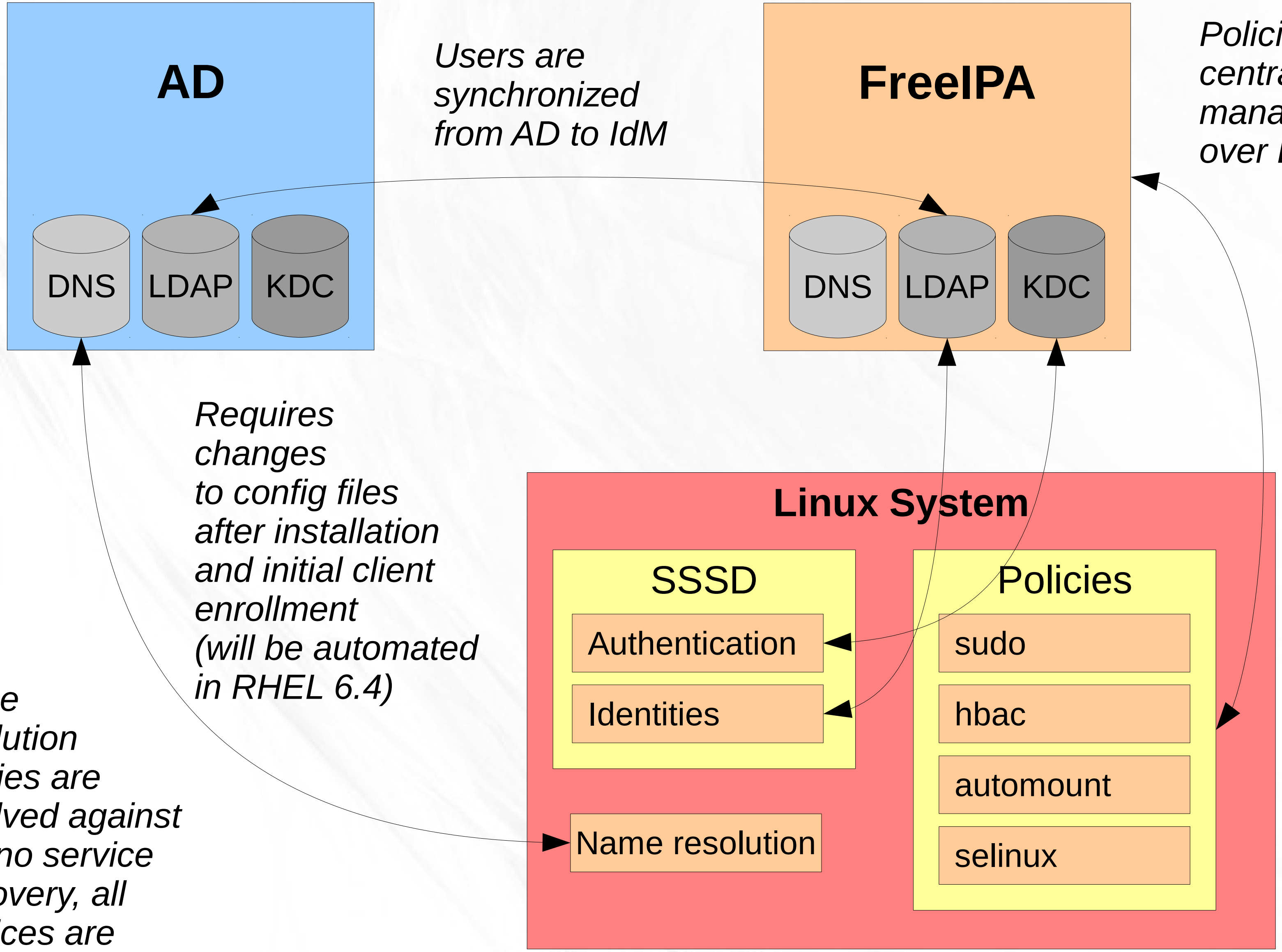
*Name resolution and service discovery queries are resolved against IdM*

# Pros and Cons of the Split Brain Solution

- Pros:
  - All authentication happens against AD
- Cons:
  - We can’t do clean upgrades from this configuration
  - It is a manual configuration

*We do not recommend this configuration.*

# FreeIPA Based Integration (AD DNS)



*Users are synchronized from AD to IdM*

*Policies are centrally managed over LDAP*

*Requires changes to config files after installation and initial client enrollment (will be automated in RHEL 6.4)*

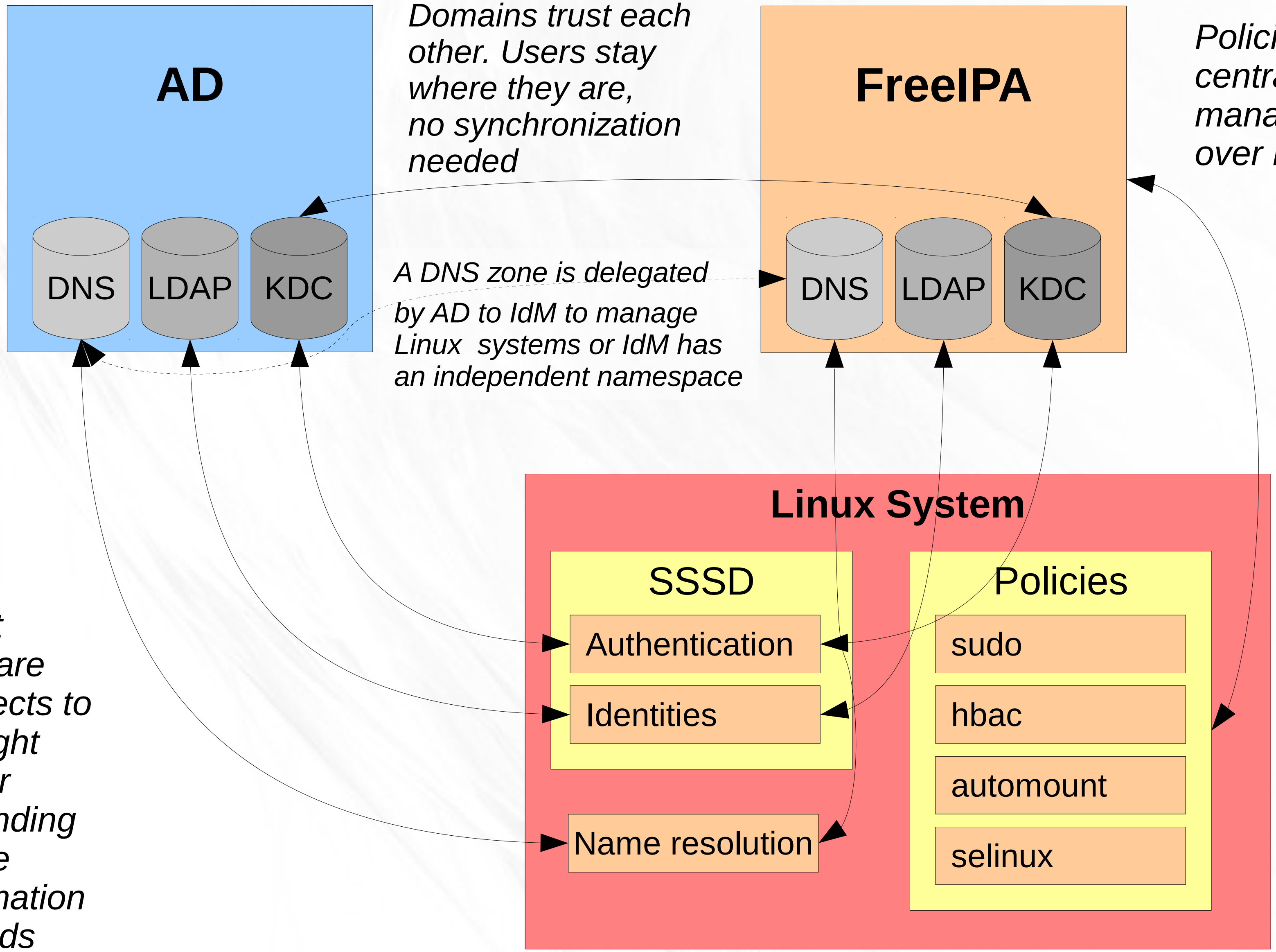
*Name resolution queries are resolved against AD, no service discovery, all services are configured explicitly*

# Pros and Cons of Integration without FreeIPA DNS

- Pros:
  - AD DNS is used
- Cons:
  - Either each client needs to be explicitly configured with the list of the servers or AD DNS needs to configure a subdomain and clients should be configured to use this subdomain
  - The service discovery is turned off or discovery is done via subdomain

*This option effectively more work for Linux admins because AD admins rule the environment.*

# FreeIPA – AD Trust Integration Option



*Domains trust each other. Users stay where they are, no synchronization needed*

*Policies are centrally managed over LDAP*

*A DNS zone is delegated by AD to IdM to manage Linux systems or IdM has an independent namespace*

*Client software connects to the right server depending on the information it needs*

# Pros and Cons of the FreeIPA Trust Integration

- Pros:
    - Reduces cost – no CALs or 3rd party
    - Policies are centrally managed
    - Gives control to Linux admins
    - Enabled independent growth of the Linux environment
    - No synchronization required
    - Authentication happens in AD
- Cons:
    - Requires proper DNS setup
    - Requires SSSD 1.9

# Summary

While direct integration is possible and in some cases required the FreeIPA based integration option is the most cost efficient and feature rich option that is currently available so it is recommended as a preferred choice for the integration of the Linux infrastructure into existing AD environments.

# Questions?