FreeIPA

TutoJRES

Jérôme Fenal – Red Hat
jfenal@redhat.com
+33 6 88 06 51 15

Red Hat

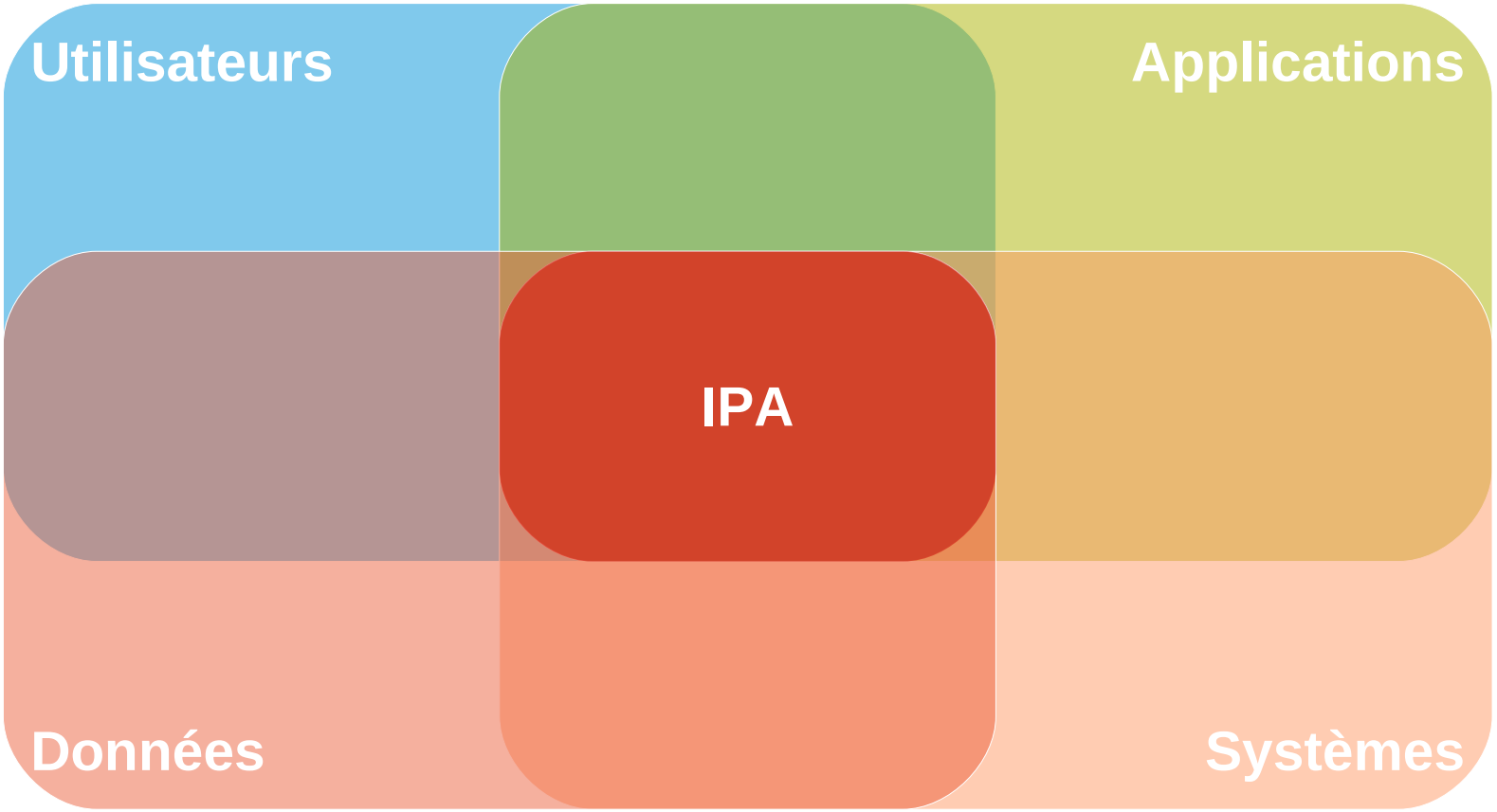
Le modèle Red Hat

Le modèle technologique Red Hat

Open source = Innovation + Stabilité + Sécurité + Qualité

FreeIPA

Le défi

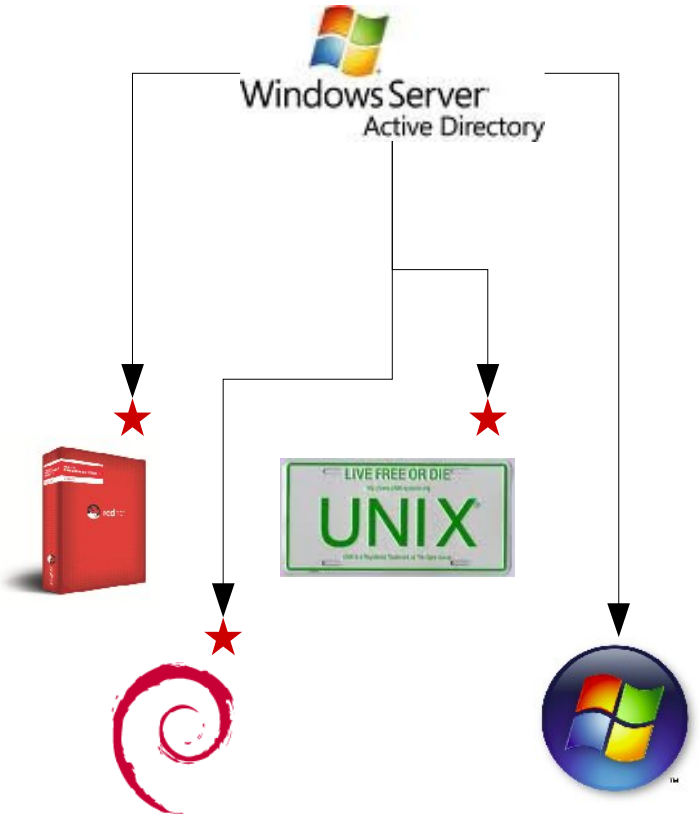


Quelles sont les autres options ?

- **Intégration spécifique ?**
  - Options:
    - LDAP ou Annuaire
    - Ajout possible de Kerberos
  - Inconvénients
    - Complexe, choix de schémas à faire
    - Nécessite une expertise LDAP & Kerberos
    - Cher à maintenir et personnaliser
    - Intégration client complexe
    - OK pour l'identité, difficile pour les politiques
- **Solution propriétaire ?**
  - Options:
    - CA Etrust Access Control for OS
    - IBM Tivoli Access Manager for OS
    - FoxT BOXS
    - Symark Powerbroker
  - Inconvénients :
    - Très chers, peu flexibles
    - Contrôlent une information vitale sous un format propriétaire
    - Intégration parfois difficile avec les OS
- **Connecter Linux à Microsoft Active Directory ?**

Pourquoi ne pas gérer les Linux avec AD?

- **Options :**
  - Samba
  - Likewise
  - Centrify
  - Quest Vintela
- **Avantages :**
  - Ré-utilisation de l'infra Active Directory
  - Fonctionne OK pour identité et authentification
- **Inconvénients :**
  - Dépendance accrue à Microsoft
  - Difficulté de gérer et auditer correctement les politiques
  - Oblige à utiliser les politiques Microsoft sur Unix
  - Ne profite pas des capacités de la plate-forme
- **Analyse :**
  - Si Linux n'est pas une plate-forme stratégique, cette option peut fonctionner
  - Si Linux est une plate-forme stratégique, IPA a plus à offrir



IPA v1

freeIPA

identity | policy | audit

- **Composants**
  - Distribution Linux (Fedora / Red Hat Enterprise Linux / CentOS)
  - 389 Directory Server
  - MIT Kerberos
  - NTP
  - Outils d'installation
  - Outils d'administration (web et ligne de commande)
- **Cas d'utilisation ciblés**
  - Authentification d'un utilisateur sur Kerberos & LDAP au lieu de NIS
  - Mise en place simple et aisée de l'environnement LDAP & Kerberos
  - Gestion centrale et aisée (IHM) des utilisateurs Linux/Unix
  - Synchronisation de base avec AD, avec des plans pour la rendre robuste
- **Raisons d'utiliser IPA**
  - Réglementations qui pousse à évacuer NIS
  - Efficacité demandée quant à la gestion des identités
  - Coût de maintenance élevé d'une solution maison LDAP/Kerberos

IPA v2 : Composants

- **Distribution Linux (Fedora / Red Hat Enterprise Linux / CentOS)**
  - 389 Directory Server
  - MIT Kerberos
  - NTP
  - Outils d'installation
  - Outils d'administration (web et ligne de commande) extensible via greffons
  - Autorité de certification & Autorité d'Enregistrement (Dogtag Certificate Server)
  - DNS (Bind)

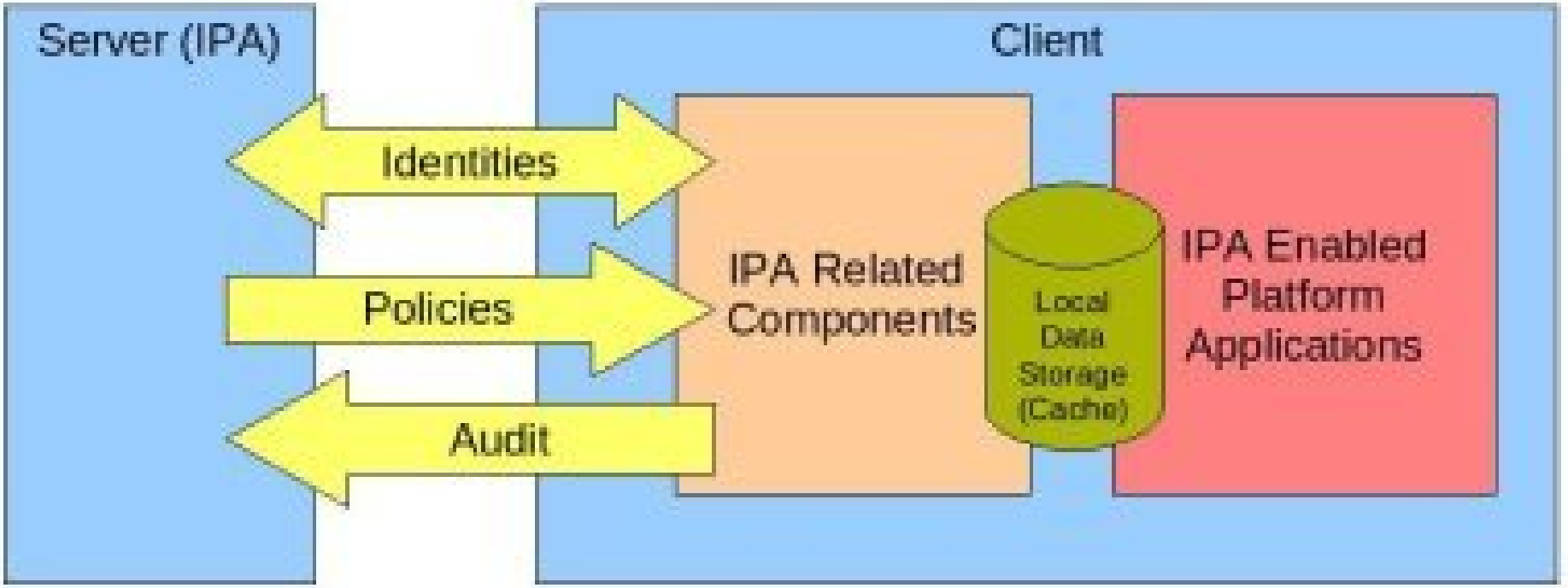
IPA v2 : Cas d'utilisation ciblés

- **Gestion de l'identité des utilisateurs (basée sur IPA v1)**
- **Gestion de l'identité des machines**
  - Intégration des nouveaux systèmes
    - En conséquence, un *principal* pour ce nouveau système doit être créé et déployé sur le système
    - Ses lettres de créances : *keytab* ou certificat pour le système
  - Authentification des systèmes
    - Les systèmes du réseau devant avoir accès au royaume IPA doivent être authentifiés dans ce royaume
    - Ces lettres de créances doivent permettre une authentification et une approbation mutuelles, du chiffrement, et des capacités de SSO pour les services et applications accédant aux ressources et autres services du royaume
- **Gestion des systèmes**
  - Gestion des systèmes indivuels, des groupes, et des instances virtuelles
  - Gestion centralisée des différents types de politiques applicables
- **Contrôle d'Accès**
  - Gestion centralisée des contrôles d'accès PAM (HBAC - *host based access control*)

IPA v2 : Raisons de l'utiliser

- **Le respect et le contrôle du respect des réglementations obligent les organisations à sortir de NIS, pour aller vers une solution centralisée de gestion de l'identité et des contrôles d'accès dans le monde Linux/Unix.**
- **Efficacité et productivité demandée quant à la gestion des identités**
- **Coût de maintenance élevé d'une solution maison LDAP/Kerberos**
- **Utilisation de services qui s'appuie sur d'autres mécanismes de sécurité**
- **Réglementation et productivité motivent une gestion centrale de la délégation des droits administrateurs**

Architecture



IPA v2

- **Fonctionnalités**
  - Support i18n étendu, dont 8 traductions
  - Évolution de l'API XMLRPC (non compatible avec IPA v1)
  - Utilisation de mod_wsgi au lieu de mod_python
  - Une Autorité de Certification est requise, et configurée par défaut
  - Réutilisation possible par l'installeur de l'ancien certificat auto-signé via --selfsign
  - Pages de manuel
  - Une règle HBAC (*Host-Based Access Control*) par défaut pour permettre à tous de se connecter à tous les systèmes.
    - Solution de facilité pour tester
    - Cette règle allow_all doit être retirée pour le déploiement
  - nscd désactivé, remplacé par sssd sur la gestion de cache
- **Mais :**
  - La CA doit être installée en locale en_US (BZ#588375)

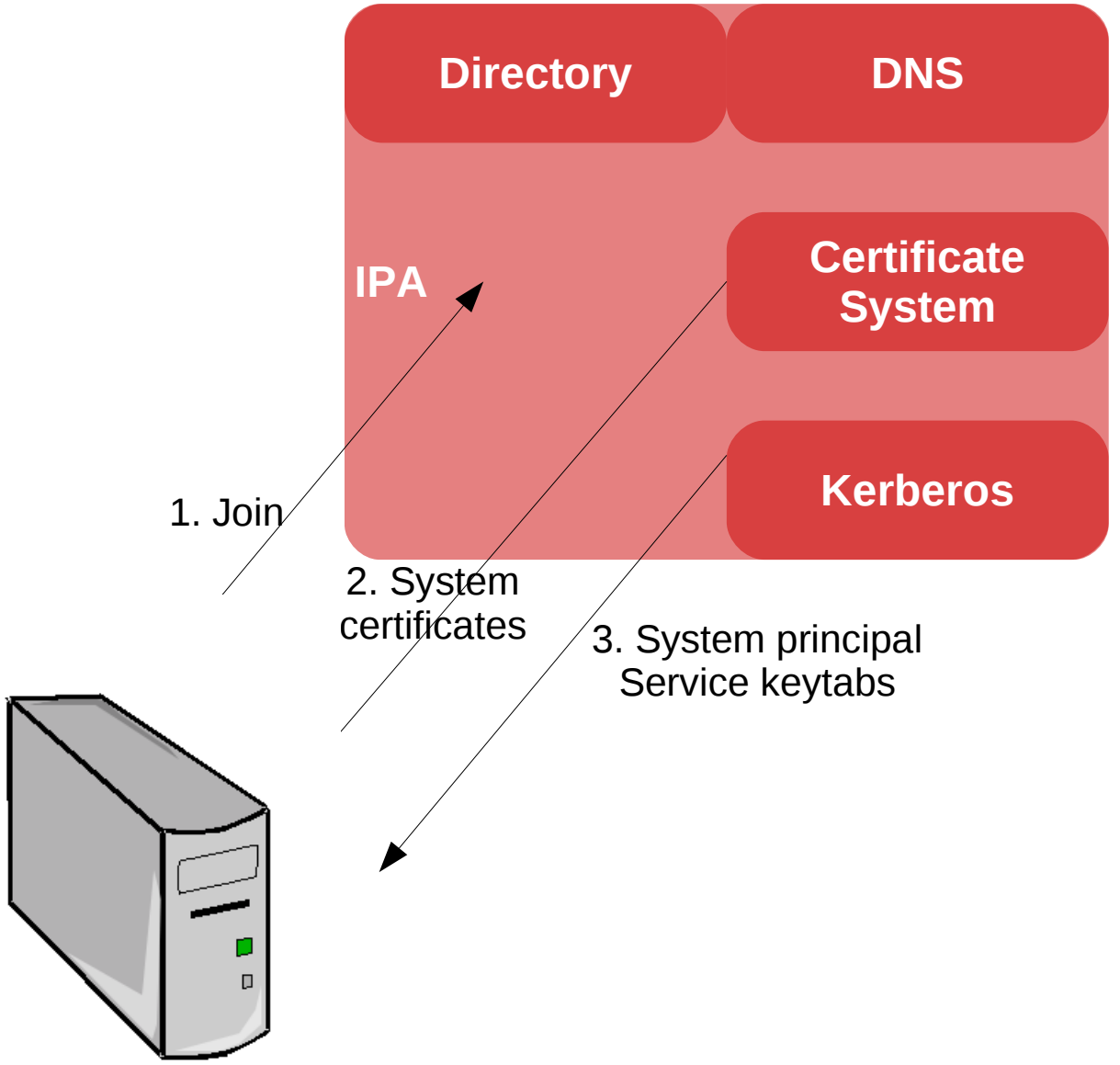
SSSD

- **Remplacement des couches nss_ldap et pam_ldap**
- **Cache mémoire**
- **Cache disque**
- **Profil persistant (à la Windows)**
- **Permet de s'affranchir de nscd**
- **Introduit dans Fedora 11**
- **Utilisable seul ou avec IPA**

certmonger

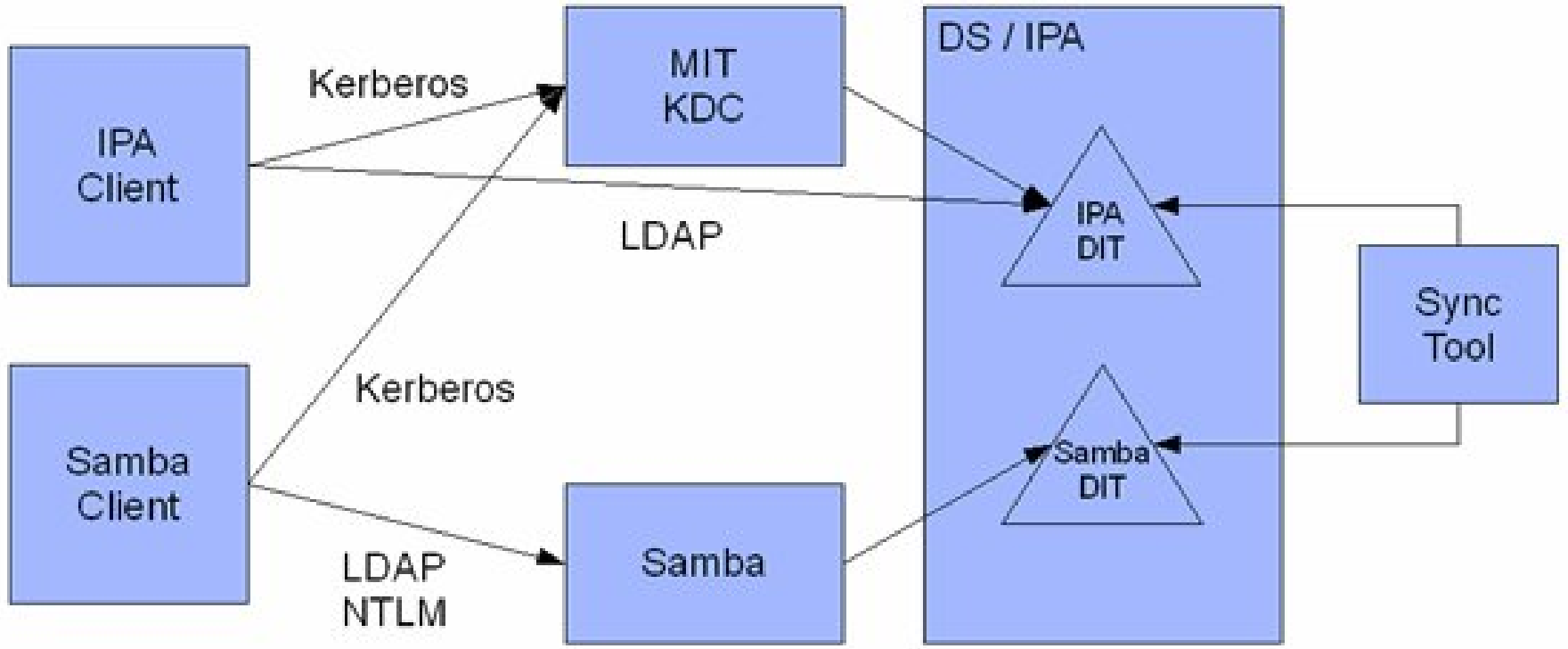
- Aims to manage certificates for services running on client systems.
- Supports multiple certificate storage formats.
- Will warn administrators of certificates approaching the end of their validity periods.
- Can attempt to re-enroll with a CA.
- Supports IPAv2 and certmaster CAs out of the box.
- Extensible to support additional CAs.

Enrôlement d'un système



IPA v3 : vos besoins

- **http://www.freeipa.org/page/V3PRD**
- **http://www.freeipa.org/page/IPAv3_development_status**
  - For IPA to become integrated and trusted by AD, IPA needs to be able to pretend as if it is an AD domain controller. This can be accomplished by integrating Samba 4 and IPA. The two components need to be able to operate on the same data and share the KDC. The following page gives deeper into the drivers and high level architecture of the proposed solution: "IPA and AD" integration.



Participez !

- **IPA v2 arrive d'ici quelques semaines**
- **Une vision unifiée de la gestion d'identité et du contrôle d'accès pour Linux et Unix**

- **Rejoignez-nous :**
  - www.freeIPA.org
  - freeIPA-devel@redhat.com
  - freeIPA-interest@redhat.com

En détail (2/2)

- Provide feedback if a -mod command is executed and no changes are performed
- Don't log passwords into files during installation
- Add option to enable pam_mkhomedirs in the IPA client installer
- Fixed a number of bugs in the pwpolicy plugin
- More detailed error messages when entries are not found
- Viewing binary in the UI shouldn't cause it to fail
- dogtag is a required component and now configured by default
- Run the XML-RPC server under mod_wsgi instead of mod_python
- Fix the --all and --raw options
- 8 translations:
  - Bengali India
  - Indonesian
  - Ukrainian
  - Kannada
  - Polish
  - Russian
  - Spanish
  - Chinese Simplified
- Other minor polish and bug fixes

En détail (1/2)

- Fix memory crash-bug in ipa-join
- Add pwpolicy2 plugin, future replacement for pwpolicy
- CSRs that don't include NEW in the header/footer blocks should work now
- Lots of clean-ups in ipa-client-install
- ipa-server-install and ipa-client-install now use backed-up files and state in /var/lib/ipa and /var/lib/ipa-client to determine whether they are already configured or not
- Fixed bug in some DNS entries that were missing a trailing dot (.)
- Fix bug in password plugin that prevented ldappasswd from working on non-kerberized users
- In the client installer we will have certmonger issue certificate requests using the subject base that IPA is configured with. This will make certmonger play nicer with the selfsign CA.
- IPA works when using external CA option again
- Stop using LDAPv2-style escaped DNs where possible
- Updated MITM integration with dogtag
- Anonymous VLV is enabled when the compat plugin is enabled making Solaris 10 clients happy
- Add a CRL URI to certificates that are issued by dogtag
- Added an ipa man page
- XML-RPC signature change. This will affect older alphas command-line utilities trying to talk to a new server
- Fixed bug in host plugin where deleting a non-qualified hostname would delete just the host, not the service entries associated with that host.
- ipa-replica-manage now uses kerberos to delete and list servers. Add still requires the DM password
-