



IPA – Identity, Policy, Audit

Karl Wirth, Red Hat

Kevin Unthank, Red Hat

What is IPA?

- A) India Pale Ale
- B) Identity, Policy, and Audit
- C) An open source project
- D) A Red Hat solution offering
- E) All of the above



**RED HAT
ENTERPRISE IPA**

Why care about IPA?

1. Compliance

(Because you have to)

- Migrate off of NIS and NIS+
- Have unified employee identity across the organization
- Change the password regularly
- Control which admins can access what machines
- Audit who accessed what when

2. Risk reduction

(To protect money, data, name)

3. Efficiency

(To save costs)

- Centrally manage security
- Group up users, machines, services
- Unified view of policy
- Unified view of audit

4. Business enablement

(To provide solutions)

- Will enable solutions based on
 - Linux desktop
 - MRG
 - Virtualization

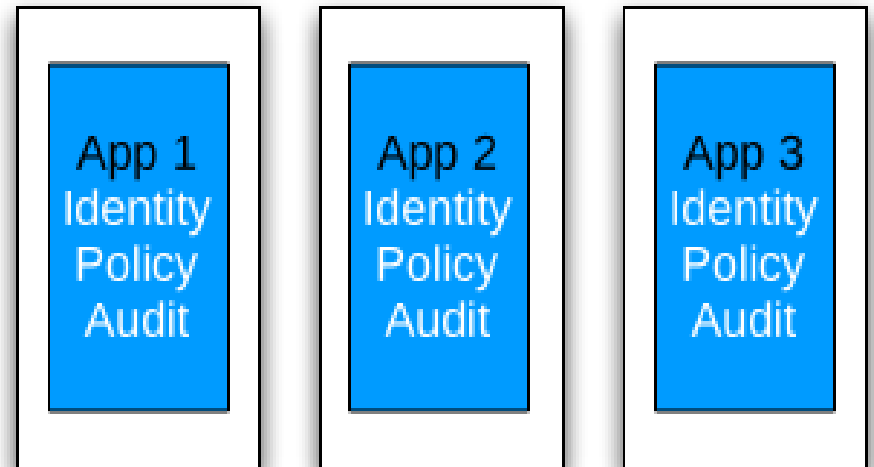
Security Information Situation Today

Many security and security management applications store and manage their own vital security information

- Identity
- Policy
- Audit

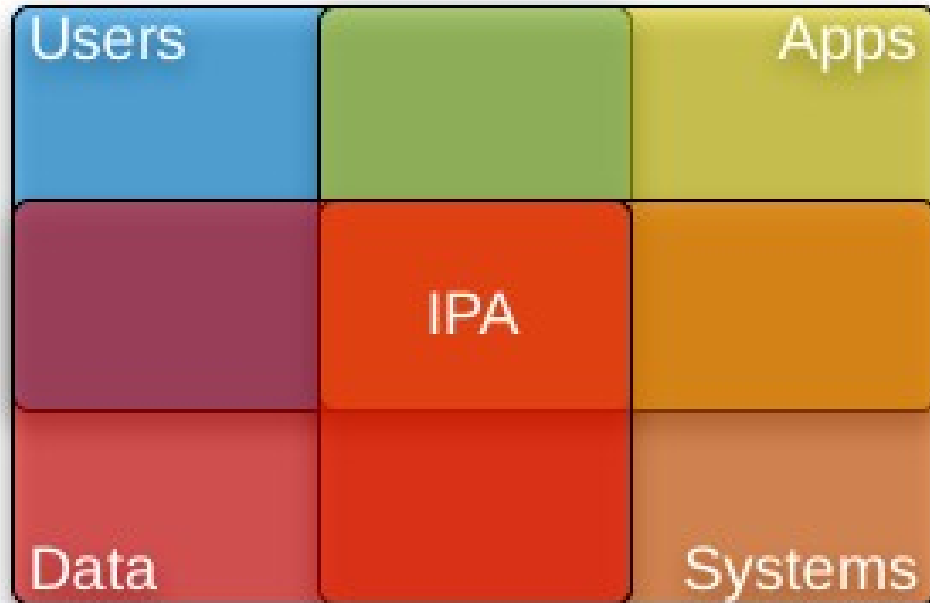
Difficult to analyze across applications, so organizations can't

- Form a full picture of their security stance
- Comply with government regulations
- Protect themselves sufficiently
- Efficiently enable their operations



What is needed?

To enable this:



Maximize freedom
Maximize efficiency

Vital security information (IPA) should be:

- Open (You own it)
- Inter-operable
- Manageable

Need a way to make it possible for vital security information

- Identity
- Policy
- Audit

to enable the freedom and efficiency of next generation IT infrastructure

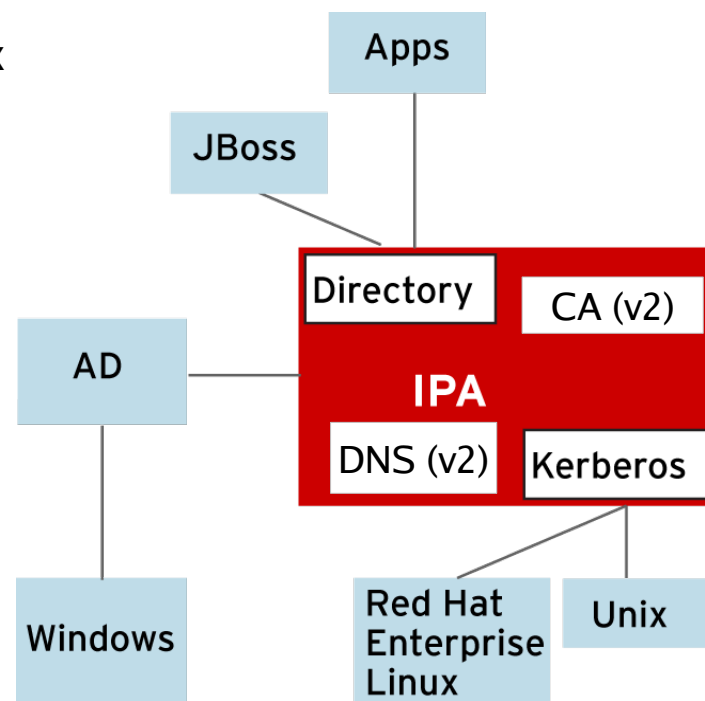
What is Red Hat Enterprise IPA?

Based on freeIPA project, www.freeIPA.org

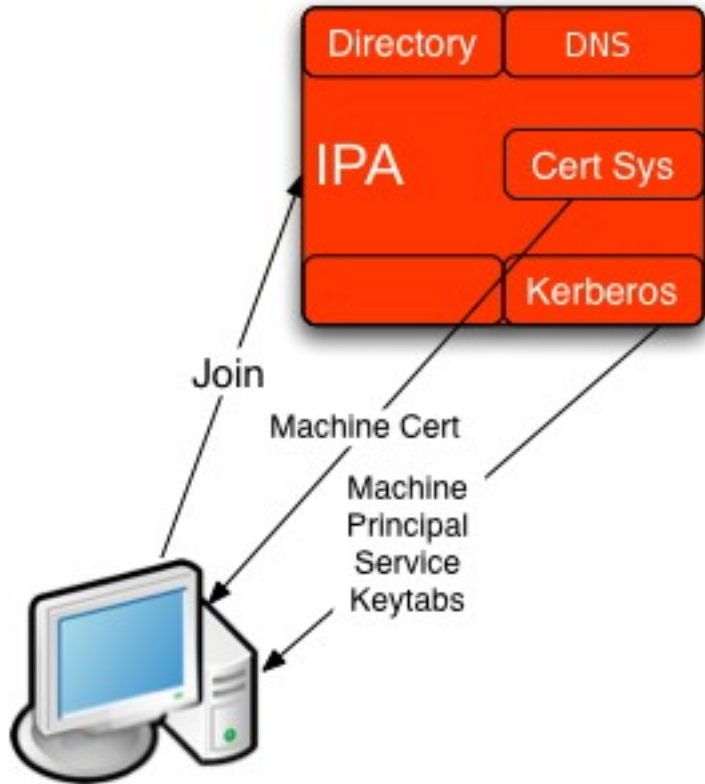
v1: Centralized user identity management for Linux/Unix

- Combine Directory and Kerberos
- Easy install and management
- Use it without being an LDAP or Kerberos expert
- One user identity, synched with AD
- Migration off of NIS
- Single sign on for users
- Basic host based access control

v2: Full Identity and Access Management for Linux/Unix



What is planned for v2?



Included DNS and Certificate Authority (not for users)

Identify and group machines, Vms, services

Simplified service authentication and establishment of secure communication

- Machine identity via Kerberos, certificate
- Process identity via Kerberos principal

Management of machine certificate

Centrally managed access control

- Extensible policy framework
- Set policy of which users can access which apps on which machines
- Centrally managed scoped admin control

Central audit database

- Centrally audit security event, logs, compliance with lockdown

What are the other options?

1. Roll your own

- *Options:*
 - LDAP or Directory.
 - Possibly add in Kerberos.
- *Problems*
 - Complex. Many schema options.
 - Need LDAP/Kerberos expertise
 - Expensive to maintain/customize
 - Client integration not adequate
 - Ok for Identity. Hard for policy.

2. Proprietary solutions

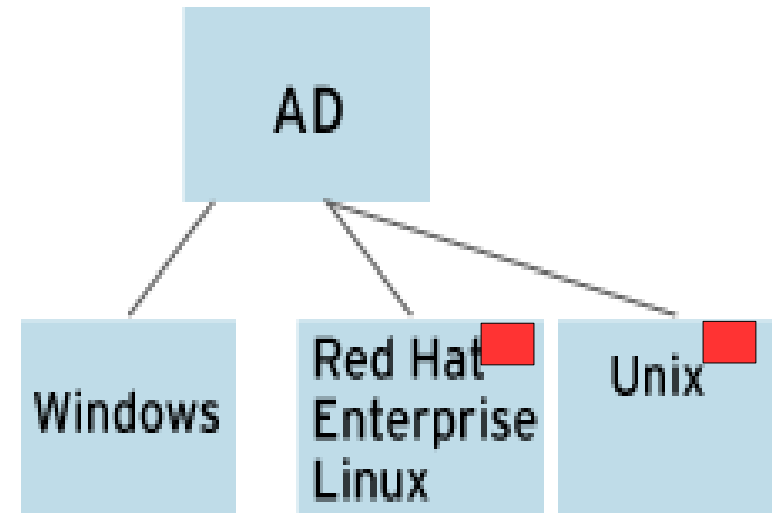
- *Options:*
 - CA Etrust Access Control for OS
 - IBM Tivoli Access Manager for OS
 - FoxT BOXS
 - Symark Powerbroker
- *Problems:*
 - Very expensive. Inflexible
 - Control vital security information in proprietary format
 - Don't always play nicely with OS

3. Connect Linux directly to Microsoft Active Directory (AD)

- *Discussed on next slide*

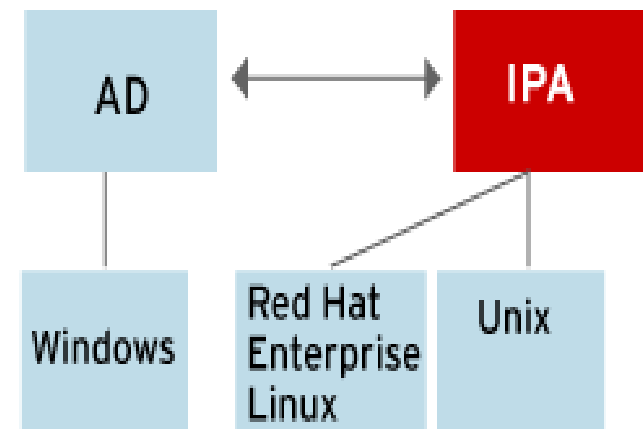
Why not manage Linux machines with AD?

- *Options:*
 - Samba
 - Likewise
 - Centrify
 - Quest Vintela
- *Benefit*
 - Reuse Active Directory infrastructure
 - Works fairly well for identity, authentication
- *Problems*
 - Increases dependence on Microsoft
 - Doesn't manage native policy and audit well
 - Forces Microsoft policy on *nix
 - Doesn't leverage platform features
- *Analysis*
 - If RHEL is not a strategic platform, these kinds of options may work
 - If RHEL is a strategic platform, consider IPA



How will IPA integrate with AD and Windows

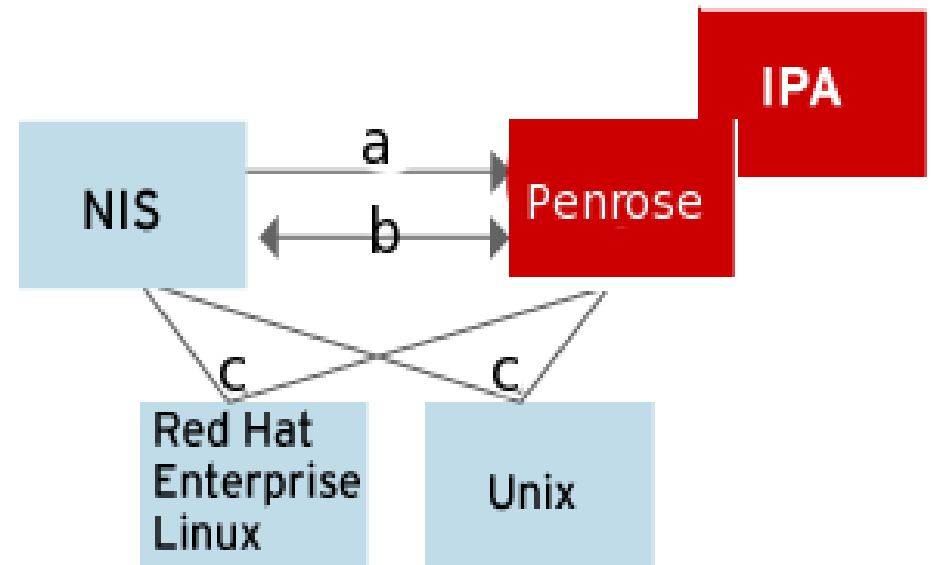
- In IPA 1: Synchronization of user identity, PW
 - Two way or one way synch
 - Flexible attributes, full posix, groups
 - Password
- Future plans
 - Kerberos Trust between IPA and AD
 - Samba 4 plug in to IPA



How can you migrate from NIS to IPA?

Leverages Red Hat Penrose Virtual Directory Server NIS migration features

- a. Import NIS data to IPA. Begin uid, gid conflict resolution.
- b. Keep data between NIS and IPA in synch
- c. Slowly switch NIS clients to point at Penrose and talk LDAP
- d. Slowly organization removes data from the NIS mapped tree in IPA and just uses the authoritative IPA userid
- e. Repeat for next NIS domain



Conclusion

IPA = Identity, Policy, Audit

Identity and Access Management for the Unix/Linux world

- v1 = User Identity Management – here now
- v2 = Adds in machines/service identity, policy, audit -- coming

Join our community and contribute!

- www.freeIPA.org
- freeIPA-devel@redhat.com
- freeIPA-interest@redhat.com



Benefits

- Compliance
- Efficiency
- Risk Reduction

