RED HAT ENTERPRISE IPA

INTRODUCTION

Red Hat Enterprise IPA enables your organization to comply with regulations, reduce risk, and become more efficient. Simply and centrally manage your Linux/Unix users and their authentication today. And in the future, your Linux/Unix machines, services, policy, and audit information.

Government and industry compliance regulations, as well as best practice risk reduction principles require an organization to establish:

- the administrative users accessing machines and services on those machines
- which machines and services users have accessed
- the actions those users took
- policies to control user access to particular machines and service
- policies around password strength to protect against unauthorized access

Establishing these things simply and centrally, in addition to the obvious security benefits, brings significant efficiencies such as:

- reduced time and manual work in an internal or external audit
- reduced time spent adjusting parameters and policies for individual machines
- more rapid deployment and migration of workloads in the environment
- increased ability to benefit from initiatives such as Red Hat Linux Automation

EXISTING SOLUTIONS

To solve these problems, organizations have essentially three options. Roll your own solution; purchase an expensive proprietary solution; or leverage an existing Microsoft Active Directory infrastructure for your Unix/Linux identity and policy.

ROLL YOUR OWN

For over a decade, organizations have used Sun's Network Information Services (NIS) and NIS+ to provide central management of identity and policy for users and machines in the Linux and Unix environment. NIS has some serious weaknesses that could cause NIS to fail some security compliance audits.

"NIS is rather insecure by today's standards. It has no host authentication mechanisms and passes all of its information over the network unencrypted, including password hashes. As a result, extreme care must be taken to set up a network that uses NIS. Further complicating the situation, the default configuration of NIS is inherently insecure." [1]

Finally, many organizations' NIS domain deployments are haphazard and do not lend themselves to simple policy creation and auditing. For example, a user named Benjamin A. Smith may be *bsmith* in one NIS domain, *bensmith* in another, and *basmith* in a third. The same is true for a machine. This makes it difficult to establish a unified policy for a user's access or to audit his actions.

The natural progression of NIS is LDAP, and many organizations have deployed an LDAP server including OpenLDAP, Fedora Directory Server, or Red Hat Directory Server to solve the class of problems discussed in this paper. For many customers this is an excellent solution. For example, Red Hat Directory Server provides the ability to centralize user and group management, supports user authentication and password policies, supports NIS netgroups and central storage of sudoers"[1] information for access control policy, and provides for a way to centralize automounts. Some organizations have deployed Kerberos servers that work together with their LDAP solution to provide single sign-on, but the resulting solution is highly complex and a constant effort is required to keep the separate Kerberos and LDAP identity stores synchronized.

However, in spite of the power and broad use of Red Hat Directory server and other LDAP servers, we would still classify this as a "roll your own" solution for the following reasons:

- These deployments require a large amount of expertise in LDAP.
- It is often not straightforward to integrate the clients of the LDAP server. Customization is required. Even so, client support is sometimes incomplete. For instance, an offline mode is not supported.
- Setup of the LDAP solution requires significant configuration. For example, choices need to be made about which schema to use.
- A Kerberos deployment adds much greater complexity and amplifies the client's problems and need for expertise.

[1] http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/s1-server-nis.html

EXISTING PROPRIETARY SOLUTIONS

A variety of software companies have developed applications to manage and enforce identity, policy, and audit within the Unix/Linux world. Examples include CA Etrust Access Control for OS, IBM Tivoli Access Manager for OS, FoxT BOXS, and Symark Powerbroker. These applications have been available for many years but still exhibit many problems when deployed within an organization, including:

- Expensive. As a result, many organizations limit their deployment of these applications to specific high-risk machines, which forces the organization to maintain two sets of solutions.
- Inflexible. These solutions are large proprietary collections of code that are difficult to enhance or customize.
- Limited interop. While many of these solutions are able to make available or utilize identity/authentication information from other applications, it is more difficult to access and leverage the policy and audit data they contain for reuse or analysis by other applications.
- Interaction with Linux. Some of these solutions have had a checkered history of robust support for Linux.

INTEGRATE DIRECTLY WITH EXISTING MICROSOFT ACTIVE DIRECTORY INFRASTRUCTURE

Many organizations already have a mission-critical Active Directory infrastructure for their Windows environment. Of course, every one of these organizations will need some integration of their Unix/Linux solution with the AD/Windows environment. The Red Hat Enterprise IPA features for synchronization with Active Directory will be discussed later.

Some organizations look to utilize this infrastructure by integrating their Unix and Linux environment into Active Directory. To do this, many use Samba and others, looking for deeper integration that doesn't exist today in Samba, turn to companies such as Likewise, Centrify, and Quest Vintela to connect Unix/Linux directly to Active Directory.

This approach is generally adequate for user authentication but not sufficient for policy, as it forces Windows' policy concepts into the Unix and Linux world. Also, Microsoft Active Directory's Group Policy is notoriously difficult to work with and extend. One organization that has taken this direct into Active Directory integration approach is now exploring how to use Red Hat Enterprise IPA in the future to manage policy.

This approach has the same weakness as other existing proprietary solutions: your organization's vital identity, policy, and audit information gets tied up in a solution not known for its ease or willingness to inter-operate.

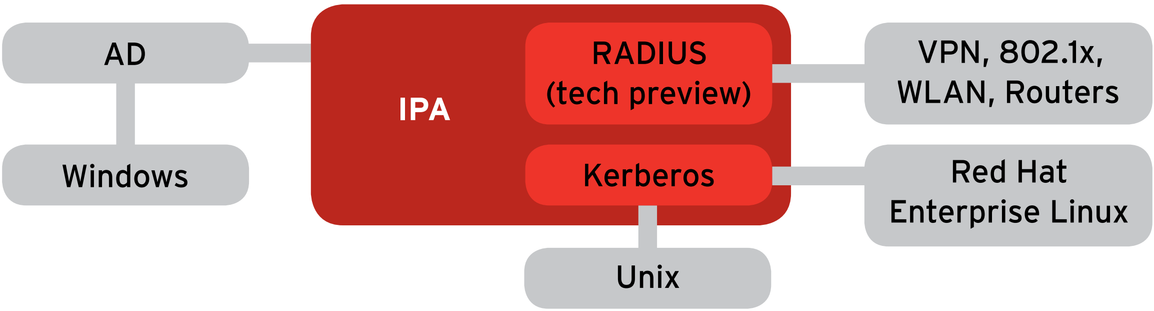
Red Hat recommends Red Hat Enterprise IPA to manage identity, policy, and audit in a Unix and Linux environment. However, we recognize that some organizations will wish to centralize entirely on Active Directory and tie Red Hat Enterprise Linux directly into Active Directory. For these organizations, Red Hat is investing heavily in Samba. Red Hat is also structuring a partnership with Likewise, whose Likewise Open (open source) and Likewise Enterprise (proprietary) supplement Samba's interaction with Active Directory. And we are willing to work with any of the major vendors providing Linux to Active Directory interoperability.

RED HAT ENTERPRISE IPA 1.0

The open source freeIPA project (www.freeIPA.org) has been working on a attractive alternative to the solutions described above. Red Hat is productizing and offering support for freeIPAv1 as Red Hat Enterprise IPA 1.0.

The focus of this release is to enable centralized user identity management for the Linux/Unix environment and build a framework that will enable future functionality.

RED HAT ENTERPRISE IPA 1.0



RISK REDUCTION AND EFFICIENCY FOR IT

Red Hat Enterprise IPA 1.0 will enable significant risk reduction and efficiency gains for IT by providing:

- Simple setup and deployment of an LDAP and Kerberos solution. Installation of IPA is a simple command line. Five minutes later you will have Red Hat Directory Server installed with the appropriate schema and MIT Kerberos v5 installed with Red Hat Directory Server as its back end. One userid shared between LDAP and Kerberos, and Kerberos gets the benefit of the directory server's multi-master replication. Setting up replicas is just as easy. Install another server and run an additional command line to provide the servers with their replication manifest. There is no need to master LDAP schemas and LDIF commands or Kerberos protocols to set up either.
- Simple, secure ongoing management. One of the goals of Red Hat Enterprise IPA is to allow you to harness the benefits of LDAP and Kerberos without having to master either. To this end, we have provided an XML over RPC interface to allow for easy command line or scripting interaction with the servers. This makes it straightforward to add a user or group or trigger a password change. For those who prefer GUIs, there is an intuitive GUI built around search. Here you can manage users and groups and password policy in version 1.
- Centralized authentication point. Red Hat Enterprise IPA allows an increasing amount of your authentication traffic to flow through one logical point. Today this includes OS logon and ongoing authentication against LDAP or Kerberos and Application logon against LDAP. Knowing who logged onto what and when allows an efficient audit today and will enable policy controls in the future.
- Services mutually authenticate and encrypt with Kerberos. Red Hat Enterprise IPA 1.0 provides an API call to allow services to request Kerberos keytabs. Two services can use these keytabs to mutually authenticate and encrypt their communication. This is a first step toward Red Hat Enterprise IPA managing the security infrastructure of your environment.

EFFICIENCY FOR END USERS

- Single sign-on with Kerberos. End users get frustrated having to constantly type the same (or a different password) to access the variety of applications they need to perform their jobs. With Red Hat Enterprise IPA in place, a user’s initial logon via PAM will result in the end user being issued a Kerberos ticket. That ticket can be presented to any application that is kerberized, resulting in the end user gaining access without having to retype a password. A variety of applications are kerberized today, and Red Hat is working to kerberize more. For instance, JBoss is working to support IPA-issued kerberos tickets in the next release of JBoss Application Server.
- End user self-service. End users will be able to access the Red Hat Enterprise IPA GUI and update their own information, such as a street address or name change, without getting access to other user’s pages.

COMPLIANCE

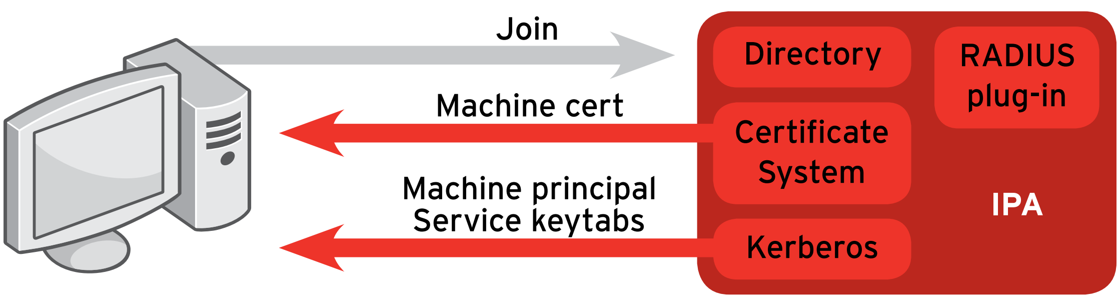
- One traceable identity for users. Many industry and government standards ask organizations to be able to easily audit user activity. Red Hat Enterprise IPA facilitates this by giving users one identity housed in the underlying LDAP server.
- Synced with Active Directory. Furthermore, this user identity can be kept in sync with the user’s identity, groups, and password in Active Directory.
- Migration away from NIS and NIS+. Many organizations are looking to migrate away from NIS and NIS+ for efficiency and compliance reasons. These organizations can move to Red Hat Enterprise IPA.

RED HAT ENTERPRISE IPA FUTURES

While Red Hat Enterprise IPA 1.0 is a robust solution in its own right, what is most exciting is the platform that it provides for future functionality.

Version 1.0 is focused on user identity management for the Unix/Linux world. The next major version will add the management of service and machine identity, policy, and basic audit. This will provide the following benefits:

RED HAT ENTERPRISE IPA FUTURES



EFFICIENCY AND RISK REDUCTION

- Easily provide and manage secure identity for machines, virtual machines, or services. Imagine that an administrator adds a new server to the datacenter. With Red Hat Enterprise IPA 2.0 in place, the administrator would authenticate on the new box against the IPA server. If the authentication is successful, IPA would trust the new box and deliver a Kerberos principal and certificate to denote the identity of the machine and Kerberos keytabs and certificates for the set of services on the box specified by the admin. When the certificates expired, Red Hat Enterprise IPA would automatically renew them. In this way, the security of the realm would be managed by Red Hat Enterprise IPA.

- Enable services to mutually authenticate and secure communications. Many services require the ability to mutually authenticate or secure their communications. Often the applications assume the presence of a certificate or Kerberos credential, leaving it to the IT organization to figure out how that happens. Red Hat Enterprise IPA will manage this for an organization.

- Easily manage who accesses what and when. Some organizations solve this problem of policy today using sudoers. Others use proprietary solutions. Others close their eyes to their lack of security and rigor in this area. Future versions of Red Hat Enterprise IPA will enable IT to group up users, services, machines, and vms, and then put in place policy that will centrally control who can access what, when. One way of describing this is centrally managed sudoers.

COMPLIANCE

- Centrally control level of access to machines and services given to admin groups. This functionality is described above. For many compliance standards, it is essential.

- Centralized audit of admin action. Future versions of Red Hat Enterprise IPA will look to bring back to a central database increasingly detailed, useful information about who accessed what when and who did what when within the Unix/Linux environment.

BUSINESS

- Externalize authentication to IPA. A basic benefit of an LDAP directory service is that it allows application developers to use the directory for authentication and not implement their own authentication system. Red Hat Enterprise IPA provides this same benefit.

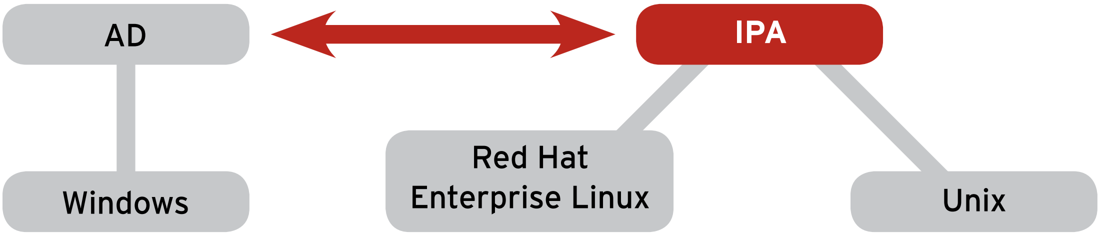
- Extensible policy framework to enable externalization of authorization to IPA. One of the goals of freeIPA is to provide similar benefit for authorization.

- Plug in architecture. Another goal of freeIPA which Red Hat Enterprise IPA plans to include is the ability to easily plug into Red Hat Enterprise IPA additional solutions and products that utilize its data and infrastructure to solve adjacent problems. An example of this is RADIUS. A RADIUS server plugged into Red Hat Enterprise IPA would enable remote access or 802.1x based authentication to be validated against the same back end Directory data, audit to be collected and combined with the LDAP/Kerberos audit data, and policy to be set coherently across the network. Initial work towards such a plug in has begun on freeIPA.org.

HOW WILL RED HAT ENTERPRISE IPA RELATE TO MY EXISTING ENVIRONMENT?

Of course, most IT organizations are not blank slates.
Red Hat Enterprise IPA will integrate well into your existing environment.

RED HAT ENTERPRISE IPA AND ACTIVE DIRECTORY



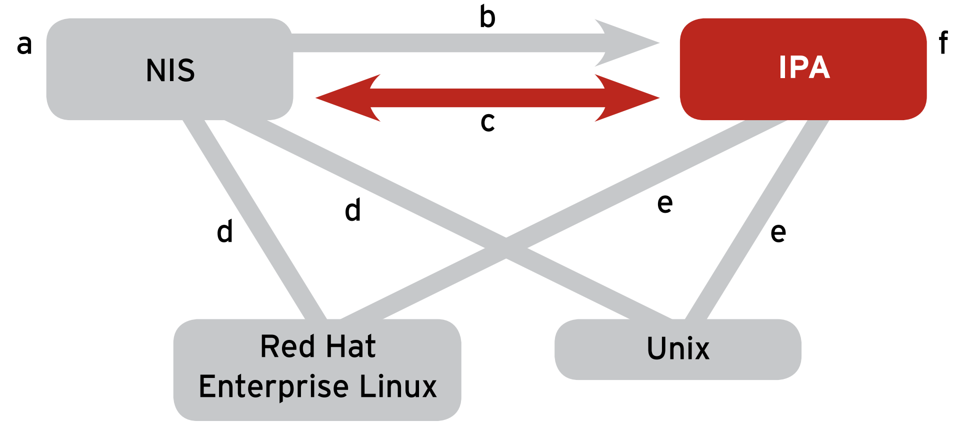
RED HAT ENTERPRISE IPA AND ACTIVE DIRECTORY

Above we discussed the strong advantages to your organization to natively manage the identity, policy, and audit for your Linux/Unix environment with Red Hat Enterprise IPA.

But Red Hat Enterprise IPA and Microsoft Active Directory cannot be an islands disconnected from one another. With this in mind, Red Hat Enterprise IPA provides basic synchronization today and will provide deeper integration in the future.

- Functionality available in Red Hat Enterprise IPA 1.0: Two way sync (or one way sync) between Active Directory and Red Hat Enterprise IPA with information such as username, group, and password.
- Future versions will provide two way sync of the full posix attributes and the ability for a user to use an Active Directory Kerberos ticket in an IPA realm.

MIGRATING FROM NIS TO RED HAT ENTERPRISE IPA



MIGRATING FROM NIS TO RED HAT ENTERPRISE IPA

For compliance, organizations must migrate away from NIS. Here is one scenario by which they could migrate from NIS to Red Hat Enterprise IPA.

- Organization maps data in a NIS domain to the IPA userid. (a)
- Organization dumps an NIS domain and moves data into a tree in IPA's directory and sets up mapping from that tree to the IPA userID. (b)
- IPA has a sync capability that keeps that NIS domain and IPA's data in sync. (c)
- Organization slowly points clients from the NIS domain to hit IPA via LDAP (e) instead of the NIS server via NIS. (d)
- Organization slowly removes data from the tree in IPA and just uses the authoritative IPA userid. (f)
- Repeat for next NIS domain.

SUMMARY

With Red Hat Enterprise IPA, your organization complies with regulations, reduces risk, and becomes more efficient. Today, you can simply and centrally manage your Linux/Unix users and their authentication. And in the future, your Linux/Unix machines, services, policy, and audit information.

Version 1 is focused on the central management of users and authentication for the Unix/Linux world. Future versions will add central manage of machine, virtual machine, and service identity, as well as basic admin policy such as centrally managed sudoers and audit. Interaction with Linux. Some of these solutions have had a checkered history of robust support for Linux.

© 2008 Red Hat, Inc. All rights reserved. "Red Hat," Red Hat Linux, the Red Hat "Shadowman" logo, and the products listed are trademarks or registered trademarks of Red Hat, Inc. in the US and other countries. Linux is a registered trademark of Linus Torvalds.