SUMMIT JBoss WORLD

PRESENTED BY RED HAT

LEARN. NETWORK. EXPERIENCE OPEN SOURCE.

redhat.

Managing Identity & Access in On-premise and Cloud Environments

Ellen Newlands
Identity Management Product Manager
Red Hat, Inc.
06.27.12

Agenda

- What is identity and access management
- Why should you care
- What are the challenges
- What does Red Hat offer now
- Identity Management overview and demo
- What’s on the roadmap
- Additional security presentations
- Let us know what you want

Identity Management (IdM) - What is it?

Identity management (IdM) describes the management of individual identities, their authentication, authorization, and privileges/permissions within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime, and repetitive tasks- *Wikipedia*

Identity Management – Why do I care?

- Control who has access to what to protect digital assets from theft and loss
- Enforce security policies for the devices that connect with the network
- Provide added security for cloud implementations
- Comply with government security and privacy regulations
  - Sarbanes-Oxley
  - Gramm-Leach-Bliley
  - HIPAA
  - FISMA, ENISA, more coming...

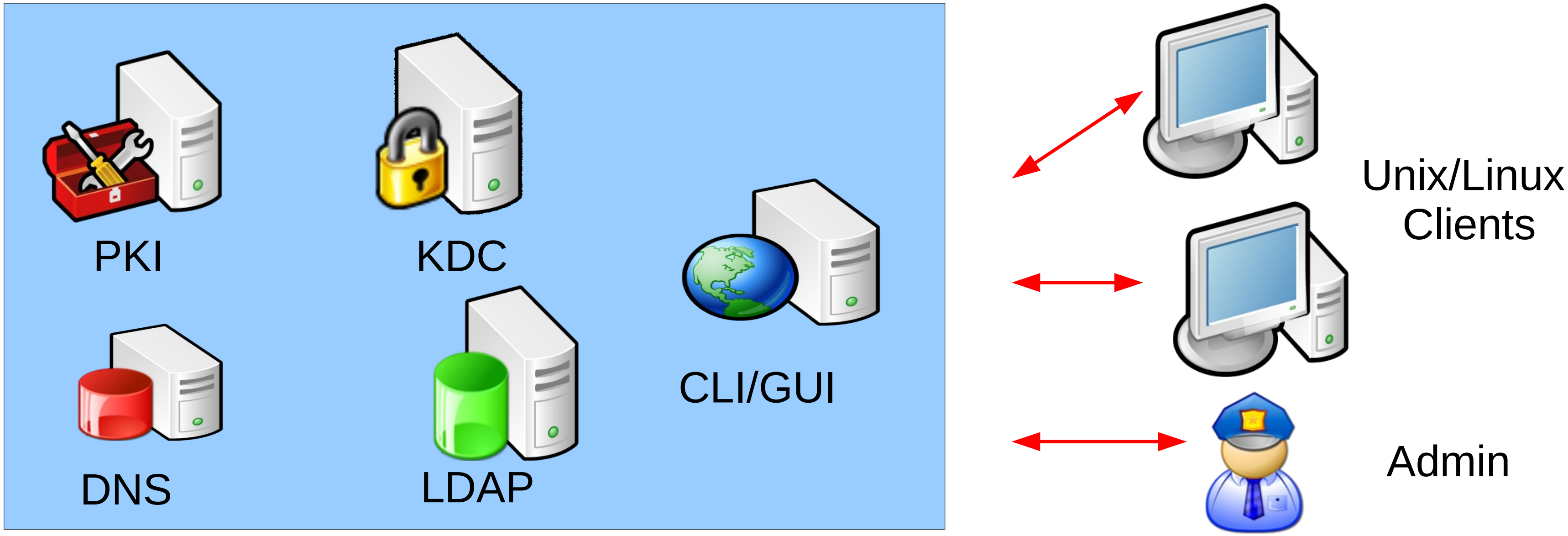
Identity Management – The Challenges

- Identity and authentication is a complex problem – many disjoint technologies exist.
  - Example: LDAP to manage identity, Kerberos to authenticate
- An identity management solution can be:
  - Complex to install, integrate and manage
  - Difficult to support and maintain
  - Proprietary and inflexible
  - Expensive, whether bought or built
  - Not well-suited for a Linux/UNIX environment

Identity Management in Red Hat Enterprise Linux – What is it?

- It is a domain controller for Linux
- Design Goals:
  - Produce a central server that stores identity information, policies related to identities and performs authentication
  - Use open source and standards-based components
  - Combine those components to provide an integrated, centralized enterprise identity management solution
  - Develop a solution that takes advantage of native Linux capabilities a domain controller for Linux
  - Deliver it as a free, integrated feature of Red Hat Linux
  - Make it easy - simple to install, deploy and manage

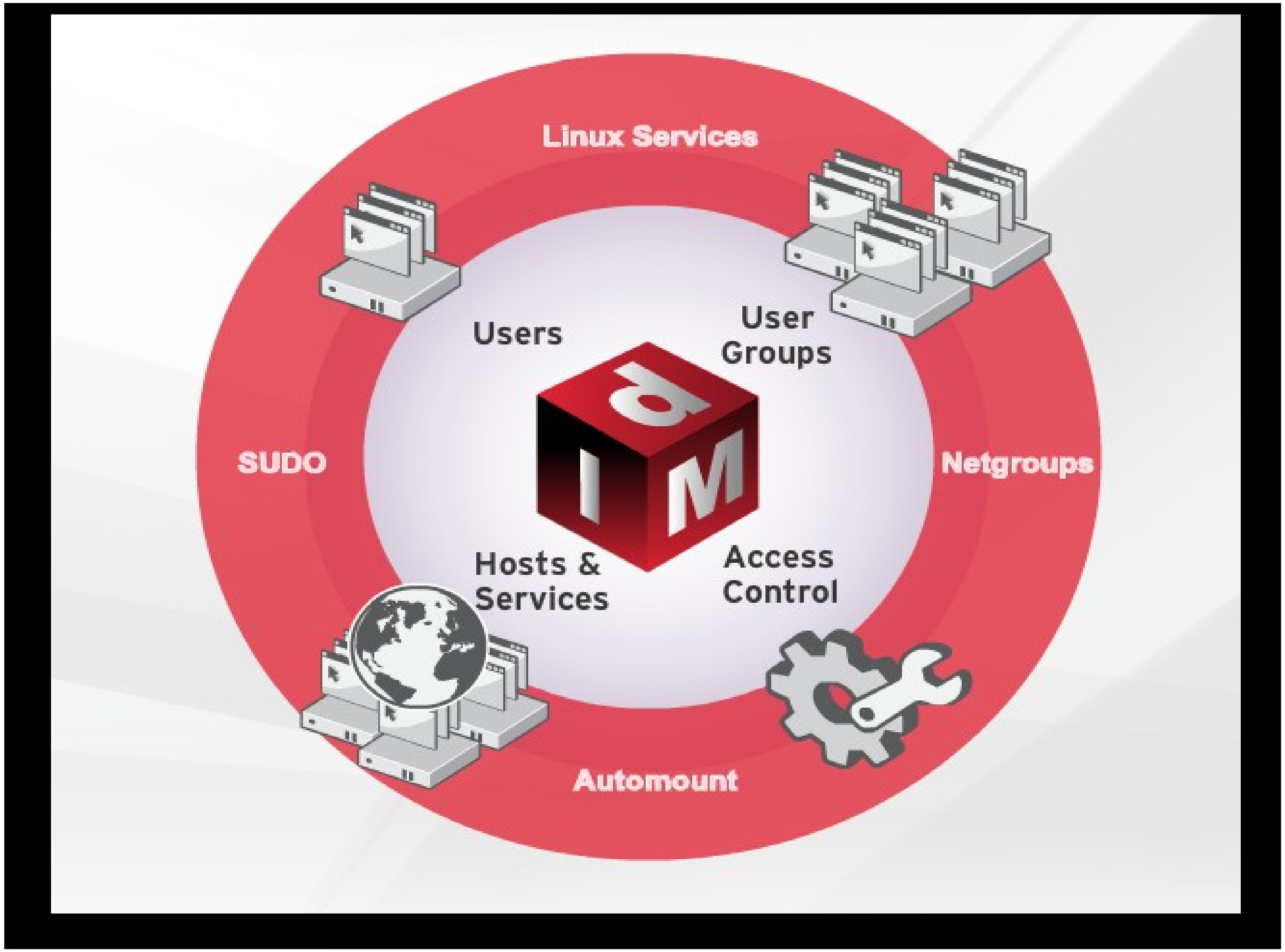
Identity Management – Simplified architecture



- **Integrated -** includes features of LDAP, PKI, Kerberos and DNS
- **Standard -** centralized authentication via Kerberos or LDAP
- **Manageable -** rich command line and web-based user interface
- **Open -** based on FreeIPA open source technology

Identity Management – Overview and Demo

http://www.youtube.com/watch?v=bzN-HSA_otk



Identity Management – Other features

- Multi-Master replication – up to 20 replicas
- Password policy management by groups
- Certificate management for hosts and services
- Can act as an NIS server for legacy systems
- Can provide different views of the LDAP data
- User private groups management
- Simplified migration from other solutions
- Integrated DNS server

IdM Client Components - Overview

- SSSD (System Security Service Daemon)
  - Part of the base installation; starting RHEL 6
  - Identity and authentication gateway
  - Replacement for:
    - pam_ldap/nss_ldap/pam_krb5
    - nscd for most of the maps
  - Predictable and consistent caching of identities
  - Pairing of the identity and authentication sources
  - Automatic Kerberos ticket tracking

IdM Client Components - Overview (continued)

- Certmonger
  - Part of the base installation starting RHEL 6.3
  - Certificate provisioning tool (get, track, renew)
  - Very useful to setup VPN network in a cloud
- IPA client
  - Client-side configuration script that configures SSSD and certmonger to work with IdM

Identity Management – Ease of use

- Built with usability in mind:
  - Simple server installation – takes 2-3 minutes
  - CLI with embedded help system
  - Comprehensive UI
  - One step client-side configuration
  - Automatic enrollment
  - Dedicated online documentation manual

Identity Management – Control your environment

Current Environment	Identity Management Value
• Multiple UNIX/Linux machines • No central identity management • Audit and compliance concerns	• Centralize identity management • Simplify user administration • Ease compliance
• Multiple UNIX/Linux machines • LDAP or Kerberos or NIS solution	• Reduce costs • Provide enterprise SSO • Simplify user administration
• Multiple UNIX/Linux machines • Active Directory central server	• Reduce costs • Increase Linux/UNIX environment control • Support native features of Linux/UNIX

Identity Management – Virtualization and Cloud

- IdM Servers:
  - Can run on bare metal and in virtual, private and public cloud environments

- IdM Clients:
  - Clients include the web, database and other servers that constitute the core of your business
  - Clients can also run on bare metal and in virtual, private and public cloud.

IdM in the Public Cloud – Caveats

- Just because you can doesn't mean you should...
- IdM servers contain "the keys to the kingdom"
- An IdM server in a public cloud requires a very high level of trust in your provider's security provisions
- With public cloud IdM deployments, client security concerns arise:
  - How to securely provision and bootstrap a VM to be integrated into the centralized IdM environment
  - How to securely call home when a VM needs to connect to resources inside the enterprise
- These security concerns are best answered on a case-by-case basis
- If you choose to deploy in a public cloud, we will be glad to help you define the right solution for your environment.

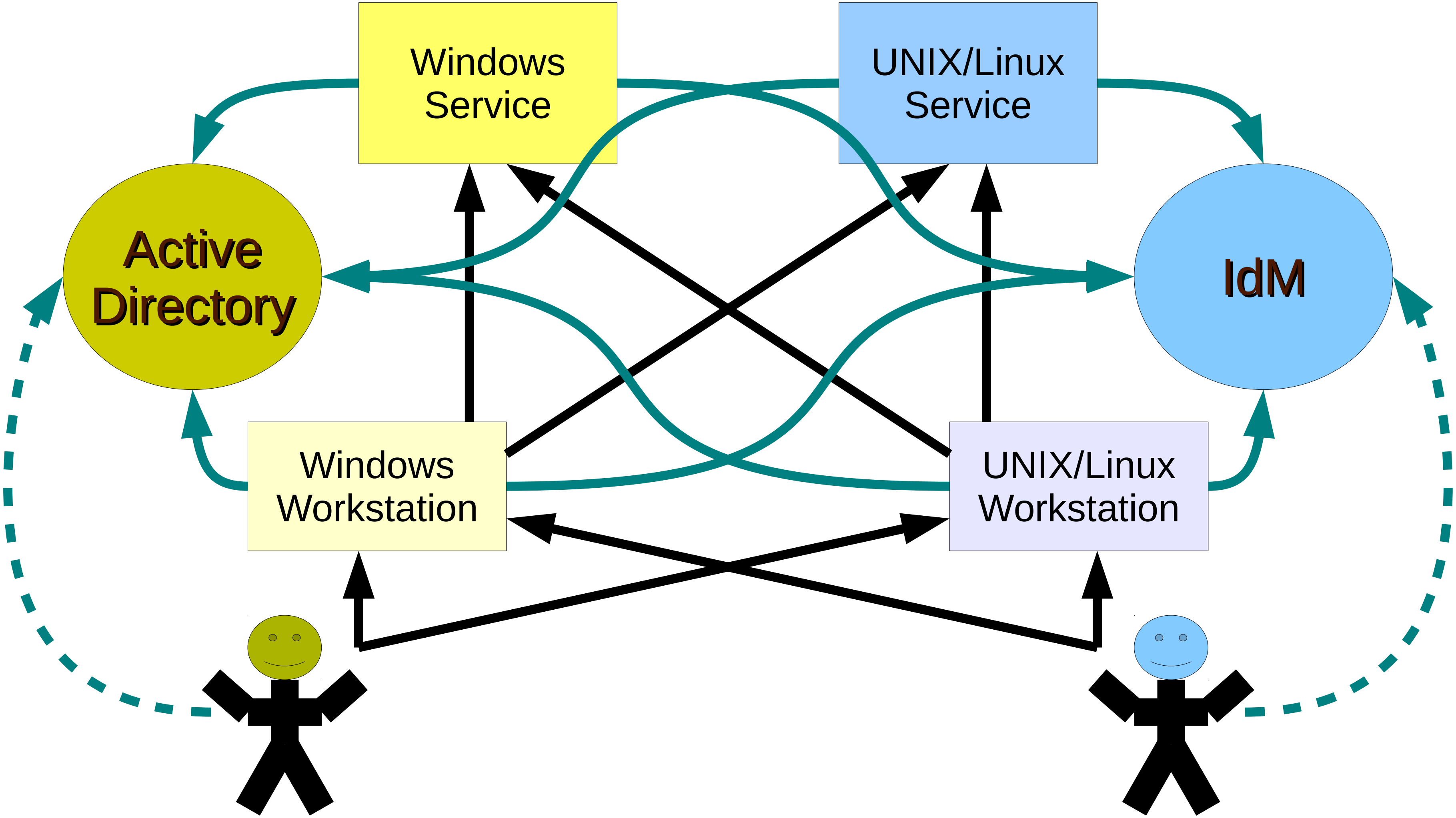
Identity Management – Success Stories

- Identity Management released in RHEL 6.2 Dec. ‘11
- Currently, more than 100 customers worldwide
- Interest is growing every day, both among Red Hat customers and in the upstream community
- One of the first adopters:
  - Running approximately 20 dynamically-provisioned replicas successfully
  - Deployment currently includes about one thousand hosts

IdM vs. Red Hat Directory Server - Comparison

Red Hat Directory Server	Identity Management
General purpose LDAP	Tuned for identity management
Flexible – do it yourself	Integrated, controlled
Default LDAP schema	Schema optimized for identity
LDAP utilities + instance management	Python-based CLI and instance mgt
Console – thick client	Web UI
LDAP Authentication	Kerberos (or LDAP) Authentication
Two-way AD synch: users & groups	One way synch from AD; users only
LDAP-based	Kerberos-based
Multiple domain suffixes	Requires another domain
Stand-alone product	Feature set free with RHEL subscription

On the Roadmap - Cross-realm Kerberos Trust



On the Roadmap – The trust use case

- Goals:
  - Support of mixed AD <-> IdM deployments
  - Eliminate the need to synch AD and IdM
- First use case:
  - User identity is in AD; but the service requested is in IdM
    - User logs in against AD, gets ticket and then accesses IdM service.
    - Authenticated AD user eSSOs into a Linux machine that is a part of an IdM domain over SSH

Roadmap - Additional features coming soon

- **In SSSD:**
  - Integration of SSSD with SUDO
  - Fully supported caching of the automount maps
  - Support native AD extensions
  - Fast caching
- **In IdM and SSSD:**
  - Centralized mgt of SELinux mappings
  - Centralized mgt of the SSH keys
- **In IdM:**
  - Further bug fixes and enhancements in the LDAP driver
  - Better handling of the DNS zones and persistent search
- **In General**
  - Customer bugs and requests
    - Installation, usability, performance, ease of use
  - IE browser on Windows support for IdM administration

Under Consideration – Need your use cases!

- Two-factor auth with Kerberos
- Password enhancements
- Monitoring & status checking
- Identity federation
- Enhanced audit capabilities
- Add a DHCP component
- And much more.......

Security - Additional Presentations

- Thursday 3:40 pm to 4:40 pm
  - Using an Open Source Framework to Catch the Bad Guy
  - Authentication/Authorization Services with SAML & XACML with JBoss
  - How Red Hat OpenShift Achieves Multi-Tenancy in the Cloud
- Thursday 4:50 to 5:50
  - Red Hat Enterprise Linux 6 AD Integration/Samba Clusters Overview
- Friday 9:45 am to 10:45 am
  - System Deployment & Security Auditing with Red Hat Network Satellite & Nessus
- Friday 11:00 am to 12:00 pm
  - Deploying IPv6 from a Platform Systems Perspective
  - Trusted Security with JBoss Enterprise Application Platform
  - Red Hat Enterprise Linux 6 AD Integration/Samba Clusters Overview

Next Steps – Let us know what you want

- See cross-realm Kerberos trust demo at Summit
- Talk to the development team in the pod
- Let us know your identity management requirements
- Participate in FreeIPA:
  - http://freeipa.org/page/Main_Page
- Try it, it’s free in Red Hat Enterprise Linux!

LIKE US ON FACEBOOK

www.facebook.com/redhatinc

FOLLOW US ON TWITTER

www.twitter.com/redhatsummit

TWEET ABOUT IT

#redhat

READ THE BLOG

summitblog.redhat.com

GIVE US FEEDBACK

www.redhat.com/summit/survey