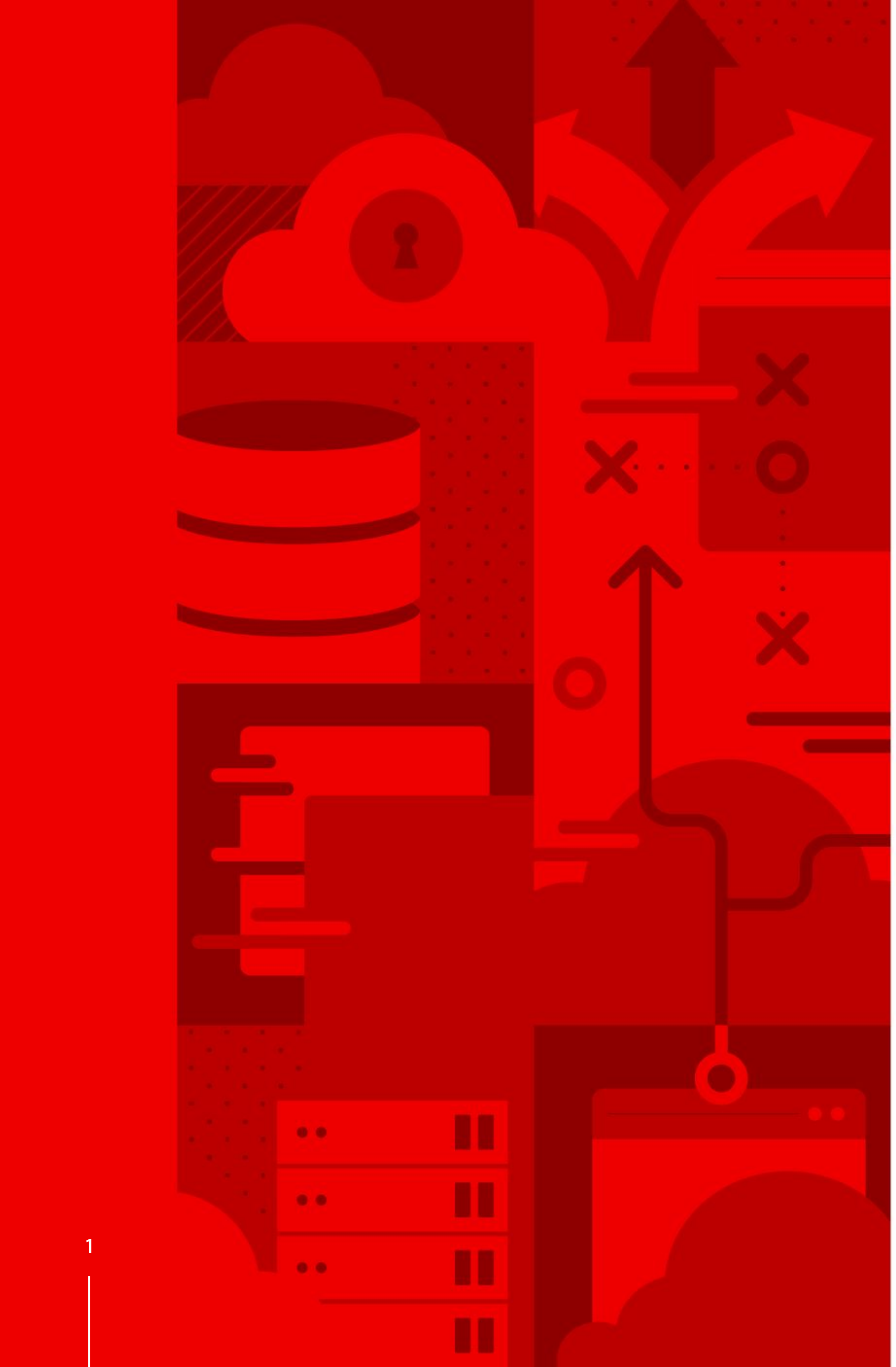

Identity Management

Red Hat Enterprise Linux Solutions

Peter Beniaris

Manager, Solutions Architecture

What we’ll discuss today

- What is Red Hat Identity Management (IdM)
- Overview of the IdM Architecture
- Managing User and Host Identities
- Implementing and Managing Policies
- Creating a Trust with Active Directory
- Brief IdM Demo

Red Hat Identity Management provides a centralized and unified way to manage identity stores, authentication, policies, and authorization policies in a Linux-based domain

- Manages the identities of users and user groups
- Manages the identities of servers and server groups
- Manages access to escalated privileges
- Allows for integration with other directory servers (e.g. Active Directory)
- Allows for Dynamic DNS for hosts managed by IdM or other DNS servers
- Allows for policy based system administration based secure identities
- Red Hat IdM is included with your Red Hat Enterprise Linux subscription
- IdM can manage non Red Hat Linux and Unix hosts

The core components of an IdM architecture include:

- 389 Directory Server
- Kerberos Key Distribution Center
- Dogtag Certificate Server
- SSSD - System Security Services Daemon
- DNS - Domain Name Server
- NTP - Network Time Protocol Server

User and host based access control is a key feature:

- Eliminate the need for /etc/passwd and /etc/group files on managed hosts
- Users mapped to unique UIDs and GIDs across the IdM domain
- Role based user groups
- Role based host groups
- Basis for creating policies based on user and host groups
- Elimination of legacy service accounts

The ability to implement and manage policies is the real strength of IdM:

- Eliminate the need for /etc/sudoers file on managed hosts
- Create and define sudo policies that integrate
    - users and user groups with hosts and host groups
    - and, centralized logging of escalated privileges
- Eliminate the need for home directories on hosts
- Create and define home and remote directory mounts
- Manage SELinux mappings

IdM has been engineered to integrate with Microsoft Active Directory (AD). This allows you to maintain one directory server as authoritative while extending granular control over your Linux domain.

- SSSD allows for direct or indirect integration with AD
- Direct integration connects Linux hosts to AD using realmd
- Indirect integration connects Linux hosts to AD via IdM
  - Publish POSIX attributes to the AD global catalog for best performance
  - Configure IdM to Trust AD in /etd/sssd/sssd.conf

Red Hat Identity Manager (IdM) is included with Red Hat Enterprise Linux (RHEL), and resources can be found in the product pages on the Customer Portal:

- RHEL Product Documentation
- Filter for IdM documentation by selecting the Identity Management category

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

in linkedin.com/company/red-hat	f facebook.com/redhatinc
youtube.com/user/RedHatVideos	twitter.com/RedHat

Red Hat