RED HAT SUMMIT

Practical Steps Implementing Red Hat Identity Management Solution

David Sirrine
Senior Technical Account Manager, Red Hat

Jerel Gilmer
SEC

June 29, 2016

Agenda

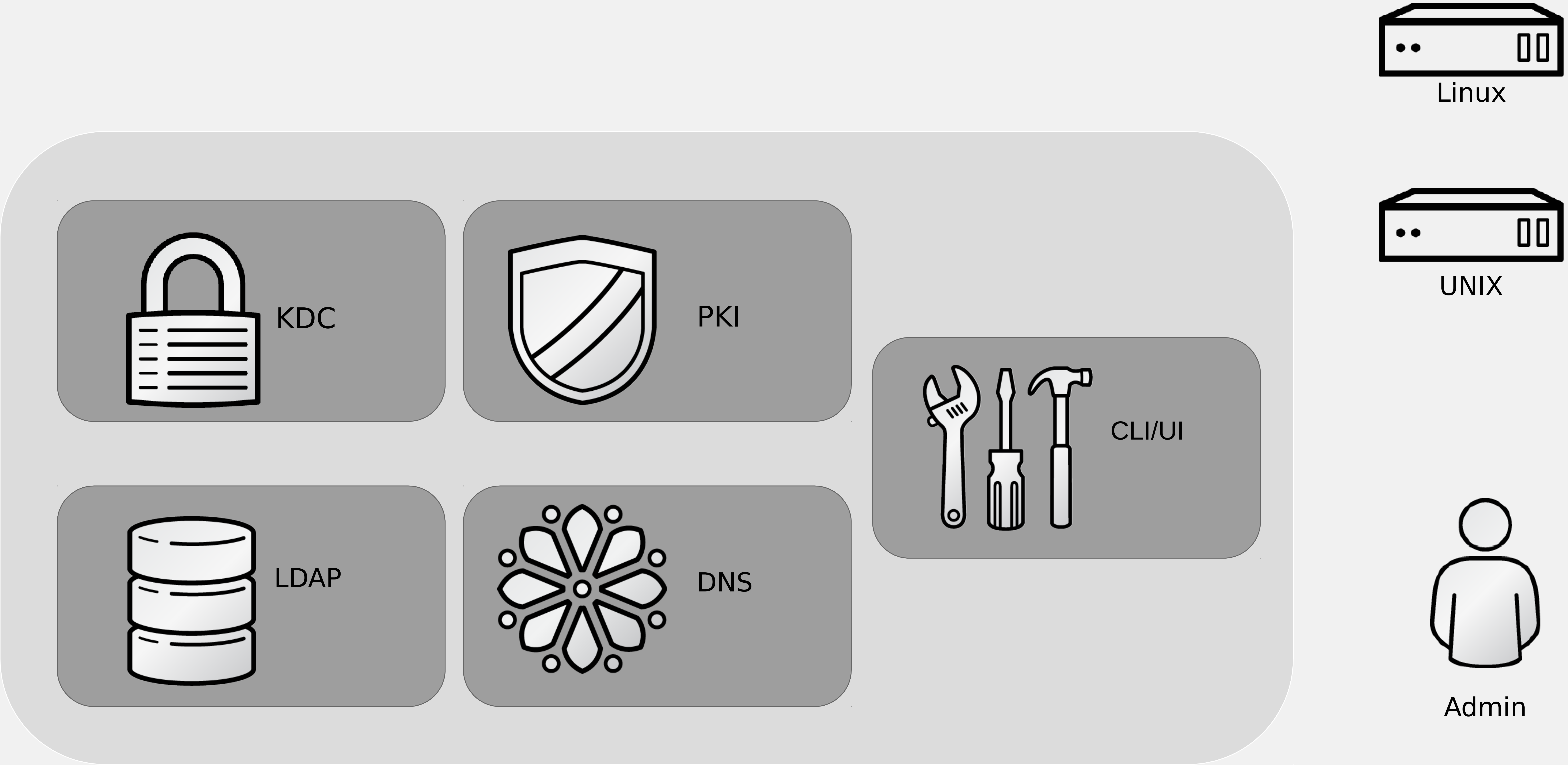
- Brief introduction to the Red Hat Identity Management Solution
- Implementation options
- Active Directory Trusts
- Real world example with the SEC

What is the Red Hat Identity Management Solution?

•Red Hat Identity Management is…

- Based on up-stream project FreeIPA
- A domain controller for your Linux environment
- Comprised various services
  - LDAP - Required
  - KDC - Required
  - DNS - Optional but highly recommended
  - PKI - Optional

Infrastructure at a glance

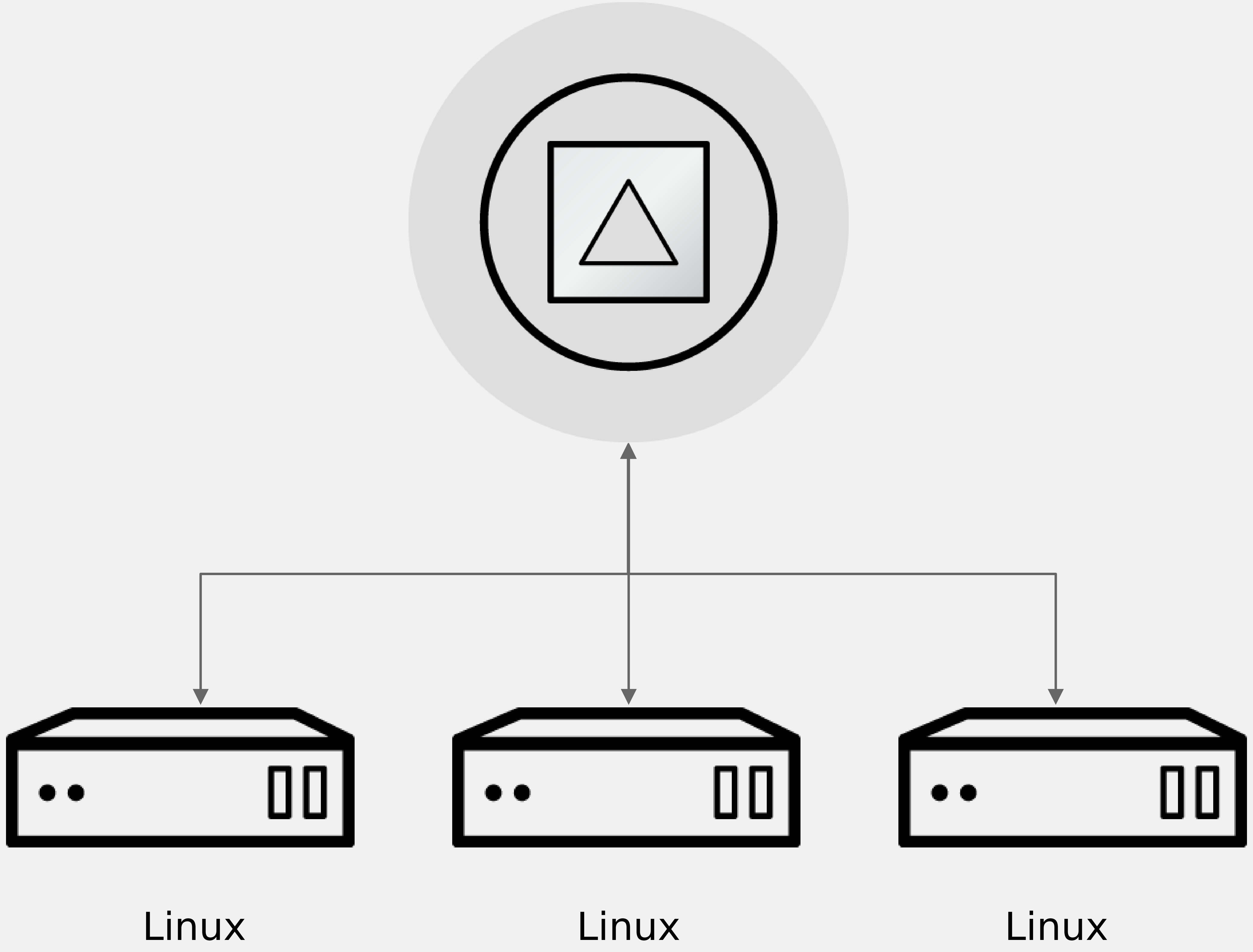


Implementation

Considerations

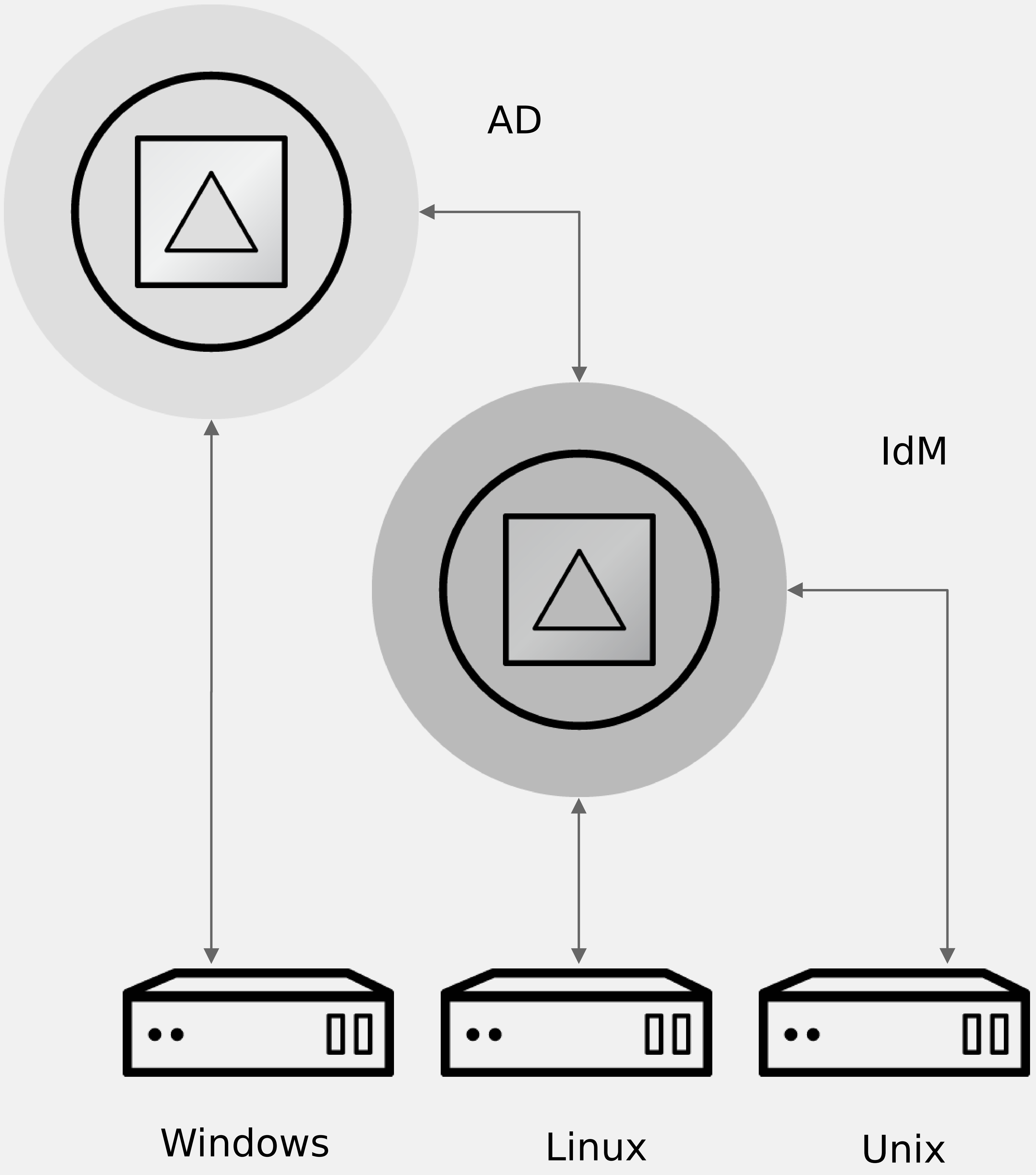
- Can’t change the realm after installation. Choose wisely!
- DNS: Avoiding name collisions by ensuring the domain name is delegated to you
- Replication: only 4 replication agreements per replica
- PKI
  - Self-signed CA
  - Subordinate CA
  - No CA
- Scale
  - 2k – 3k clients
  - 16GB RAM gets 100,000 users and 50,000 groups

IdM Standalone

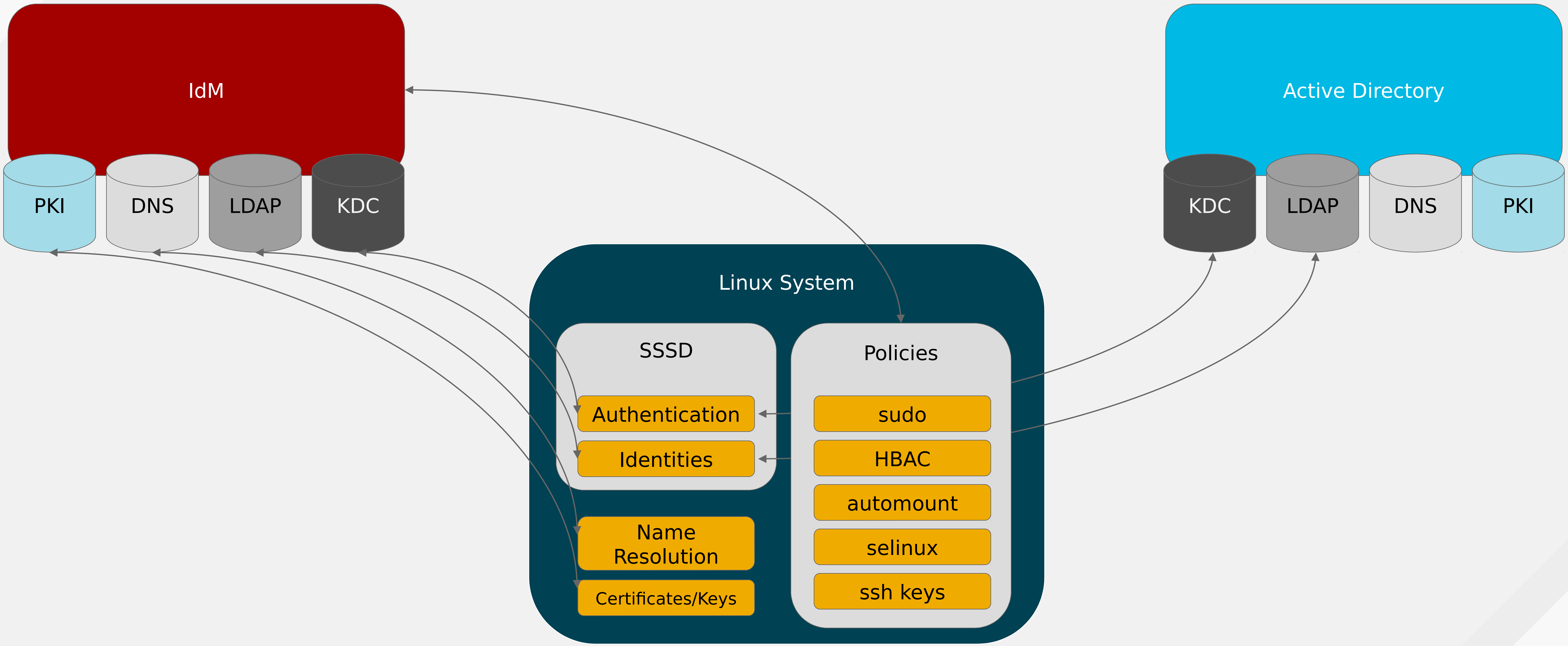


- Provides user and group management
- Policy management
  - sudo
  - automount
  - sshkeys
  - Certificates
    - User certs
    - Host certs
    - Service certs
- Possibly duplicated efforts for user and group management

Active Directory Integration



- Speak the language of Microsoft Admins
  - Setup and functionality similar to how AD cross forest trusts are set up
- AD maintains sole source of Identity/Groups
- Cross forest trust
- Easy setup
  - ipa trust-add
- Passes Kerberos PAC back to IdM
- Policy applied via group membership as listed in PAC


IdM
PKI
DNS
LDAP
KDC
Active Directory
KDC
LDAP
DNS
PKI
Linux System
SSSD
Authentication
Identities
Name Resolution
Certificates/Keys
Policies
sudo
HBAC
automount
selinux
ssh keys

Real World Example: SEC

Problem Statement

- With over 1000 systems across multiple RHEL versions and legacy Solaris platforms, SEC needed a central product to manage:
  - User administration
  - System acces
  - Sudo privileges
  - Audit reporting
- Additional needs were to:
  - Reduce turnaround time on useraccess requests
  - Provide ability to produce on-demand reports
  - Provide framework to potentially automate access requests

Solution

- After performing market analysis, IdM was the clear winner.
- SEC choose IdM based on:
  - Ability to centralize all components of user access management
  - Ability to integrate with MS Active Directory
  - Completely open source software allowing customization
- In evaluating alternative products, it was determined that the products were:
  - Proprietary; difficult to customize
  - Sparsely-used in the industry; less documentation available online
  - High Priced

Implementation

- First phase was to install and configure IdM in the environment
  - Multiple IdM nodes in each data center for redundancy
  - Extend schemas to incorporate Solaris systems
- Second phase was to audit current access levels across the environment
  - Scripts were developed to capture users/groups and sudo privileges
  - Users and groups were added to IdM
  - Standardization of UIDs/GIDs, shells, and home directories
- Third phase was to migrate systems to IdM
  - Outage schedule was created
  - Custom migrating scripts used to create hands-off migration process
    - System UIDs/GIDs reconciled to match IdM
    - HBAC rules and sudo rules automatically created in IdM

Lessons Learned

- With any new product, there is a learning curve.
  - Needed additional time to educate users and administrators on IdM
- Project scope included centralizing service accounts; Would rethink this approach
- Changing deadlines compressed migration schedule
- Unable to achieve initial goal to trust users from AD environment due to:
  - AD accounts were PIV enabled, causing issues with SSSD at the time
  - AD admins had reservations configuring two-way trust
- IdM didn’t have the capability to provide delegated admin permissions
  - No ability for multiple admin teams to only modify system they managed

Working With Red Hat Support

- Engaging with Red Hat early on helped with project success; assisting with system architecture and product education
- Red Hat Support submitted RFEs that were applicable to our environment such as:
  - One-way Active Directory trusts
  - PIV support
  - Delegated permissions
  - Performance improvements
- Red Hat Support timely identified and resolved any product bugs

Roadmap of SEC environment

- Automate user request workflow
- Implement Active Directory Trusts
- Improved auditing and logging
- Improved reporting
  - Working with Red Hat engineering to implement custom reporting into existing plugin architecture for future broad release

Wrap-up

Resources: Docs

- Linux Domain Identity, Authentication, and Policy Guide
  - https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/index.html
- Windows Integration Guide
  - https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Windows_Integration_Guide/index.html
- System-Level Authentication Guide
  - https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System-Level_Authentication_Guide/index.html

Resources: Community

- FreeIPA - www.freeipa.org
  - Project trac: https://fedorahosted.org/freeipa/
  - Code: http://git.fedorahosted.org/git/?p=freeipa.git
  - Mailing lists:
    - freeipa-users@redhat.com
    - freeipa-devel@redhat.com
    - freeipa-interest@redhat.com
- SSSD - fedorahosted.org/sssd/
- Mailing lists:
  - sssd-devel@lists.fedorahosted.org
  - sssd-users@lists.fedorahosted.org

Resources: Other

- Training
  - http://www.freeipa.org/page/Documentation#FreeIPA_Training_Series
- Blog aggregation
  - http://planet.freeipa.org/
- FreeIPA demo instance in the cloud
  - http://www.freeipa.org/page/Demo

Questions?

RED HAT
SUMMIT

LEARN. NETWORK.
EXPERIENCE OPEN SOURCE.