redhat.

Identity Management In Red Hat Enterprise Linux

Dave Sirrine
Solutions Architect

Agenda

Goals of the Presentation

- Identity Management problem space
- What Red Hat Identity Management solution is about?
- What problems Identity Management solution solves?
- Benefits of the Red Hat Identity Management solution
- Identity Management solution architecture
- Provide examples of some real-world use cases that can be solved with the identity management capabilities Red Hat offers

Agenda

Goals of the Presentation

Or...

- Understand what you want to know
- Answer your questions
- Help you to make decisions
- Establish a dialog

Identity Management Problem Space

redhat.

What is Identity Management?

- What does this mean to you?
- What issues are you running into in this area?

Identity Management Problem Space

There are four main problems we try to solve with IdM

- Central management of identities
- Provide various authentication mechanisms
- Access control
- Central management of Linux policies

Identity Management Problem Space

Main aspects

- **Identities**
  - Where are my users stored? What properties do they have? How is this data made available to systems and applications?
- **Authentication**
  - What credentials do my users use to authenticate? Passwords? Smart Cards? Special devices? Is there SSO? How can the same user access file stores and web applications without requiring re-authentication?

Identity Management Problem Space

Main aspects, continued

- **Access control**
  - Which users have access to which systems, services, applications? What commands can they run on those systems? What SELinux context is a user is mapped to?
- **Policies**
  - What is the strength of the password? What are the automount rules? What are Kerberos ticket policies?

Red Hat Vision

- In the past each application had its own database, identity management solutions were copying data around for a system of record (HR systems usually) to all application databases
  - This is hard to manage, keep secure and in sync and thus is a bad practice
- User, system and service accounts should be managed in the dedicated system and not copied around
  - Single set of credentials instead of disjoint passwords copied around
  - Policies for passwords and other credentials defined and enforced by one system
  - Enterprise Single-Single-On

Benefits

Identity Management in Red Hat Enterprise Linux enables customers to:

- Significantly simplify their Identity Management infrastructure
- Meet modern compliance requirements like PCI DSS, USGCB, STIG
- Reduce the risk of unauthorized access or unauthorized privilege escalation
- Create a foundation for a highly dynamic and scalable, cloud and container capable, operational environment
- Automate deployment of new systems, VMs and containers with preconfigured identity, authentication and access control capabilities
- Reduce the cost of day-to-day operation

Benefits

Identity Management in Red Hat Enterprise Linux enables customers to:

- Minimize investment into the underlying infrastructure
- Improve user experience with enterprise wide single-sign-on across heterogeneous environment
- Enable tighter application integration into the identity management fabric
- Manage identity information and authentication credentials for users, services, systems and devices


What’s new in 7.4
redhat.

Updates to IdM in 7.4

- Integration with external DNS providers through nsupdate
- FIPS 140-2 compliant
- SSSD Short Name support
- Improved Smart Card capabilities
  - Map cards to AD user record
  - Map a single smart card to multiple roles
  - Custom attributing mapping


Overview of the Identity Management Components
redhat.

Components of the Portfolio

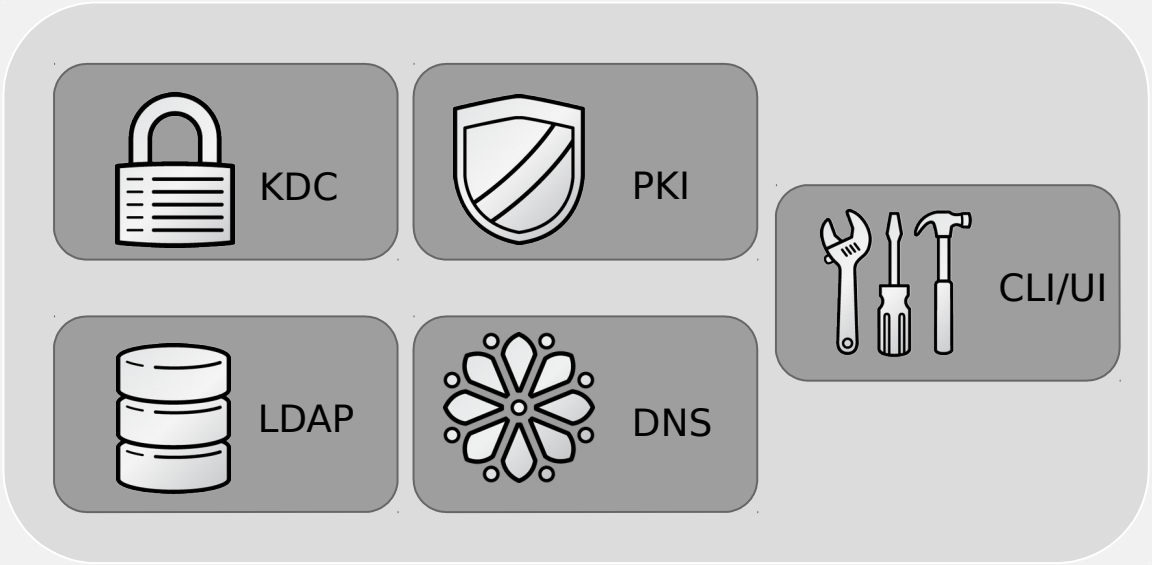
- Identity Management in Red Hat Enterprise Linux (IdM)
- SSSD
- Certmonger
- Keycloak IdP
- Apache modules

Identity Management (IdM)

- Domain controller for Linux/UNIX environments
- Based on the FreeIPA open source project
- Combines LDAP, Kerberos, DNS and certificate management capabilities
- Provides centralized authentication, authorization and identity information for Linux/UNIX infrastructure
- Enables centralized policy and privilege escalation management
- Integrates with Active Directory on the server-to-server level

FreeIPA/IdM

High Level Architecture



Comparison

Area	DS	IdM
Use	General purpose LDAP server	Domain controller for Linux/UNIX
Extensibility	Highly customizable	Preconfigured data and object model
Interfaces	LDAP, command line tools, admin console	Rich CLI, JSON RPC API, Web UI
Schema & tree	LDAPv3 compliant, tree design up to deployment	Optimized for domain controller use case
Authentication	LDAP	LDAP, Kerberos with SSO, Certificate based
AD integration	User synchronization	Advanced integration via cross forest trusts
Replication	Up to 20 masters + unlimited read only replicas and hubs	Up to 60 active masters
Scalability	Scales well beyond 100K objects	Has limitations beyond 100K objects


Costs

What is the cost?

- All mentioned components and solutions are provided using Red Hat Enterprise Linux without extra charge
- No third party vendors involved
- Deployment is easy and integrated – saves time
- The main cost is server side subscriptions, but one server can serve about 2-3K clients

Wrap-up

Resources

Summary

- 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

Summary

- FreeIPA
  - Project wiki: 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: https://fedorahosted.org/sssd/
  - Mailing lists:
    - sssd-devel@lists.fedorahosted.org
    - sssd-users@lists.fedorahosted.org

Training Materials and Blogs

- 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?

Finally


SUPPORTING SLIDES
redhat.

Use Cases and Challenges

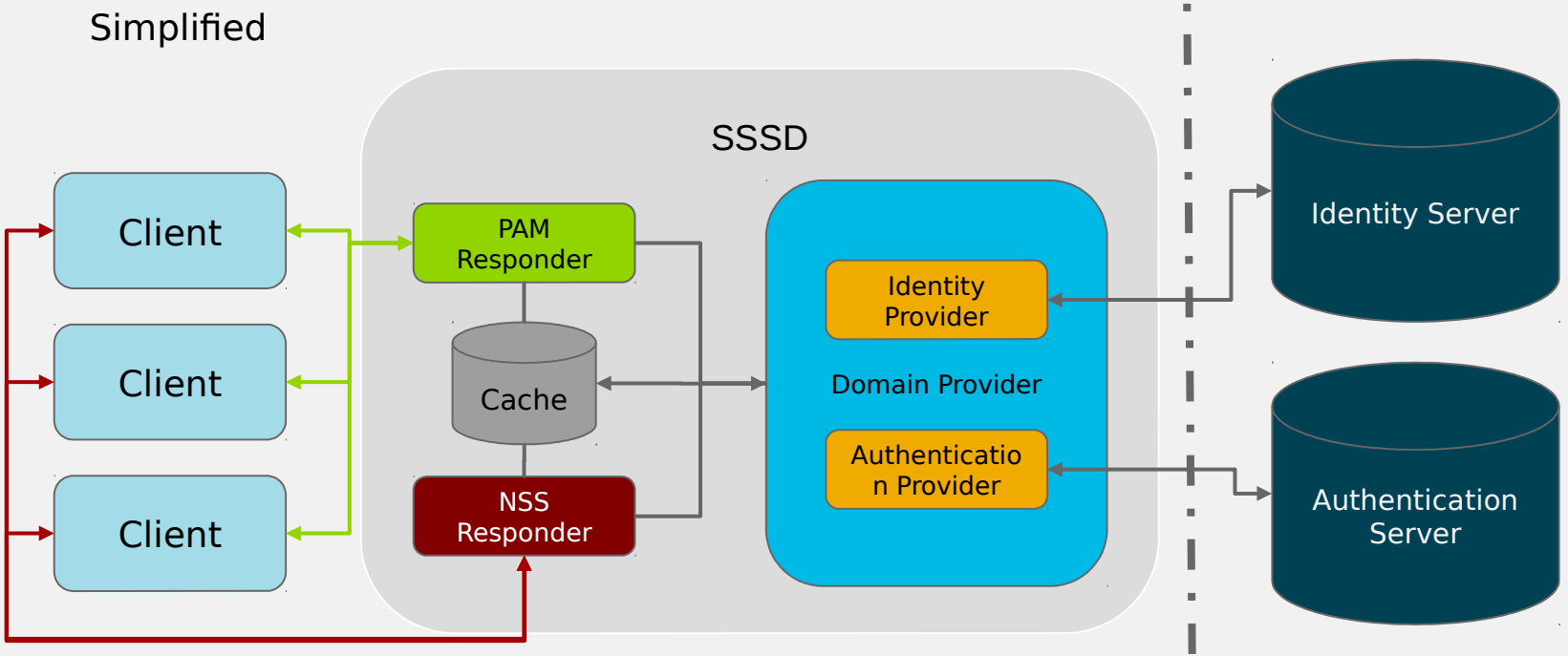
- **How can I provide centralized authentication?**
- How to address Active Directory interoperability challenges?
- Can I define access control to hosts without copying configuration files?
- Can I manage SSH keys for users and hosts?
- Can I provide centralized SUDO, automount, SELinux user mappings?
- How can I provide certificates for services, hosts, devices and users?
- Is there a cost effective solution that provides strong authentication using OTP?
- Can I provide a smooth SSO experience for my users inside the enterprise?
- How can I integrate my applications into the same identity space?

SSSD (System Security Services Daemon)

- Client-side component
- Part of Red Hat Enterprise Linux and many other Linux distributions
- Allows connecting a system to the identity and authentication source of your choice
- Caches identity and policy information for offline use
- Capable of connecting to different sources of identity data at the same time

SSSD Architecture

Simplified



Certmonger

- Client side component
- Connects to central Certificate Server and requests certificates
- Tracks and auto renews the certificates it is tracking

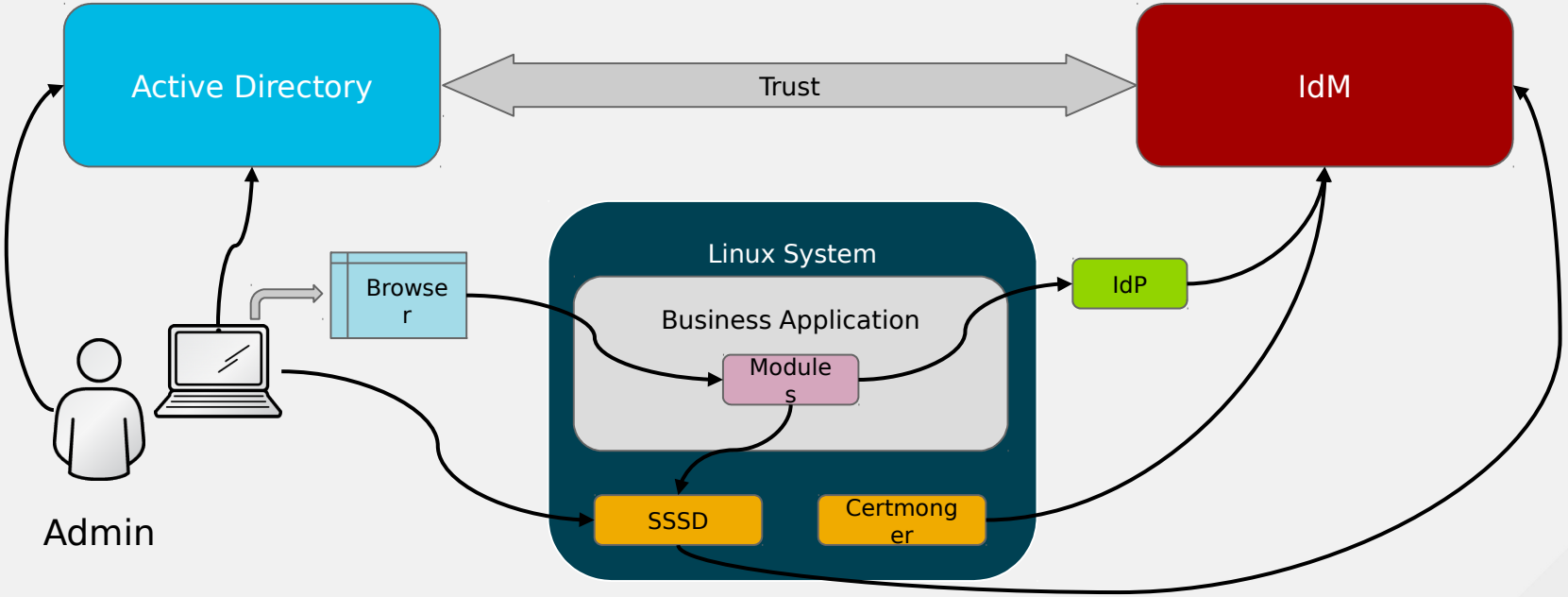
Red Hat SSO

- Identity Provider implementation
- Allows federation between different applications using SAML, OIDC based SSO

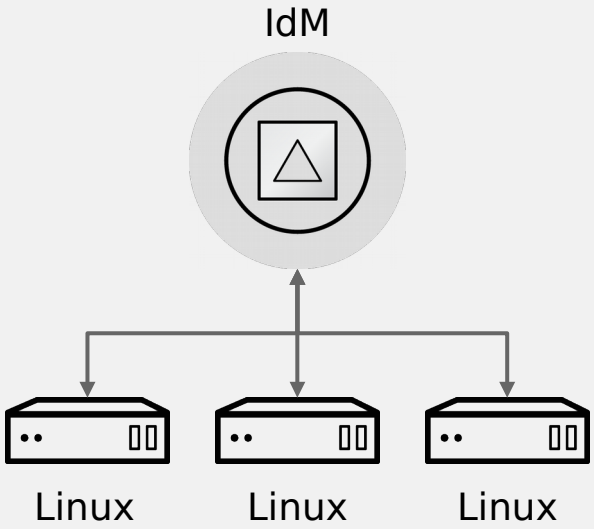
Apache Modules

- Modules that can be integrated with Apache server
- Modules that support forms-based, Kerberos, certificate-based or SAML authentication
  - We are working on OIDC authentication
- Authorization and identity data lookups are also possible using corresponding modules

Example Architecture



Centralized Authentication



Steps:

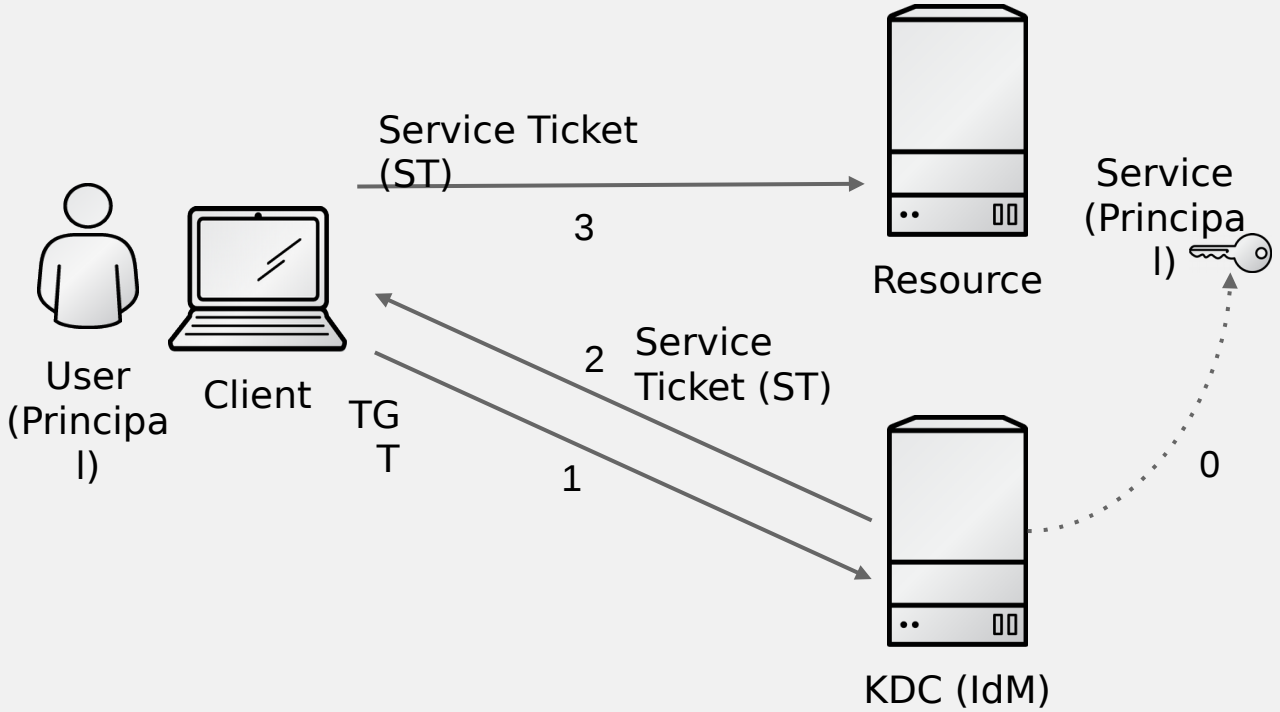
- Consolidate your user accounts
- Load your user data into a IdM
- Connect your Linux/UNIX systems to IdM
  - ipa-client-install

Why would I use IdM?

- Different authentication methods:
  - LDAP, Kerberos, OTP, Certificates
- Integrated solution
  - Easy to install and manage
- Integrates with AD
- Better security management for Linux hosts

Kerberos SSO

Accessing a resource

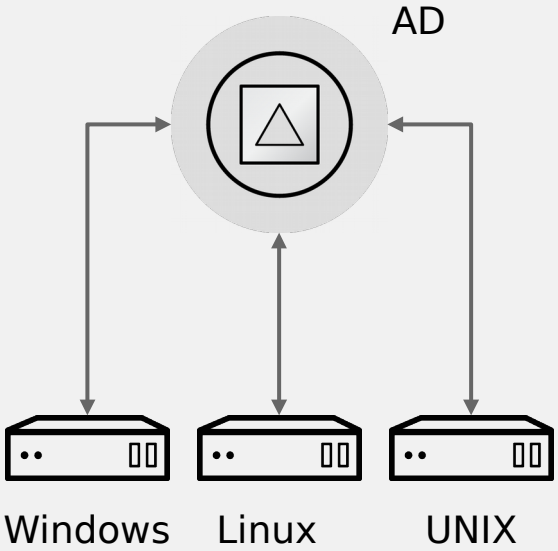


Kerberos Flow

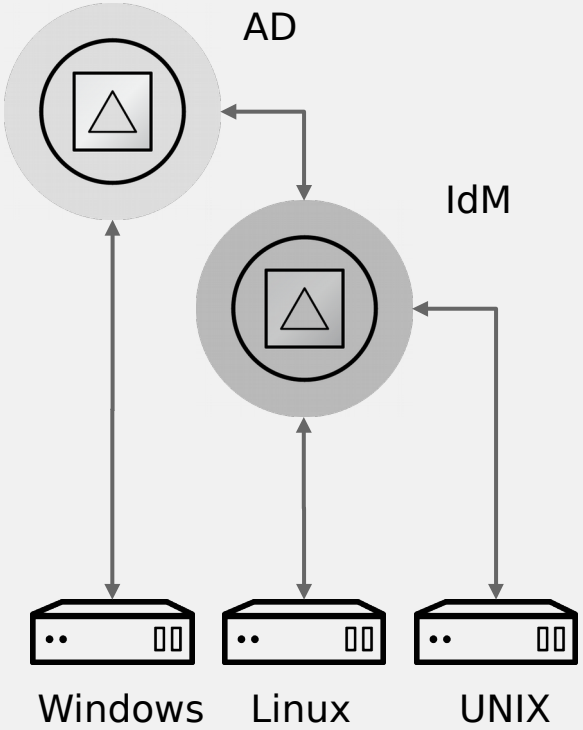
- User logs into the system that is connected to a Kerberos server
  - It can be: Kerberos KDC, Active Directory or IdM
- User authenticates (0) and gets a ticket granting ticket (TGT) from the Kerberos server
- User accesses a resource (for example NFS client)
- Kerberos library will request a service ticket from KDC (1 - 2)
- The ticket is presented to the service (for example NFS server) (3)
- The server decrypts ticket using its Kerberos key (stored in a keytab)
- Keys are distributed at installation/configuration time, and can be rotated as necessary

Connecting Systems

Integration Options



Direct Integration



Indirect Integration

Integration Paths

Overview

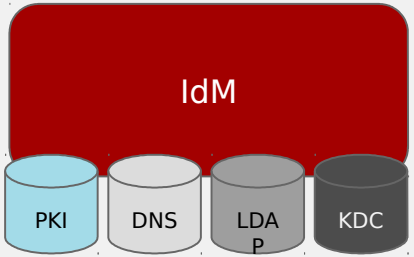
- User and password synchronization (not recommended)
- Cross forest trusts (recommended)

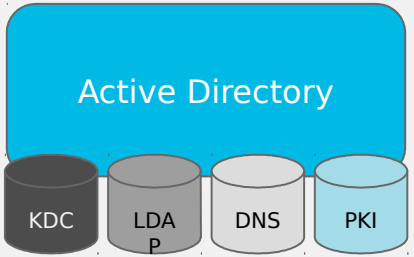
Synchronization Solution

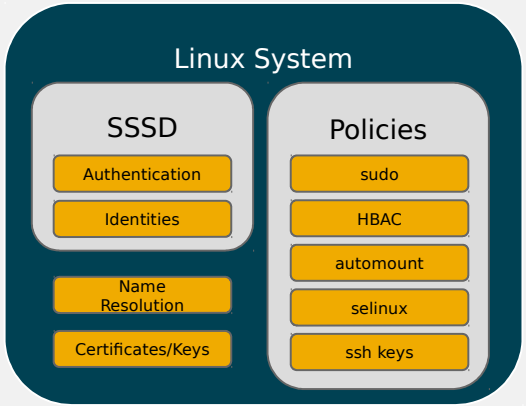
Overview

- LDAP level synchronization
- AD is the authoritative source - one way sync
- No group synchronization, only users
- Only one domain can be synchronized
- Single point of failure - sync happens only on one replica
- Limited set of attributes is replicated
- Passwords need to captured and synced
  - Requires a plugin on every AD DC
  - Mismatch of password policies can lead to strange errors

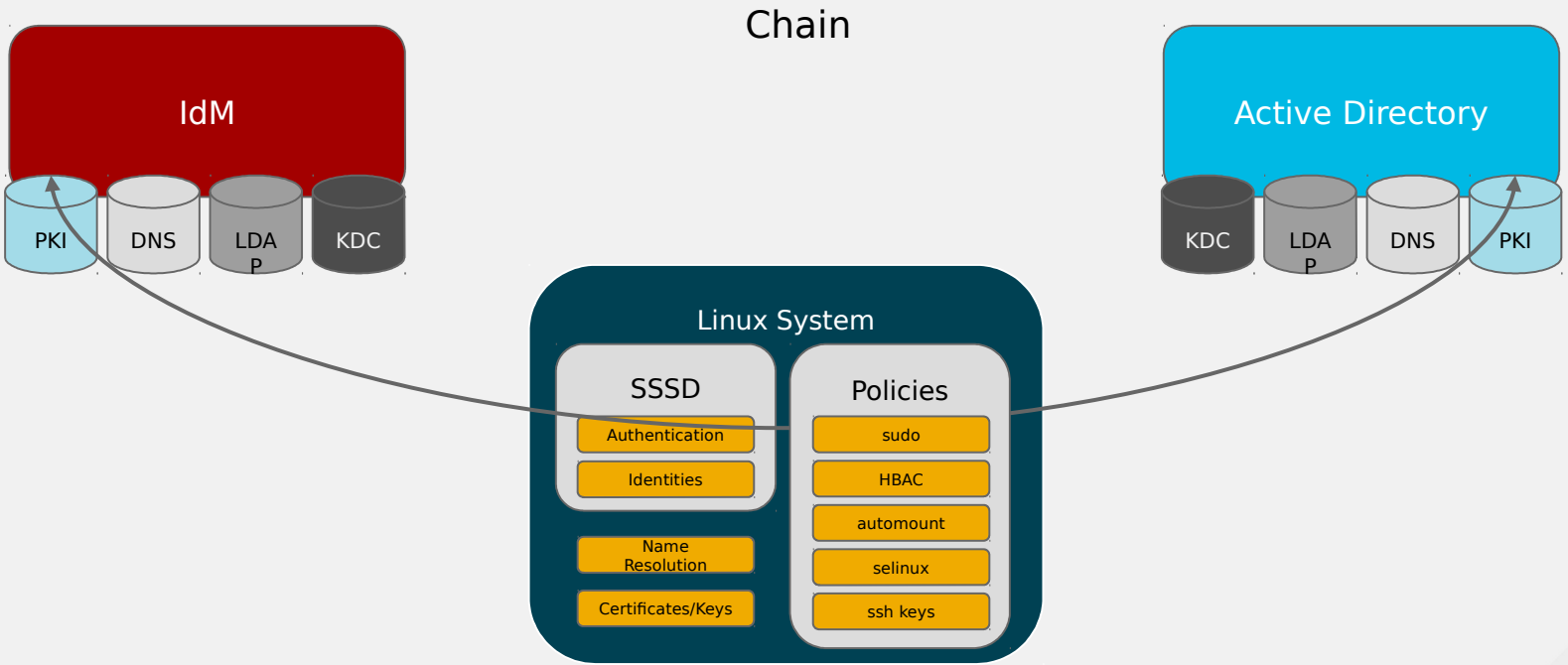
IdM - AD Integration with Trust



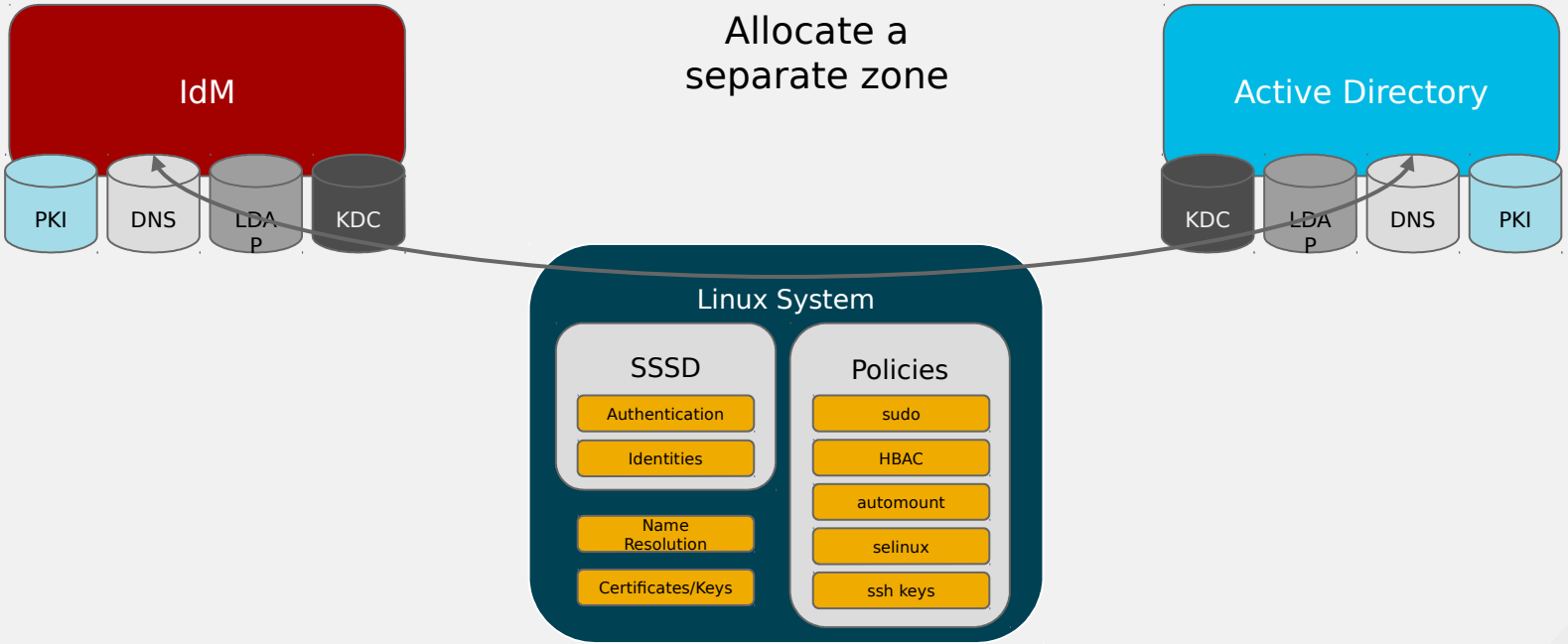




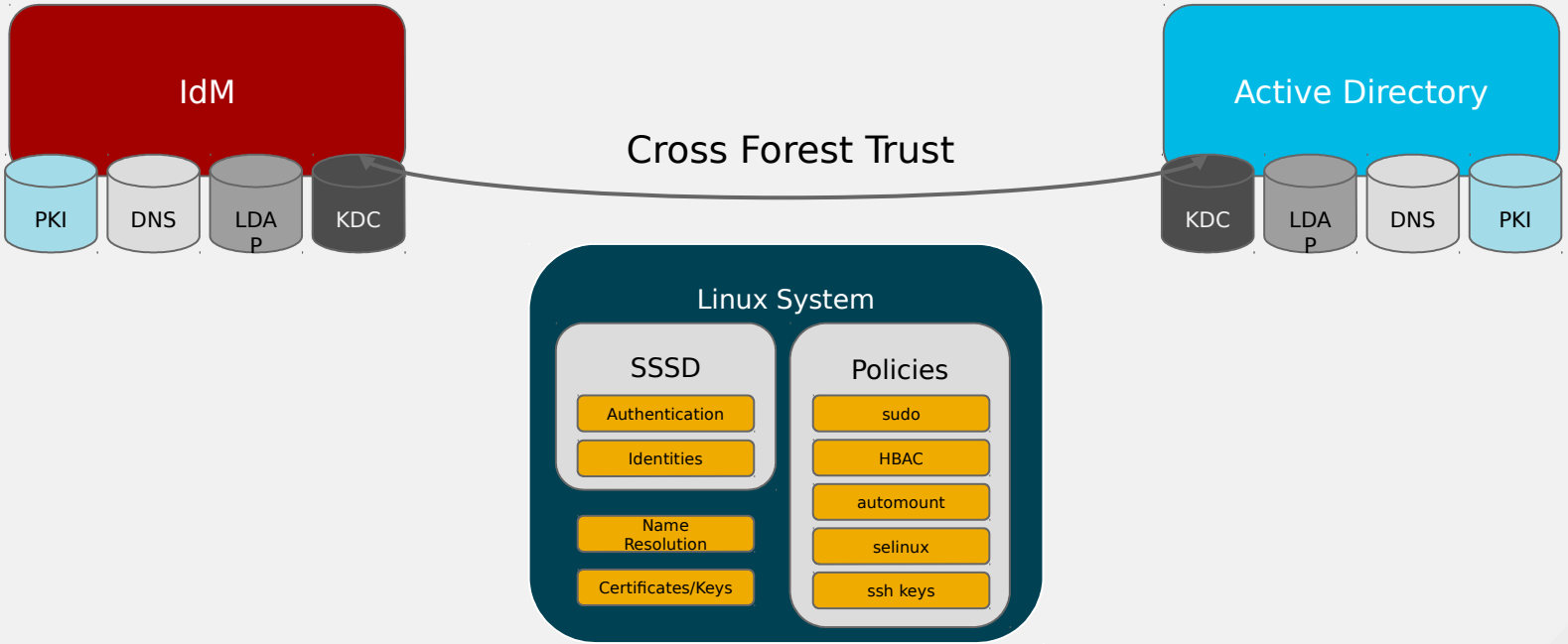
IdM - AD Integration with Trust



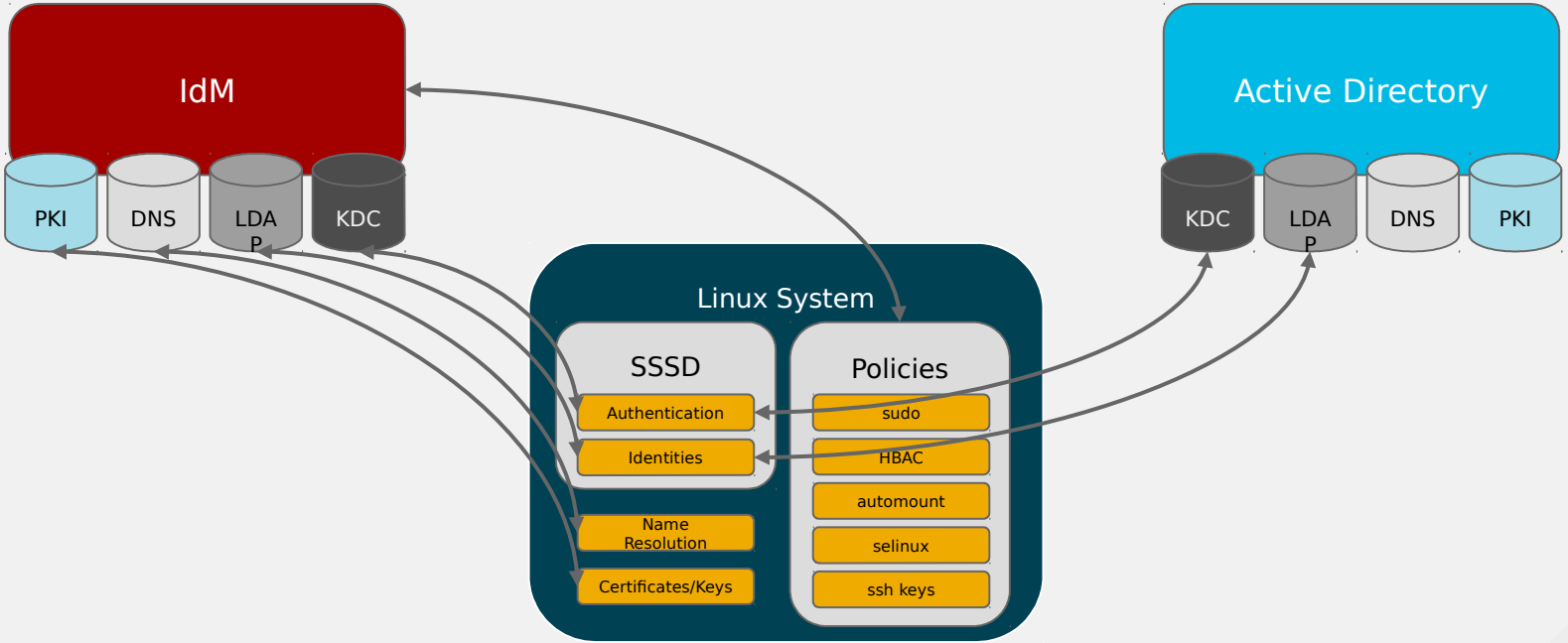
IdM - AD Integration with Trust



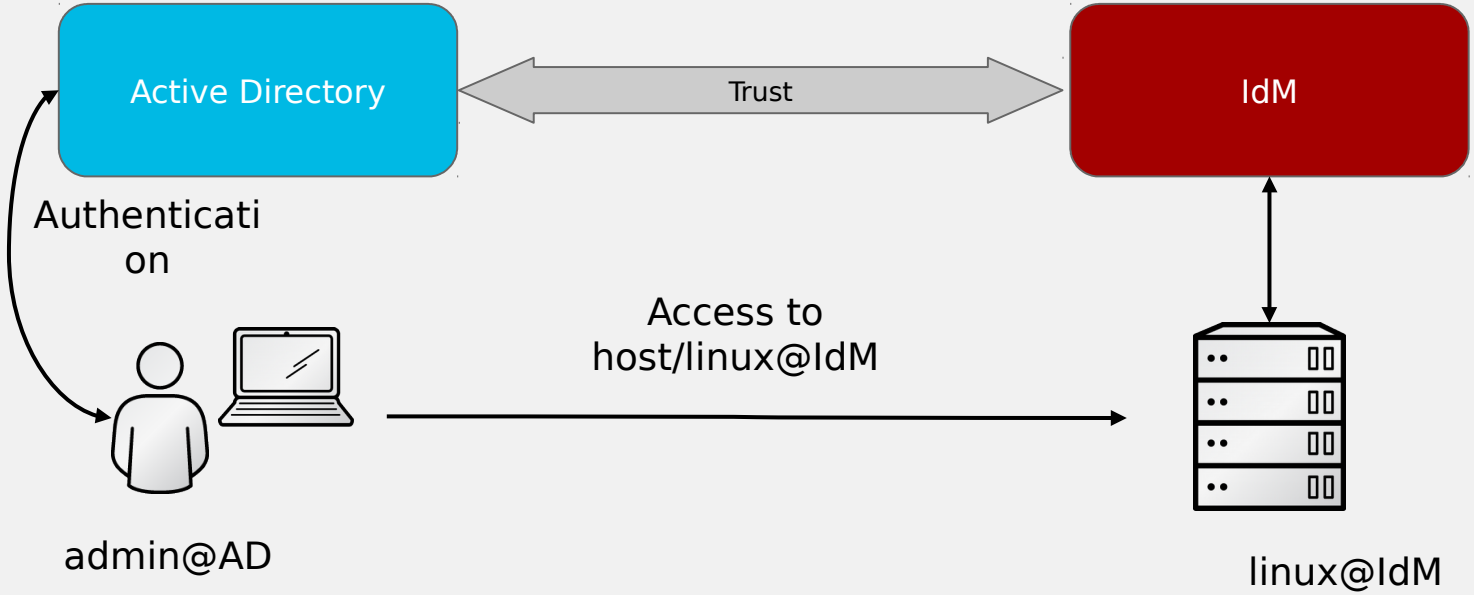
IdM - AD Integration with Trust



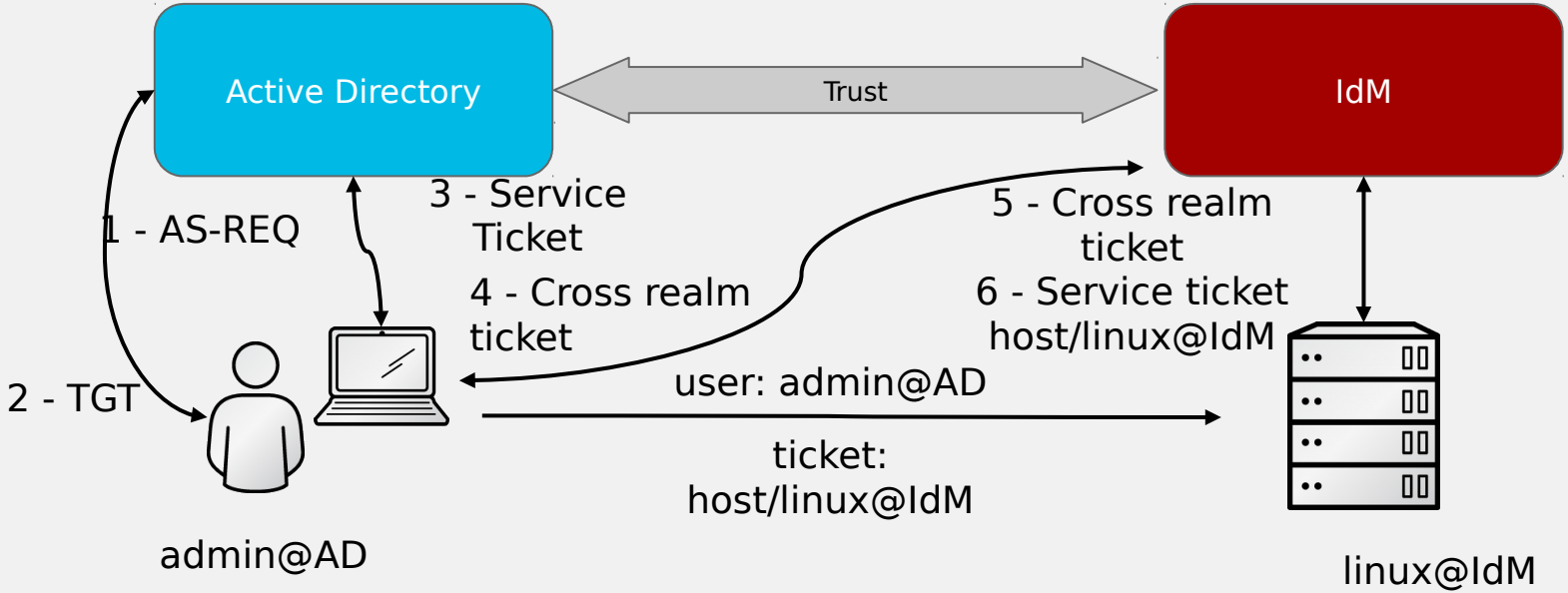
IdM - AD Integration with Trust



Trust Setup


Active Directory
Trust
IdM
Authenticati
on
Access to
host/linux@IdM
admin@AD
linux@IdM

Ticket Exchange



Trust

Details

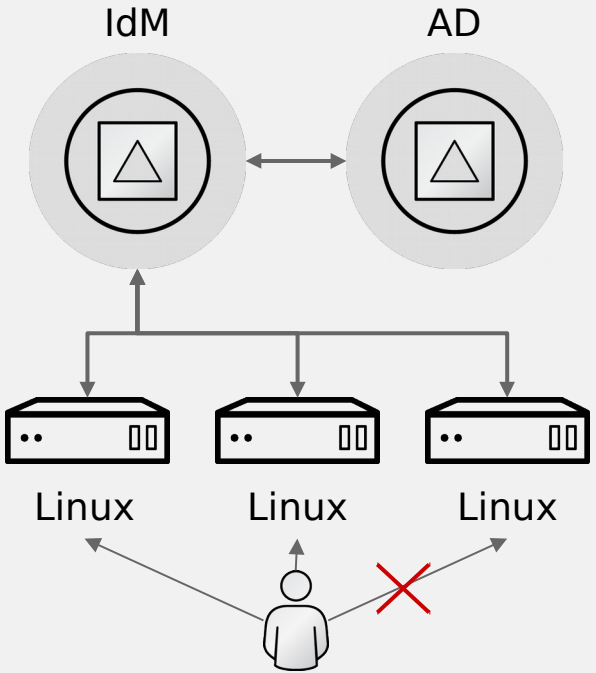
- Allows users of one Forest to access resources in a different Forest provided the two Forest admins previously set up an agreement.
- The foundation of this agreement are cryptographic keys shared by the two Forests.
- Cross-forest trust are established by the root domains (only)
- Two-way and one-way trust (IdM trusts AD)
  - AD/Samba DC trusting IdM is on the roadmap
- Trust agents (different behavior of different replicas)
- Migration from the sync to trust

User Mapping

Details

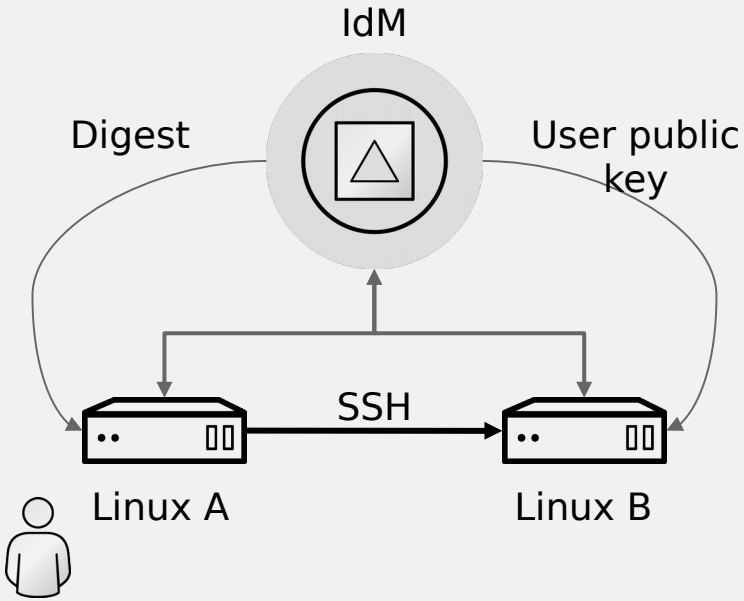
- Can leverage SFU/IMU for POSIX (brown field)
  - This functionality is deprecated by Microsoft
- Can do dynamic mapping of the SIDs to UIDs & GIDs (green field)
- Static override with ID views
  - Other data can be overwritten too
    - SSH Keys
    - OTP & Certificates in future

Host Based Access Control



- Host based access control:
  - Which users or group of users can access
  - Which hosts or groups of hosts
  - Using which login services:
    - console, ssh, sudo, ftp, sftp, etc.
- You define rules centrally
- Works with trusted AD users

SSH Key Management



- Host public keys uploaded at the client installation time
- User can upload his public key to IdM manually
- When user SSHs from a system A the public key of to the target system B is delivered to system A (no manual validation of digest)
- User public key is automatically delivered to system B
- Works with trusted AD users

Smart Cards

Problem

- Authentication using certificates on smart cards required mapping of the user identity in the certificate to the user on the operating system
- pam_pkcs11 was able to do mapping using local file which is not scalable
- pam_krb5 requires Kerberos extension in a certificate which is usually not there
- SSSD being the gateway and provider of different authentication methods against multiple identity sources did not support smart card authentication

Smart Cards

Solution

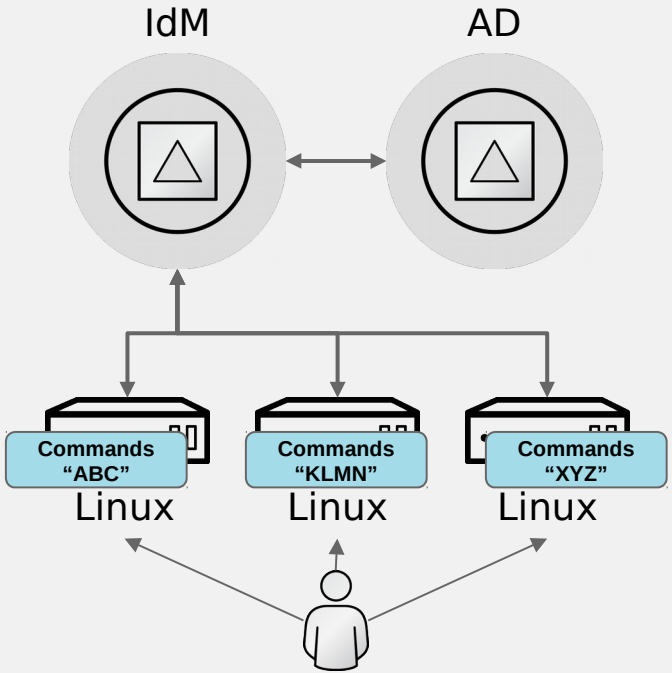
- pam_pkcs11 and SSSD are fixed to do dynamic mapping of the certs to users via an LDAP lookup
- SSSD will be able to authenticate users that have certificates registered in IdM
- The certificate can be issued by an external CA
- SSSD might be able to authenticate users with certificates registered in AD (experimental)

Smart Cards

Benefit

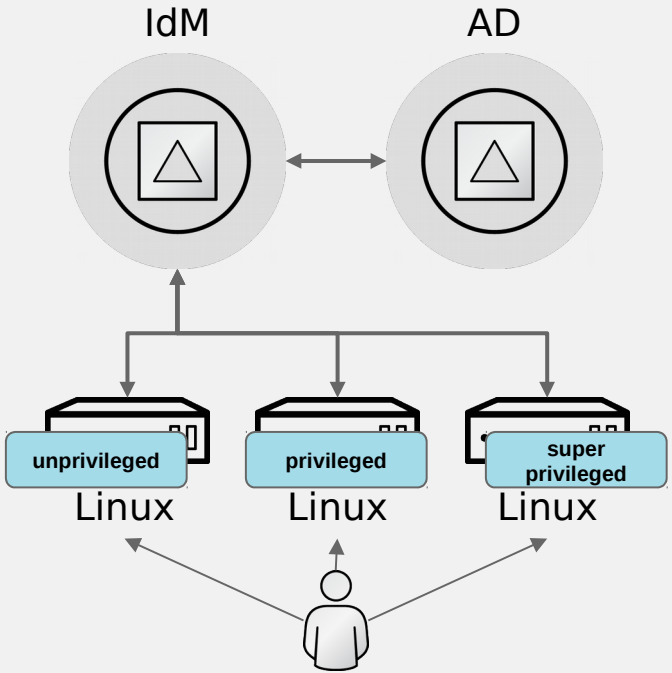
- Benefit:
  - Customers can use IdM and SSSD to provide smart card based authentication into Linux environment using SSH
  - The solution is now much easier to manage and is scalable
- Reference:
  - https://fedorahosted.org/sssd/wiki/DesignDocs/SmartcardAuthenticationStep1

SUDO Integration



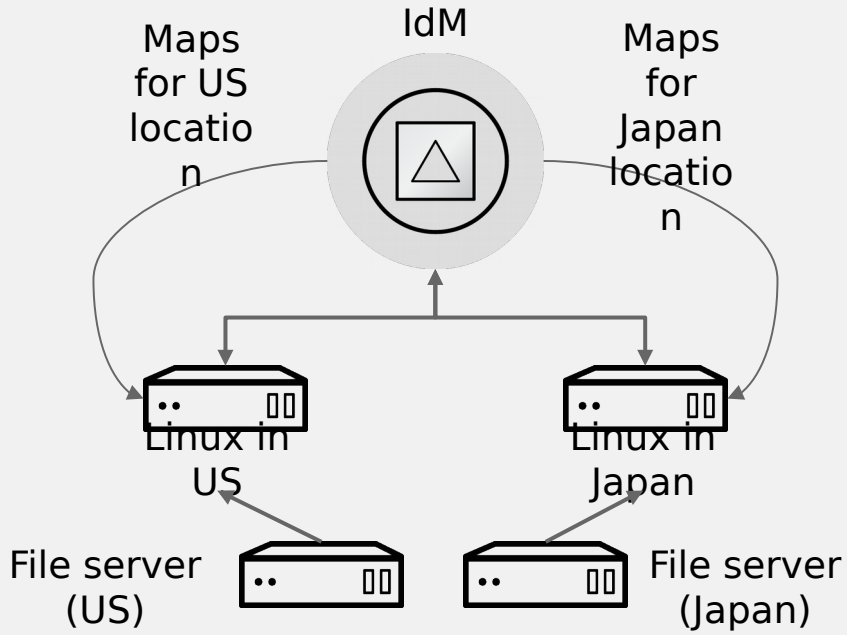
- Centrally define commands and groups of commands
- Define which groups of users can run these commands or groups of commands on which hosts or groups of hosts
- Rules are enforced on client
- Rules are cached (in SSSD)
- Capability is integrated into the sudo utility
- Works with trusted AD users

SELinux Integration (user mapping)



- Mappings can be defined centrally
- Allow different users on different systems have different SELinux context
- Default SELinux labels are available in IdM configuration
- Mappings are enforced on the client
- Mappings are cached (by SSSD)
- Works with trusted AD users

Automount

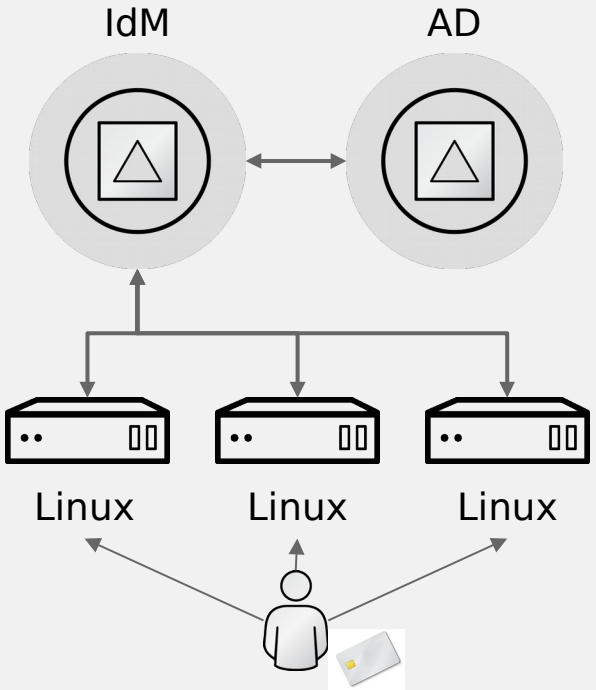


- Define direct or indirect maps
- Associate maps with a particular location
- Configure clients to pull data from that location (part of the LDAP tree)
- Maps are defined centrally
- Maps are applied on the client
- Maps are cached
- Maps are integrated with autofs

Certificate Management

- Subjects
  - Users, hosts, devices, services
- Profiles
  - Different certificates can have different extensions
- Virtual Sub-CAs (in works)
  - A CA per a particular purpose
- Tracking and renewal of certificates using certmonger

Certificate Authentication



- IdM user with a certificate or smart card
- AD user with a certificate or smart card in direct or indirect integration (in works)
- Certificate authentication into IdM UI/CLI (in works)

THANK YOU


plus.google.com/+RedHat


facebook.com/redhatinc


linkedin.com/company/red-hat


twitter.com/RedHatNews


youtube.com/user/RedHatVideos