

Red Hat Identity Management



Agenda

- Identity Management (IdM) in Red Hat Enterprise Linux
- System Security Services Daemon (SSSD)
- Active Directory Integration
- Demo
- Public Resources

Red Hat Identity Management

Identity Management (IdM) in Red Hat Enterprise Linux

Identity Management in Red Hat Enterprise Linux

- **Implements Standards-Based, Integrated Components**
 - Kerberos, LDAP, DNS and x.509 certificates provide a simple integrated identity management solution
- **Reduces costs**
 - Leverage Red Hat IdM for your RHEL (and other Linux/Unix!) servers, potentially reducing licensing costs for third-party directory servers like Active Directory.
- **Simplify Management**
 - Consistent user, group, sudo, selinux, automounts (and more!) management throughout the RHEL environment

Identity Management in Red Hat Enterprise Linux

- **Enhances Security**
 - Centralizes authentication, authorization and access control for UNIX/Linux environments
- **Provides eSSO (enterprise Single Sign-On) via Kerberos**
 - Enables users to access many different enterprise resources after their initial log-in without having to log in again and again
- **Centralizes Administration and Control**
 - Easily consolidate and manage identity servers in a UNIX/Linux environment; with the option to interoperate with Active Directory

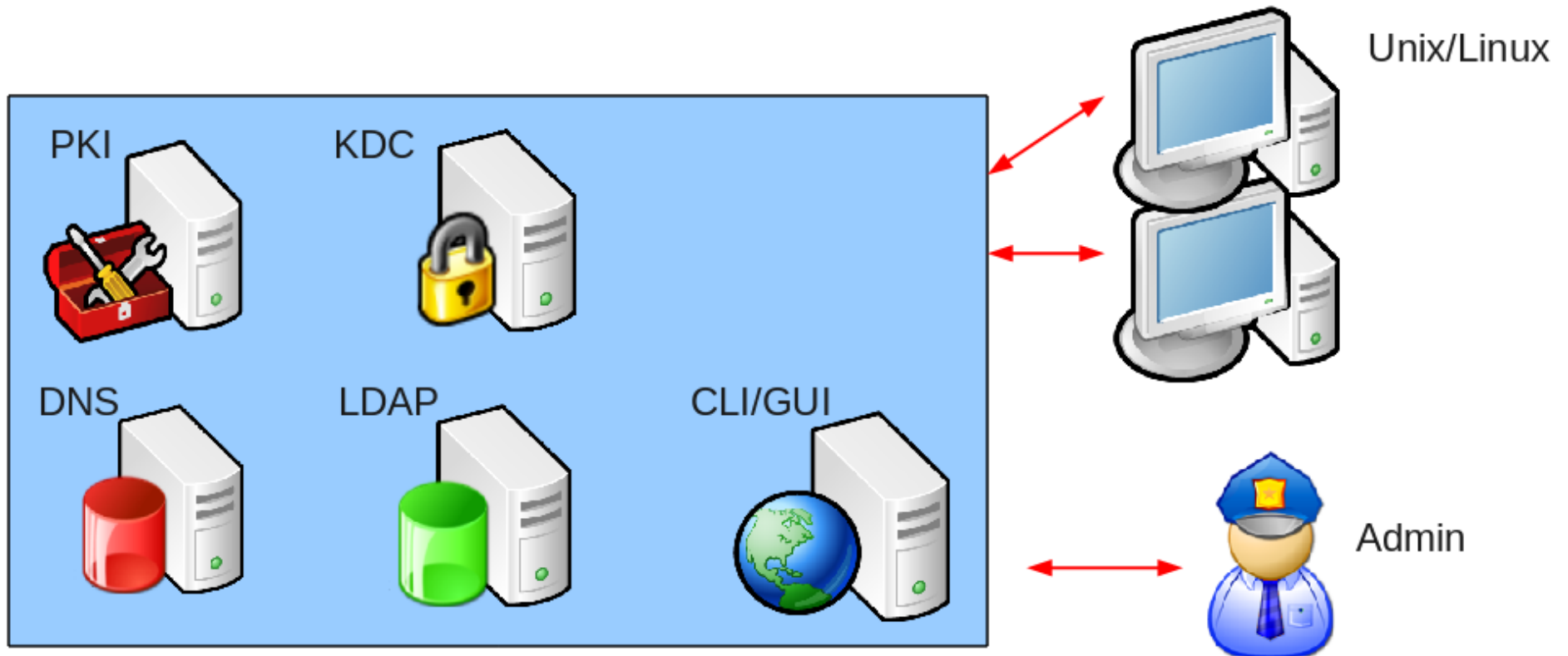
Identity Management in RHEL: Features

- Command Line Interface
- Web Based GUI
 - Management Console
 - User Self Service
- Enterprise SSO for Kerberos aware applications
- Interoperability with Microsoft Active Directory domains
- Smooth migration paths from NIS and LDAP services
- Two Factor Authentication w/One Time Passwords (OTP)
- Up to 20 servers and replicas and an unlimited number of clients in a single domain (~ 2,000 clients per server)

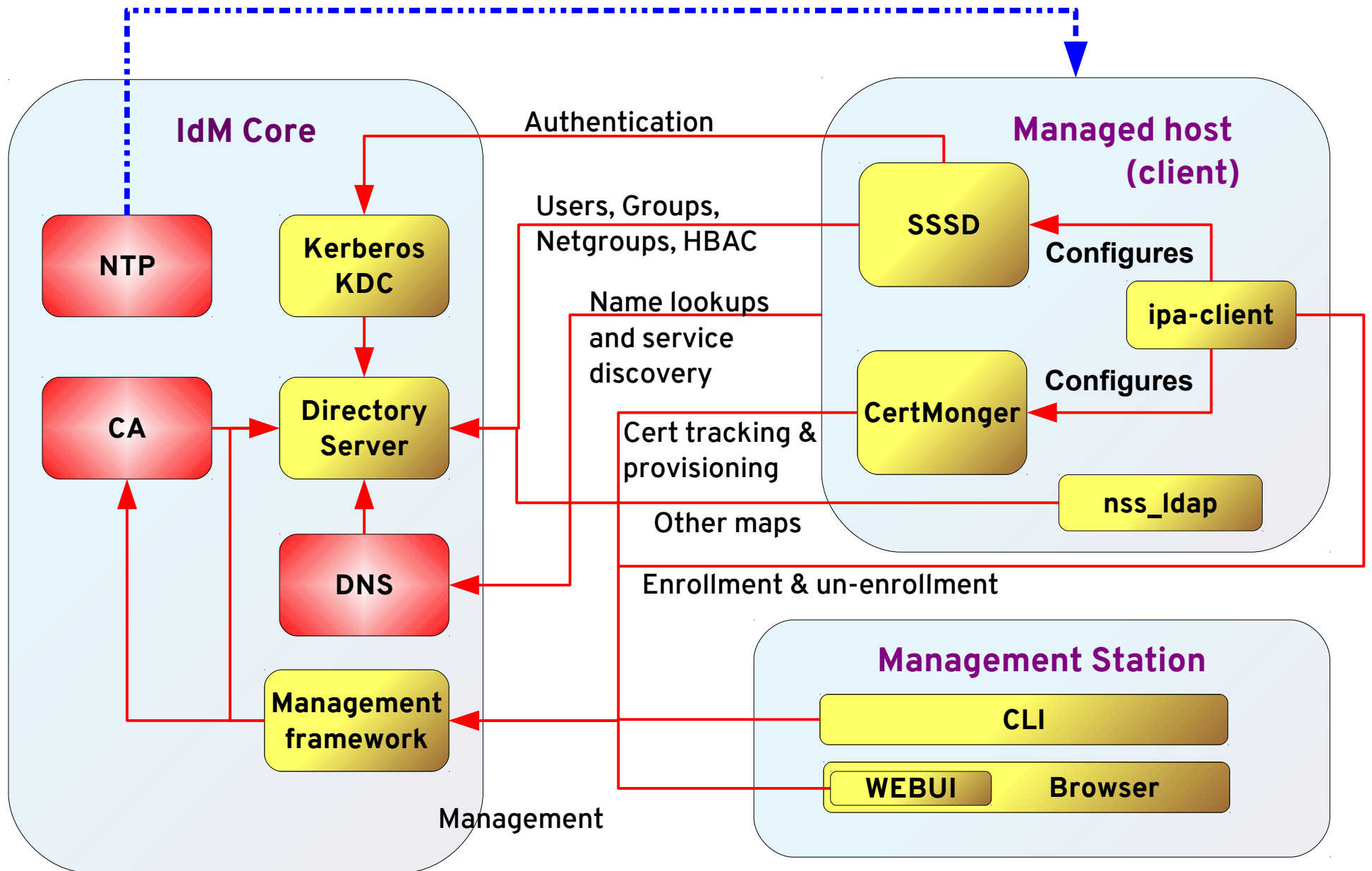
Identity Management in RHEL: Features

- Centralized management of:
 - Automounts
 - Global Password Policies
 - Host Based Access Control (HBAC)
 - Integrated DNS (optional - can be delegated)
 - Selinux Configurations and User Mappings
 - SSH Key Management
 - Host Fingerprints
 - User SSH keys
 - SSL Certificate Management
 - Server, Services and Users
 - Sudoers

IdM - simplified architecture view



IdM Components in Red Hat Enterprise Linux



IdM Design Considerations

- **Internal or External DNS**
 - Internal easier to manage, but customers usually have their own DNS already
 - Side step the problem via zone delegation
- **Desired integration with Active Directory**
 - User/Group and Password Sync
 - Active Directory Trusts (RHEL7)
- **Multi-Site**
 - Server selection (6.4), Preferred servers
- **Certificate Setup**
 - Root CA or subordinate CA

Red Hat Identity Management

System Security Services Daemon (SSSD)

What is SSSD?

- The System Security Services Daemon (SSSD) provides access to different identity and authentication providers. SSSD is an intermediary between local clients and any configured data store. Local clients connect to SSSD and then SSSD contacts the external providers. SSSD provides a number of benefits for administrators:
 - Credential caching / Offline authentication
 - Reduced load on authentication/identification servers
 - Able to handle multiple configurations simultaneously

What is SSSD?

- SSSD recognizes domains, which are associated with different identity servers. Domains are a combination of an identity provider and an authentication method
- SSSD works with LDAP identity providers
 - IdM in RHEL
 - Red Hat Directory Server
 - OpenLDAP
 - Microsoft Active Directory
- SSSD also works with other native LDAP authentication or Kerberos authentication

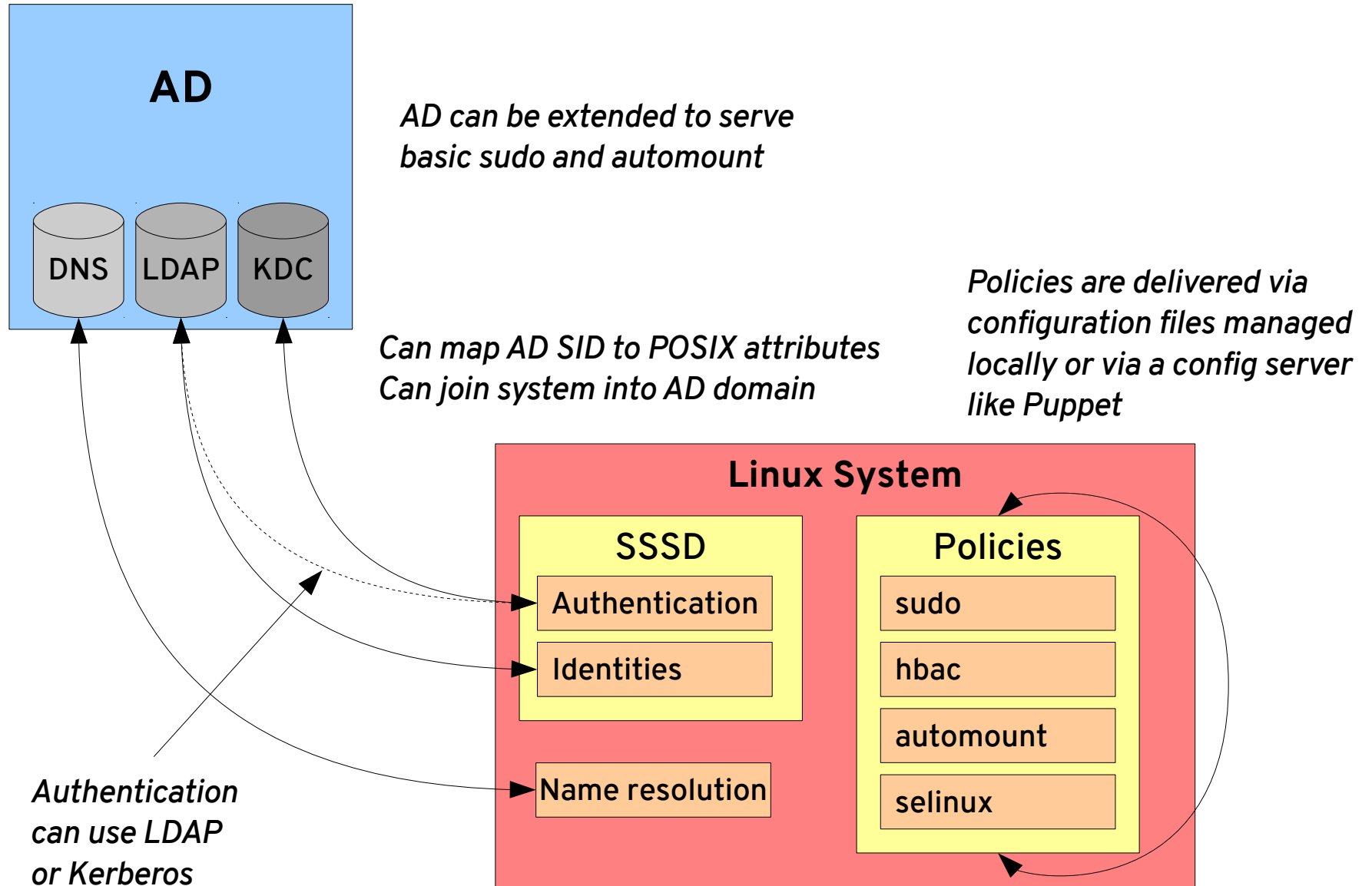
SSSD Technical Details

- How do I know if sssd is being used
 - Is the service running (sssd)
 - In /etc/nsswitch.conf, look for the 'sss' directive
- Documentation
 - Primary documentation for SSSD is in the RHEL Deployment Guide
- Identification Provider / Authentication Provider Combinations
 - LDAP / LDAP
 - LDAP / Kerberos
 - LDAP / Proxy
 - Proxy / LDAP
 - Proxy / Kerberos
 - Proxy / Proxy

Red Hat Identity Management

Active Directory Integration

Direct SSSD → AD Integration Option

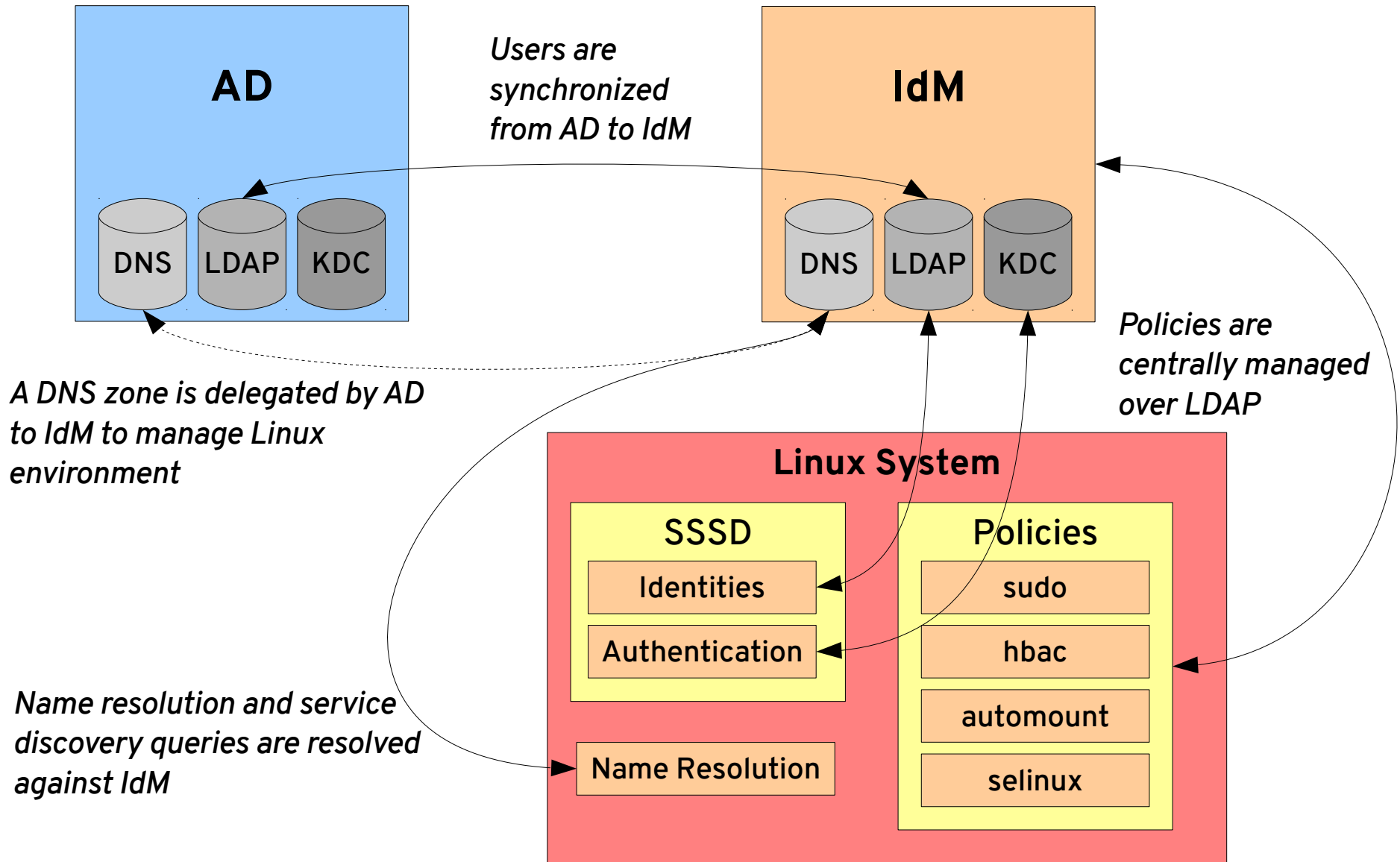


Pros and Cons of Direct SSSD → AD Integration

- **Pros:**
 - Does not require third party software
 - Does not require SFU/IMU (RHEL 6.4 and newer)
 - Supports trusted domains with IPA (RHEL 6.4 and newer)
 - Perceived more stable than Winbind
- **Cons:**
 - Does not support trusted AD domains
 - Does not support some advance AD optimizations
 - Policy management requires separate configuration mechanisms such as Satellite and Puppet

IdM → AD Synchronization Option

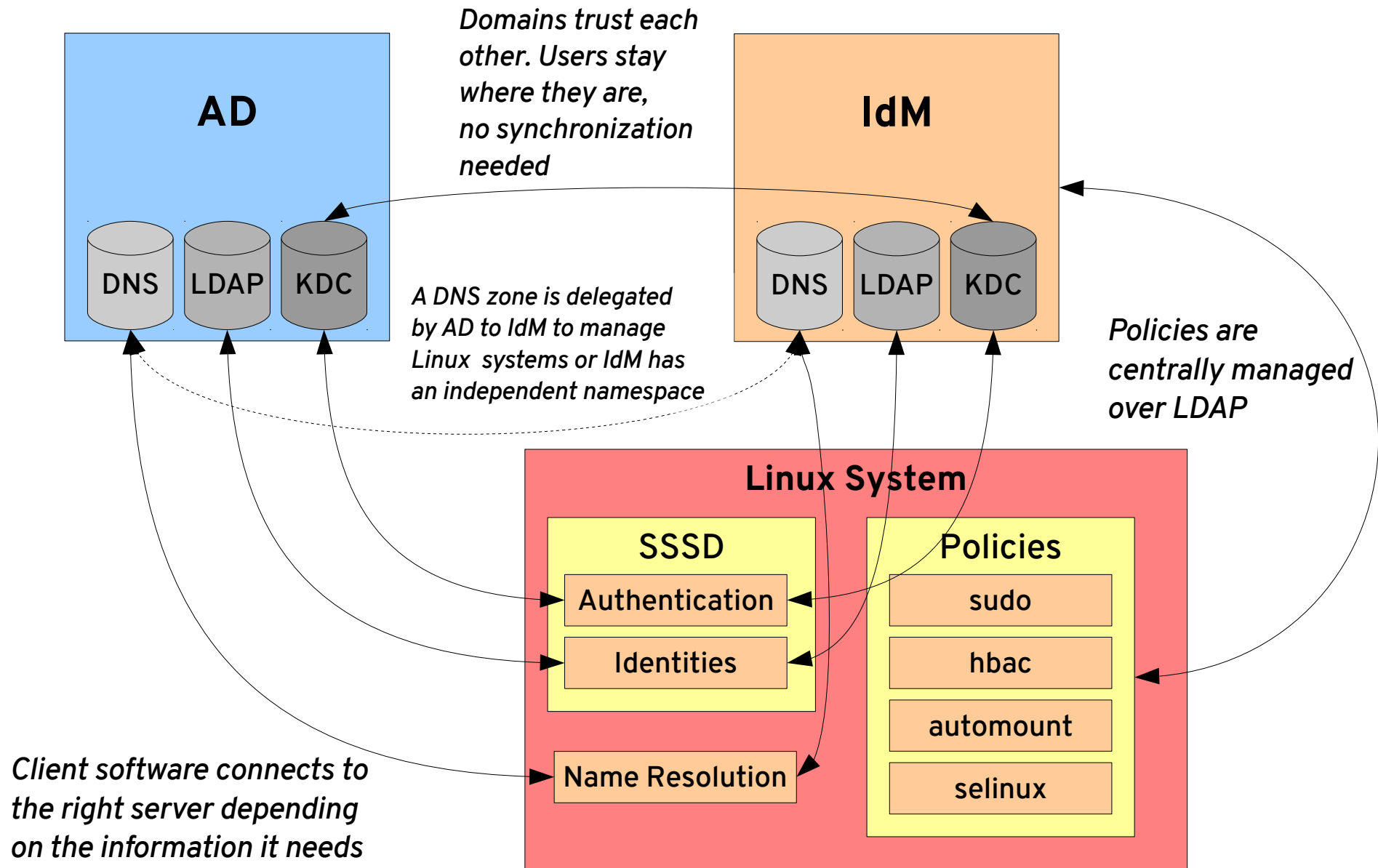
**** Supported, not Recommended ****



Pros and Cons of IdM → AD Synchronization

- **Pros:**
 - Reduces cost – no CALs or 3rd party
 - Policies are centrally managed
 - Gives control to Linux admins
 - Enabled independent growth of the Linux environment
- **Cons:**
 - Requires user and password sync
 - Authentication does not happen in AD
 - Requires proper DNS setup

IdM ↔ AD Trust Integration Option



Pros and Cons of IdM ↔ AD Trust Integration

- **Pros:**
 - Reduces cost – no CALs or 3rd party
 - Policies are centrally managed
 - Gives control to Linux admins
 - Enabled independent growth of the Linux environment
 - No synchronization required
 - Authentication happens in AD
- **Cons:**
 - Requires proper DNS setup
 - Requires latest SSSD
 - Requires RHEL 7

Red Hat Identity Management

Demo

<http://bit.ly/1lj8zVv>

Red Hat Identity Management

Public Resources

Public Resources

- Customer Portal:
 - <http://red.ht/20Aw1hw>
- Product Documentation:
 - <http://red.ht/1Ac5cUp>



Questions?