Identity Management
in Red Hat Enterprise Linux 8 beta

Dmitri Pal
Director, Software Engineering, Red Hat, Inc.
09-May-2019

What is this presentation about?

Let us set expectations!

What is this presentation about?

- Who in the audience does not use Identity Management from Red Hat but considers it and came to learn more?

What is this presentation about?

- Who in the audience does not use Identity Management from Red Hat but considers it and came to learn more?
- Who in the audience uses Identity Management in Red Hat Enterprise Linux (IdM) and wants to:
  - Learn how to get most out of the solution?
  - Find a solution to a specific problem?
  - Share their experiences about the deployments and discuss challenges and successes?

What is this presentation about?

- Building identity management solution for your enterprise
- Getting the most out of your deployment
- What is next
- Staying connected

Building an Identity Management solution for your enterprise

What do we hear?

- How do I build my overall IdM solution for the enterprise connecting all the layers to avoid fragmentation?
- Should I use the Directory Server or IdM? What is the difference?
- What is the role of the RH-SSO? Is it the same as IdM?
- I have an existing LDAP solution and I need to consolidate around Active Directory (AD), what should I do?

IdM vs. Directory Server

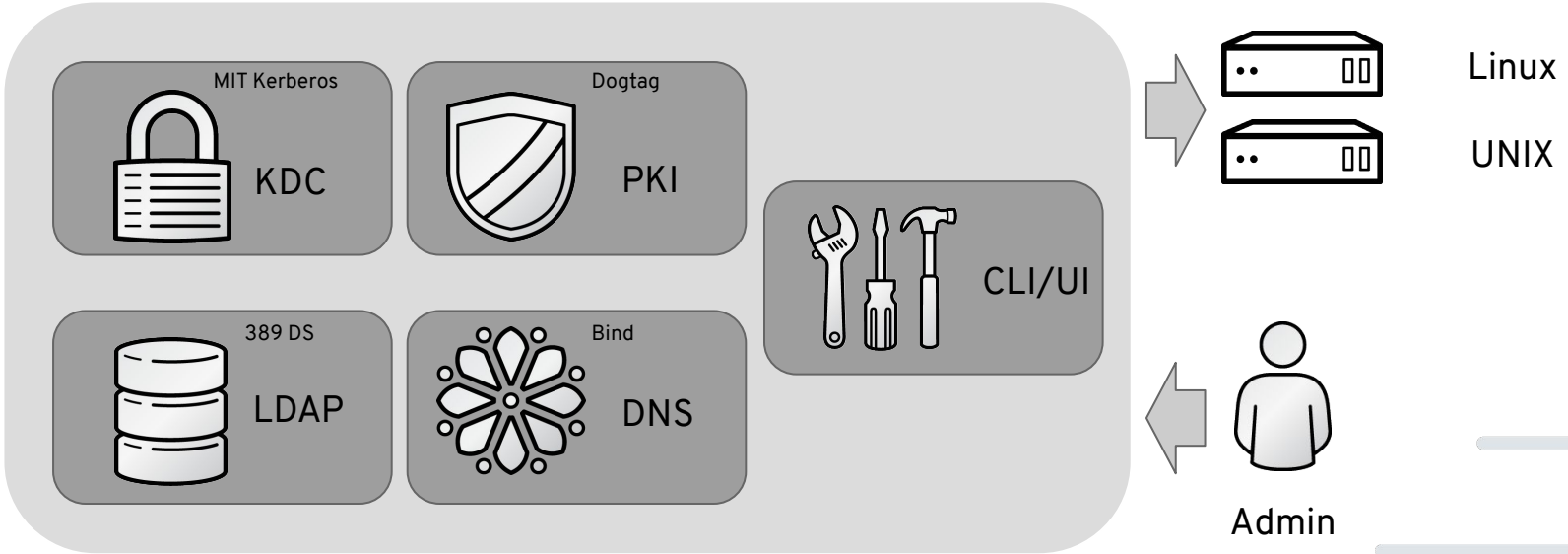
What is IdM?

- IdM – Identity Management in Red Hat Enterprise Linux
- Based on FreeIPA open source technology
- IPA stands for Identity, Policy, Audit
  - Focused on identities and related policies
  - A separate project is ongoing in the audit space
- Built into operating system - comes with the RHEL subscription

What Problems IdM Solves?

- Central management of authentication and identities for Linux clients
  - Improvement over standalone LDAP/Kerberos/NIS based solutions
  - Simplify and automate management of the infrastructure
- Gateway between the Red Hat Enterprise Linux and Active Directory.
  - Supports Active Directory forest trusts (recommended)
  - User and Password synchronization (not recommended)

IdM High Level Architecture



https://access.redhat.com/articles/1586893

What is the best fit for IdM?

- Best fit:
  - Manage user population inside the enterprise
  - Manage Linux/UNIX systems, policies and access
  - Integrate with Active Directory
  - As a replacement for existing LDAP solutions used for internal identities
- Can be used:
  - As a back end for external facing applications (but not generally recommended)
  - As a replacement for existing LDAP solutions used for external identities
- Not a good fit (yet):
  - Highly customizable back end is required
  - Huge amount of data (hundreds of thousands of entries)

What is Red Hat Directory Server?

- LDAPv3 Compliant LDAP server
- Red Hat distributed and supported version of 389 DS project
  - Identity Management uses 389 DS as its foundation
- Flexible and extensible
  - Schema and DIT can be extended at your discretion
- High performance
  - Scales to globally distributed deployments
- Provides multi-master replication
- Reliable and robust
- Offered as a stand alone product

What problems does DS solve?

- General purpose replicated identity storage
- A reliable storage for user accounts and other related data as a back end of a business application
- High volume of read and authentication operations
- Custom design of objects and data
- Distributed and complex topologies with replication
  - Allows read only replicas and replication policy
- Drop-in replacement for existing costly 3rd party LDAP solutions

What is the best fit for DS?

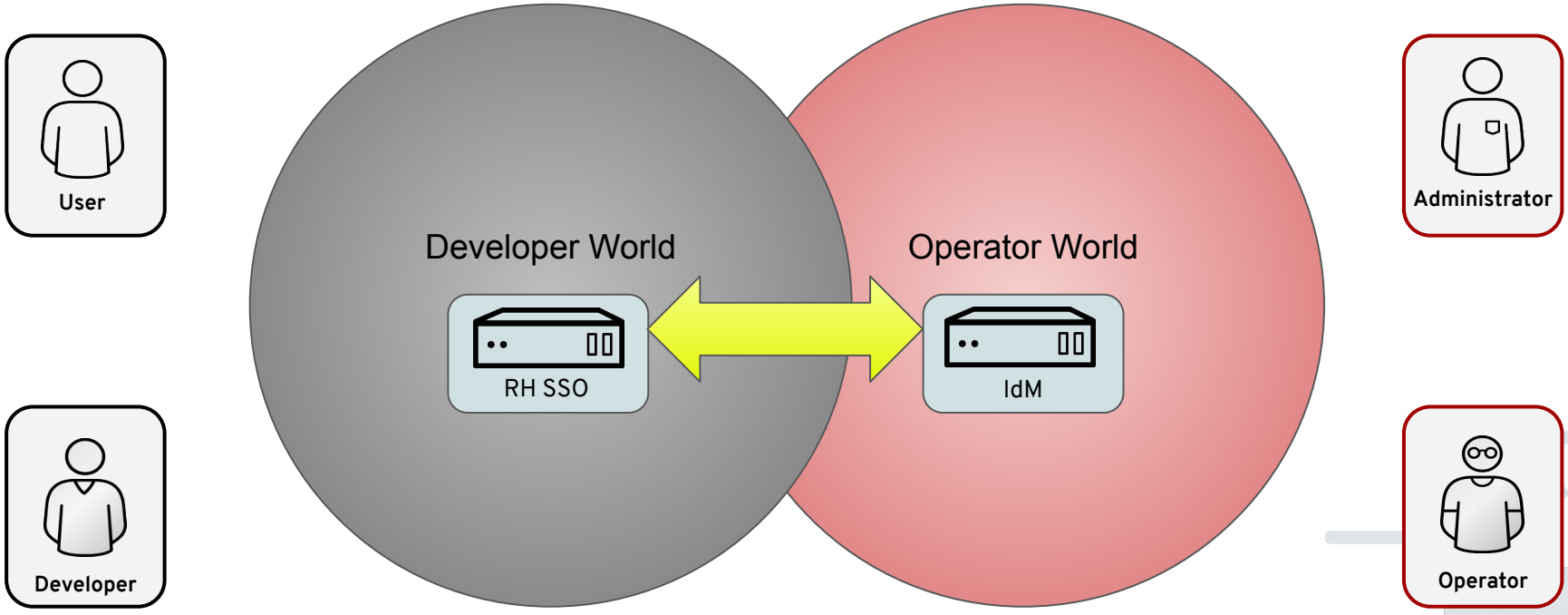
- Best fit:
  - Back end for externally facing applications
  - Cases where a lot of customisation is required
  - A drop-in replacement for the existing LDAP solution
- Can be used:
  - To manage identities inside the enterprise (but not recommended)
- Not a good fit:
  - Systems, policies, certificate, key management inside enterprise

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, 2FA
AD integration	User synchronization	Advanced integration via cross forest trusts
Replication	Up to 20 masters + unlimited read only replicas/hubs	Up to 60 active masters
Scalability	Scales well beyond 100K objects	Has limitations beyond 100K objects

IdM vs. RH-SSO

RH SSO and IdM



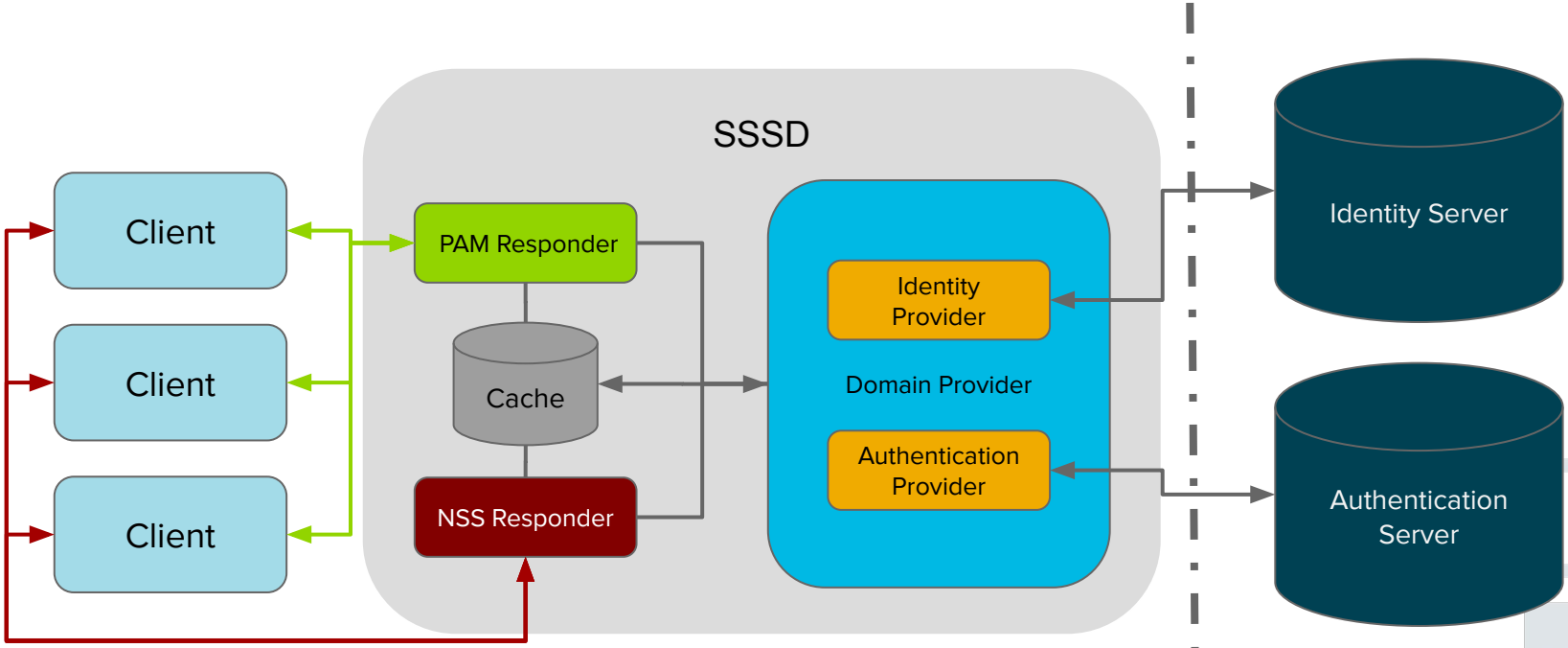
For more details see [Red Hat Summit 2017 presentation]

SSSD

What is SSSD?

- SSSD = System Security Services Daemon
- SSSD is a service used to retrieve information from a central identity management system (AD, IdM, IdM + AD trust).
- Provides authentication (LDAP, Kerberos) and access control (Host-based, GPO, LDAP filter, white/black list, etc.)
- Provides online and offline identity services for a host and applications on top (via apache modules and DBus interface)
- Takes care of the server discovery and failover
- Enables two factor authentication

What is SSSD?


SSSD
Client
Client
Client
PAM Responder
Cache
NSS Responder
Identity Provider
Domain Provider
Authentication Provider
Identity Server
Authentication Server

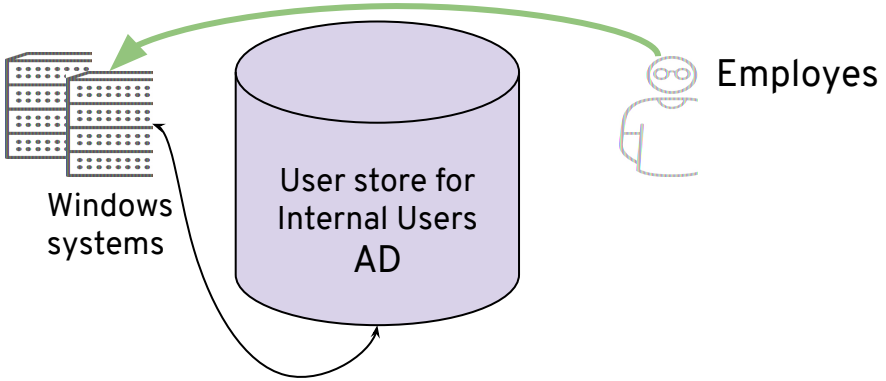
Building a solution

Recommended Architecture

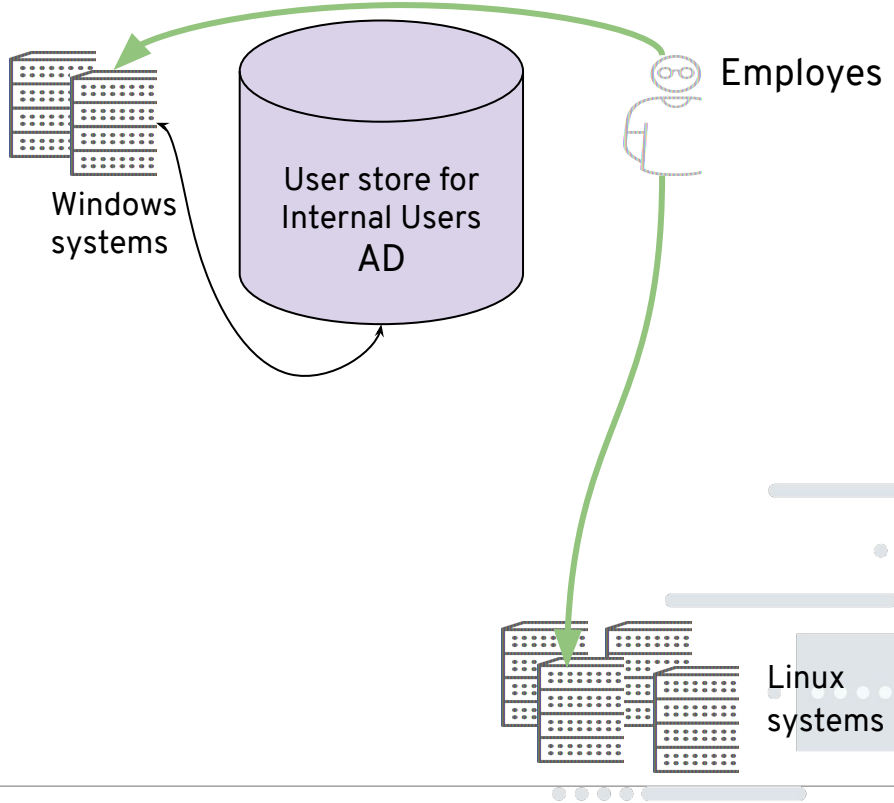
Employes

Recommended Architecture

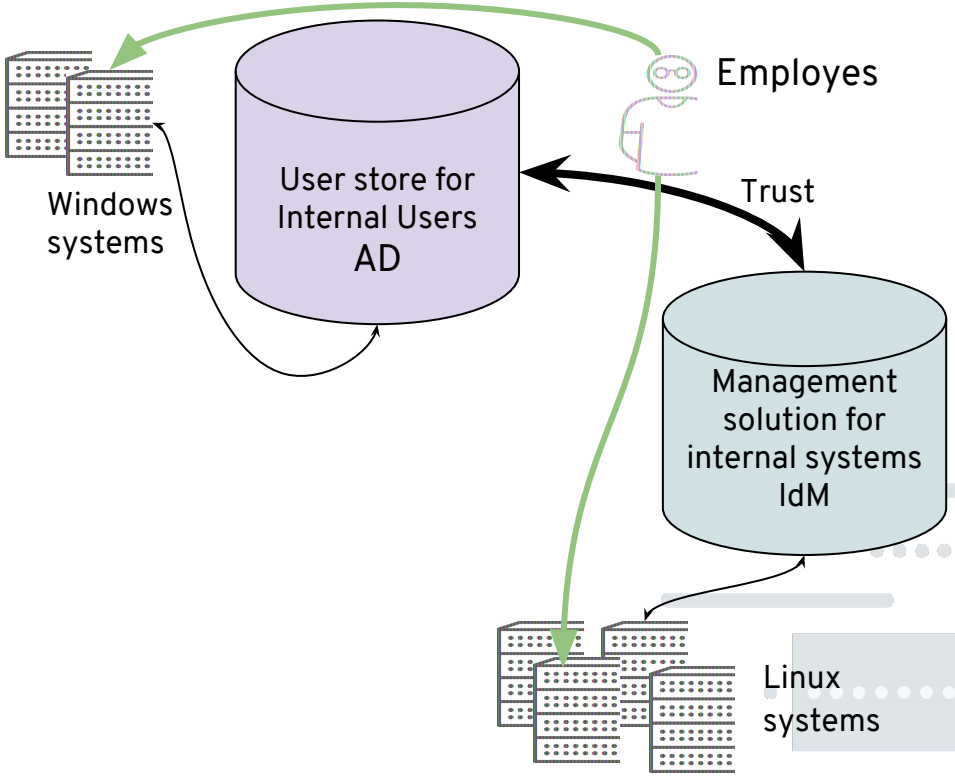
Recommended Architecture



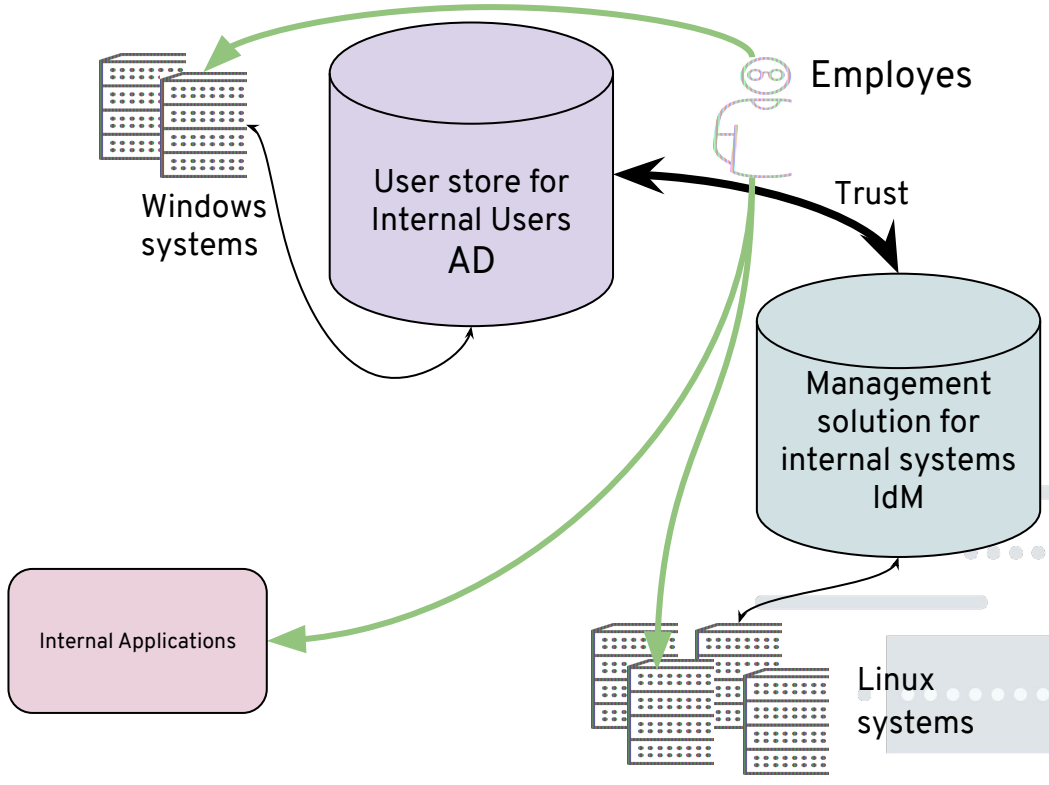
Recommended Architecture



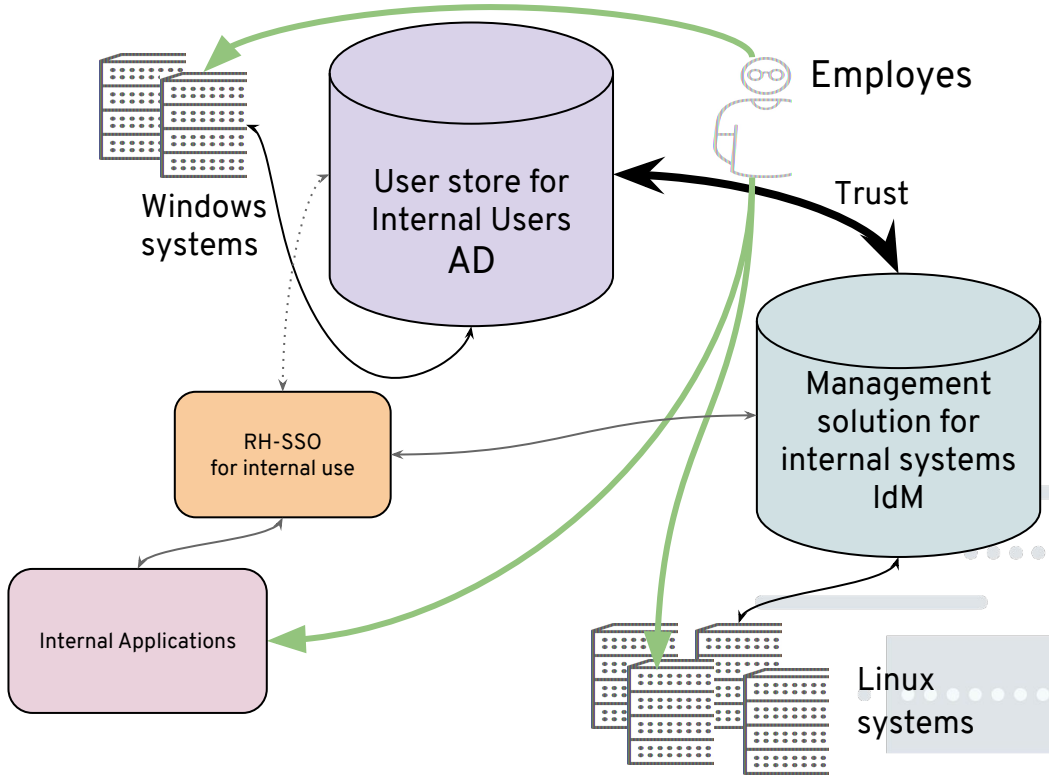
Recommended Architecture



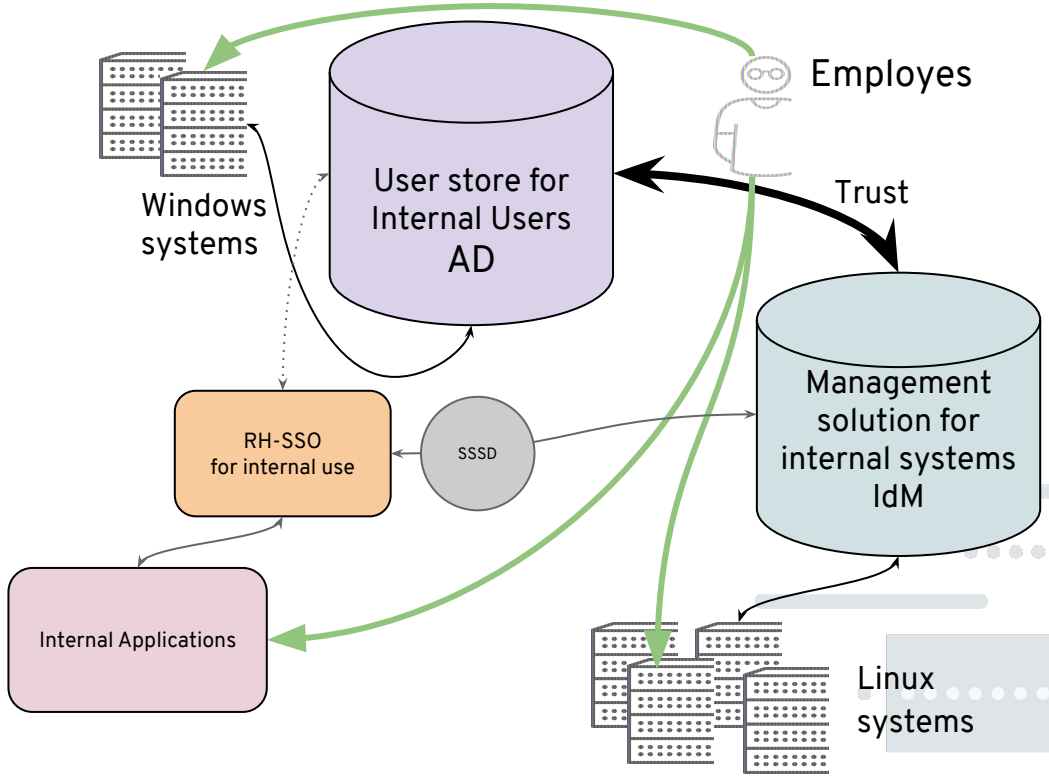
Recommended Architecture



Recommended Architecture

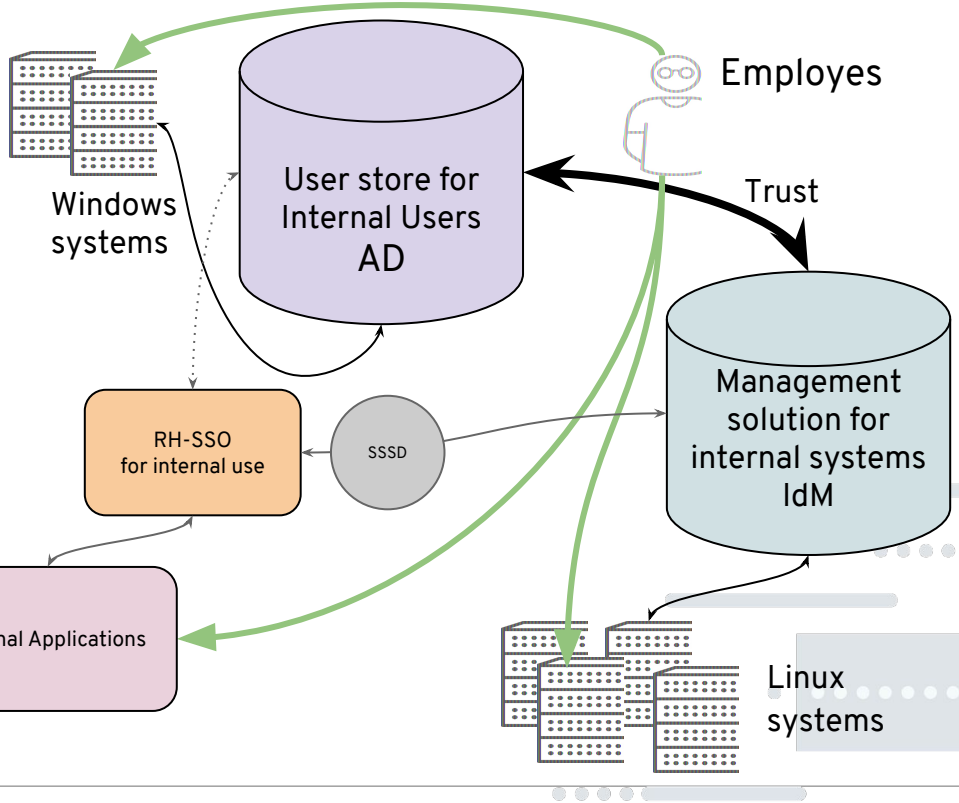


Recommended Architecture

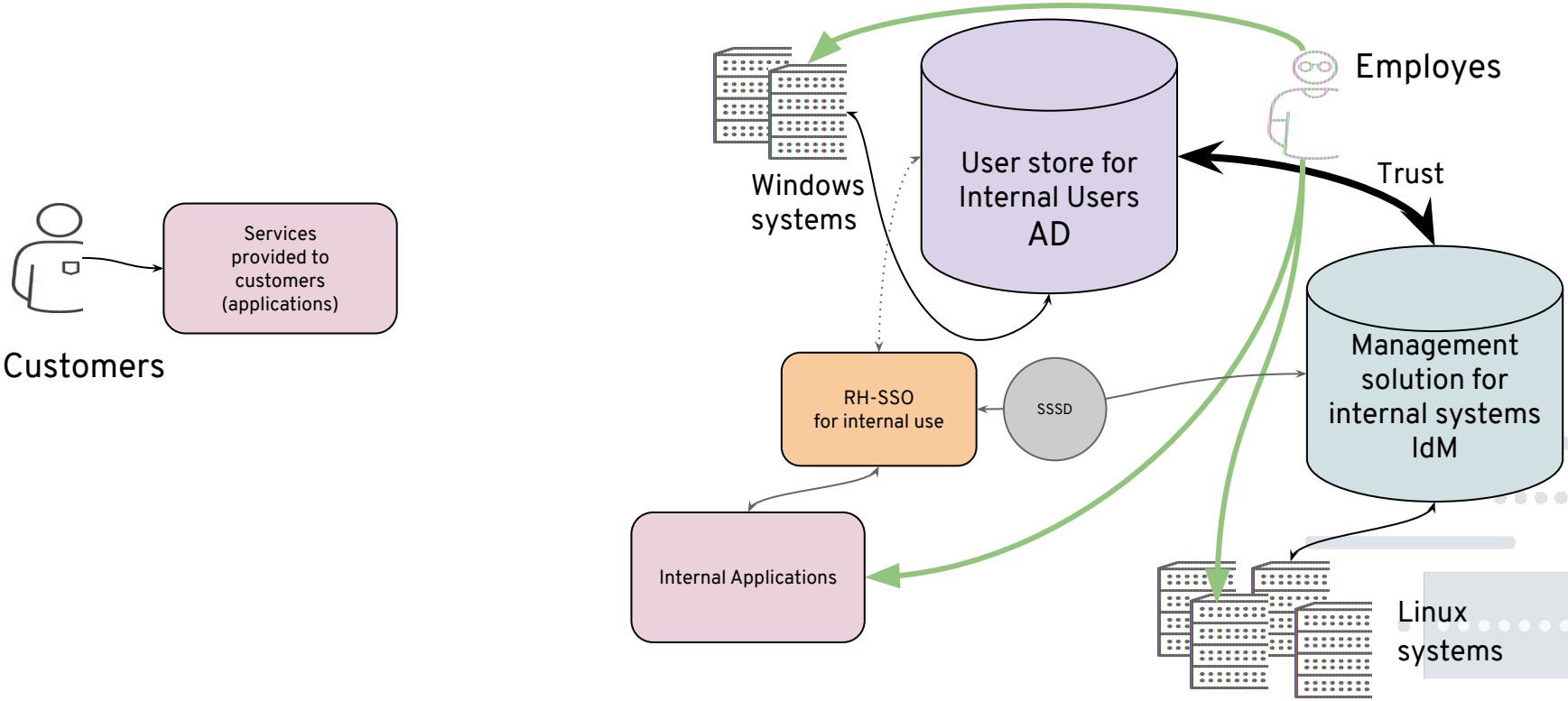


Recommended Architecture

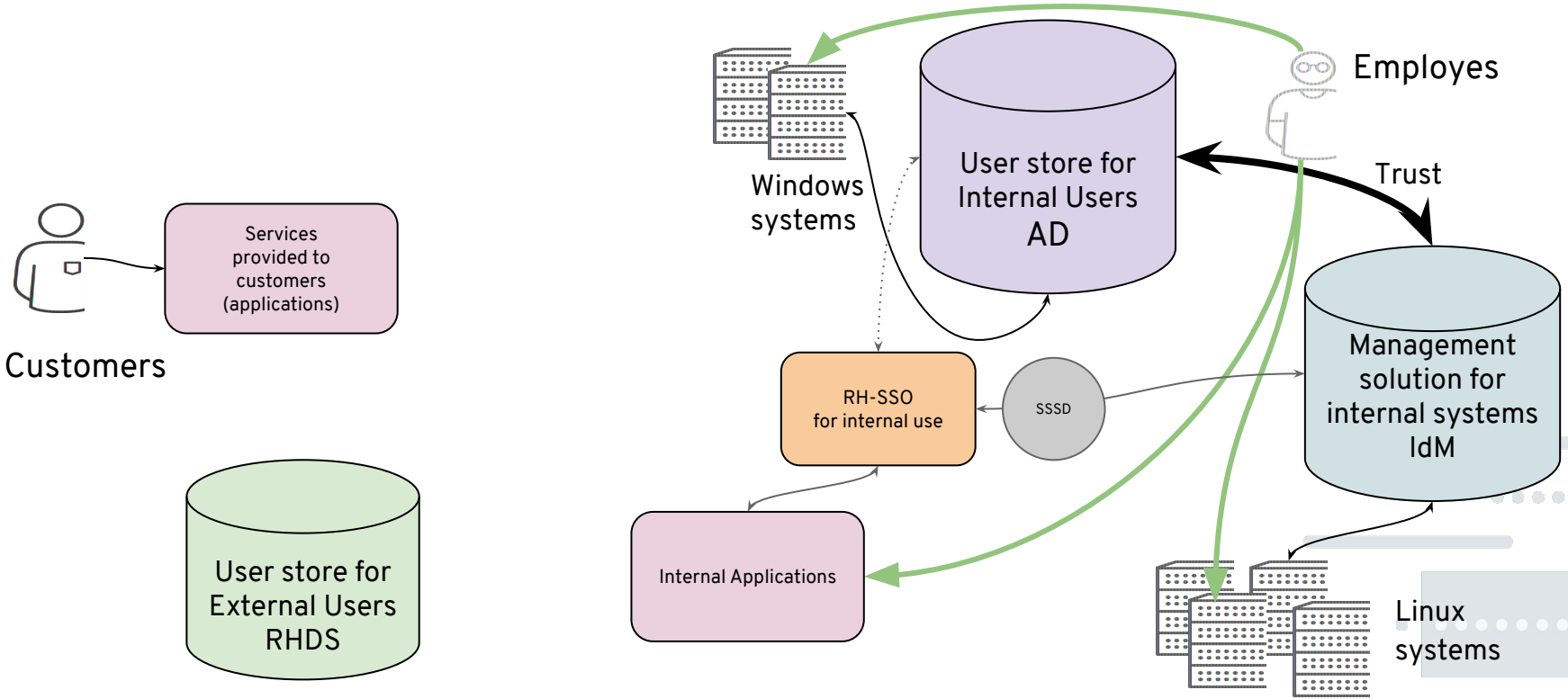
Customers



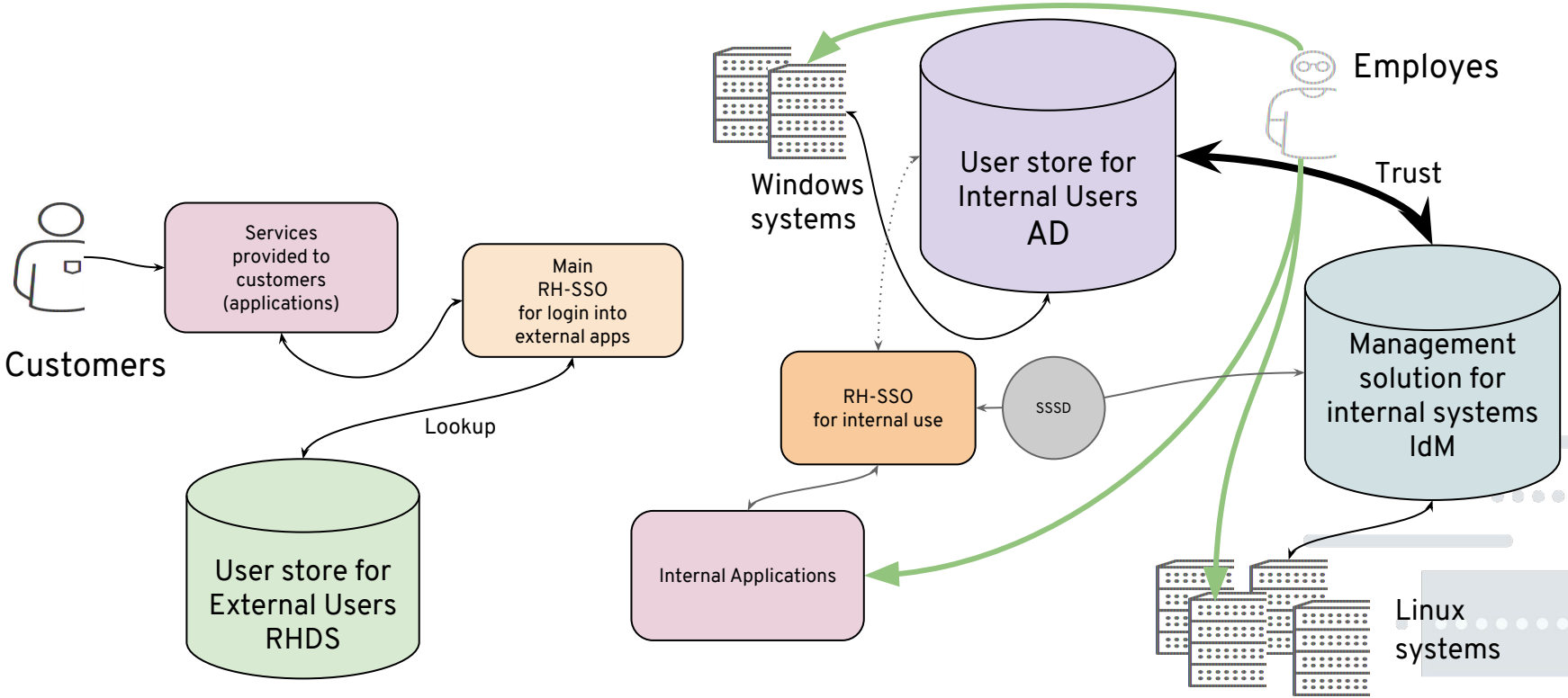
Recommended Architecture



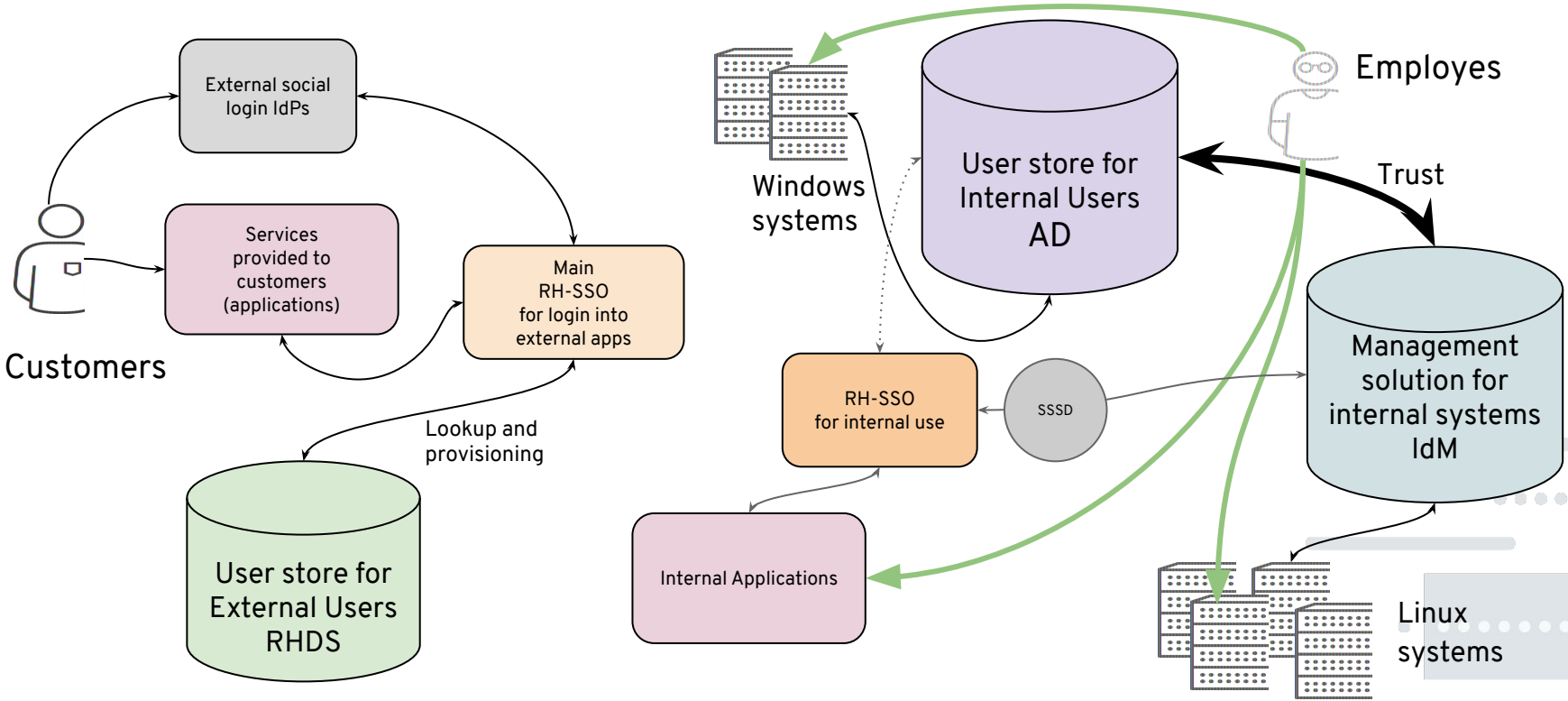
Recommended Architecture



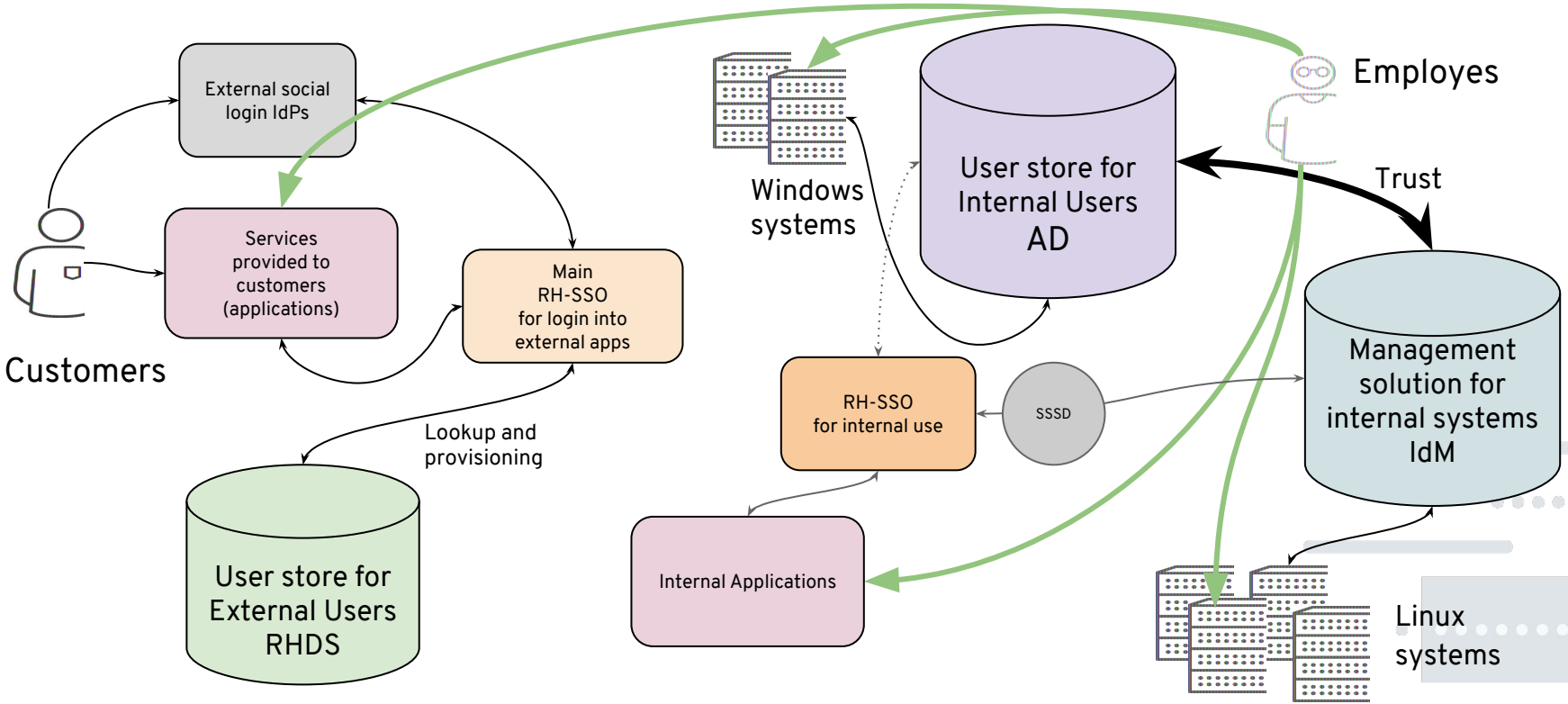
Recommended Architecture



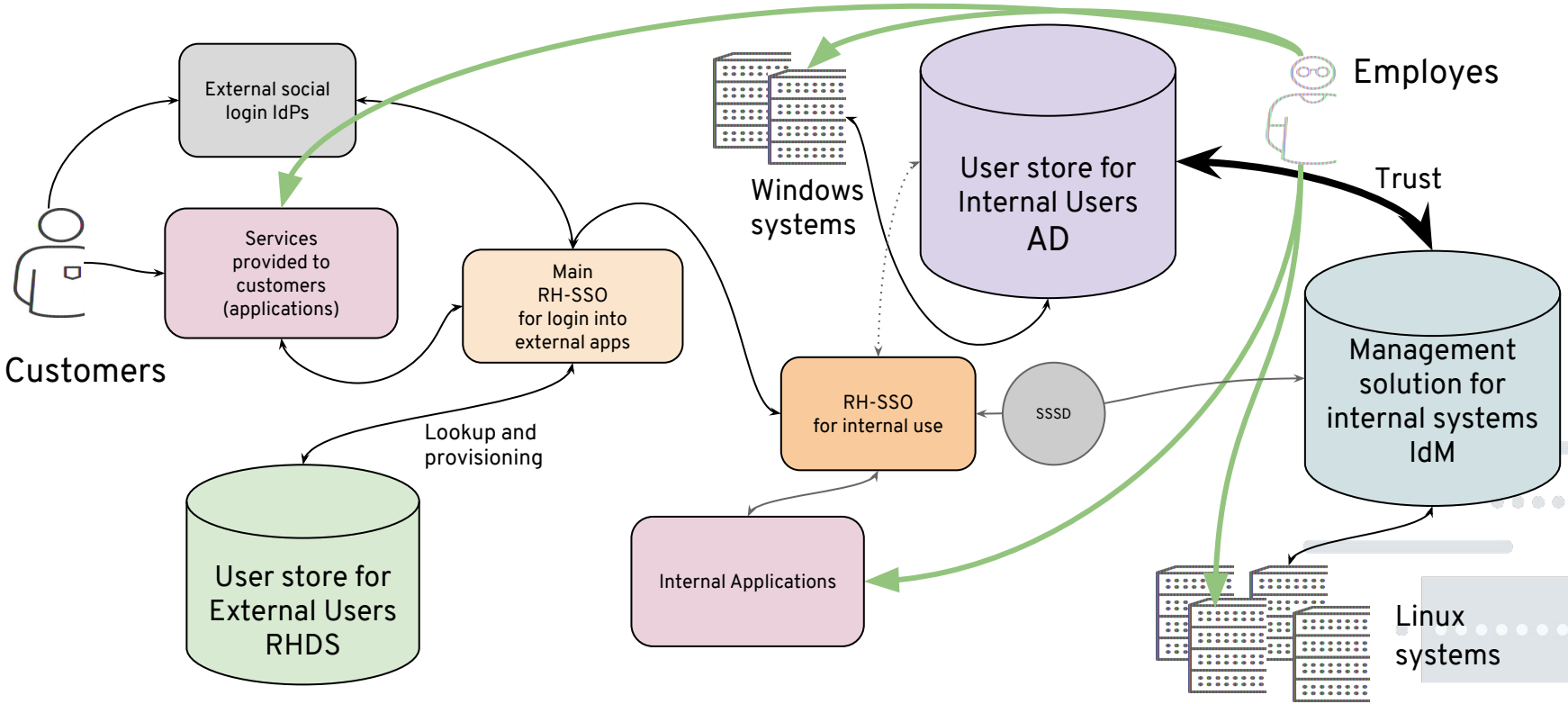
Recommended Architecture



Recommended Architecture



Recommended Architecture



From a 3rd party Directory to the Red Hat Directory Server or IdM

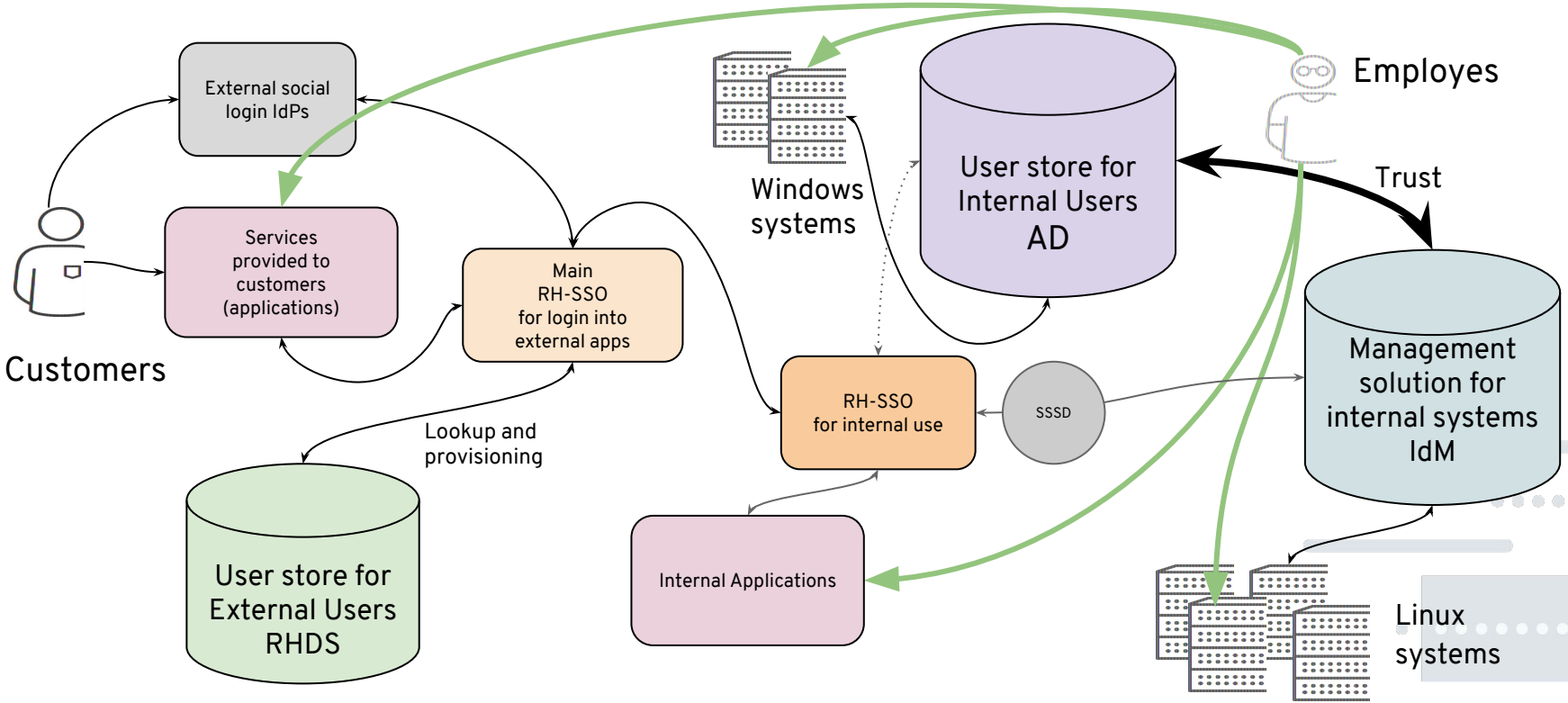
When it makes sense to move to DS?

- Renewal with a costly vendor
- A lot of LDAP customisation
- No time for re-design
- I want a stop gap solution now!

When is it better to move to IdM?

- Building next gen infrastructure
  - Thinking about scalability, growth, automation for the whole environment
- Have a funded project
- Have time to do things right
  - Need to think the transition through
  - Last year's presentation was all about it

Move to this Architecture!



How?

- Move users and groups to AD
- Deploy IdM
- Establish trust
- Start deploying new clients into the IdM realm
  - Deprecate and convert old clients to use IdM

    -or-

  - Let old clients die on a vine using old integration approach

Key factors for success

- Work with the vendors (Microsoft, Red Hat) to help you
  - Engage consulting and support (TAM)
- Take your time and plan ahead
- This is not as simple as it might look, there will be challenges

Getting the most from your Identity Management solution

What do we hear?

- Can I use two-factor authentication in my deployment?
- How do I make sure AD administrators can manage IdM environment?
- How do I define and know who can access what systems?
- I already have IdM running on Red Hat Enterprise Linux 7. What should we expect in the case of Red Hat Enterprise Linux 8?

Using two-factor authentication

Types of the 2FA

- PKI-based => Smart Card based 2FA
- One-time password/passcode based 2FA

Smart Card use cases

- My users are in AD
- They have certificates assigned or mapped to them in AD
  - The mapping can also be stored in the IdM overrides
- Users have smart cards issued to them
- I might connect Linux systems to AD directly or via the AD ⇔ IdM trust
- I would like to use smart cards to login into Linux systems

Can I?

Yes, for the local logins, when you are physically at the system

Smart Card use cases

- Can I log remotely from a Windows system into a Linux system?

Yes, but you need to use client side software, for example putty-cac

Smart Card use cases

- Does Red Hat support client side software on Windows, i.e. putty-cac?

No

Smart Card use cases

- After a remote login can I use a smart card authentication for sudo?

No - you have to authenticate using other credential (password, OTP)

Smart Card use cases

- Can I jump to other hosts with a single-sign-on after a smart card authentication?

No. putty-cac does not support proxying of the smart card.

Workaround:

- Use smart card authentication for login into a Windows system
- Leverage acquired Kerberos ticket for single-sign-on into a Linux system
- If you want to hop, configure kerberos ticket forwarding

Limitations:

- You will need to use password for sudo (there is no ability to use Kerberos for sudo)
- If you plan to use trust target Linux systems must be in a different DNS domain from AD
- Forwarding ticket granting tickets (TGT) is not the best practice

Smart Card use cases - Future

- Too many things for smart card login are still cumbersome…
- Red Hat Enterprise Linux 8 comes with a Web Console
- Web Console is integrated with SSSD and can leverage central authentication with IdM and AD (extra configuration is needed)
- Web Console is being worked on to provide:
  - Smart card authentication into a host
  - Smart card authentication into a sudo shell
  - Login into the system and hop to another system from the shell
- Benefit: no need for extra client components - connect with a browser
- Come to the Red Hat Enterprise Linux or IT Optimisation booth to discuss

Smart Card use cases - more

Use Case	Availability
I manage users in IdM and want to login into Linux systems using smart cards.	RHEL 7.2
I manage users in AD, I have a trust with IdM, I want to login into Linux systems using smart cards, user certificates are stored in AD or in the IdM ID overrides.	RHEL 7.3
I manage users in AD, I have a trust with IdM, I want to login into Linux systems using smart cards but I want to have a mapping to the certificate to the user and not store or match certificates in a binary form.	RHEL 7.4
I manage users in AD, I do not use IdM, my Linux systems are joined directly to AD and I want to login into Linux systems using smart cards. I will upload certificates into AD.	RHEL 7.5
I manage users locally on a Linux and want to login with a smart card. I want to use binary matching or do a flexible mapping of a certificate to a user.	RHEL 8.0
I manage users in AD, I do not use IdM, my Linux systems are joined directly to AD and I want to login into Linux systems using smart cards. I want to use flexible matching instead of matching the whole cert.	RHEL 8.0 (matching is managed locally in SSSD)

OTP authentication use cases

- My users are in IdM
- I would like to authenticate these users with OTP-based 2FA

Can I?

Yes, you can assign OTP tokens inside IdM (FreeOTP, Google Authenticator, Yubikeys or any standard HOTP/TOTP token)

OTP authentication use cases

- My users are in IdM
- I would like to authenticate these users with OTP-based 2FA from a 3rd party solution like RSA

Can I?

Yes, you can configure IdM to proxy authentication to an external solution using RADIUS protocol.

OTP authentication use cases

- In both cases above can I define which hosts or services can be accessed by users who authenticated with a single factor - password vs. two factor password+code?

Yes, you can configure Authentication Indicators. You can define hosts and services that require 2FA.

OTP authentication use cases

- But… majority of my users are in AD… and I use trust with IdM

Can I do a 2FA with AD users then?

No. 2FA authentication for AD users is not possible yet (requires SPAKE).

Workaround:

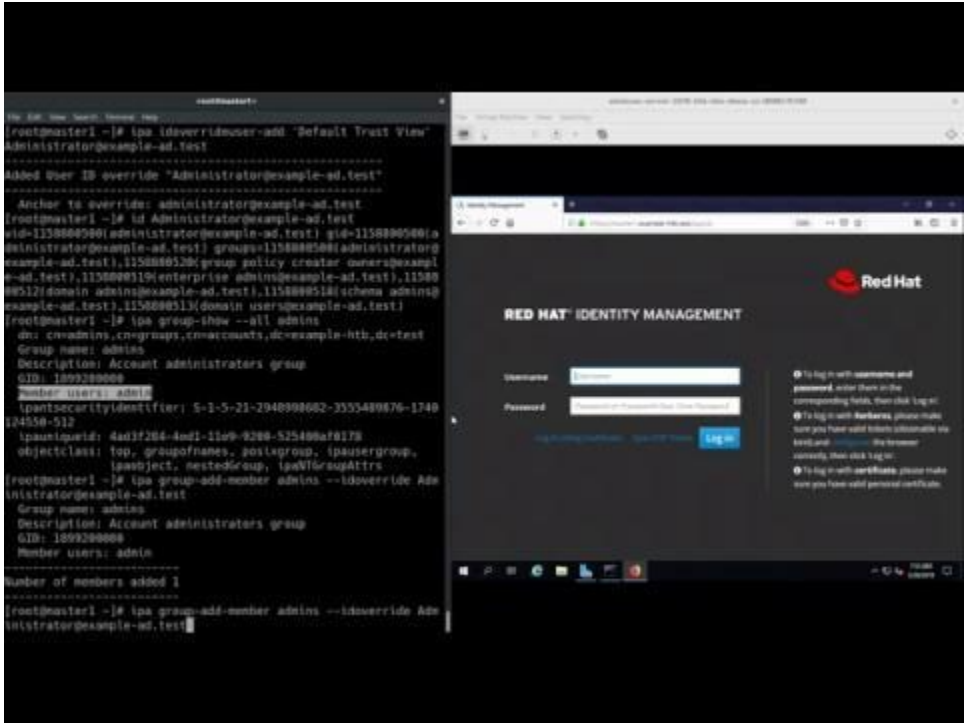
- Create users that require OTP authentication in IdM. You can use synchronization feature, IdM user management capabilities or create a script that will add users to IdM
- Assign those users tokens in IdM or configure proxy to a 3rd party solution like RSA

Managing IdM as an Active Directory Admin

Managing IdM by AD admins

- Can I manage IdM being an AD admin in the trust setup?

Managing IdM by AD admins



Managing IdM by AD admins

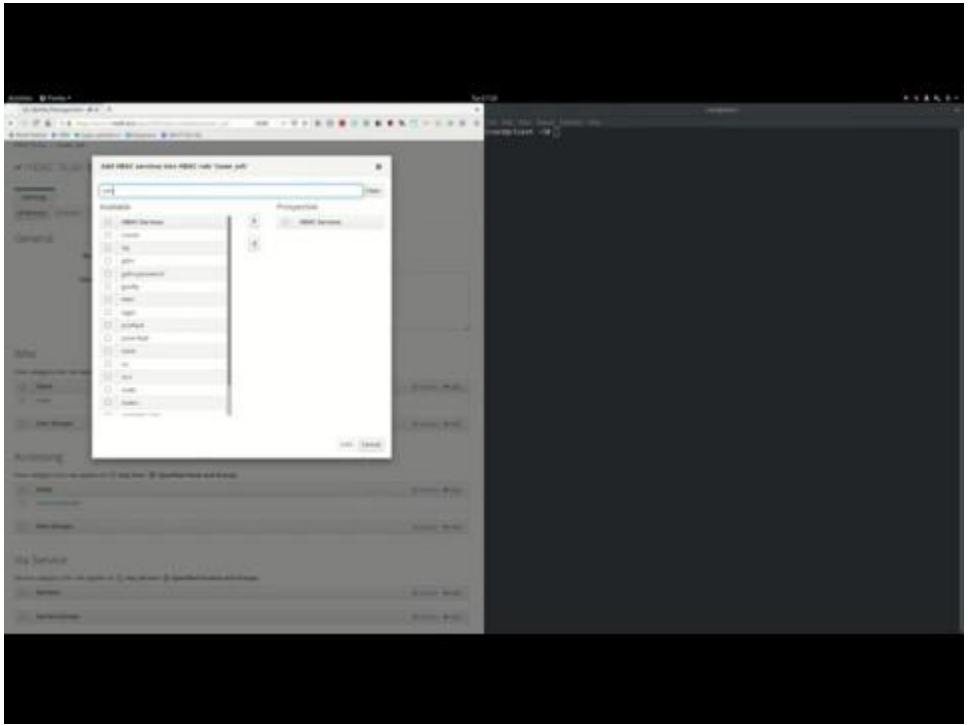
- Establish a trust
- Create an ID override for an AD user
- Add this override to the admins group
- Login as an AD admin to manage information in the IdM UI

Access control attestation report

Who can access a system?

- As an administrator I would like to know which users have access to the system?

Who can access a system?



Any limitations I should know about?

- In the trust setup the solution will show IdM groups but will not explicitly expand the list of the AD users
- The solution does not work yet for AD users in a direct integration setup

Upgrading to IdM in Red Hat Enterprise Linux 8

How do I move to IdM in RHEL 8?

- This is not an in place upgrade like with minor versions
- You need to deploy new replicas running RHEL 8 and remove RHEL 7 replicas
- Your RHEL 7 deployment must be upgraded to at least 7.6
- Your RHEL 7 deployment must be running with domain level 1
- Do not forget to move certificate tracking to a new server after you rotated all your replicas
- Do not run mixed environment for a long period of time (months) to avoid consistency problems

What is Next for IdM and SSSD?

What are we working on?

- Tools to improve administrative experience:
  - Healthcheck
  - Discover and reassign CRL/Renewal master
- Automation using Ansible
  - Server install
  - Client install
  - Adding replication agreements
- IdM in FIPS mode
- SSSD and Winbind alignment

More tools, more discovery, more automation, more remediation

Staying Connected

Staying Connected

- Collaborate in the community (freeipa.org)
- Participate in the official Beta
- Participate in the high-touch-beta (TAM is recommended)
- Collaborate in downstream development (TAM is required)

Join US on Thursday at 2:30 in CBC - 1 for a round table talk

(space is limited to 18 people)

Questions?

RED HAT SUMMIT

THANK YOU


linkedin.com/company/Red-Hat


facebook.com/RedHatinc

youtube.com/user/RedHatVideos


twitter.com/RedHat