IDENTITY AND ACCESS MANAGEMENT

Choosing the right tool for the right job

Ellen Newlands, Boleslaw Dawidowicz, Dmitri Pal
Product Manager, Engineering Manager, Engineering Director

05.03.2017

Agenda

- Introduction of the challenges
- Identity management problem space from the developer perspective
- Identity management problem space from the infrastructure perspective

INTRODUCTION

Digital Transformation: Dramatic changes for IT

> *“The business environment today is pushing companies to respond to ever increasing competition.*
>
> *In order to remain competitive, they have to deliver their services faster, at greater scale, and do so efficiently in order to remain profitable.*
>
> *These demands drive* ***application developers*** *to create new applications and deliver them faster.*
>
> *This further places stress on the* ***IT Operations team*** *who has to provide a scalable, on-demand infrastructure that can service the Developers.”*
>
> Gartner

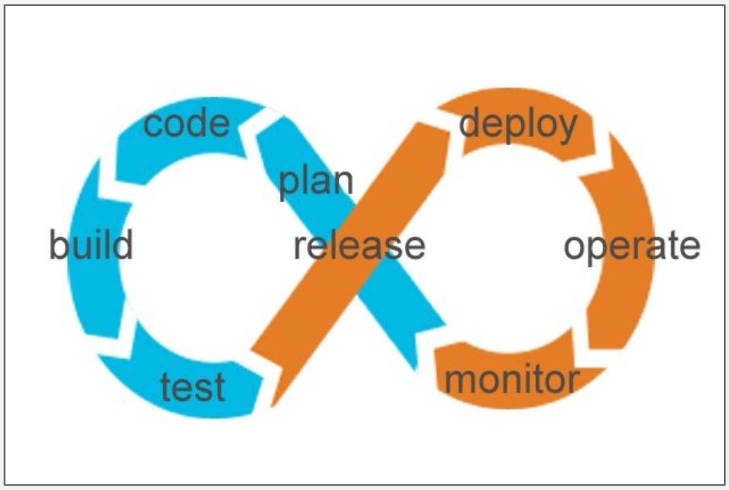
CEO
Competitive pressure driving digital transformation

LINE OF BUSINESS
Challenged to deliver services faster, at scale, and more efficiently

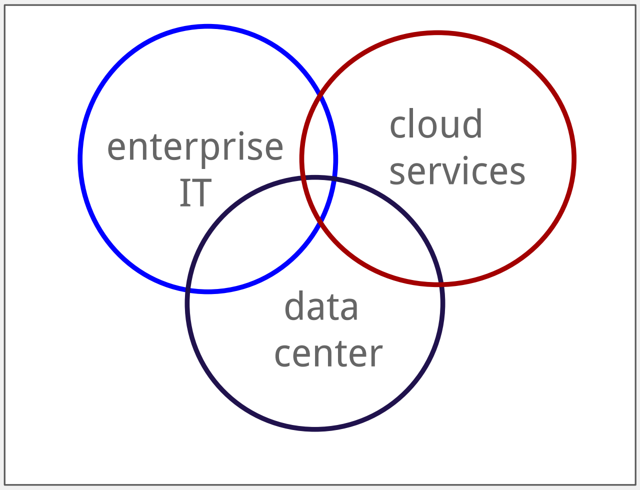
DEVELOPERS
Need to develop applications faster with greater productivity

IT OPERATIONS
Must provide infrastructure agility, on-demand that scales as needed

Digital Transformation: The new approach



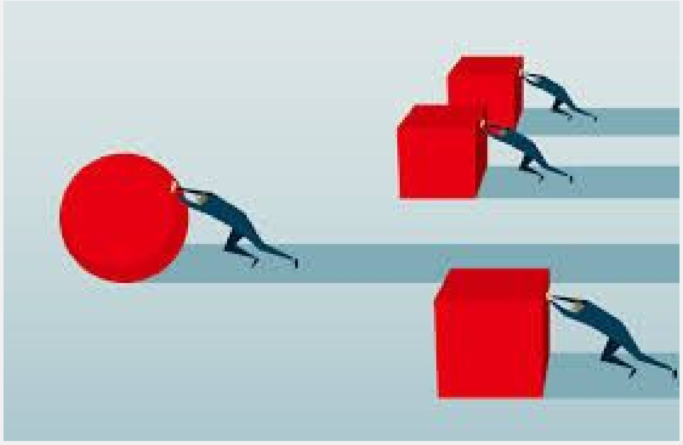
DevOps



IT Environment

Benefits of Digital Transformation

- Gain efficiency
- Improve productivity
- Increase agility
- Move faster



Identity Management Fabric

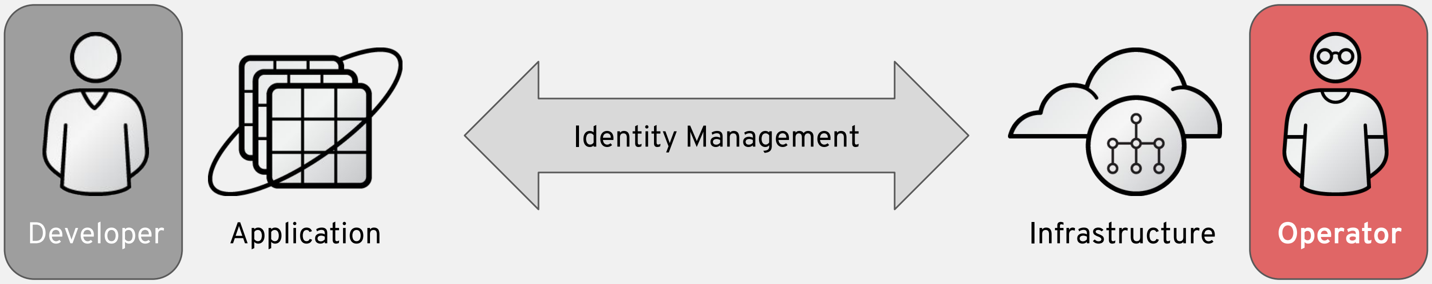
Introduction

Projects, products, components and technologies that solve a wide spectrum of the challenges that modern enterprise faces:

- Across private and public clouds
- While deploying bare metal systems, virtual machines and containerized payloads
- With wide proliferation of identity and authentication identity and authentication sources
- With productivity demands requiring single-sign-on across multiple levels and protocols

Identity Management Fabric

Foundation of Digital Transformation

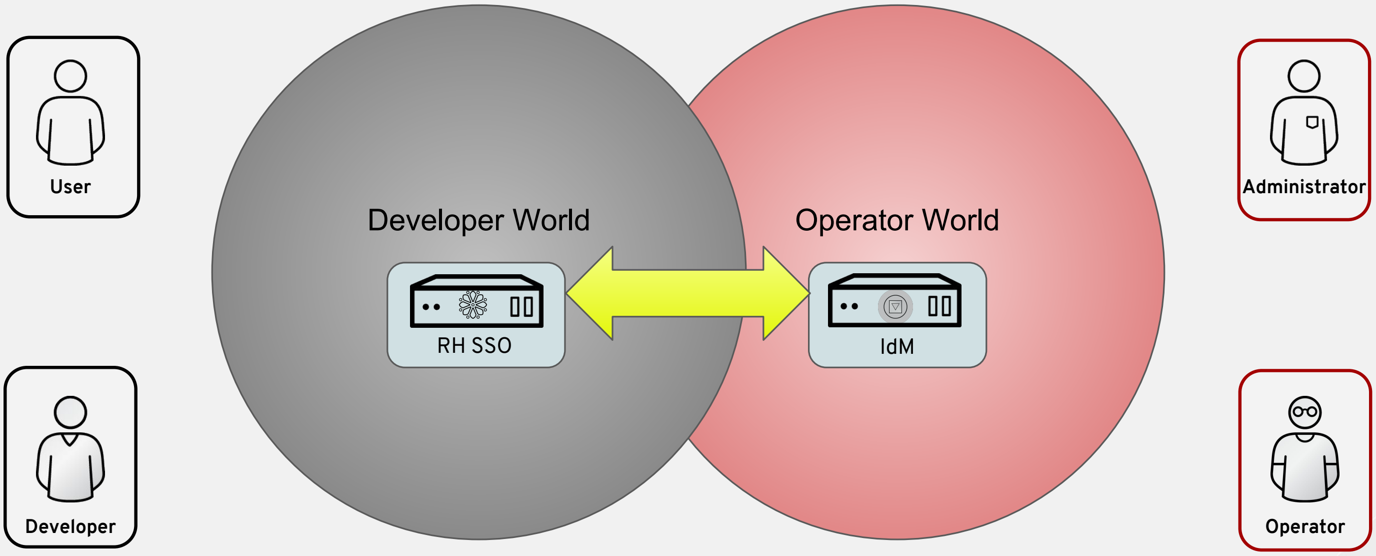


DEVELOPMENT

PRODUCTION

Identity Management Fabric

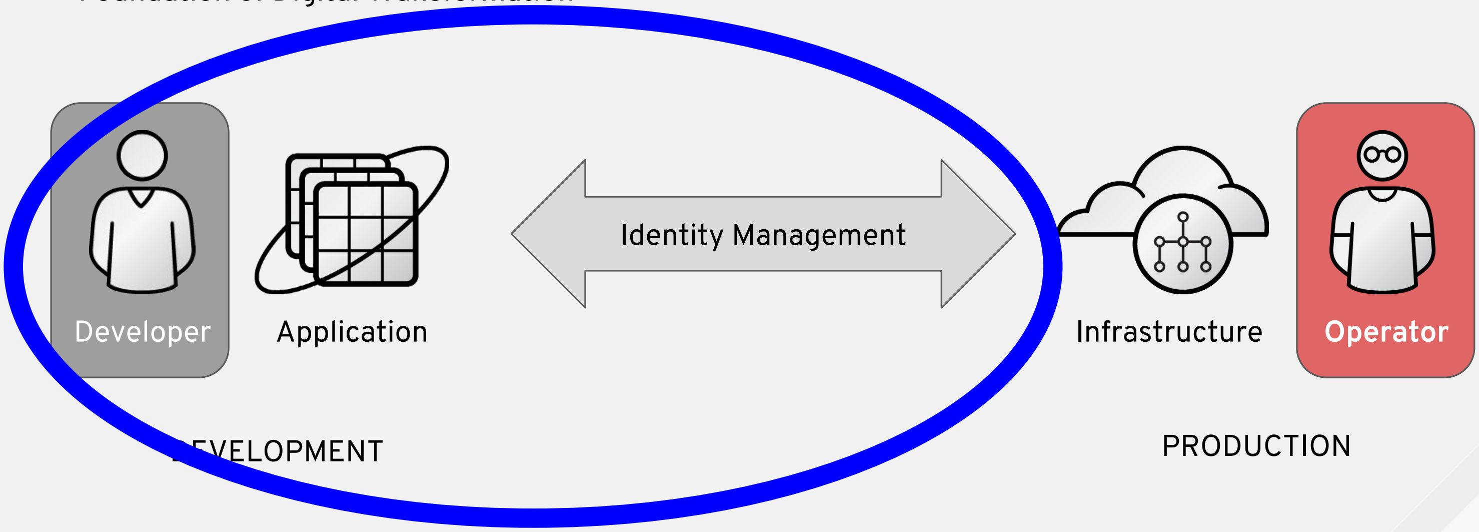
Core Components



Developer Perspective

Identity Management Fabric

Foundation of Digital Transformation



Developer

Application

Identity Management

Infrastructure

Operator

DEVELOPMENT

PRODUCTION

Challenge:
Modern application requirements

Modern application requirements

Development Perspective

Modern application requirements

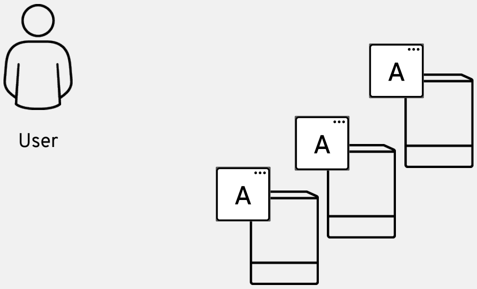
Development Perspective

User

Modern application requirements

Development Perspective

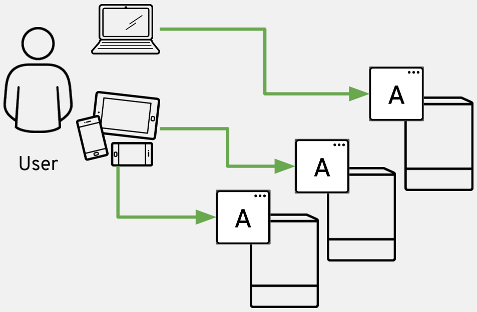
- **SSO between different UIs and applications**



Modern application requirements

Development Perspective

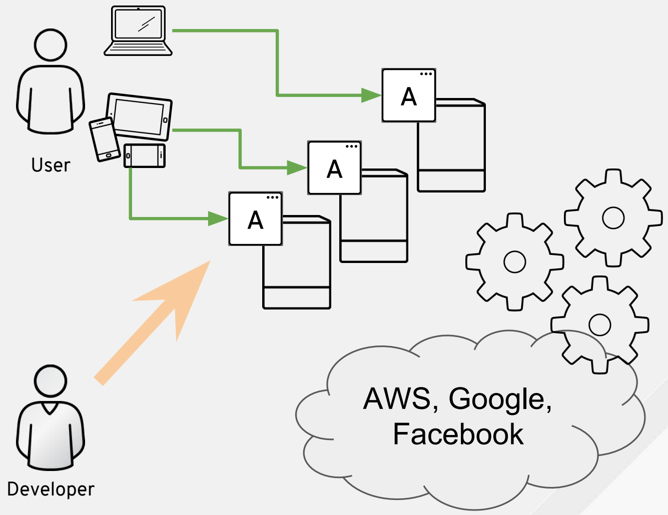
- SSO between different UIs and applications
- **Modern apps**
  - **Mobile**
  - **HTML5**
  - **Client side / Stateless**



Modern application requirements

Development Perspective

- SSO between different UIs and applications
- Modern apps
  - Mobile
  - HTML5
  - Client side / Stateless
- **(Micro)Services Oriented Architecture**
  - **REST Services & APIs**



Solution

RH-SSO provides

Development Perspective

RH-SSO provides

Development Perspective

- **SAML 2.0**
  - **Identity Provider implementation**
  - **Service Provider libraries for Enterprise Application Platform**

RH-SSO provides

Development Perspective

- SAML 2.0
    - Identity Provider implementation
    - Service Provider libraries for Enterprise Application Platform
- **OpenID Connect / OAuth2**
    - **Authorization Server implementation**
        - **Compliance with all five OpenID Connect profiles**

RH-SSO provides

Development Perspective

- SAML 2.0
  - Identity Provider implementation
  - Service Provider libraries for Enterprise Application Platform
- OpenID Connect / OAuth2
  - Authorization Server implementation
    - Compliance with all five OpenID Connect profiles
- **Easy to use integration libraries and agents / adapters**
  - **Securing different applications and services within very few trivial steps**

RH-SSO provides

Development Perspective

- SAML 2.0
    - Identity Provider implementation
    - Service Provider libraries for Enterprise Application Platform
- OpenID Connect / OAuth2
    - Authorization Server implementation
        - Compliance with all five OpenID Connect profiles
- Easy to use integration libraries and agents / adapters
    - Securing different applications and services within very few trivial steps
- **Management UI fully backed by REST endpoints and CLI to manage all server configuration aspects**

Challenge:
Modern interconnected applications and services in the cloud

(Services and applications acting on behalf of a user)

Being fit in modern days...

Development Perspective

Being fit in modern days...

Development Perspective

Being fit in modern days...

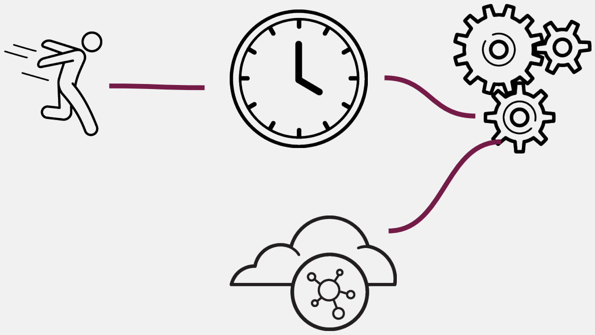
Development Perspective

- **Jogging session gets tracked on a smartwatch**

Being fit in modern days...

Development Perspective

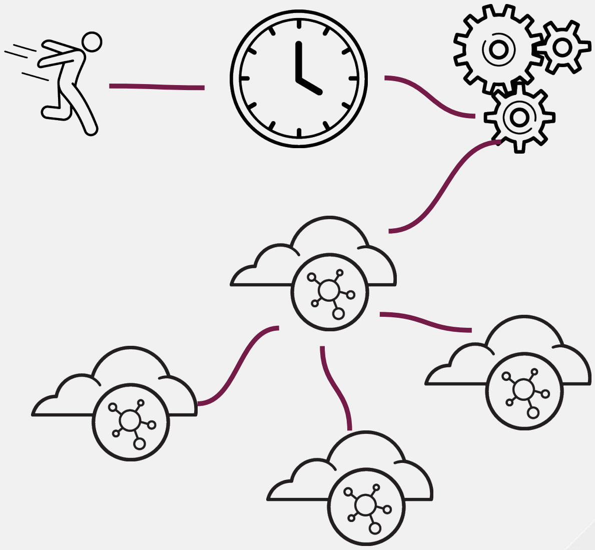
- Jogging session gets tracked on a smartwatch
- **Route, pace, HR and etc. get uploaded automatically to the web portal**



Being fit in modern days...

Development Perspective

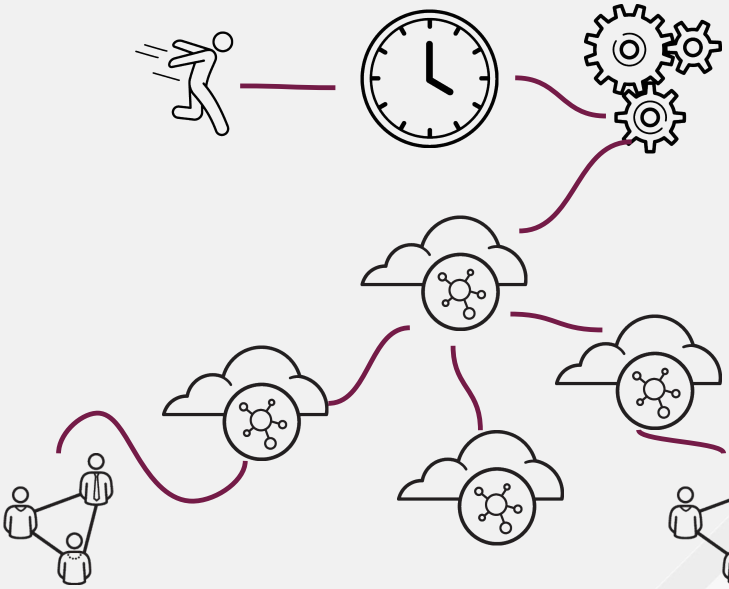
- Jogging session gets tracked on a smartwatch
- Route, pace, HR and etc. get uploaded automatically to the web portal
- **Other social portals for runners automatically pull the data**



Being fit in modern days...

Development Perspective

- Jogging session gets tracked on a smartwatch
- Route, pace, HR and etc. get uploaded automatically to the web portal
- Other social portals for runners automatically pull the data
- **Everything gets automatically published on social media**



Modern Token based security

Development Perspective

Modern Token based security

Development Perspective

- **Modern applications act on behalf of users and are interconnected**

Modern Token based security

Development Perspective

- Modern applications act on behalf of users and are interconnected
- **All happening AUTOMATICALLY and ON BEHALF of a user**

Modern Token based security

Development Perspective

- Modern applications act on behalf of users and are interconnected
- All happening **AUTOMATICALLY** and **ON BEHALF** of a user
- **Authorization and Delegation based on long living tokens**
  - **Granted once and valid for long time**
  - **Centrally managed active sessions**
  - **Possible to be revoked at any time by the user**

Solution

RH-SSO provides

Development Perspective

RH-SSO provides

Development Perspective

- **OpenID Connect / OAuth2 - Authorization Server implementation**
  - **Standards designed specifically for this use case**

RH-SSO provides

Development Perspective

- OpenID Connect / OAuth2 - Authorization Server implementation
  - Standards designed specifically for this use case
- **Single place to define token configuration**
  - **Lifespan and etc.**
  - **Define included attributes, mappings and roles**

RH-SSO provides

Development Perspective

- OpenID Connect / OAuth2 - Authorization Server implementation
    - Standards designed specifically for this use case
- Single place to define token configuration
    - Lifespan and etc.
    - Define included attributes, mappings and roles
- **Centralized Session Management**
    - **Users able to review and invalidate active sessions**
    - **Admins able to revoke access to compromised clients/tokens**
    - **Single Log Out from several different HTML5 Apps!**

Challenge:
Applications being prone to developer mistakes

Offloading the developer

Development Perspective

Offloading the developer

Development Perspective

- **Security concerns require high expertise**
  - **XSS, CSRF, SQL Injection…**
  - **Cryptography, Encryption, Hashing algorithms**
  - **Evolving best practices**

Offloading the developer

Development Perspective

- Security concerns require high expertise
  - XSS, CSRF, SQL Injection…
  - Cryptography, Encryption, Hashing algorithms
  - Evolving best practices
- **Every application shares same typical requirements**
  - **Login / Registration screen**
  - **User / Role management UIs**
  - **Password policies**
  - **Logging / Audit**

Offloading the developer

Development Perspective

- Security concerns require high expertise
  - XSS, CSRF, SQL Injection…
  - Cryptography, Encryption, Hashing algorithms
  - Evolving best practices
- Every application shares same typical requirements
  - Login / Registration screen
  - User / Role management UIs
  - Password policies
  - Logging / Audit
- **High risk of introducing vulnerabilities if every time implementing from scratch**

Offloading the developer

Development Perspective

- Security concerns require high expertise
  - XSS, CSRF, SQL Injection…
  - Cryptography, Encryption, Hashing algorithms
  - Evolving best practices
- Every application shares same typical requirements
  - Login / Registration screen
  - User / Role management UIs
  - Password policies
  - Logging / Audit
- High risk of introducing vulnerabilities if every time implementing from scratch
- **Keeping up with new security threats**

Solution

RH-SSO provides

Development Perspective

RH-SSO provides

Development Perspective

- **Easy to apply integration libraries and agents / adapters**
    - **Securing different applications and services within very few trivial steps**

RH-SSO provides

Development Perspective

- Easy to apply integration libraries and agents / adapters
  - Securing different applications and services within very few trivial steps
- **Set of customizable and themable GUIs for**
  - **User, Role and Authorization Policies management**
  - **Authentication and Registration for end users**
  - **User self service**

RH-SSO provides

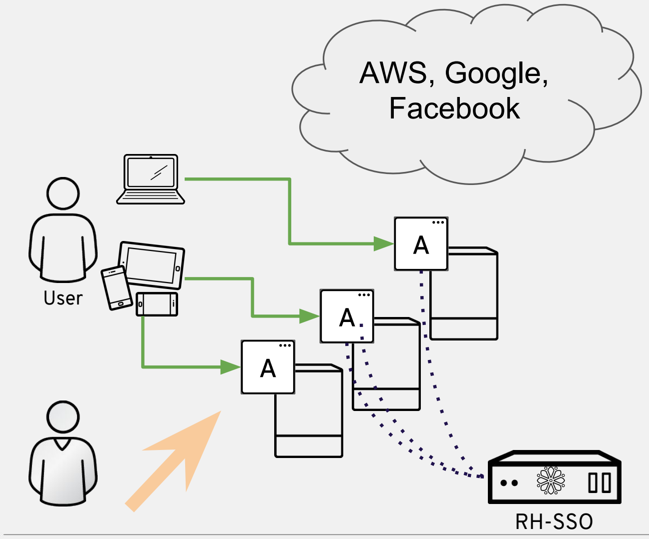
Development Perspective

- Easy to apply integration libraries and agents / adapters
  - Securing different applications and services within very few trivial steps
- Set of customizable and themable GUIs for
  - User, Role and Authorization Policies management
  - Authentication and Registration for end users
  - User self service
- **Out of the box**
  - **Password policies & Two Factor Authentication**
  - **Session Management & Logging**
  - **Different Authentication flows & methods**
  - **Both RBAC and ABAC with flexible policies**

Challenge:
Integration with existing infrastructure

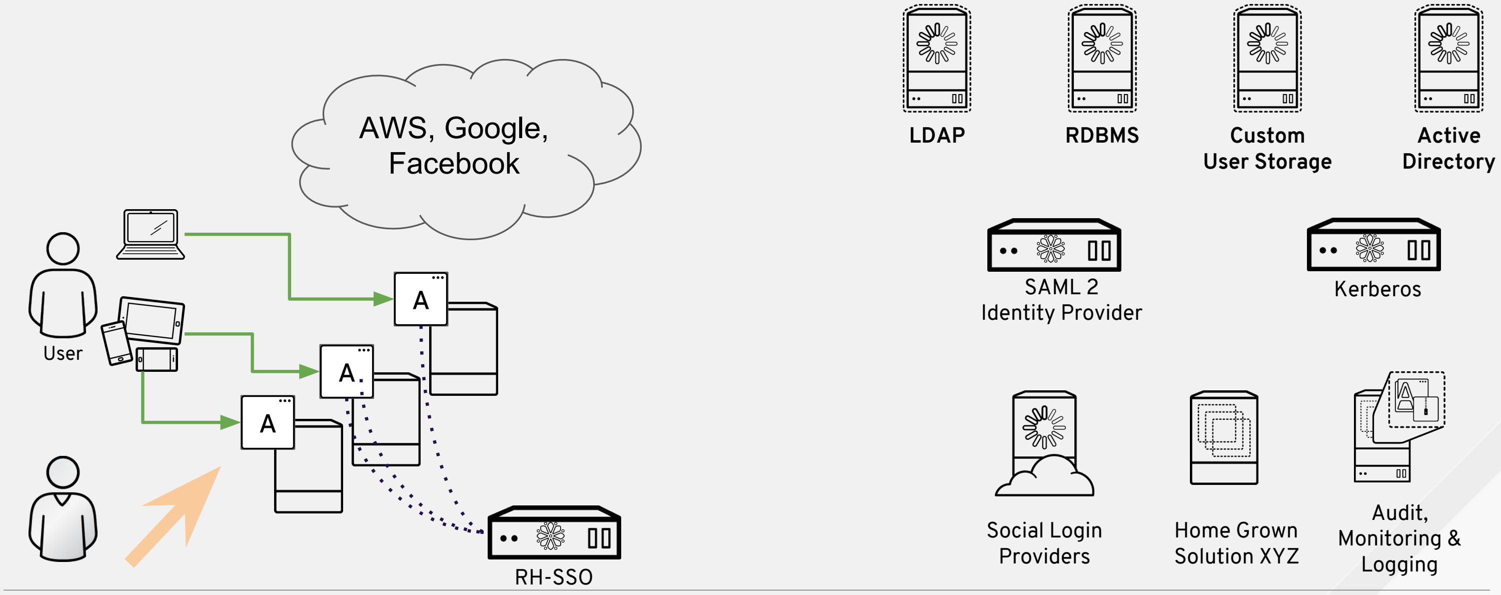
Integration with existing infrastructure

Development Perspective



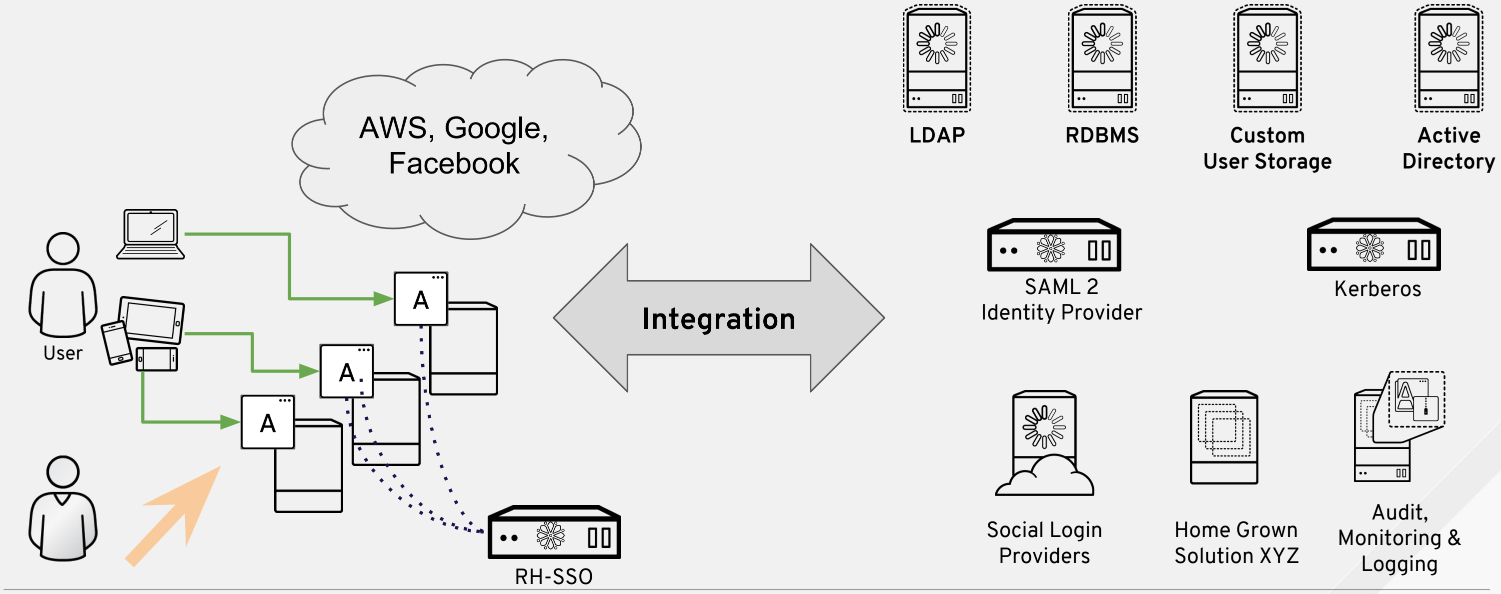
Integration with existing infrastructure

Development Perspective



Integration with existing infrastructure

Development Perspective



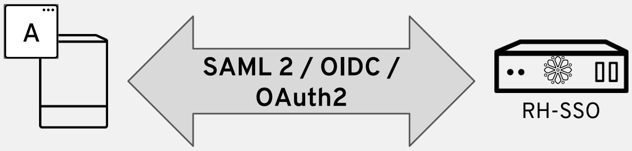
Solution

RH-SSO

Development Perspective

RH-SSO

Development Perspective



A

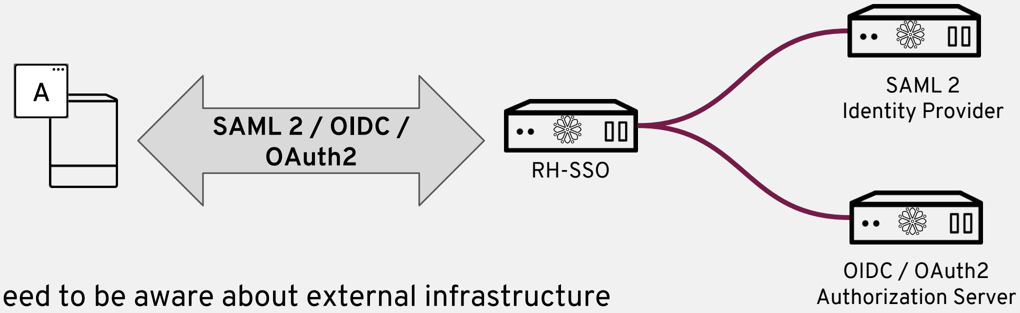
SAML 2 / OIDC / OAuth2

RH-SSO

- Application doesn’t need to be aware about external infrastructure
    - Only relying on standards like OpenID Connect / OAuth2 or SAML2

RH-SSO

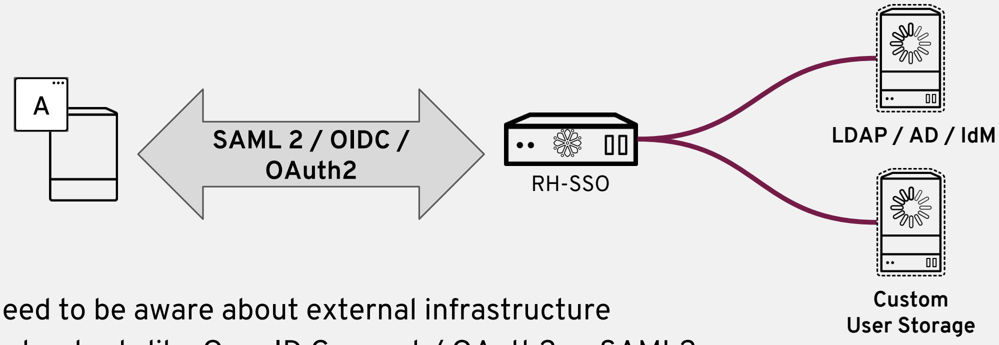
Development Perspective



- Application doesn’t need to be aware about external infrastructure
  - Only relying on standards like OpenID Connect / OAuth2 or SAML2
- **Can act as a proxy separating application while leveraging authentication from**
  - **External SAML 2 Identity Provider**
  - **External OpenID Connect / OAuth2 Authorization Server**

RH-SSO

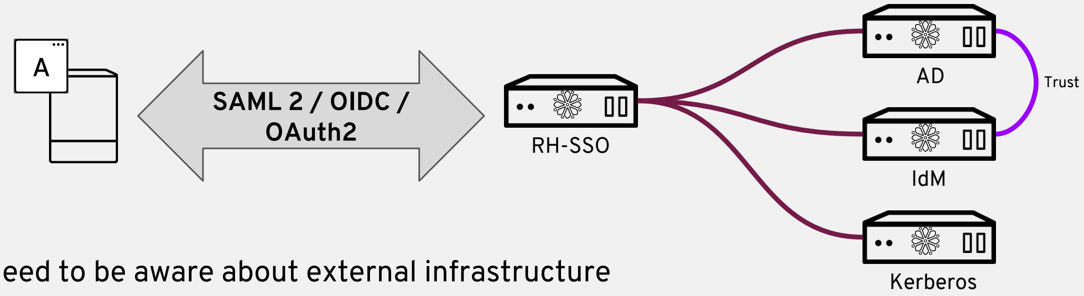
Development Perspective



- Application doesn’t need to be aware about external infrastructure
  - Only relying on standards like OpenID Connect / OAuth2 or SAML2
- Can act as a proxy separating application while leveraging authentication from
  - External SAML 2 Identity Provider
  - External OpenID Connect / OAuth2 Authorization Server
- **Integrates with external user storage providers**
  - **LDAP / Active Directory / IdM**
  - **Custom implementations**

RH-SSO

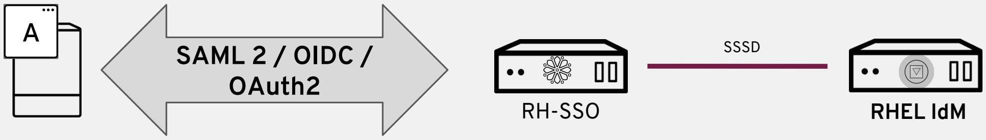
Development Perspective



- Application doesn't need to be aware about external infrastructure
  - Only relying on standards like OpenID Connect / OAuth2 or SAML2
- Can act as a proxy separating application while leveraging authentication from
  - External SAML 2 Identity Provider
  - External OpenID Connect / OAuth2 Authorization Server
- Integrates with external user storage providers
  - LDAP / Active Directory
  - Custom implementations
- **Kerberos authentication propagation**
  - **GSSAPI / SPNEGO**
  - **SSO from Operating System to Web Application**

RH-SSO

Development Perspective



A

SAML 2 / OIDC / OAuth2

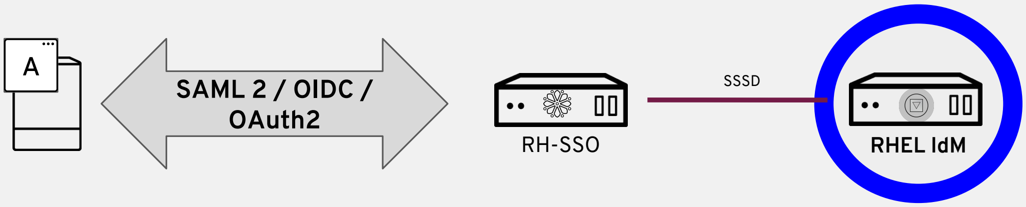
RH-SSO

SSSD

RHEL IdM

RH-SSO

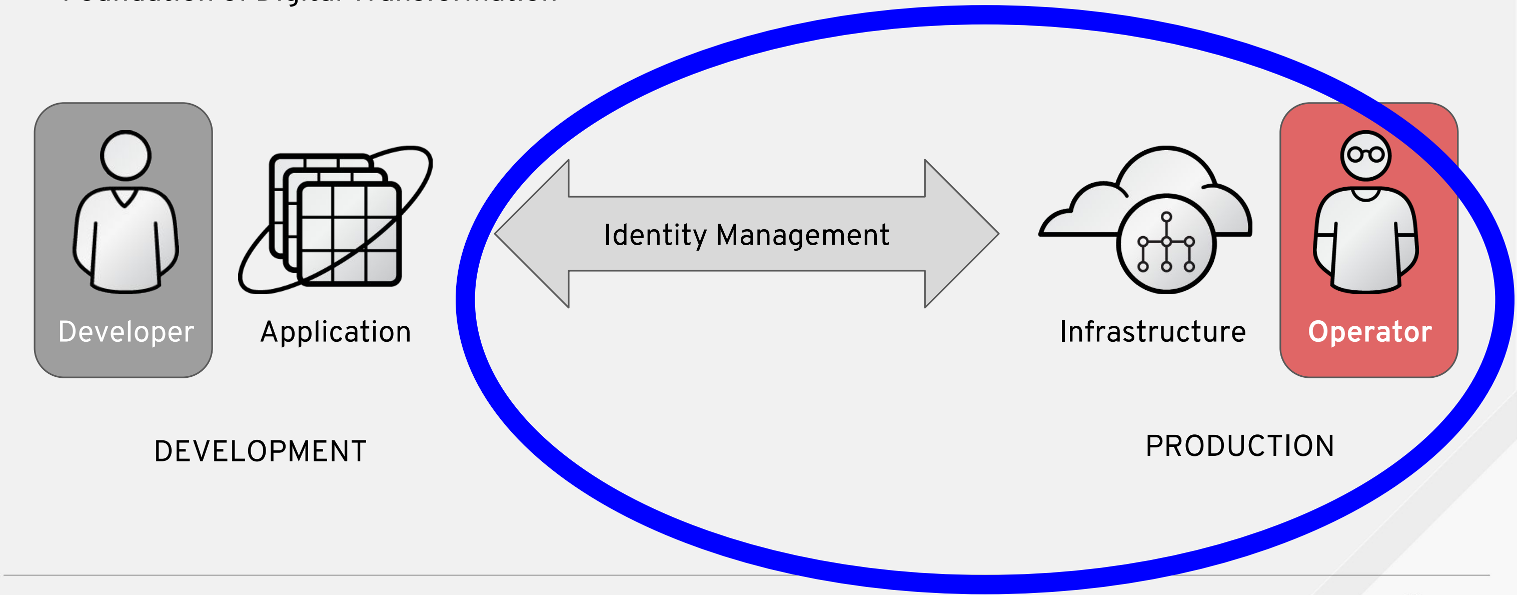
Development Perspective



Infrastructure Perspective

Identity Management Fabric

Foundation of Digital Transformation



Developer

Application

Identity Management

Infrastructure

Operator

DEVELOPMENT

PRODUCTION

Infrastructure Layer

Introduction

- **Application is the king - it provides business value**

Infrastructure Layer

Introduction

- Application is the king - it provides business value
- **Infrastructure is needed to allow applications to run**

Infrastructure Layer

Introduction

- Application is the king - it provides business value
- Infrastructure is needed to allow applications to run
- **Applications can run as rpms or containers on top of a host**

Infrastructure Layer

Introduction

- Application is the king - it provides business value
- Infrastructure is needed to allow applications to run
- Applications can run as rpms or containers on top of a host
- **Host can be:**

Infrastructure Layer

Introduction

- Application is the king - it provides business value
- Infrastructure is needed to allow applications to run
- Applications can run as rpms or containers on top of a host
- Host can be:
  - **Traditional full OS system**

Infrastructure Layer

Introduction

- Application is the king - it provides business value
- Infrastructure is needed to allow applications to run
- Applications can run as rpms or containers on top of a host
- Host can be:
  - Traditional full OS system
  - **Bare bones node like Atomic**

Infrastructure Layer

Introduction

- Application is the king - it provides business value
- Infrastructure is needed to allow applications to run
- Applications can run as rpms or containers on top of a host
- Host can be:
  - Traditional full OS system
  - Bare bones node like Atomic
  - **VM in a virtualized environment like RHV or cloud:**

Infrastructure Layer

Introduction

- Application is the king - it provides business value
- Infrastructure is needed to allow applications to run
- Applications can run as rpms or containers on top of a host
- Host can be:
  - Traditional full OS system
  - Bare bones node like Atomic
  - VM in a virtualized environment like RHV or cloud:
    - **Private - OpenStack**

Infrastructure Layer

Introduction

- Application is the king - it provides business value
- Infrastructure is needed to allow applications to run
- Applications can run as rpms or containers on top of a host
- Host can be:
  - Traditional full OS system
  - Bare bones node like Atomic
  - VM in a virtualized environment like RHV or cloud:
    - Private - OpenStack
    - **Public - AWS, Google Cloud, Azure, ...**

Challenge:
Provide infrastructure that can be trusted

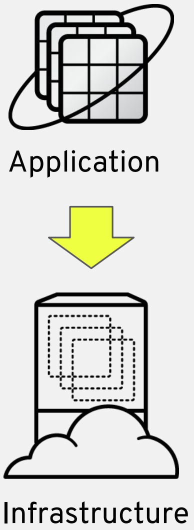
Why infrastructure needs to be trusted?

Analogy

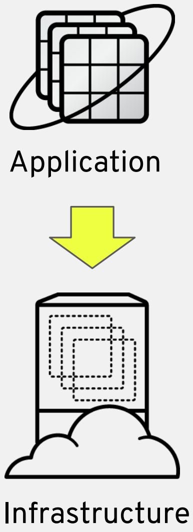
Analogy

Application

Analogy



Analogy

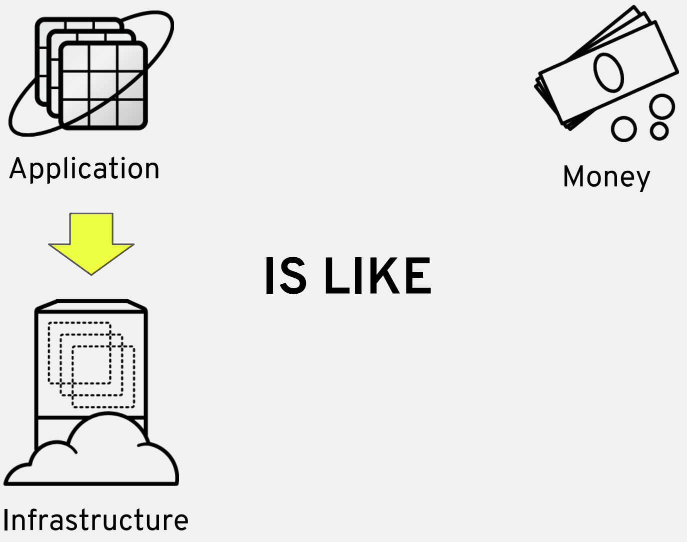


Application

Infrastructure

IS LIKE

Analogy



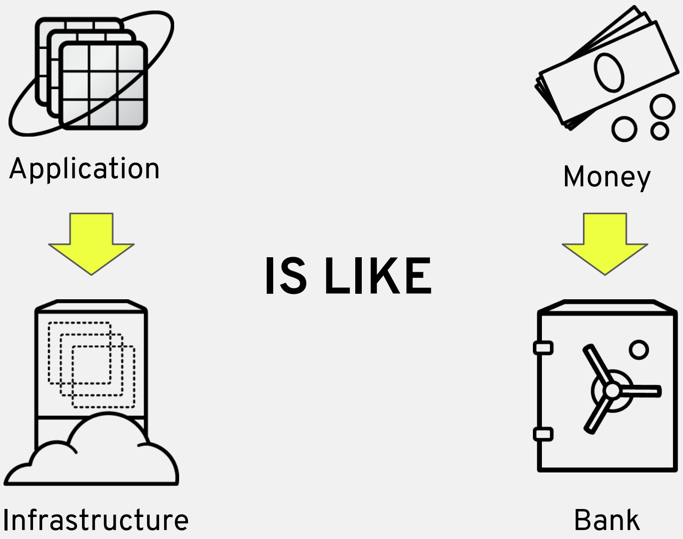
Application

Infrastructure

IS LIKE

Money

Analogy



How to make infrastructure trustworthy?

Concepts

Overview

Concepts

Overview

- **Trust is based on identity and authentication**

Concepts

Overview

- Trust is based on identity and authentication
- **To be trusted elements of the infrastructure need to have identity and perform authentication**
  - We are talking about systems and services here - not users!

Concepts

Overview

- Trust is based on identity and authentication
- To be trusted elements of the infrastructure need to have identity and perform authentication
    - We are talking about systems and services here - not users!
- **To be able to authenticate a component needs to have a credential**
    - Key, secret, password

Concepts

Overview

- Trust is based on identity and authentication
- To be trusted elements of the infrastructure need to have identity and perform authentication
  - We are talking about systems and services here - not users!
- To be able to authenticate a component needs to have a credential
  - Key, secret, password
- **A credential needs to be created in some way**
  - You can’t bake it into an image or container - this can be easily leaked

Concepts

Overview

- Trust is based on identity and authentication
- To be trusted elements of the infrastructure need to have identity and perform authentication
  - We are talking about systems and services here - not users!
- To be able to authenticate a component needs to have a credential
  - Key, secret, password
- A credential needs to be created in some way
  - You can’t bake it into an image or container - this can be easily leaked
- **Credential needs to be delivered or synthesized**

Concepts

Overview

- Trust is based on identity and authentication
- To be trusted elements of the infrastructure need to have identity and perform authentication
  - We are talking about systems and services here - not users!
- To be able to authenticate a component needs to have a credential
  - Key, secret, password
- A credential needs to be created in some way
  - You can’t bake it into an image or container - this can be easily leaked
- Credential needs to be delivered or synthesized
- **You can’t rely on manual operations**

Concepts

Overview

- Trust is based on identity and authentication
- To be trusted elements of the infrastructure need to have identity and perform authentication
  - ○ We are talking about systems and services here - not users!
- To be able to authenticate a component needs to have a credential
  - ○ Key, secret, password
- A credential needs to be created in some way
  - ○ You can’t bake it into an image or container - this can be easily leaked
- Credential needs to be delivered or synthesized
- You can’t rely on manual operations
- **The solution needs to have a chain of trust**

Solution

Identity Management - IdM

Introduction

- **IdM is the domain controller for Linux/UNIX systems**

Identity Management - IdM

Introduction

- IdM is the domain controller for Linux/UNIX systems
- **Allows systems joined to the domain to have identities and authenticate**

Identity Management - IdM

Introduction

- IdM is the domain controller for Linux/UNIX systems
- Allows systems joined to the domain to have identities and authenticate
- **Once system has an identity and a credential it can connect to different services and additional layers of security on top**

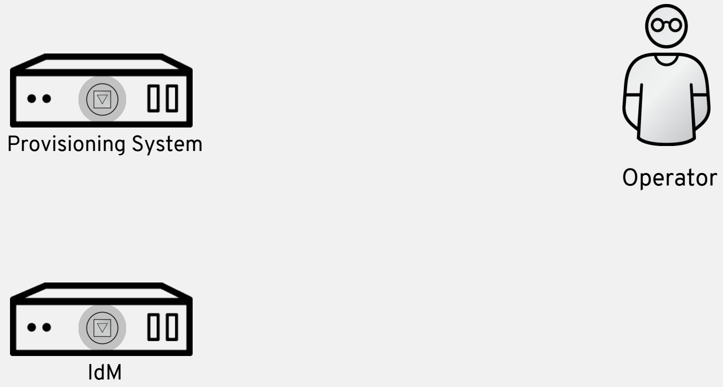
Identity Management - IdM

Introduction

- IdM is the domain controller for Linux/UNIX systems
- Allows systems joined to the domain to have identities and authenticate
- Once system has an identity and a credential it can connect to different services and additional layers of security on top
- **This allows building chain of trust layer by layer**

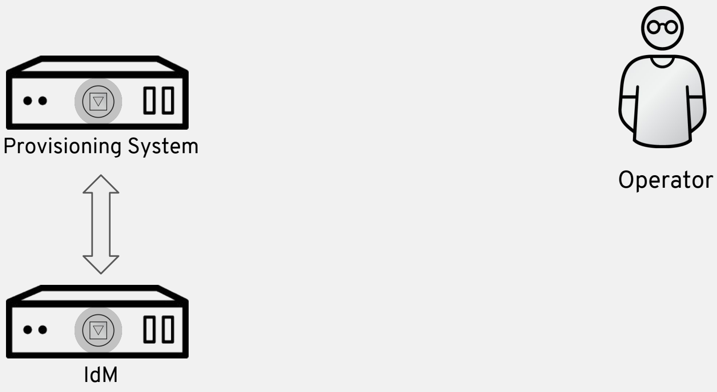
Automatic Domain Enrollment

Overview



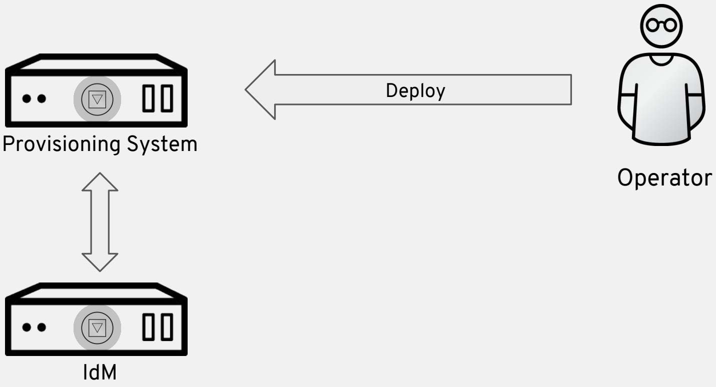
Automatic Domain Enrollment

Overview



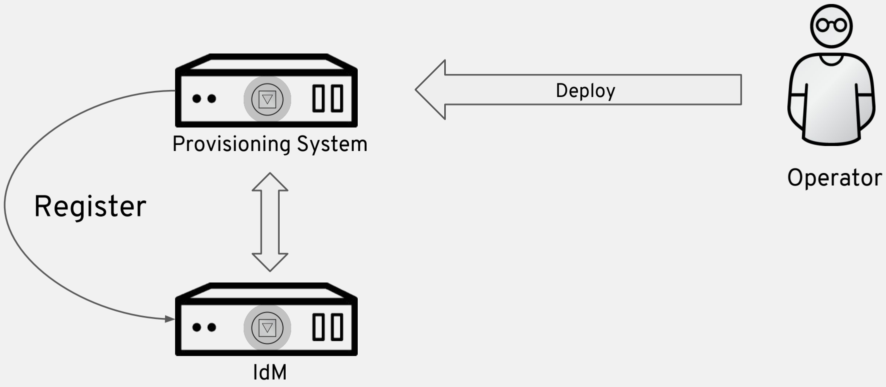
Automatic Domain Enrollment

Overview



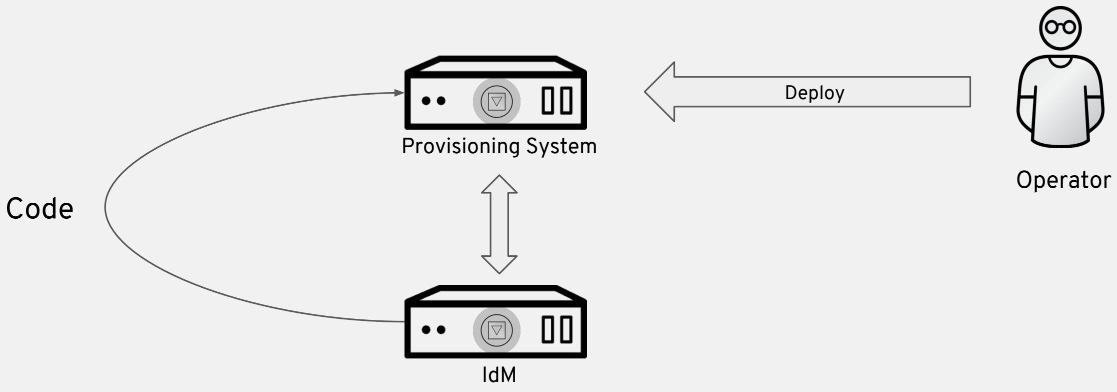
Automatic Domain Enrollment

Overview



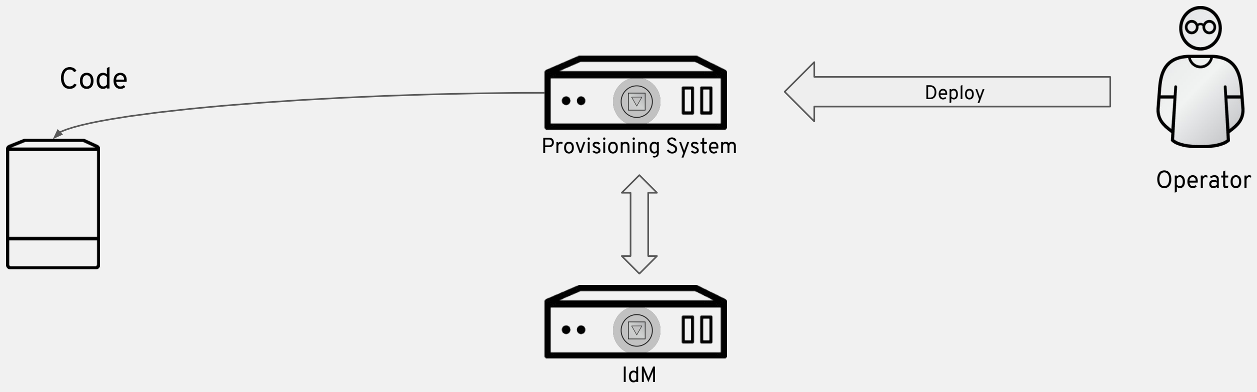
Automatic Domain Enrollment

Overview



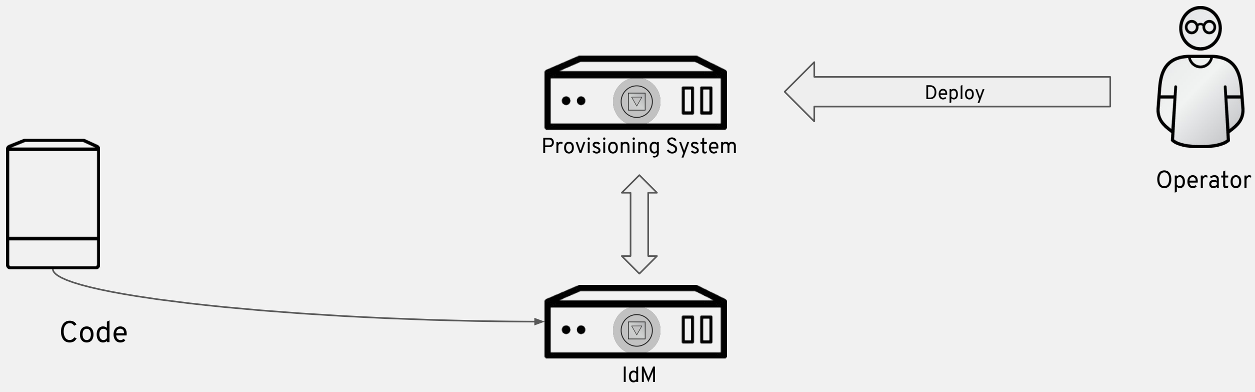
Automatic Domain Enrollment

Overview



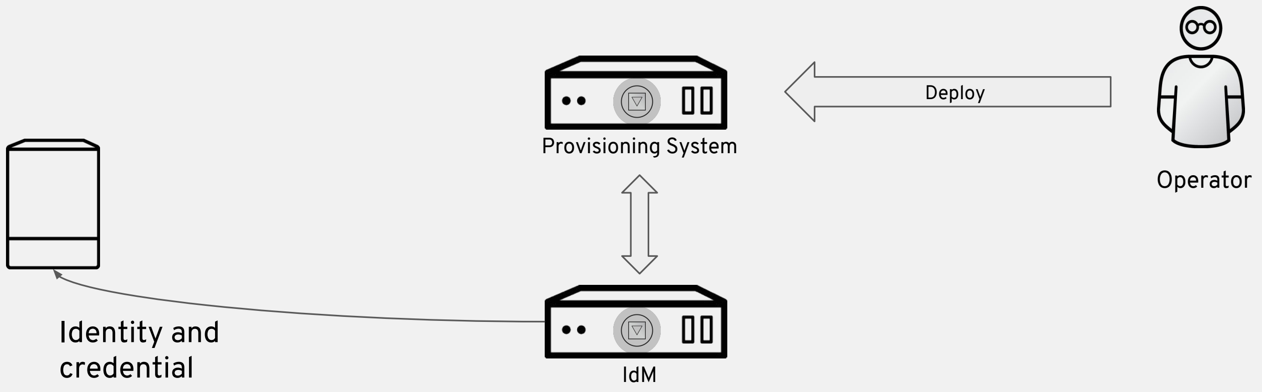
Automatic Domain Enrollment

Overview



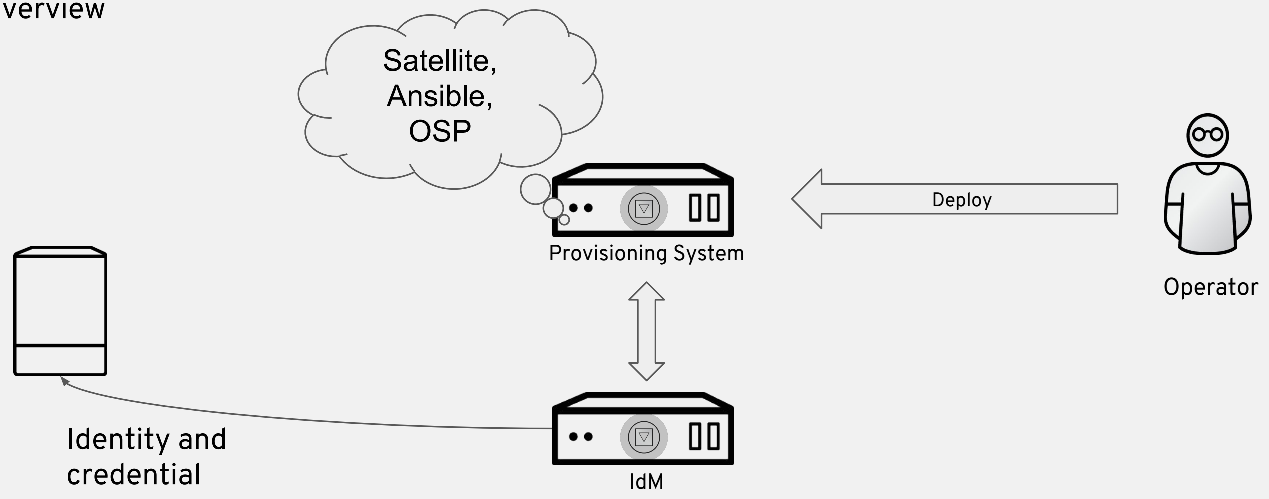
Automatic Domain Enrollment

Overview



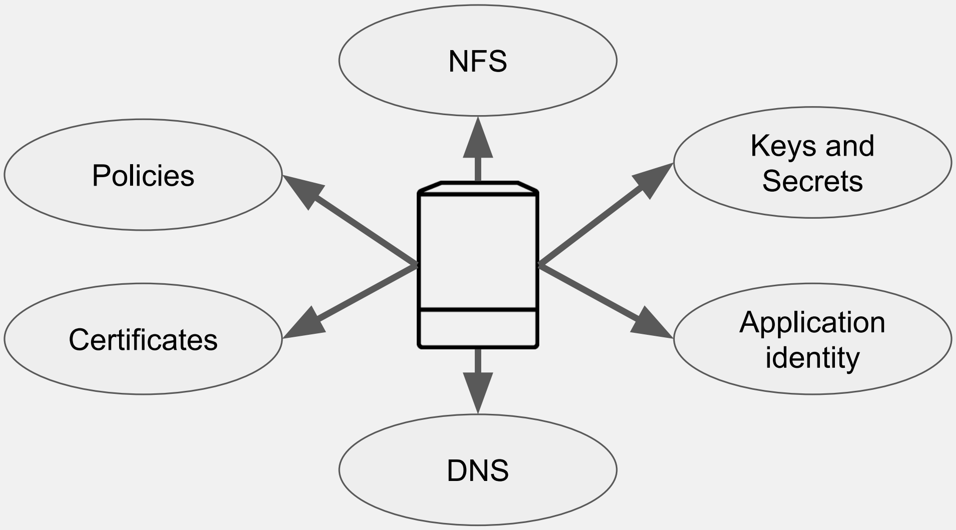
Automatic Domain Enrollment

Overview



System Interaction Capabilities

Overview



Identity Management - IdM

More

- **IdM provides interoperability with Active Directory**

Identity Management - IdM

More

- IdM provides interoperability with Active Directory
  - **IdM manages Linux domain**
    - System and service identities
    - Policies - host based access control, sudo, SELinux user mapping
    - Provides certificates and keystore
    - POSIX attributes for Active Directory users

Identity Management - IdM

More

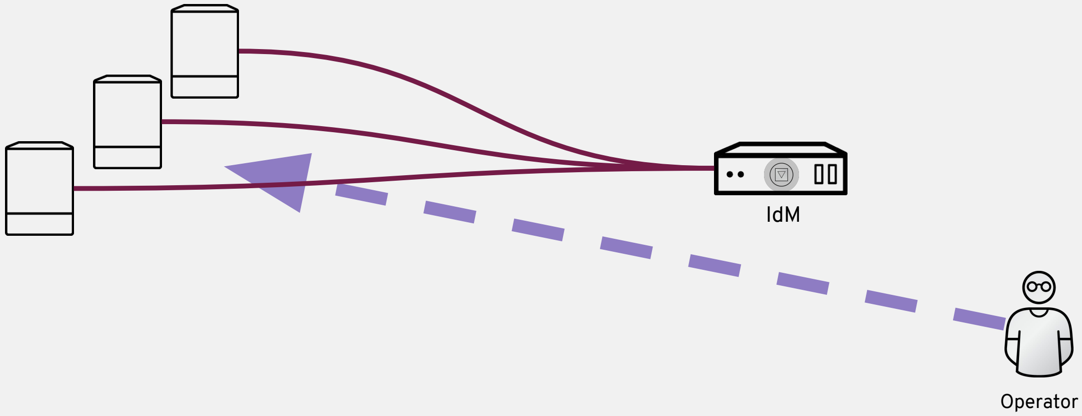
- IdM provides interoperability with Active Directory
  - IdM manages Linux domain
    - System and service identities
    - Policies - host based access control, sudo, SELinux user mapping
    - Provides certificates and keystore
    - POSIX attributes for Active Directory users
  - **Users are in Active Directory**
    - Attributes, groups
    - Credentials and related policies
    - Audit trail

Identity Management Fabric

End-to-end solutions

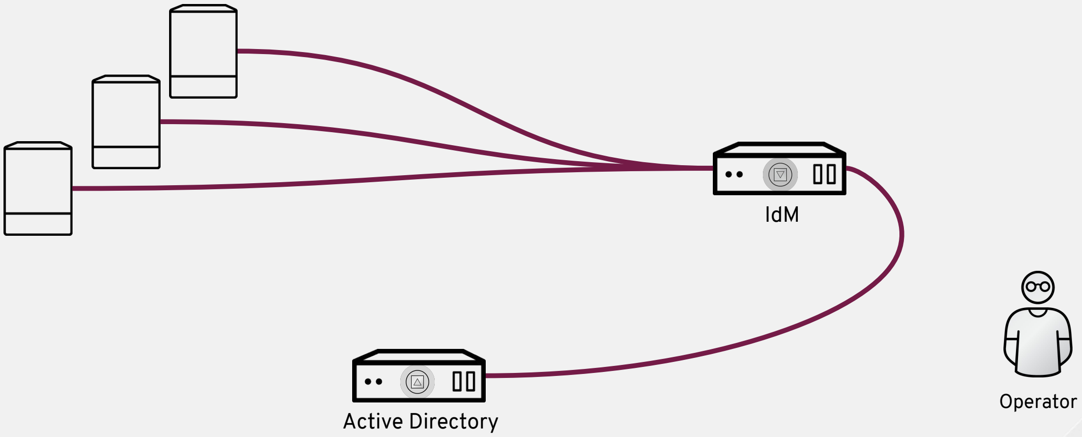
Identity Management Fabric

End-to-end solutions



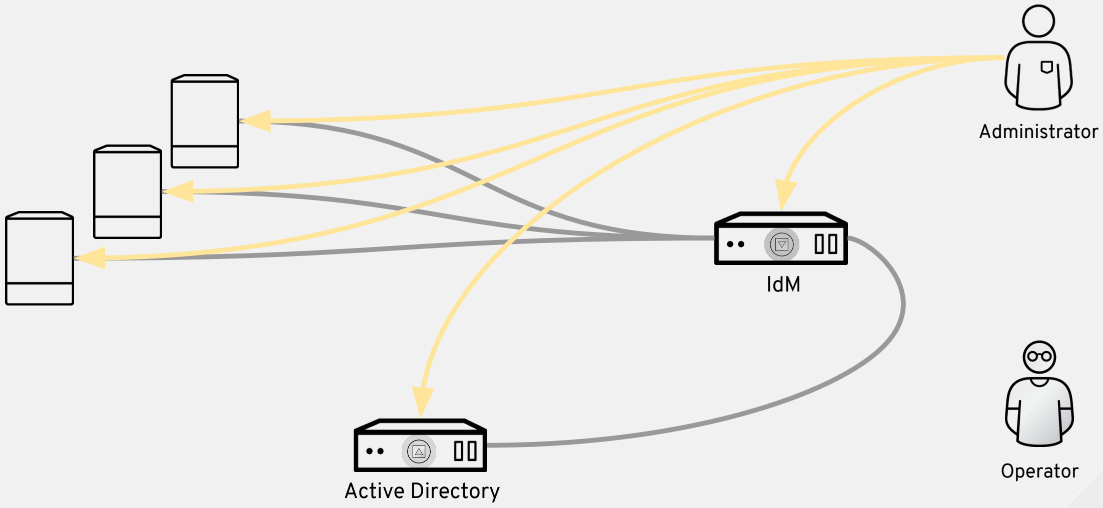
Identity Management Fabric

End-to-end solutions



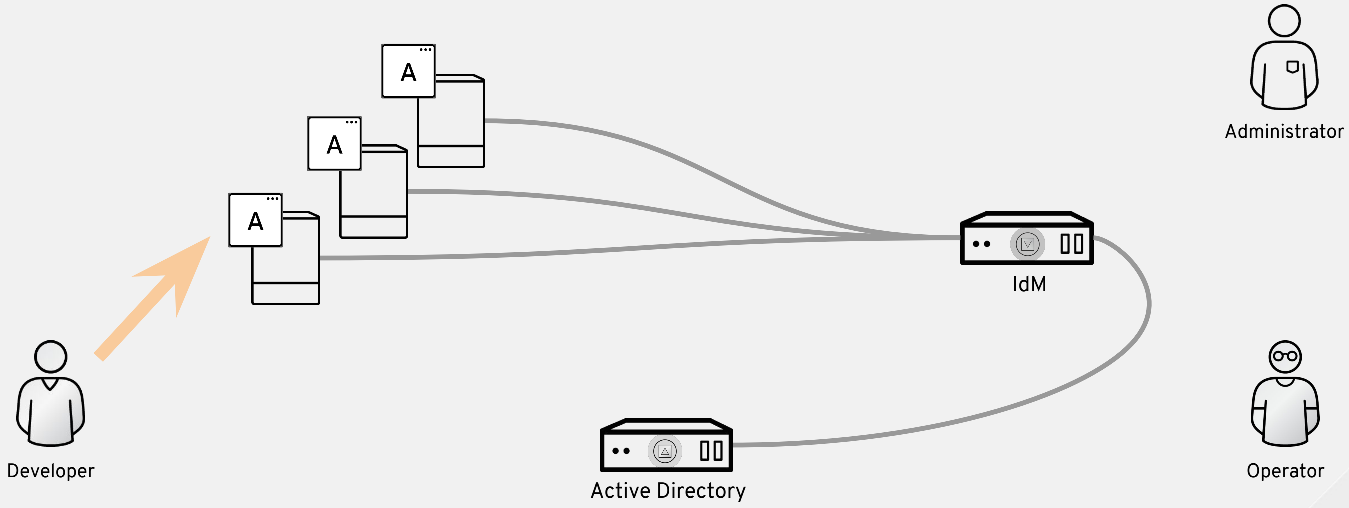
Identity Management Fabric

End-to-end solutions



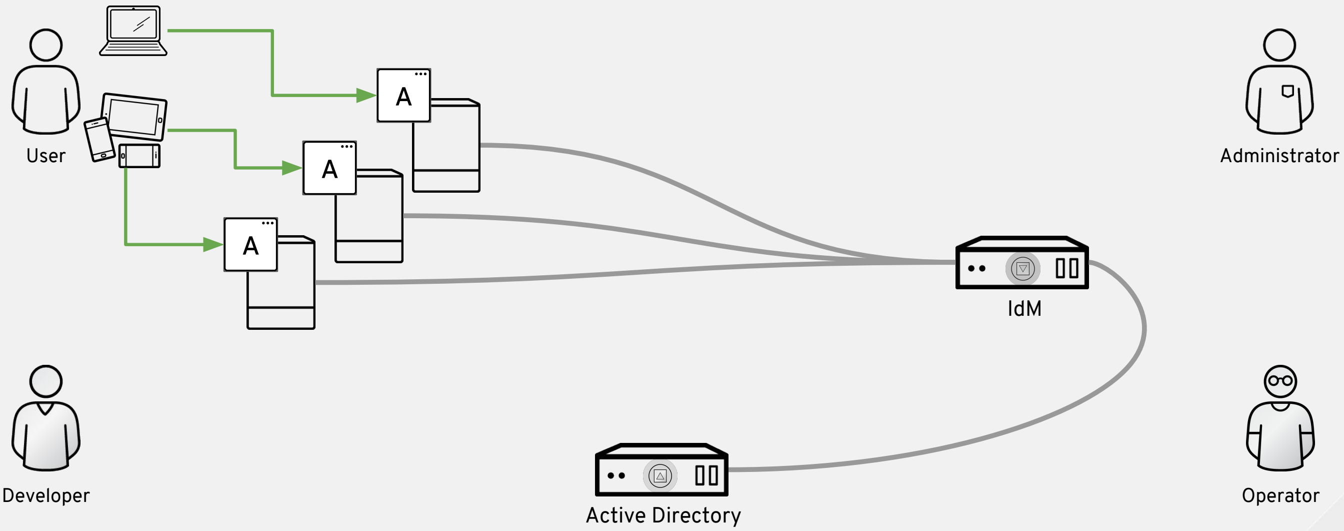
Identity Management Fabric

End-to-end solutions



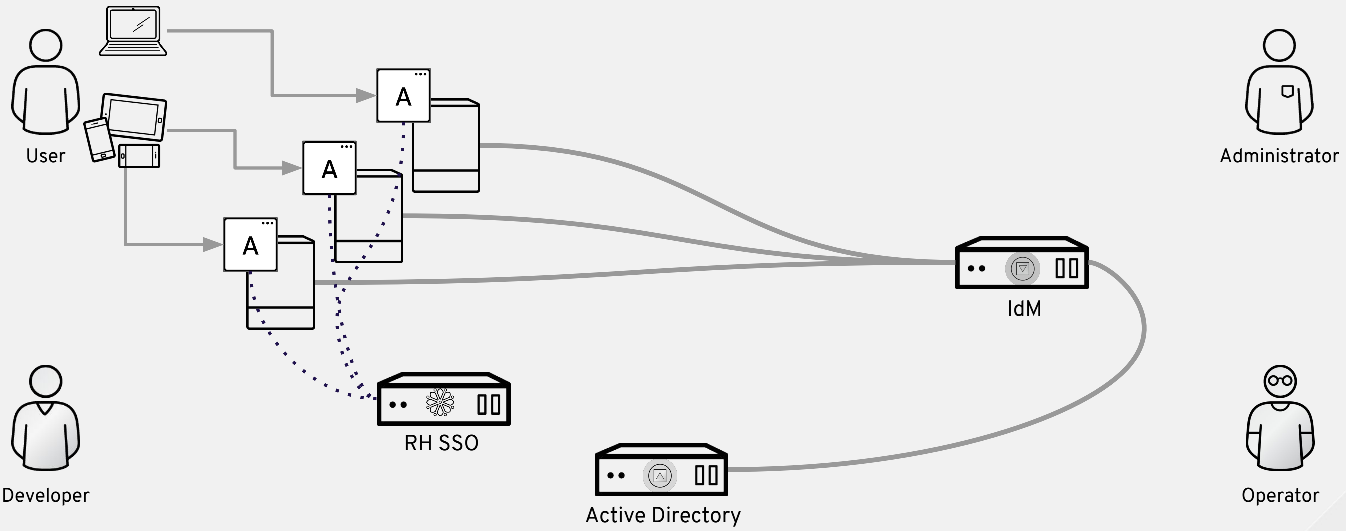
Identity Management Fabric

End-to-end solutions



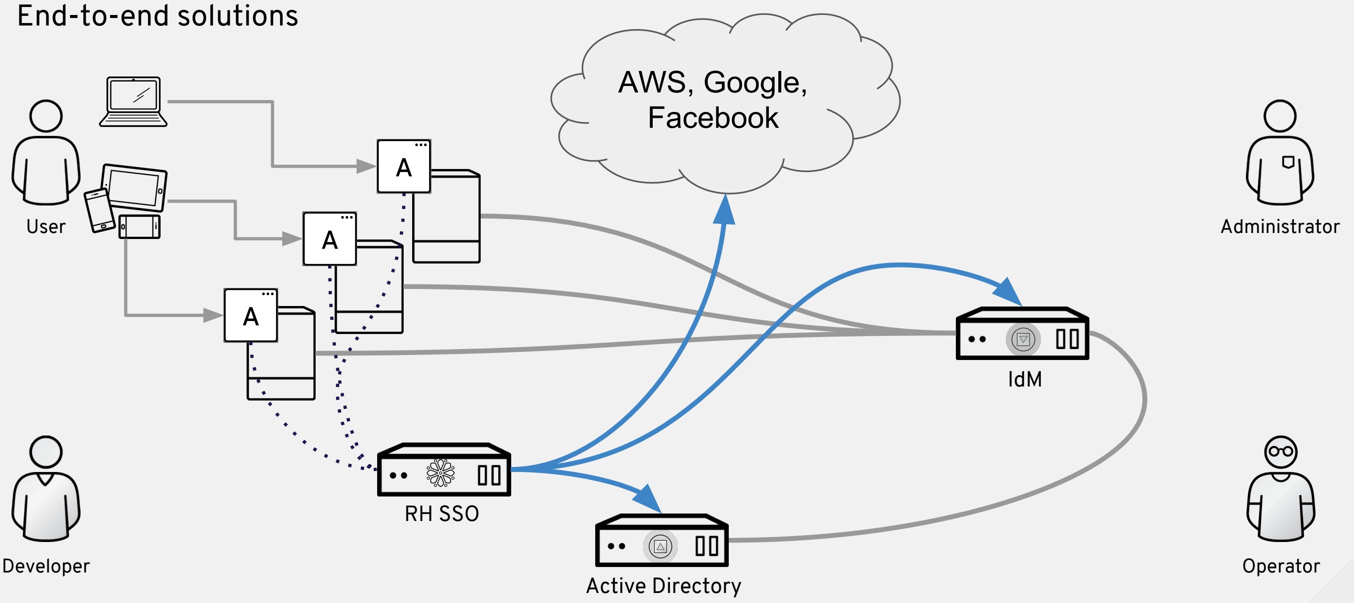
Identity Management Fabric

End-to-end solutions



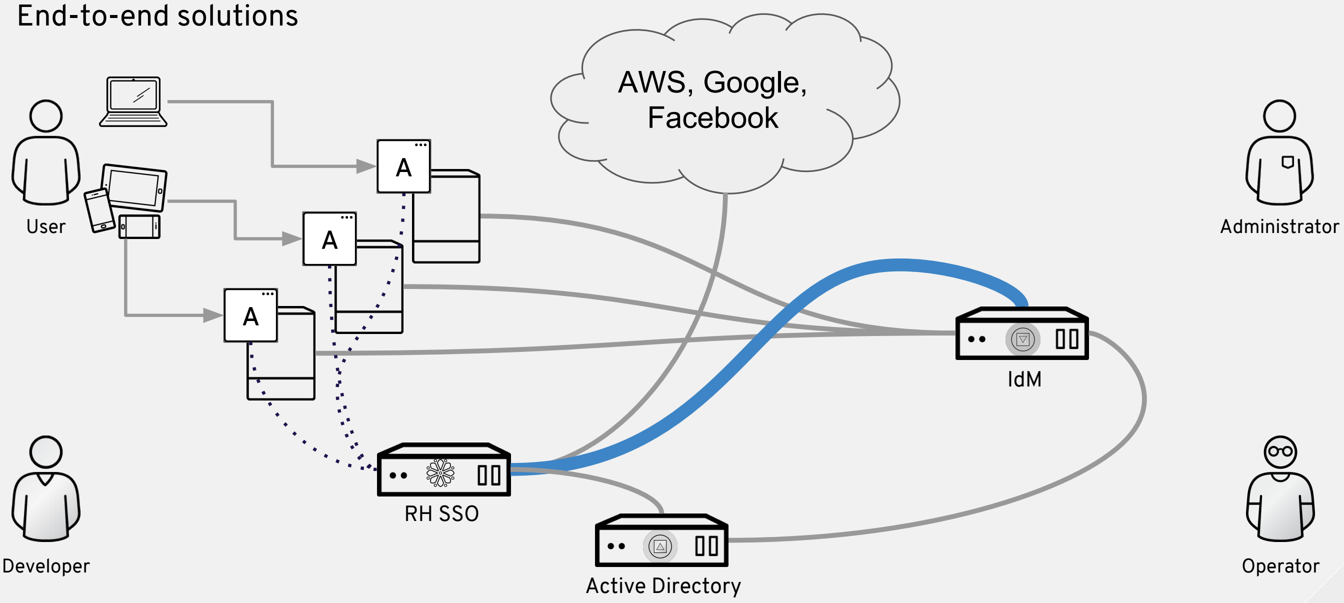
Identity Management Fabric

End-to-end solutions



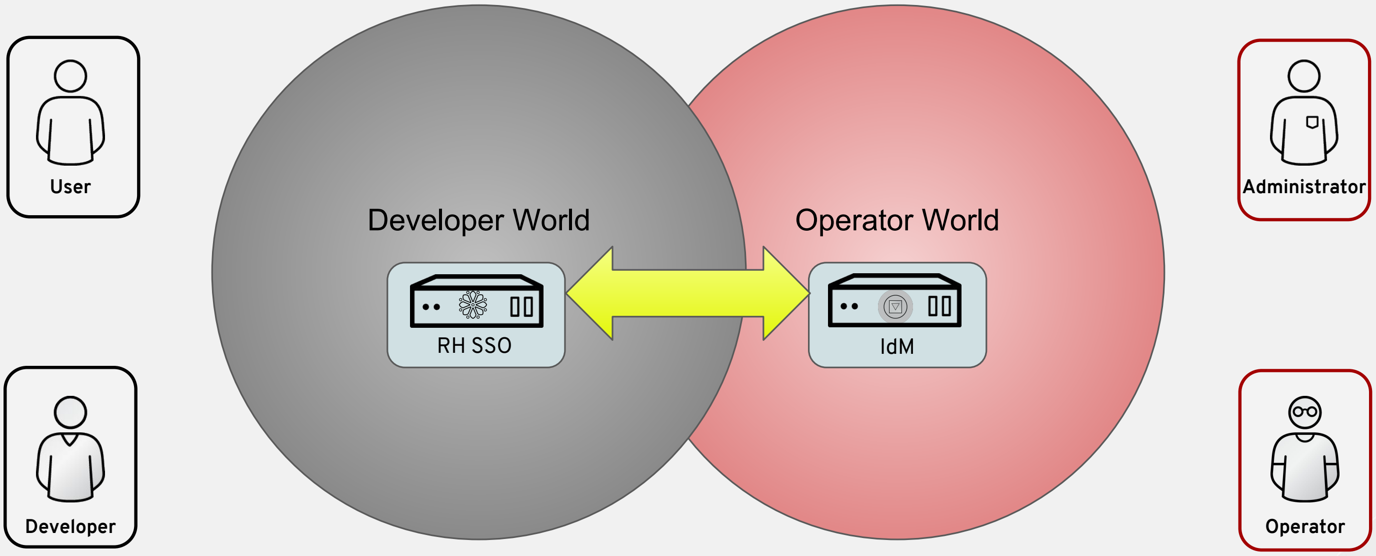
Identity Management Fabric

End-to-end solutions



Identity Management Fabric

Core Components



Additional Summit Resources

- Drop by the Security Pod in the Partner Pavilion for a demo
- Come talk with our experts at the Expert Bar
- Presentations today at 4:30
  - S104939 Identity Management and Compliance in OpenShift
  - S104897 - Easily secure your front- and back-end applications with KeyCloak

Questions?

RED HAT
SUMMIT

THANK YOU

plus.google.com/+RedHat

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHatNews

RED HAT SUMMIT

LEARN. NETWORK.
EXPERIENCE
OPEN SOURCE.

#redhat #rhsummit

redhat.