Open Source Identity Management in the Enterprise

Or: How I learned to Stop Worrying and Love SAML

Brian J. Atkisson, RHCA II
Principal Systems Engineer

LISA 2014: Open Source Identity Management in the Enterprise

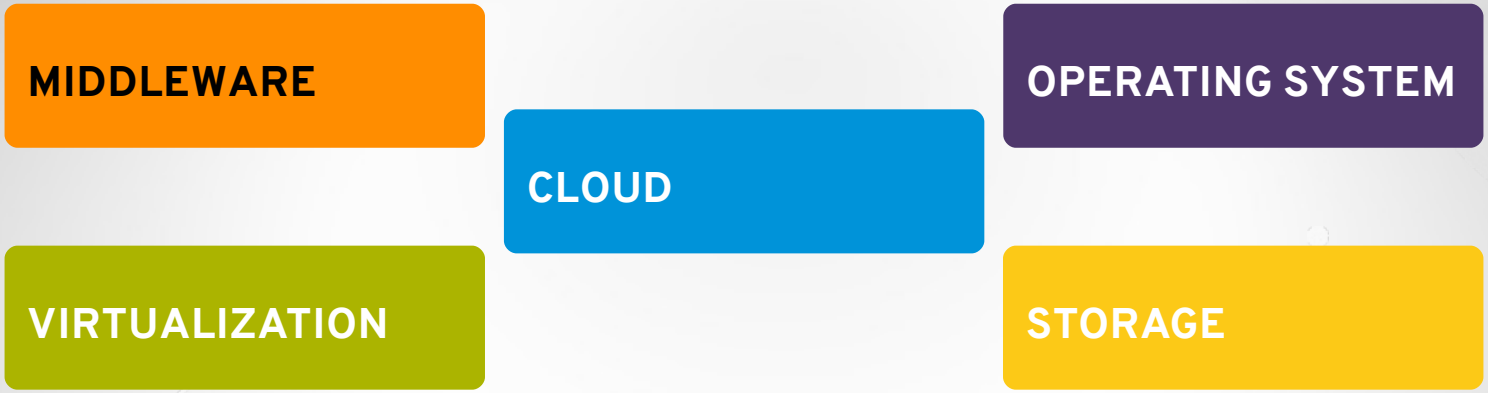
This talk will discuss how Red Hat IT utilizes and integrates open source solutions to offer a seamless experience for internal users. Specifically, we will cover how Red Hat incorporates SAML, Kerberos, LDAP, Two-Factor Authentication, PKI certificates, and how end-user systems are able to function in this multi-platform, fluid BYOD environment. Recent experiences will be shared on how Red Hat is scaling this identity management platform to utilize true single sign-on in cloud environments. Finally, best practices and future plans will be discussed as part of a Q&A session

Agenda – Open Source Identity Management at Red Hat

- About Red Hat
- Overview
- Users and Devices
- LDAP
- Kerberos
- Two Factor Auth
- SAML
- PKI
- IdM/IPA

WHAT WE DO

We offer a range of mission-critical software and services covering:



THE BENEFITS

- ✓ Flexibility
- ✓ Faster technology innovation
- ✓ Better quality
- ✓ Better price/performance
- ✓ Long-term deployment
- ✓ Better security—assurance
- ✓ Shared development: Accelerated innovation
- ✓ Open collaboration: Products that meet customer needs

Red Hat IT

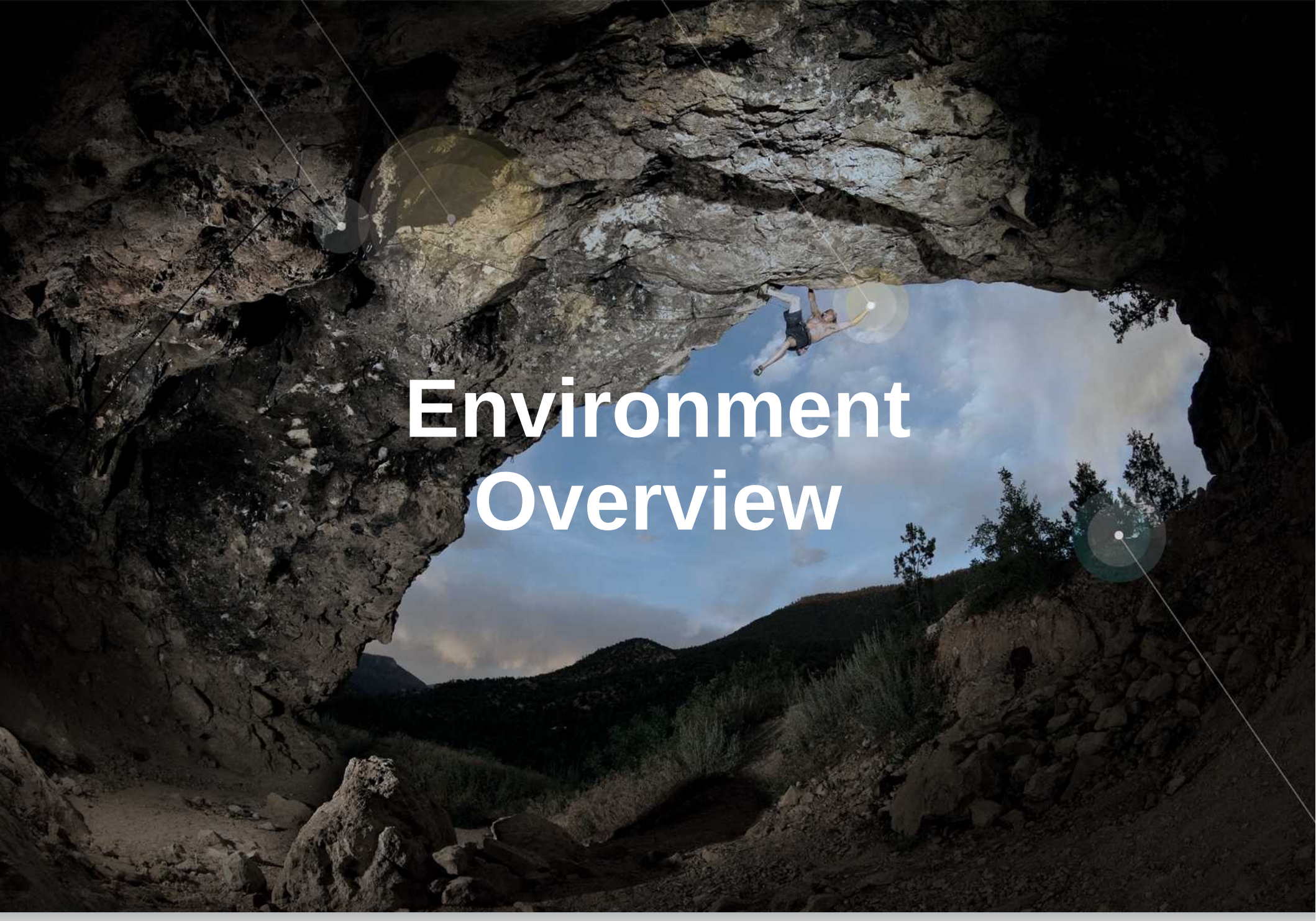
- IT has development and operational responsibilities for internal- and external-facing production and pre-production services.
  - {www,rhn,access}.redhat.com
  - Email/collaboration
  - Identity Management
  - Data management
  - Data Center services
  - Virtualization
  - Hosted Environments
  - SaaS Applications
  - User support

Identity and Access Management (IAM) Team

- Small development group focusing on identity management solutions, which are the content of this presentation.
  - Application Engineers
  - Systems Engineers
- Operational support is provided by another team of Systems Administrators

About Me

- 8 years at Red Hat
- Architecture and Design work in virtualization and identity management
- 15 years experience in systems administration and engineering
- 6th LISA attendance
- RHCA II, RHCE (2000), RHCDS, RHCVA, CCNA, ITIL, BS


Environment
Overview

Data Center Physical Infrastructure

- Red Hat Storage [Gluster] (NFS)
- NetApp Storage (NFS and block)
- Cisco UCS Blade Servers
  - Virtualized Environments
- IBM X-Series and
  Cisco UCS Rack-mount
  - Large DBs, etc.
- Cisco and Juniper Network Hardware
- Various appliances
  - (F5 load balancers, IPS, etc)

Data Center Software

- 99.99% RHEL Server
  - RHEL 4,5,6,7 in Production
- Fully Virtualized (mostly)
- RHEV and OpenStack
  - 200 hypervisors
  - 10 managers
- Virtualization Environment Details
  - https://access.redhat.com/node/701683

Something, Something, Something Cloud

- Internal OpenShift Enterprise deployment for PaaS
- AWS IaaS
- OpenStack Self-Service
- SaaS Applications
- Foreman backed by RHEV for self-service puppetized development VMs

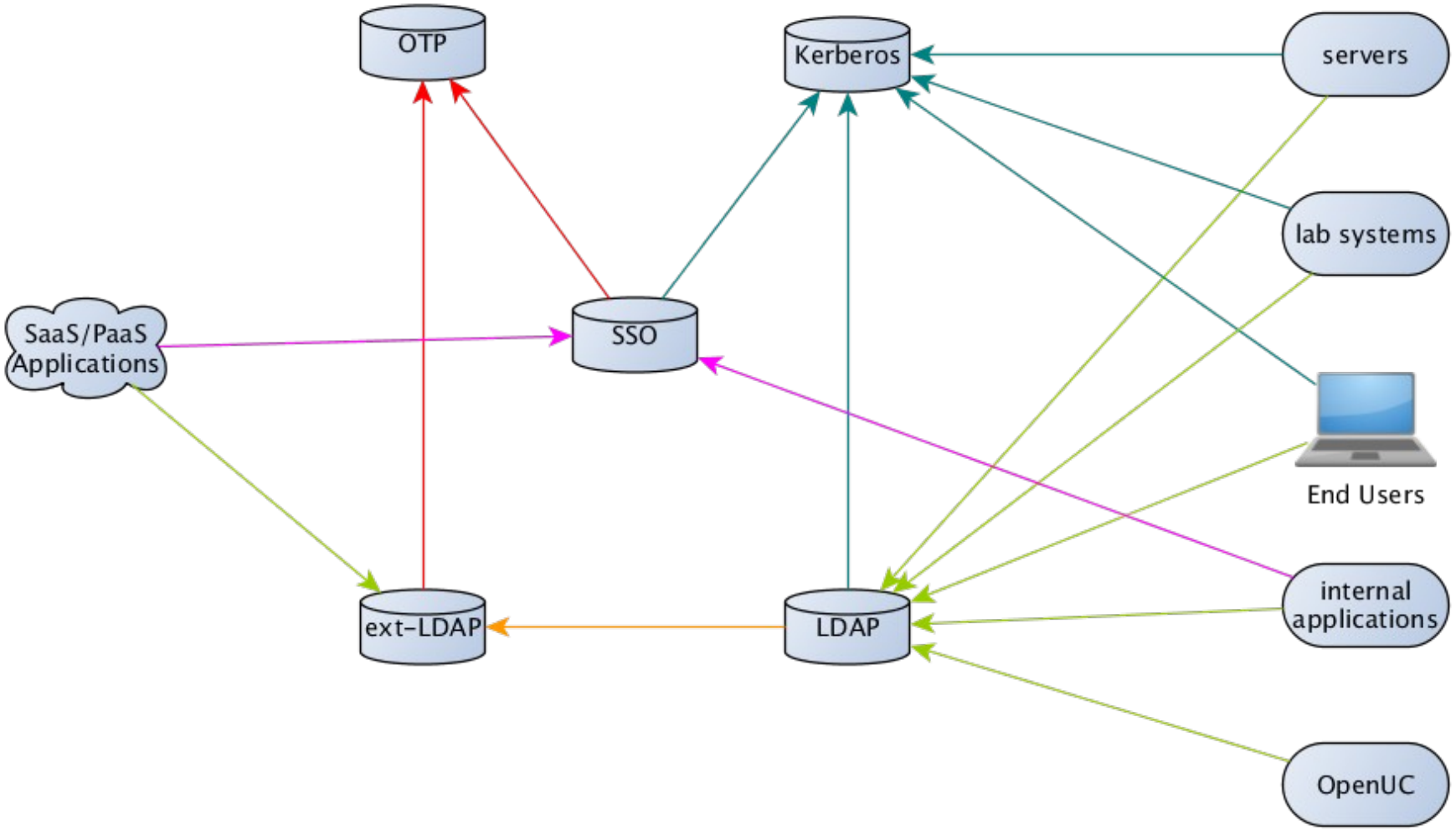
Configuration Management - Puppet

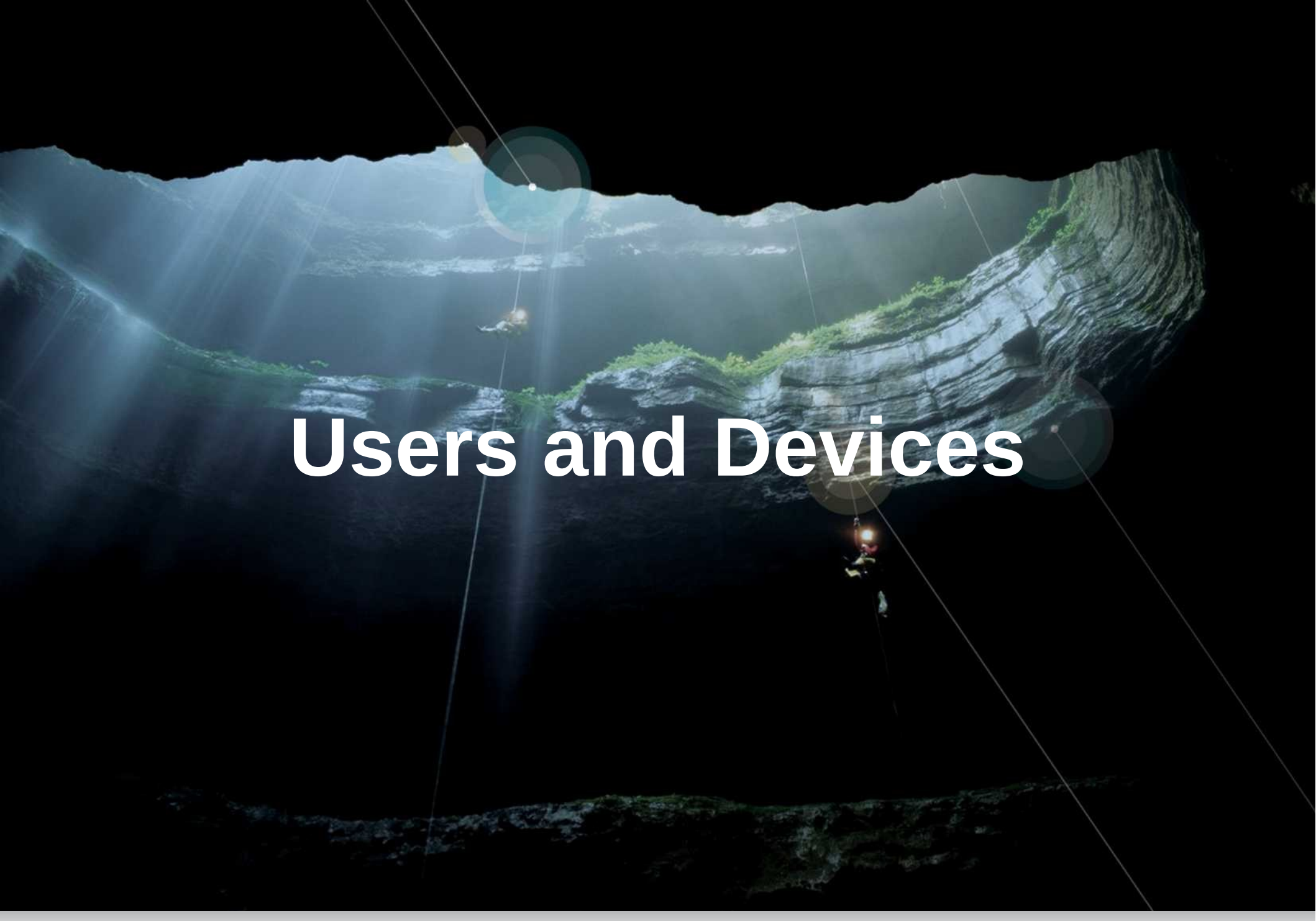
- Custom Puppet modules for each application, fully automated builds
  - 188 modules written internally
  - ~500,000 lines of manifests
- 43 puppet masters globally
- Open Source version
- Red Hat Satellite 6 and Foreman
  - ENC
  - Reporting

Configuration Management

- Puppet modules are Git repos
  - branches for dev*/qa/stage/production
  - New functionality added in feature branches and merged into dev -> qa -> stage -> prod
- Use Git post-commit script for distributing modules to puppet masters
- Custom code for mapping branches to environments
  - r10k does something similar
- Commit hooks
  - Syntax checking
  - Branch parenting

Identity Management Overview




Users and Devices

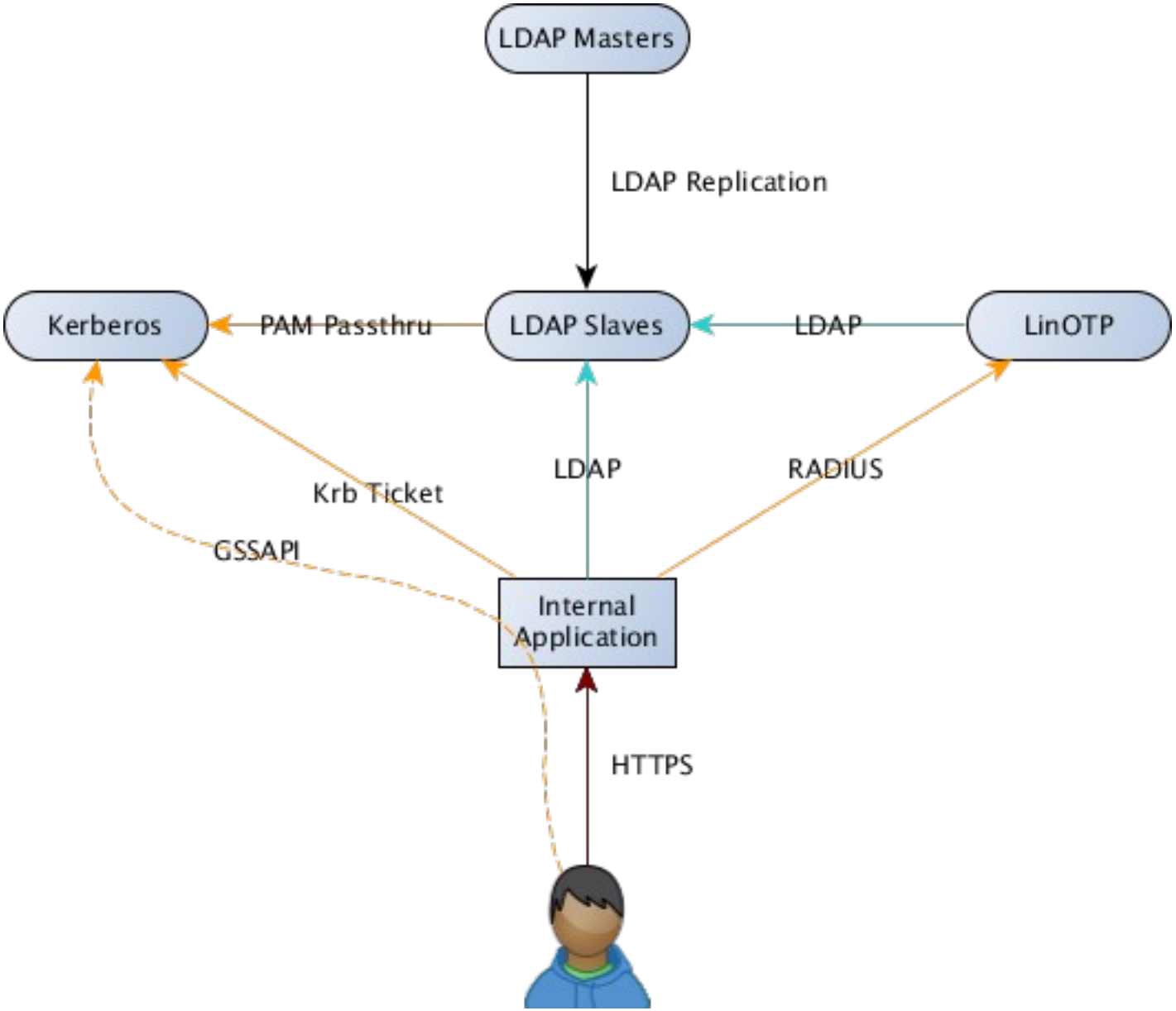
User Types

- Highly Technical Engineers
  - >50% of the company
- Sales and Marketing
- Administrative
- Legal
- Finance
- HR, Facilities, etc

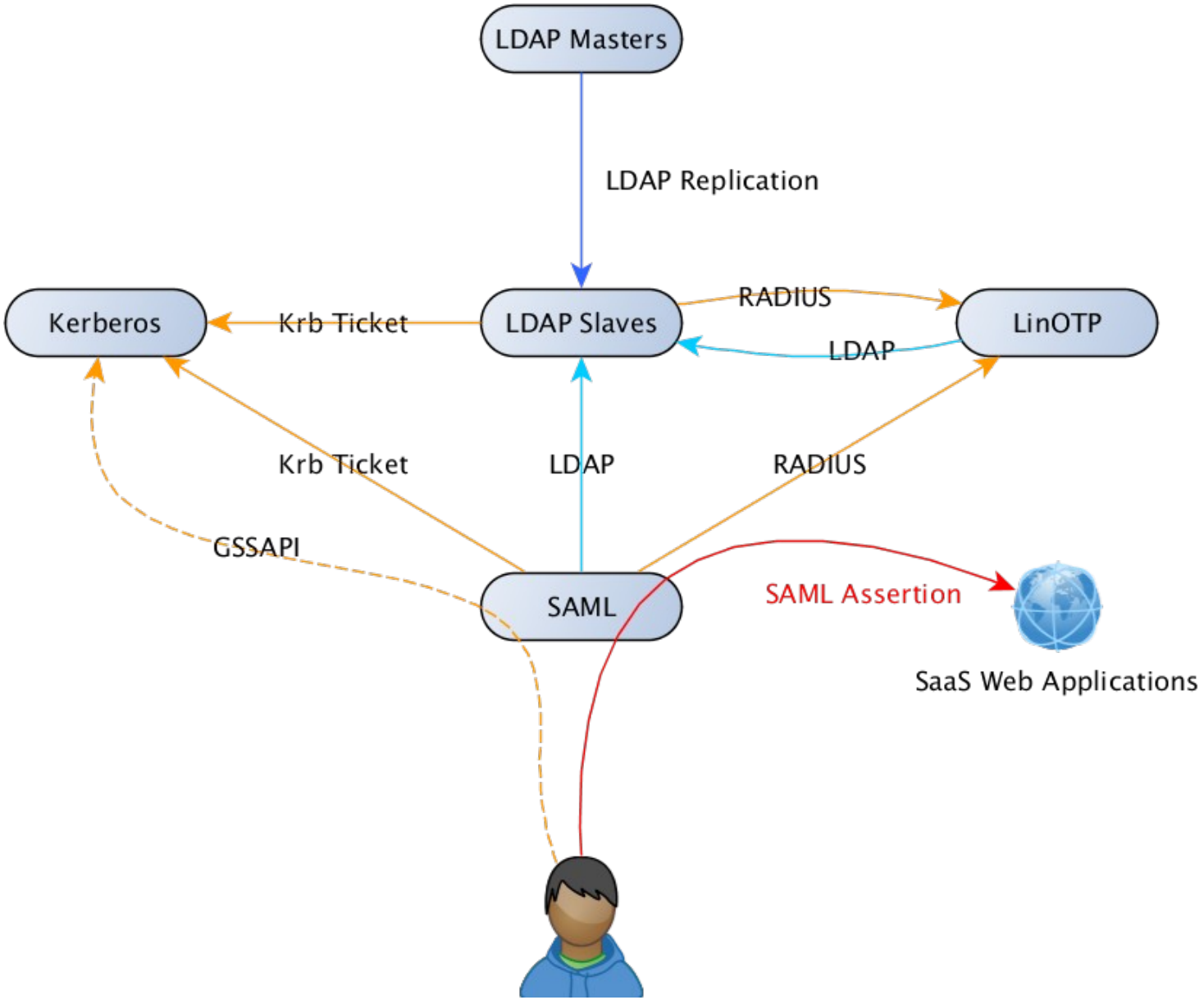
User Devices - Choice

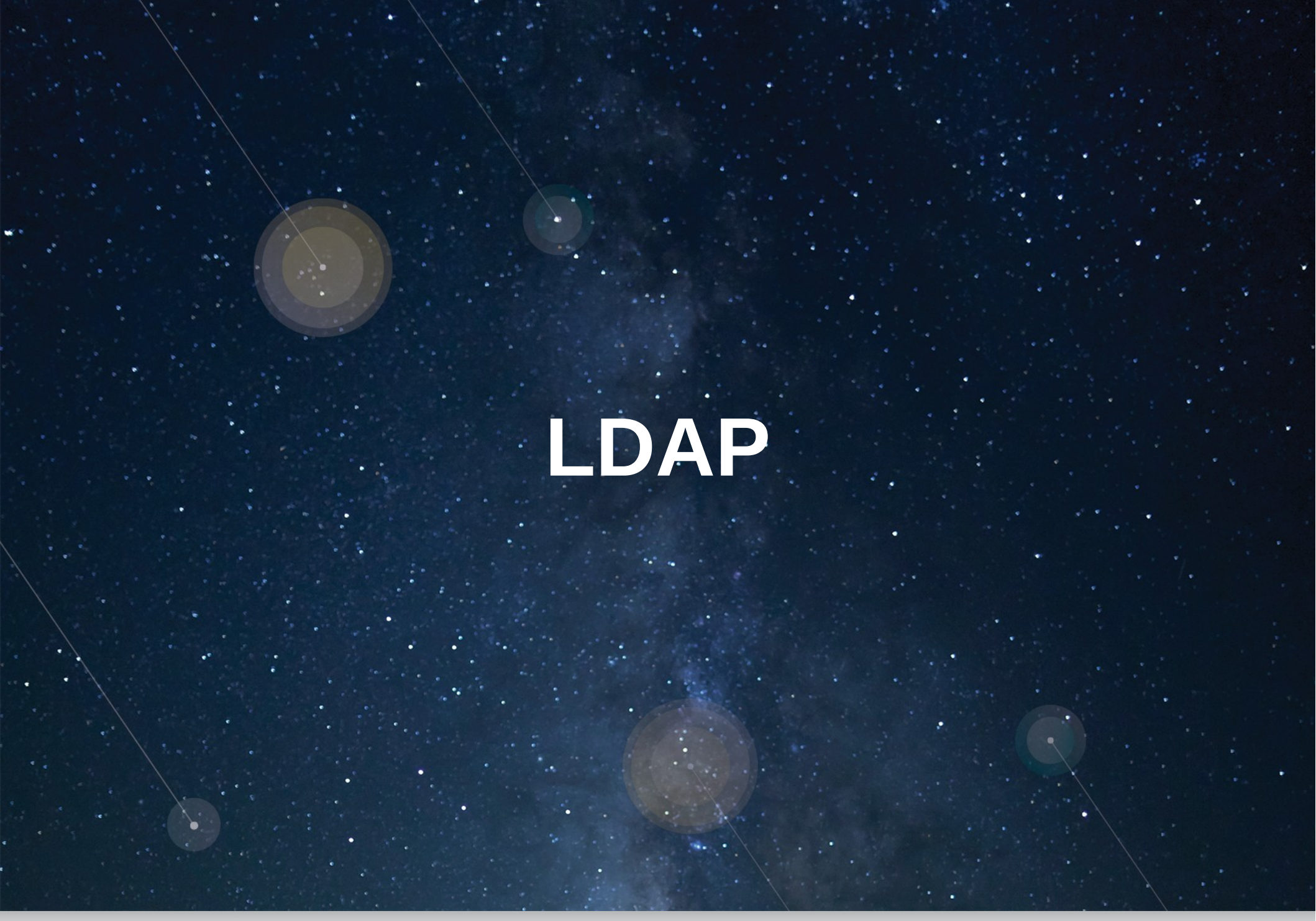
- RHEL CSB (managed)
  - Non-technical users
- Fedora, RHEL, rawhide or other Linux flavor (self-managed)
  - Engineers across all departments
- Windows
  - Small population for legal, HR, etc.
- Mac OS
- Android
- iOS
- Everything else

Internal Application Access



External/SaaS Application Access




LDAP

Red Hat Directory Server

- Originally migrated from NIS to RHDS in 2006, after Netscape Acquisition
- Currently running on RHDS 9.1 on RHEL 6.6
- 36 nodes in production globally
- ~130,000 objects
- Hardened, stable, multi-master architecture
- After the acquisition, Red Hat open-sourced RHDS as 389 Directory Server
- 389 DS remains the upstream open source project

LDAP – Not Just an Internet Directory

- User accounts
- Groups
  - PosixGroups
  - GroupOfNames
- Application Data Storage
  - Mail routing
  - Account management
  - Role data
  - Public key storage

RHDS Puppet Module

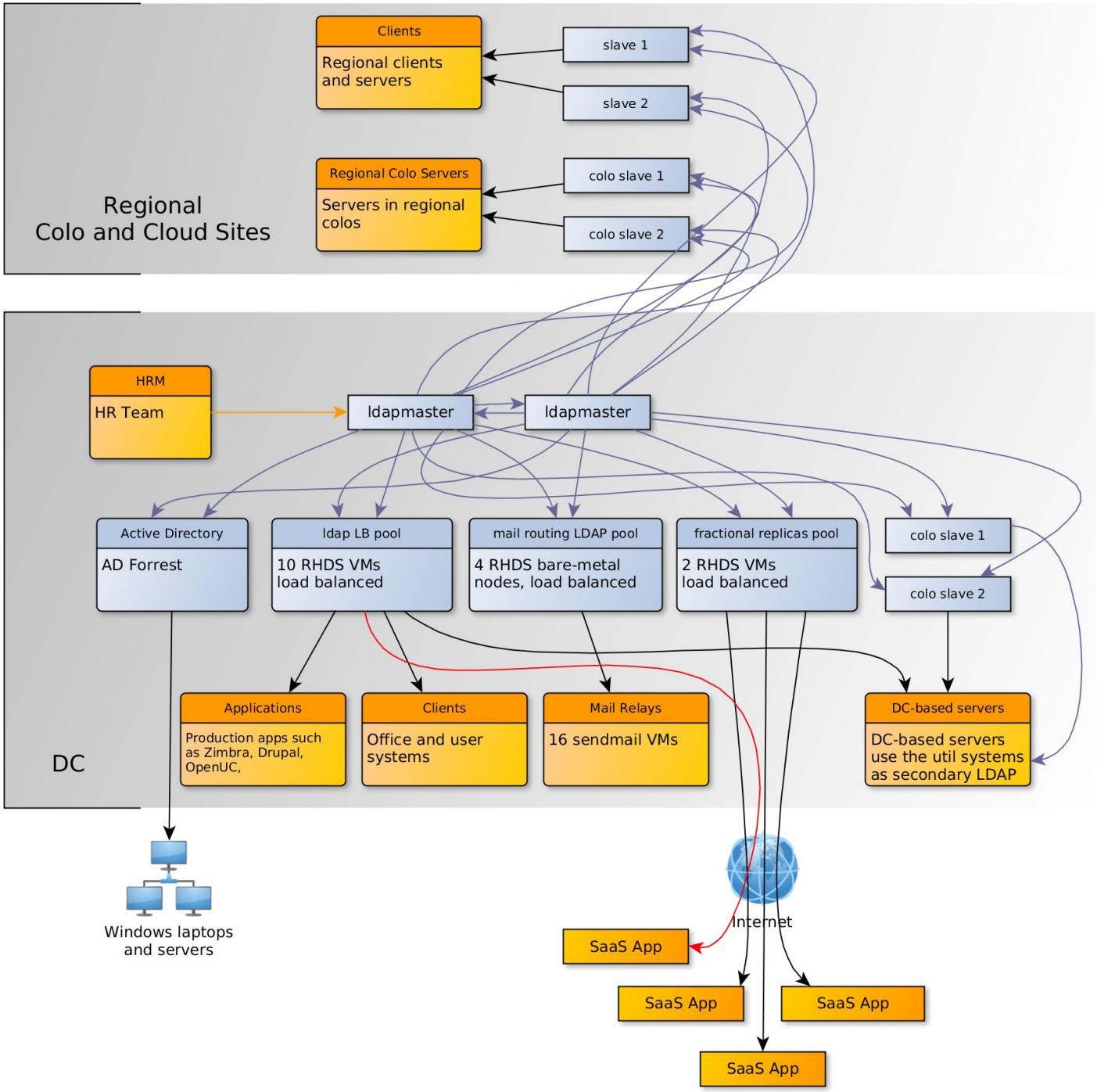
- RHDS installation/configuration
- Replication agreement creation
  - Multi-master and slave agreements
- Full TLS configuration
  - Manage NSS database
- Will be uploaded to the Puppet Forge

Custom Schema

- Schema can be viewed at
  http://people.redhat.com/batkisso/LISA
- User Information
  - users, groups
- Automation
  - Full user life cycle management
- Sendmail
  - Mail Routing
- GPG Keys
  - GPG Native Key Server Integration

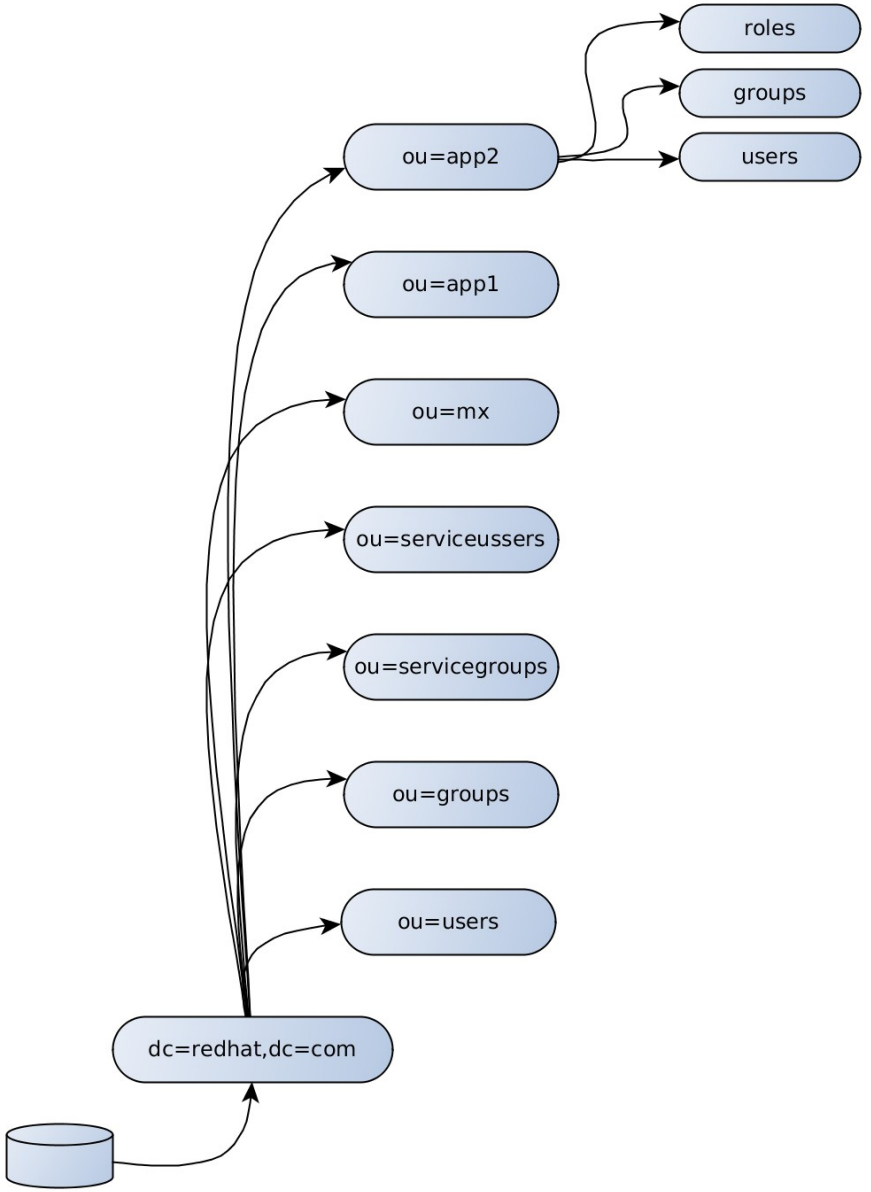
```
dn: cn=schema
attributeTypes: (
  1.3.6.1.4.1.3401.8.2.8
  NAME 'pgpBaseKeySpaceDN'
  DESC 'Points to DN of PGP keys.'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  SINGLE-VALUE
  )
attributeTypes: (
  1.3.6.1.4.1.3401.8.2.9
  NAME 'pgpSoftware'
  DESC 'pgpSoftware attribute for PGP'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
  )
attributeTypes: (
  1.3.6.1.4.1.3401.8.2.10
  NAME 'pgpVersion'
  DESC 'pgpVersion attribute for PGP'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE
  )
attributeTypes: (
  1.3.6.1.4.1.3401.8.2.11
  NAME 'pgpKey'
  DESC 'pgpKey attribute for PGP'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
  SINGLE-VALUE
  )
```

Replication



LDAP Tree

- Flat ou=users
- PosixGroups in ou=groups
- groupOfNames and groupOfUniqueNames in ou=servicegroups
- Applications may have their own structure under ou=<appname>



User Data Sources

- Goal is for all systems consuming user information to pull from LDAP, rather than HRM, CAFM, etc.
- LDAP service considered authoritative for account information (uid, gid, email, etc)
- Employee information pulls from HRM solution
- Office data (address, cube number, etc) pulled from facility management system
- Some attributes are self-service with a GUI front-end (phone number, IRC nick name, etc)
- User GPG and SSH public key publishing

ou=mx

- Large tree with 80,000 aliases
- Used for mail routing
- Replaces sendmail access and aliases files
- GUI Front-End

```
dn: sendmailMTAKey=user,ou=mx,dc=redhat,dc=com
rhatMTAExternalCode: OK
sendmailMTAKey: user
sendmailMTAHost: int-mx
sendmailMTAAliasGrouping: aliases
objectClass: sendmailMTA
objectClass: sendmailMTAAlias
objectClass: sendmailMTAAliasObject
objectClass: rhatSendmailMTA
objectClass: top
rhatEmailAddress: user@redhat.com
sendmailMTAAliasValue: user@destination.mail.redhat.com
```

RHDS Plugins

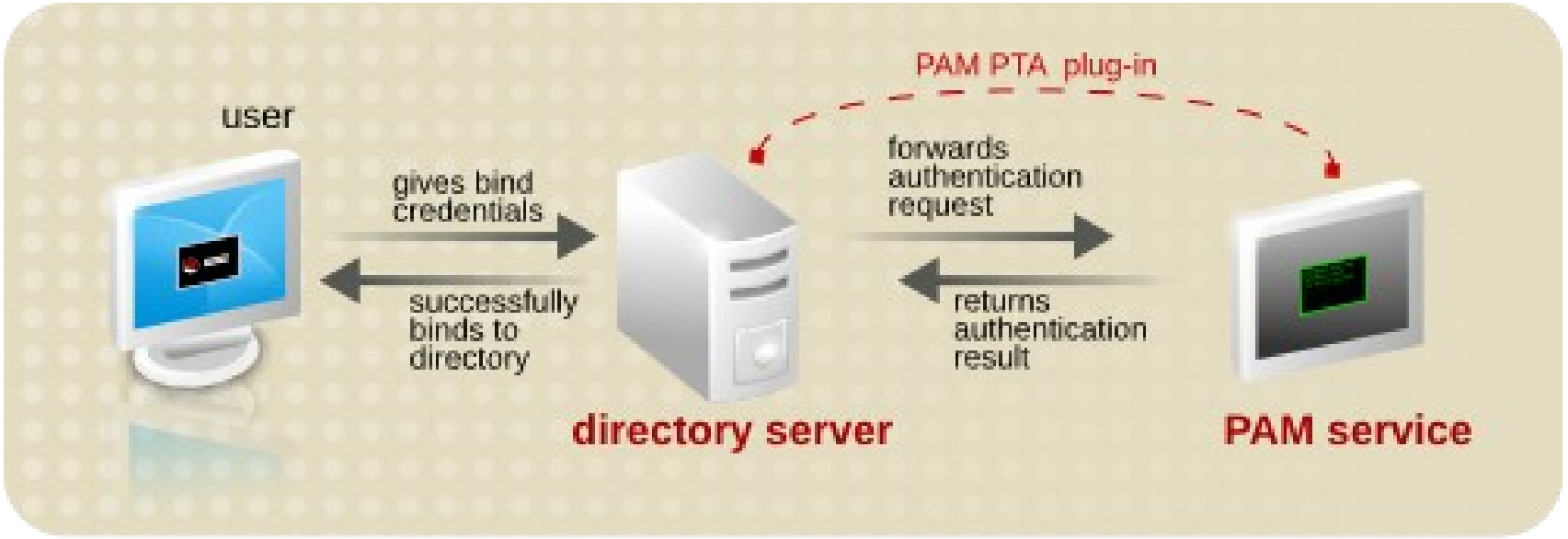
- RHDS has a plugin architecture, allowing for custom functionality
- Plugins used internally
  - PAM Pass-Through Authentication
  - NIS
  - memberOf

```
dn: cn=it,ou=servicegroups,dc=redhat,dc=com
cn: it
objectClass: groupOfUniqueNames
objectClass: top
uniqueMember: uid=user,ou=users,dc=redhat,dc=com
...

dn: uid=user,ou=users,dc=redhat,dc=com
memberOf: cn=employee,ou=userclass,dc=redhat,dc=com
memberOf: cn=it,ou=servicegroups,dc=redhat,dc=com
...
```

PAM Pass-Through Authentication

- Allows users to authenticate to RHDS with their Kerberos password, in addition to GSSAPI, by passing credentials to the PAM layer
- Any PAM authentication source will work



Kerberos

MIT Kerberos

- Standard Kerberos realm
- Single master
- Every CoLo
  - 2 slaves DC services
  - >=2 user-facing slaves
- Possible to promote a slave into a master, requires 30 minutes of manual work
- Puppet module for automated installation

The Kids Love Their Kerberos

- GSSAPI is highly adopted throughout the organization, one-time authentication provides full work-day access.
- The kerberos realm is almost as old as the company itself
- Used by both technical and non-technical users (via SSSD) to provide true internal Single Sign-On functionality
- Unified SSO authentication across all personal, lab and data center hosts and applications

Two Factor Authentication

Two Factor Authentication

- Use open source LinOTP project
  - Enterprise support
- Primary / Secondary architecture
- Soft Token Support
  - Red Hat's FreeOTP app for iPhone/Android
  - Google Authenticator
- Hard Tokens
  - Gemalto
  - Yubikey

Where 2FA is Used

- Transiting Untrusted -> Trusted Border
- Some applications
  - HRM
  - SOX/PCI systems
  - Others

One Time Passwords – Application Support

- LinOTP, like many 2FA systems, can use RADIUS for application and system integration
- Some apps can't speak RADIUS, but speak LDAP
  - PAM pass-through plugin can provide application OTP support

SAML

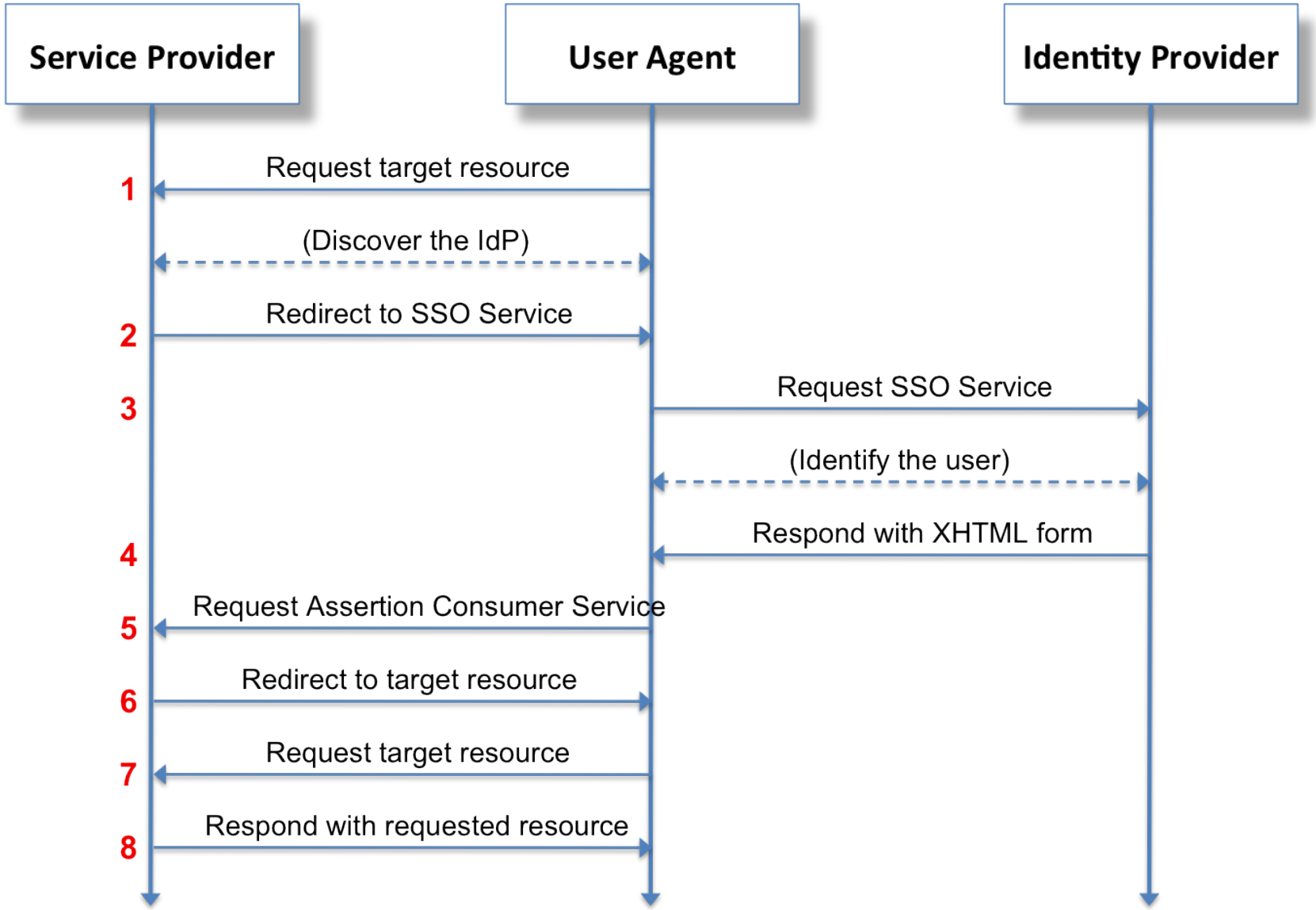
SAML

- “Security Assertion Markup Language (SAML) is an XML-based open standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.” - Wikipedia
- Federated Authorization and Authentication, mainly for ***web-based*** applications
- SAML 2.0 standard released in 2005

SAML – New Found Love

- Gained traction in the last couple years as hosted/SaaS applications have drastically increased popularity among IT shops
- SAML v1.0 approved as an OASIS standard in 2002

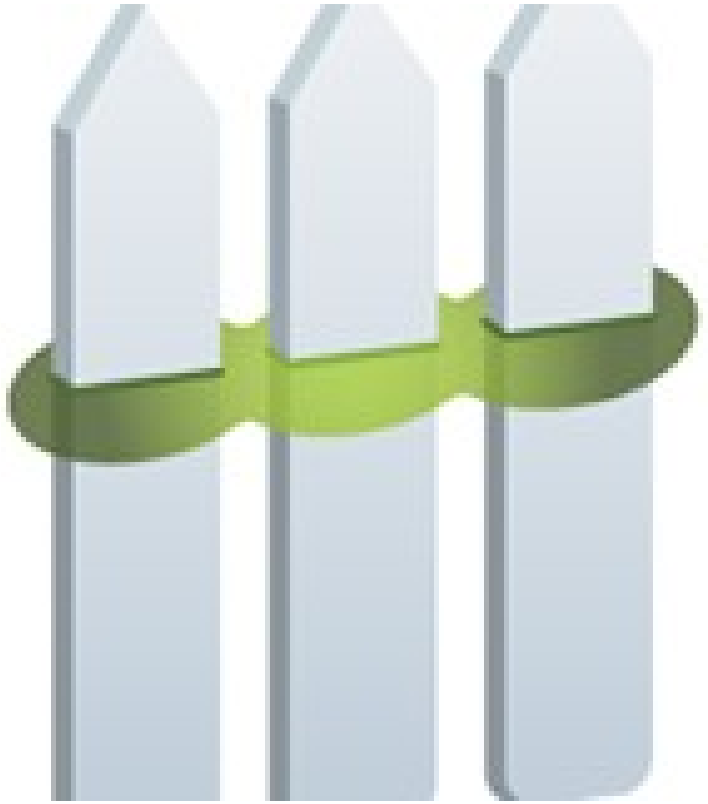
Identity Provider / Service Provider Interaction



Source: Wikipedia

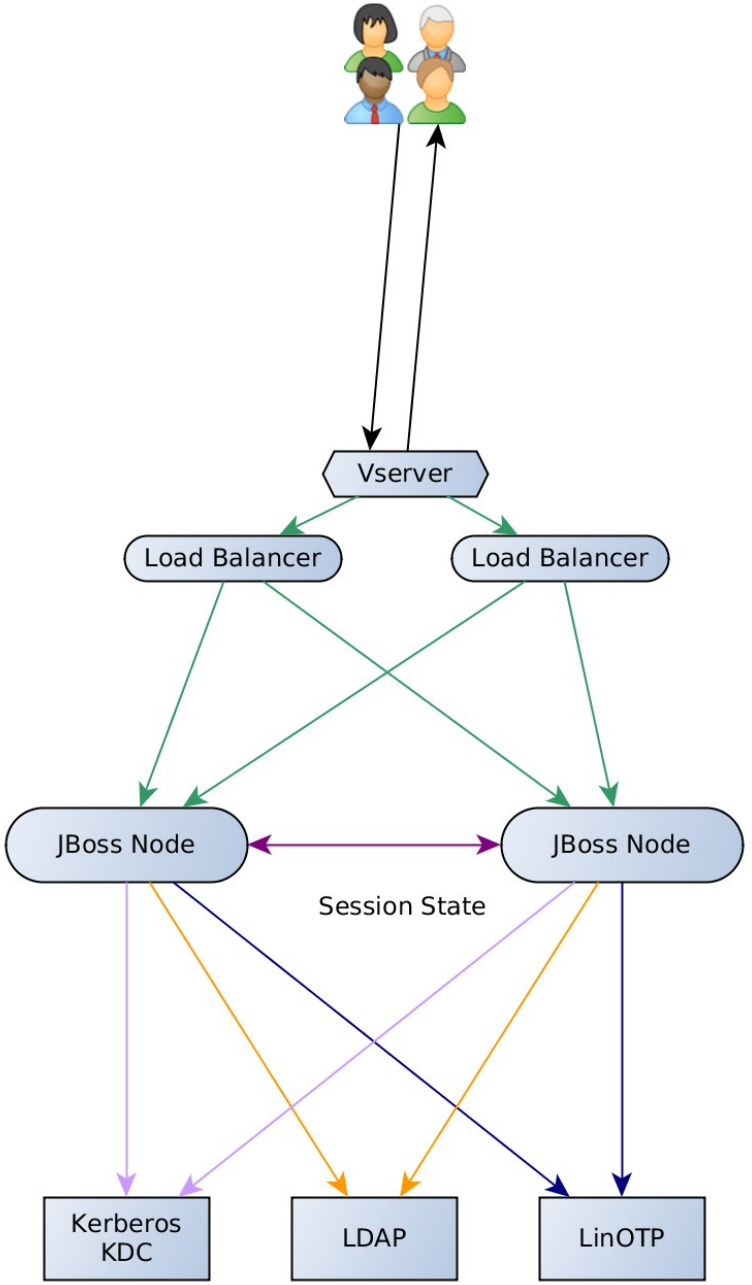
SAML Identity Provider

- The identity management components of JBoss are provided by a sub-project called PicketLink
- SAML 2.0 Federation Standard support and others
- Red Hat IT uses a custom JBoss EAP Application, based on the one of the PicketLink QuickStarts



Red Hat IdP Architecture

- JBoss EAP 6.3.2 (CP02)
- Load balanced traffic
- Redundant EAP IdP application nodes
- Authentication performed by OTP or Kerberos calls
- Authorization uses LDAP for role mapping



Configuration Management

- IdPs are completely puppetized
- Templated metadata for easy SP additions
- Clustered architecture allows for non-disruptive changes
- Exploded WAR deployed via Puppet
- Weekly release of new code and SP integrations
- SP libraries and modules puppetized, allowing easy integration of non-SAML enabled apps

JBoss/PicketLink RFEs

- Close collaboration with PicketLink developers and Red Hat Support to bring new functionality into the framework.
  - Kerberos GSSAPI support
  - Session Replication between EAP cluster nodes
  - Assertion signature granularity
  - Logout

Kerberos GSSAPI / SAML SSO Bridge

- Provides SAML IdP Authentication via a Kerberos TGT ticket
- Fallback to OTP should the user not have a ticket or be coming from an untrusted source
- Full support for GSSAPI Auth in EAP 6.3.2 (CP02)

Session Replication with OTP

- JBoss has an elegant session replication protocol
- Replication was designed to 'replay' the user's password upon failover
- Would not work in a OTP environment
- Our JBoss Login module for this has been contributed back to the community
- Allows for rolling maintenance and releases
- IdP achieved 100% uptime in the last year

Federated Logout

- The SAML Spec implementation for federated logout requires the IdP to sequentially log the user out of each Service Provider via redirects.
- This does not scale, leads to a poor user experience and can be interrupted by any misbehaving SP
- Nice summary: https://wiki.shibboleth.net/confluence/display/SHIB2/SLOIssues
- We are working on a way to concurrently log the user out of all SPs. Not perfect, but better than the alternative. This will be contributed back to the community.

Service Providers (SP)

- SaaS vendors will typically support the SAML 2.0 required functionality and some of the optional standards.
- We have seen issues with SPs and IdPs implementing the optional SAML specs in incompatible ways
- IdP-SP metadata exchange often requires a lot of back-and-forth, give yourself plenty of time.

Open Source Libraries and modules

- A variety of open source service provider software exists for integrating SAML into your application
- JBoss PicketLink
  - QuickStarts available
- Shibboleth / OpenSAML
- PySAML
- SimpleSAMLphp
  - Great tool for IdP debugging
  - Drupal integration
- Ruby-saml
- Apache modules
  - mod_auth_mellon
  - mod_auth_saml

mod_auth_mellon

- Works very similar to mod_auth_kerb, except provides SAML 2.0 authentication
- Now included in RHEL 6.6+ (base)
- Patched by RH IT to support wider range of IdPs (including PicketLink)
- mod_auth_mellon + reverse proxy allows you to front-end virtually any application with SAML authentication
- Just rolled out SAML support for our Zimbra environment using this solution, more applications are planned

mod_auth_mellon Configuration

- [RHEL6.6]# yum install -y mod_auth_mellon
- Copy IdP metadata to /etc/httpd/conf/ss-idp-metadata.xml
- Add /etc/httpd/conf.d/mellon.conf
- Hit https://$sp/secret/endpoint/metadata for SP data to pass to the IdP
- Assumes vhost/SSL already configured

```
cat /etc/httpd/conf.d/mellon.conf
<Location /secret>
   AuthType "Mellon"
   MellonEnable "auth"
   MellonDecoder "none"
   MellonVariable "cookie"
   MellonSecureCookie On
   MellonUser "NAME_ID"
   MellonSetEnv "e-mail" "mail"
   MellonEndpointPath "/secret/endpoint"
   MellonDefaultLoginPath "/secret"
   MellonSessionLength 86400
   MellonOrganizationURL "http://www.redhat.com"
   MellonSPPrivateKeyFile /etc/pki/tls/certs/auth-mellon.pem
   MellonSPCertFile /etc/pki/tls/certs/auth-mellon.pem
   MellonIdPMetadataFile /etc/httpd/conf/ss-idp-metadata.xml
   MellonSamlResponseDump On
   MellonSessionDump On
</Location>
```

mod_auth_mellon Apache ProxyPass

```
cat /etc/httpd/conf.d/check.conf
<Location /check/>
   MellonEnable "off"
</Location>
```

```
included from vhost config...

#Turn on proxy to ssl hosts for connection to mail.corp.redhat.com
SSLProxyEngine On

#Make sure we pass vhostname to backend systems
ProxyPreserveHost On

#Exclude local data
ProxyPassMatch ^/endpoint !
ProxyPassMatch ^/check/are_you_alive.php !

ProxyPass / webmail.example.com
ProxyPassReverse / webmail.example.com
```

PKI

Public Key Infrastructure – Red Hat Certificate System

- Provides highly secure end-to-end PKI Solution for enterprises
- Support for Smart Card Authentication
- FIPS 140-2 Level 2 validated
- Hardware Key Management (HSM) Support
- RHCS Uses Directory Server as a back-end
- Highly available, fault tolerant design thanks to RHDS-level replication
- Upstream Project: Dogtag Certificate System

RHCS Components

- Certificate Authority
  - Process Signing Requests
- Token Management System
  - Smart cards
- Data Recovery Manager
  - Encryption Key Escrow
- Registration Authority
  - Flexible user-facing system for self-service
  - SCEP Enrollment (network devices)
- OCSP Responder
  - Certificate Revocation Lists
  - Responder for Certificate Status

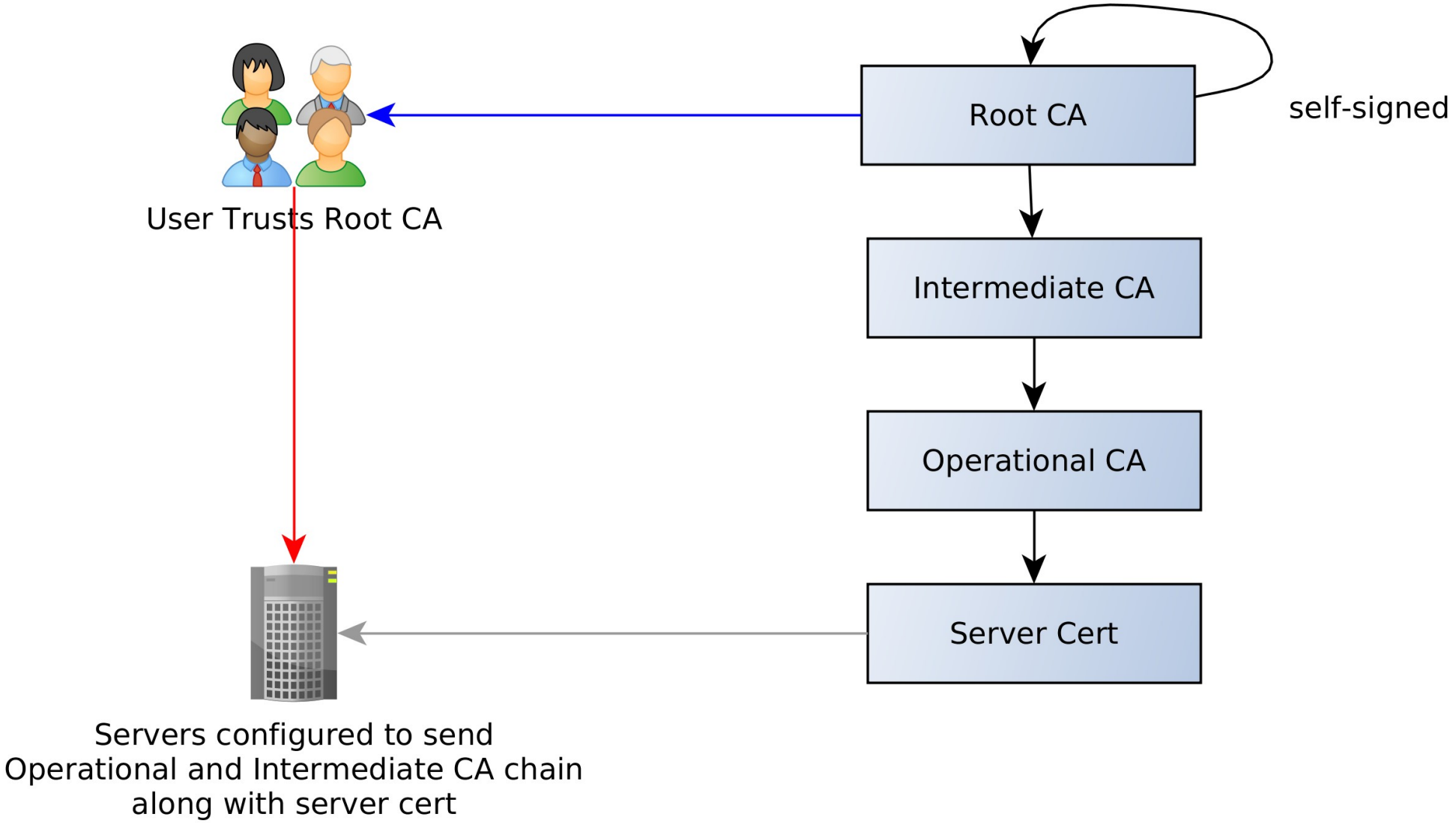
Red Hat IT Use Cases

- General internal server encryption and identification
- TLS Client Auth
  - Mobile devices
  - Intra-app communication (SAML, cloud apps, etc)
- Subscription management
- SCEP for network devices

Red Hat Certificate System - IT

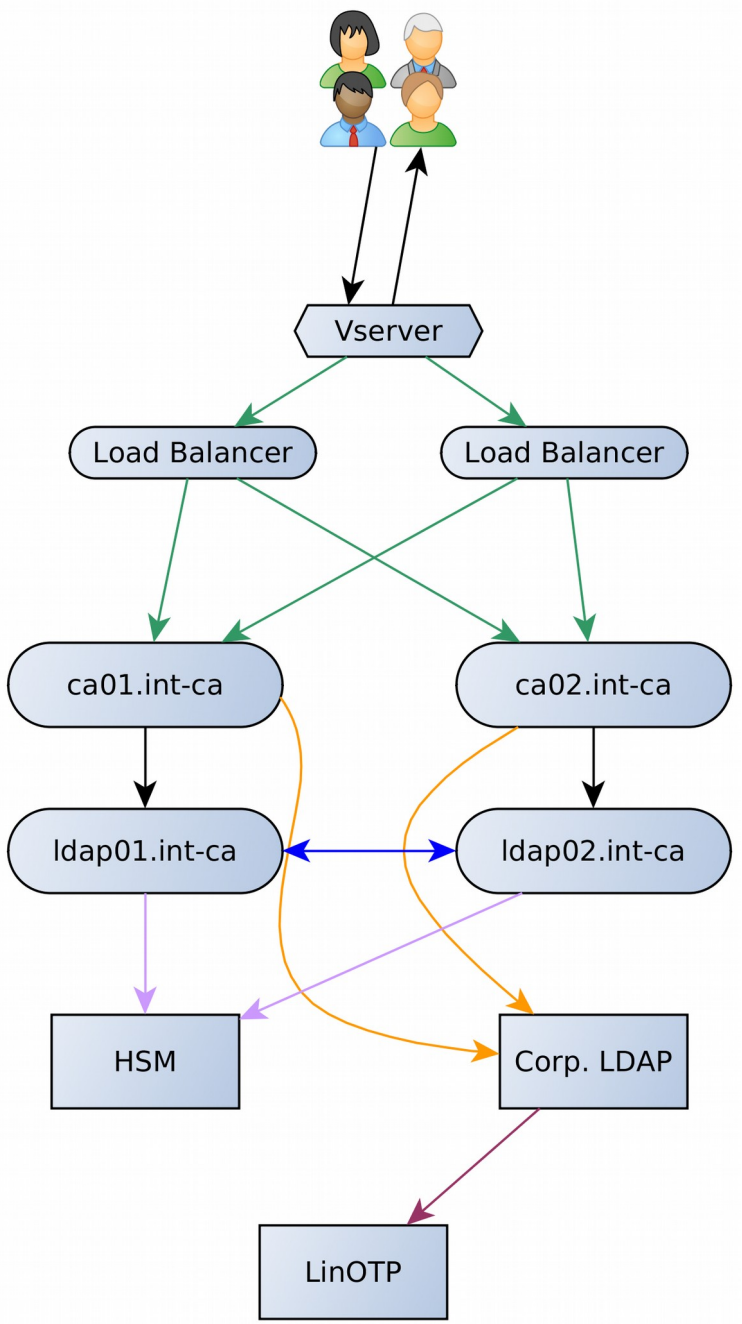
- Multi-Data Center
- 3 tier design
- Redundant HSMs
- Puppetized deployment and installation
- Offline root and intermediate CAs
- SHA512 Message Digest cipher
- Self-Service user certificates for all associates
- Self-Service server certificates for sysadmin groups
  - Custom plugin to support group authz

RHCS Cert Chain



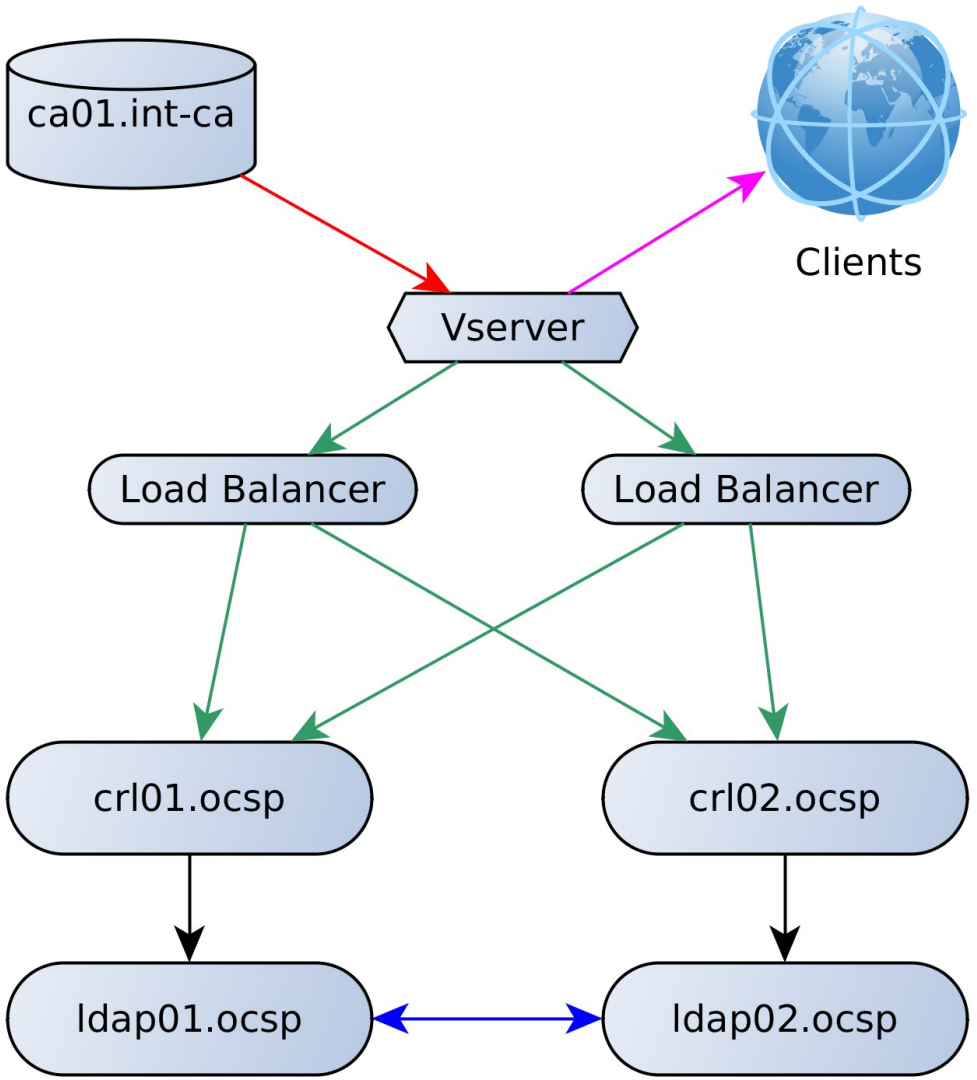
CA Cluster Architecture

- Load Balanced
- CA clones
- RHDS masters with bi-directional replication
- Corp. LDAP for Self-Service authz
- Corp. LDAP with Pam-Passthru to OTP for authn

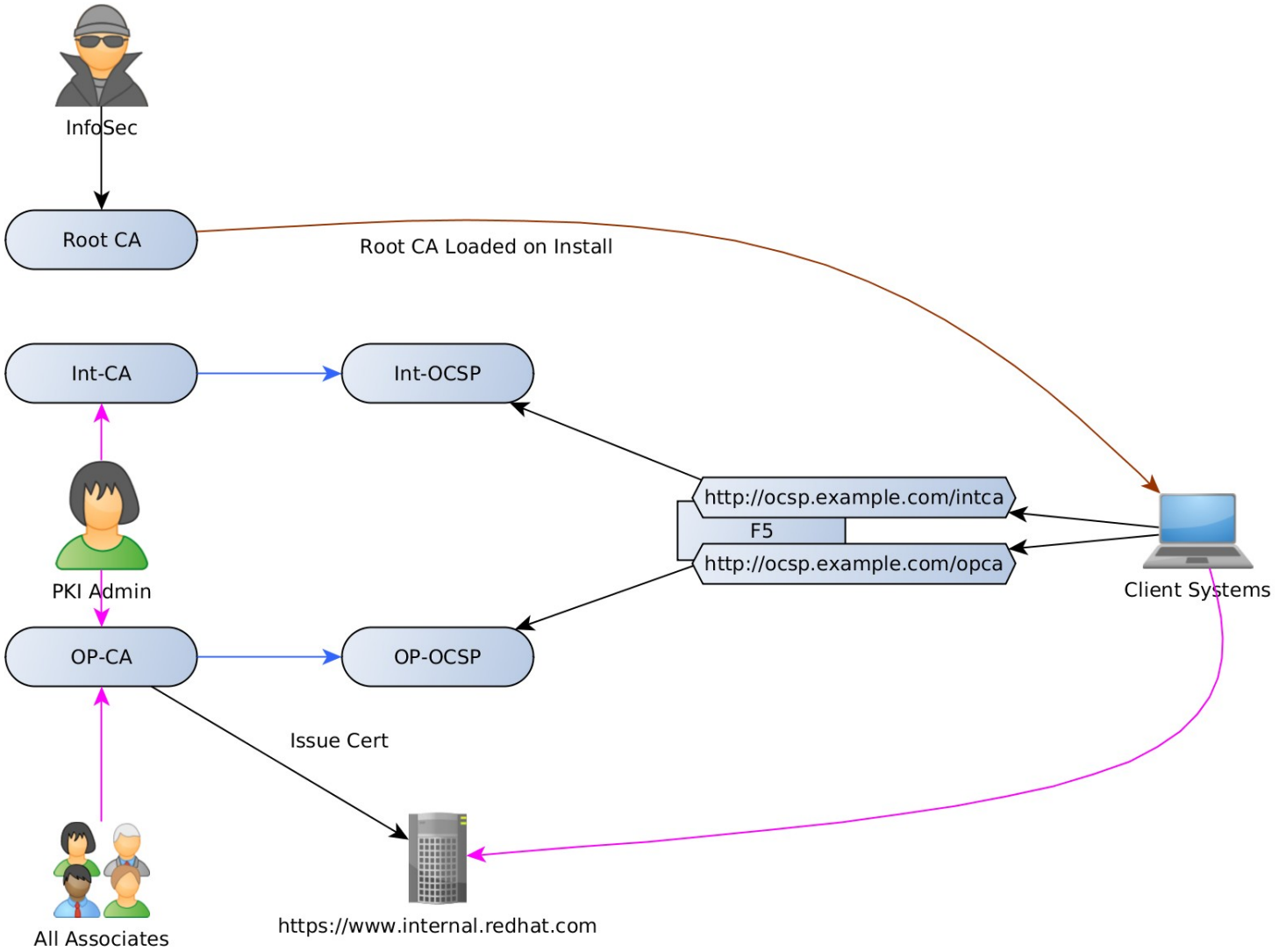


OCSP Cluster Architecture

- CA (01 node) cluster publishes certs to OCSP cluster
- Load Balanced
- OCSP nodes
- RHDS masters with bi-directional replication



PKI Environment Overview

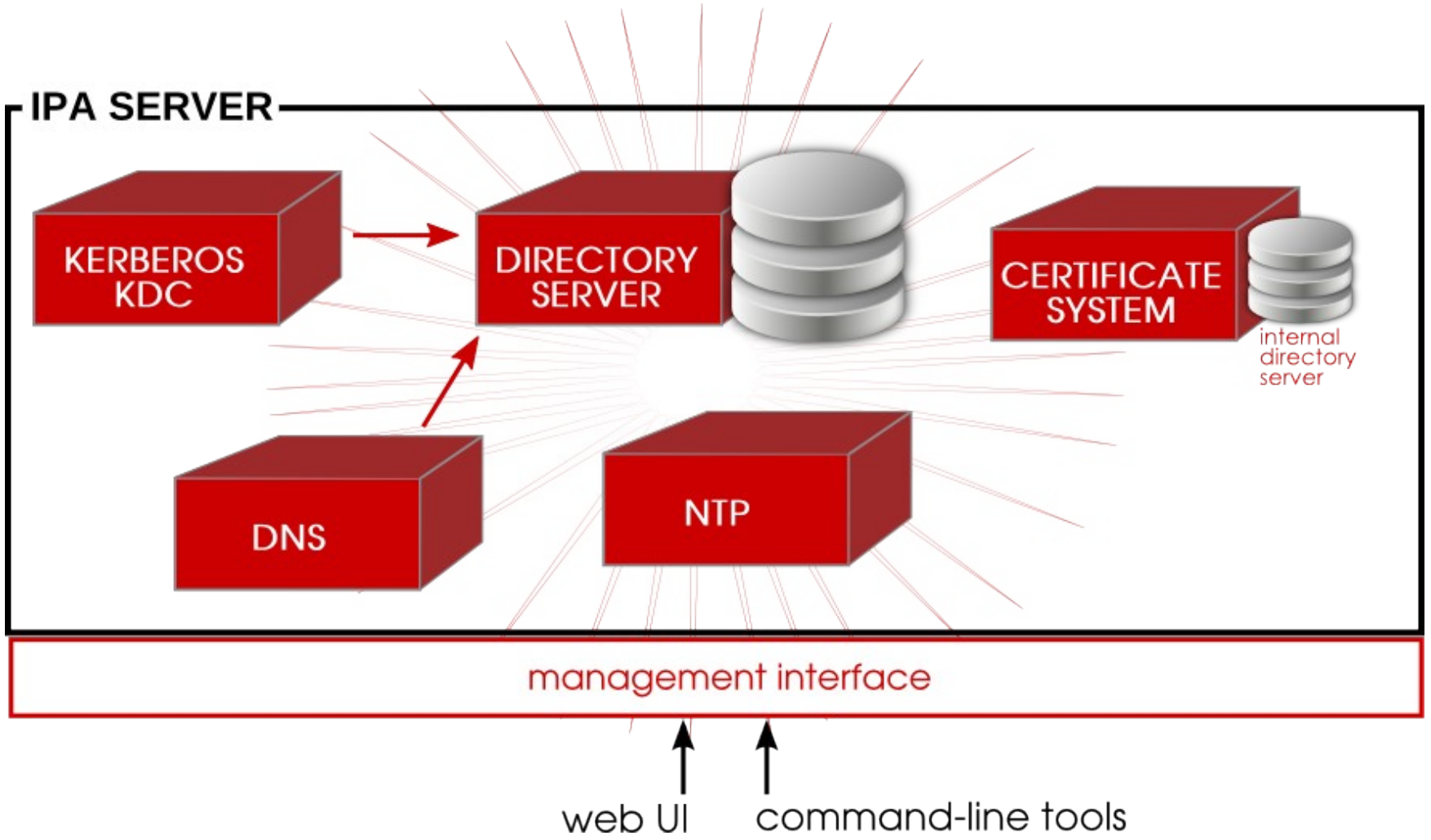


IdM / FreeIPA Overview

Red Hat IdM

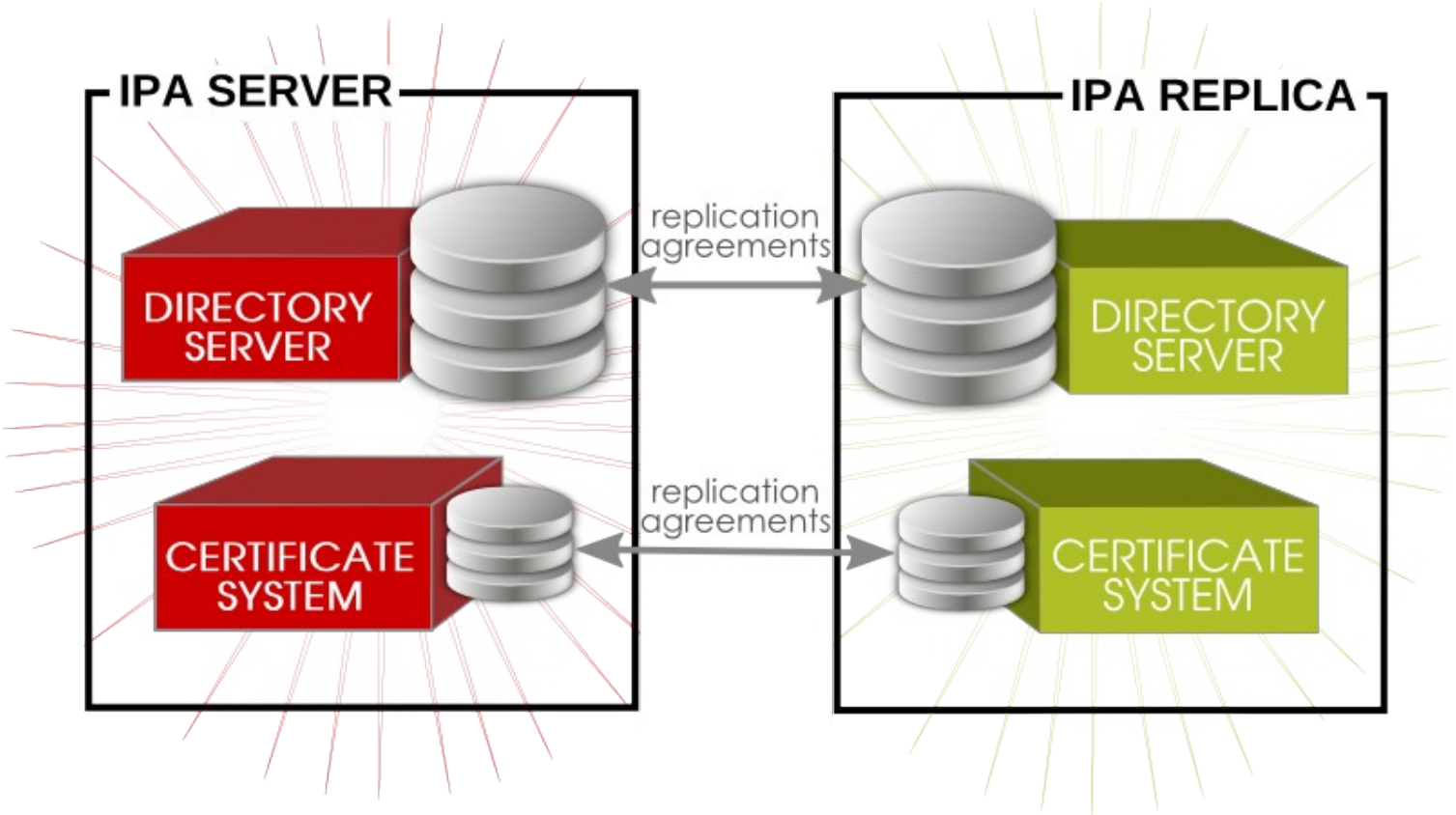
- Red Hat Identity Management
- Product that is essentially 'AD for Linux'
- Combines LDAP, Kerberos and PKI into a single solution
  - OTP, Bind, NTP, AD integration
- Fantastic GUI and CLI tools
- FreeIPA is the upstream project, IdM is the stabilized version included in base RHEL for free

IdM Overview



IdM High Availability

- Utilizes RHDS as a back-end for all data
- Supports up to 20 master servers

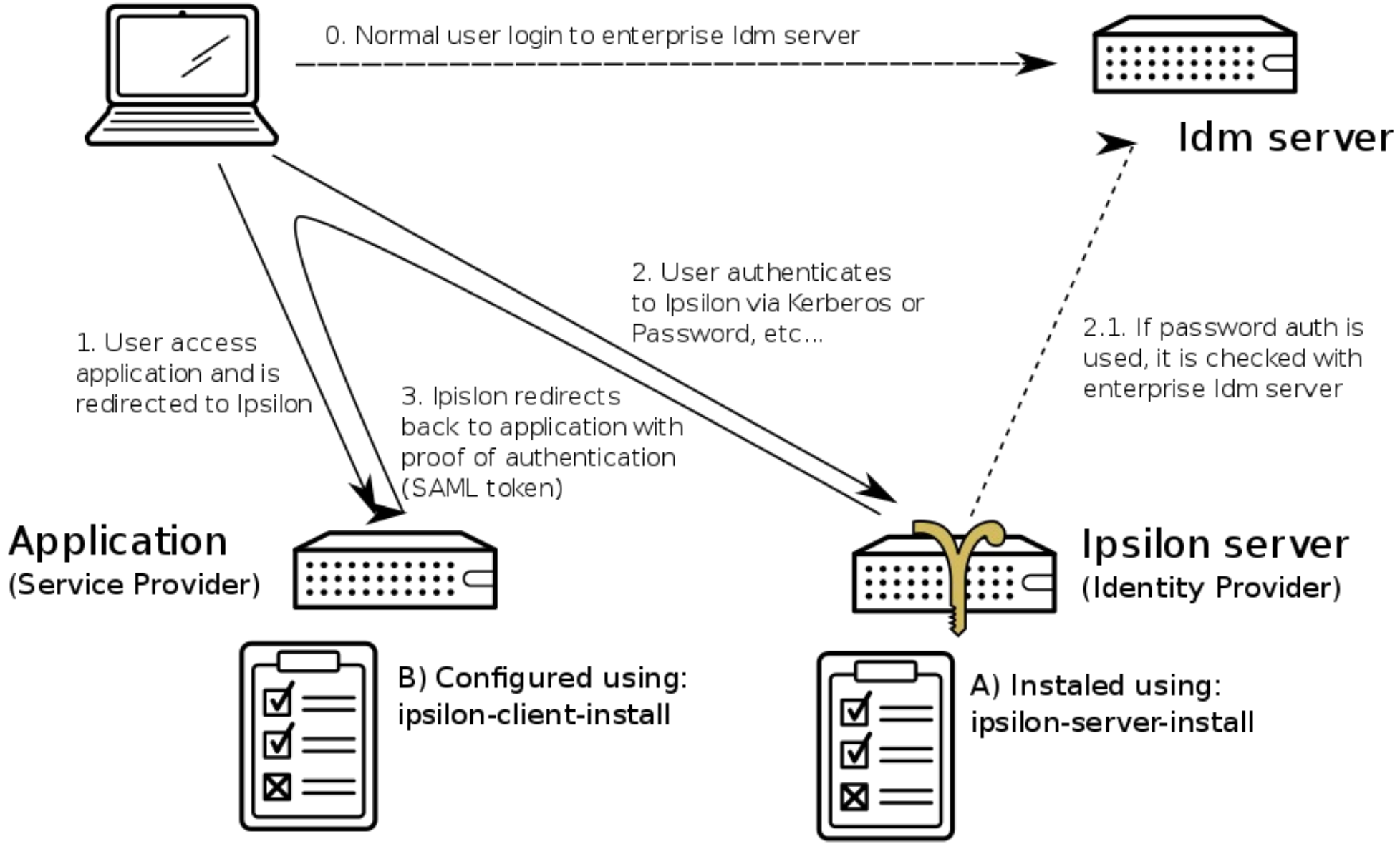


IdM

- Kerberos uses IdM LDAP back-end for replication
  - Replaces kprop and it's known limitations
  - Multi-master
- Integrated Bind solution
  - Secure, easy DDNS
- Integrated PKI
- Windows AD Sync
- Rapidly evolving feature-set
  - See FreeIPA.org for new features

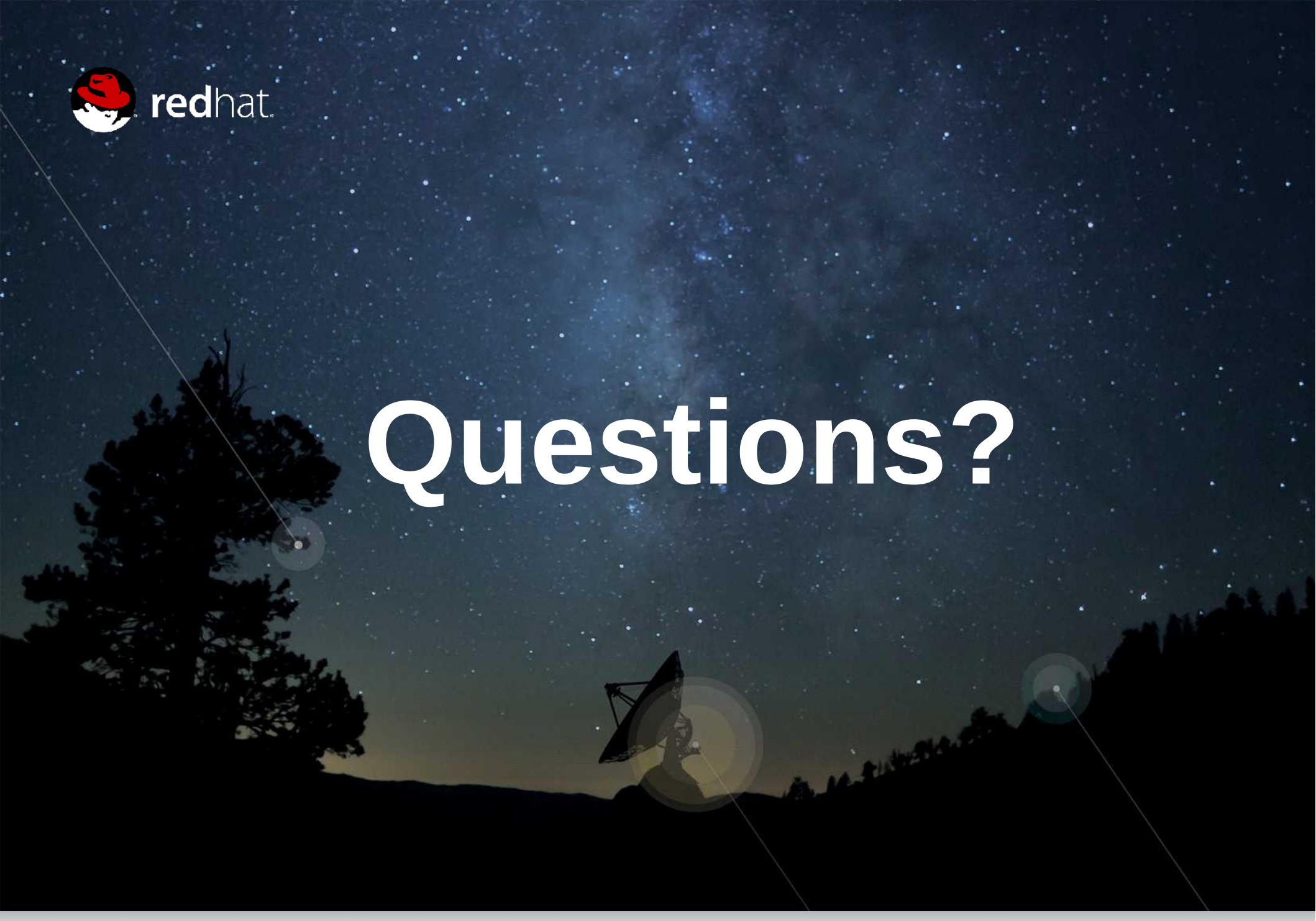
Ipsilon – SAML IdP for IdM (in development)

https://fedorahosted.org/ipsilon



Closing

- Red Hat & Open Source Identity Management solutions
- IdM/IPA bundles these nicely into a robust, simple solution
  - Businesses and orgs looking to use something other than AD to manage unix hosts (any flavor)
- Stand-alone solutions
  - RHDS / 389 DS
  - JBoss EAP / Wildfly PicketLink
  - RHCS / Dogtag


redhat.
Questions?

Links

- Brian J. Atkisson
  - walrus@redhat.com
  - Freenode: walrus
  - http://people.redhat.com/batkisso/LISA
    - LDAP GPG and Sendmail schema
    - RHDS Plugin Configs
    - mod_auth_mellon configs
- RHEV Environment Overview
  - https://access.redhat.com/node/701683