Red Hat Security related Technologies

Alfred Bach
abach@redhat.com

Red Hat

Red Hat OpenSource Technologies solving Security Issues

Network Based Disc Encryption

Network-Bound Disk Encryption (NBDE) allows for hard disks to be encrypted without the need to manually enter the encryption passphrase when systems are rebooted. In RedHat/CentOS 7 and 8, this is achieved using a tang server and the clevis framework.

Identity Management

FreeIPA is an integrated Identity and Authentication solution for Linux/UNIX networked environments. A FreeIPA server provides centralized authentication, authorization and account information by storing data about user, groups, hosts and other objects necessary to manage the security aspects of a network of computers.

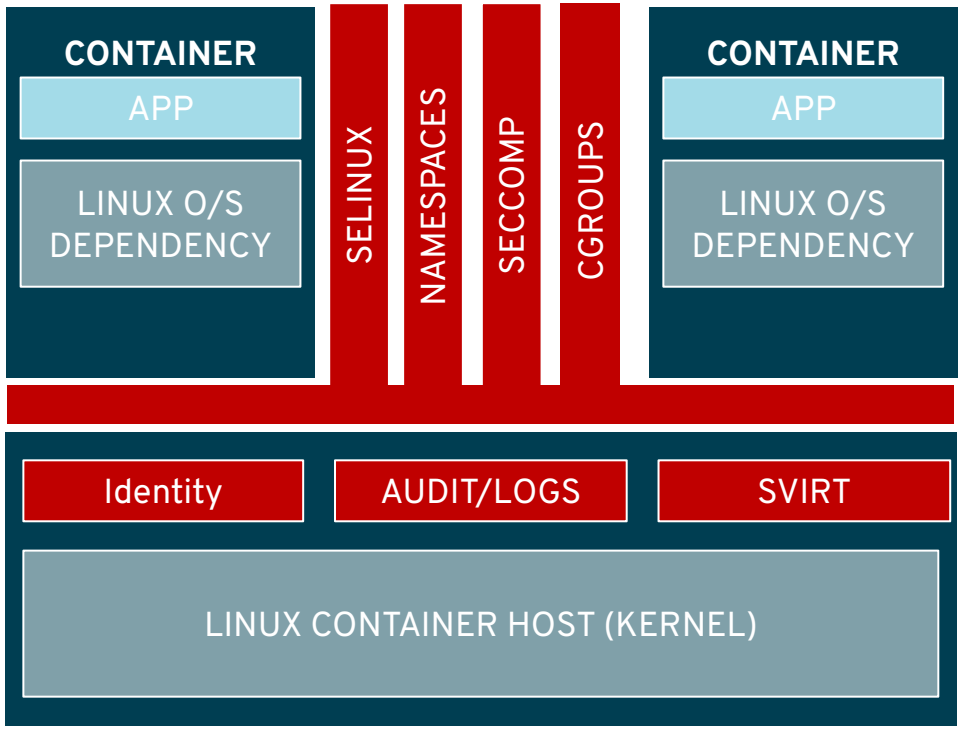
Single Sign On - KeyCloak

Add authentication to applications and secure services with minimum fuss. No need to deal with storing users or authenticating users. It's all available out of the box.

Container Security Begins With Host Security

Red Hat containers inherit RHEL industry leading security practices

- Security in the RHEL host applies to the container
- Potent combination of SELINUX and Kernel Namespaces
- Protects not only the host, but containers from each other
- Common Criteria certification*
  including container framework
- FIPS validated crypto modules*
- TPM/vTPM (v2) for automatic decryption



- Common Criteria certification for RHEL 8 is WIP / RHEL 8.1 FIPS status is Implementation Under Test

SELinux mitigates container runtime vulnerabilities

SELinux Mitigates container Vulnerability

January 13, 2017 | Joe Brockmeier

< Back to all posts Tags

A new CVE, (CVE-2016-9962), for the docker container runtime and runc were rec
released. Fixed packages are being prepared and shipped for RHEL as well as Fedo
CentOS. This CVE reports that if you `exec` d into a running container, the processe
the container could attack the process that just entered the container.

https://www.redhat.com/en/blog/selinux-mitigates-container-vulnerability

Latest container exploit (runc) can be blocked by SELinux

February 28, 2019 | Dan Walsh

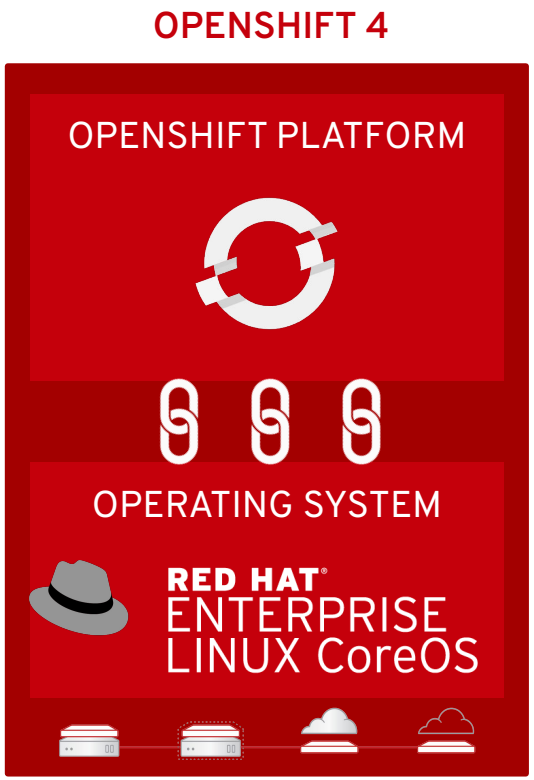
< Back to all posts Tags: *Security*, *Containers*

A flaw in runc (CVE-2019-5736), announced last week, allows container processes to "escape" their containment and execute programs on the host operating system. The good news is that well-configured SELinux can stop it.

https://www.redhat.com/en/blog/latest-container-exploit-runc-can-be-blocked-selinux

Red Hat CoreOS

The Immutable Container Optimized Operating System



Role in OpenShift Ecosystem

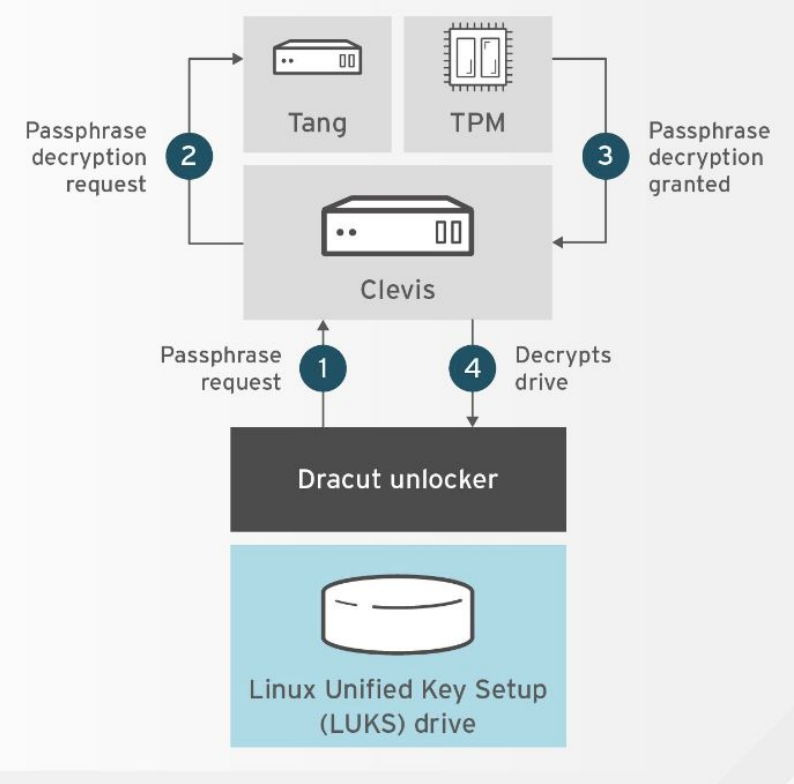
- Versioned and validated for specific OpenShift version
- Required for masters. RHEL option for workers
- User space read-only

Managed by the OpenShift Cluster

- Considered a member of an OpenShift Deployment
- Configuration managed by the Machine Config Operator
  - Container runtime
  - Kubelet configuration
  - Authorized container registries
  - SSH Configuration

Network Bound Disc Encryption

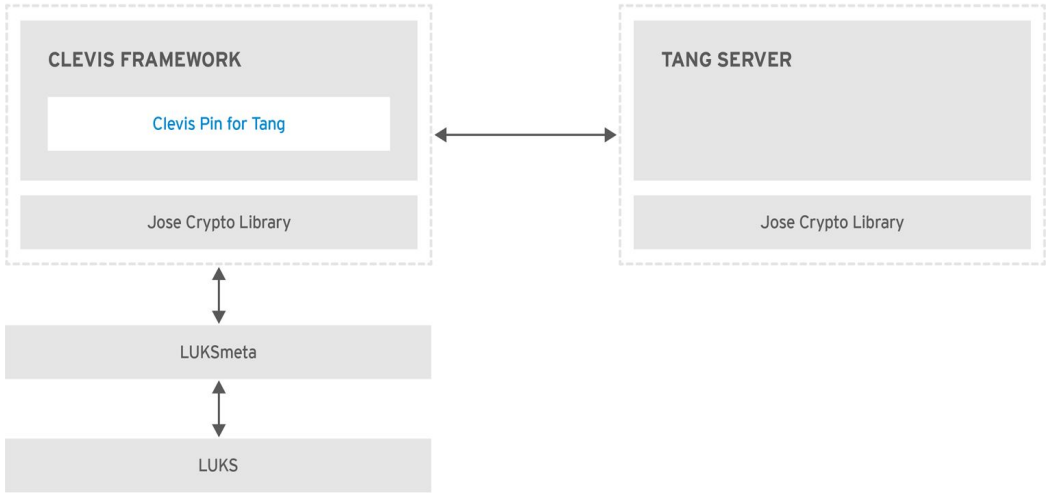
Clavis and Tang



NETWORK BOUND DISK ENCRYPTION enables encryption and decryption of disks only on a trusted network, making data unusable if removed from the network.

- Network key service (Tang or TPM)
- Automated decryption client framework (Clevis)
- Dracut unlocker
- SystemD unlocker
- Udisks2 unlocker

Network-bound disk encryption



RHEL_453350_0717

Tang is a server for binding data to network presence. It makes a system containing your data available when the system is bound to a certain secure network. Tang is stateless and does not require TLS or authentication. Unlike escrow-based solutions, where the server stores all encryption keys and has knowledge of every key ever used, Tang never interacts with any client keys, so it never gains any identifying information from the client.

Clevis is a pluggable framework for automated decryption. In NBDE, Clevis provides automated unlocking of LUKS volumes. The **clevis** package provides the client side of the feature.

A *Clevis pin* is a plug-in into the Clevis framework. One of such pins is a plug-in that implements interactions with the NBDE server – Tang.

Identity Management

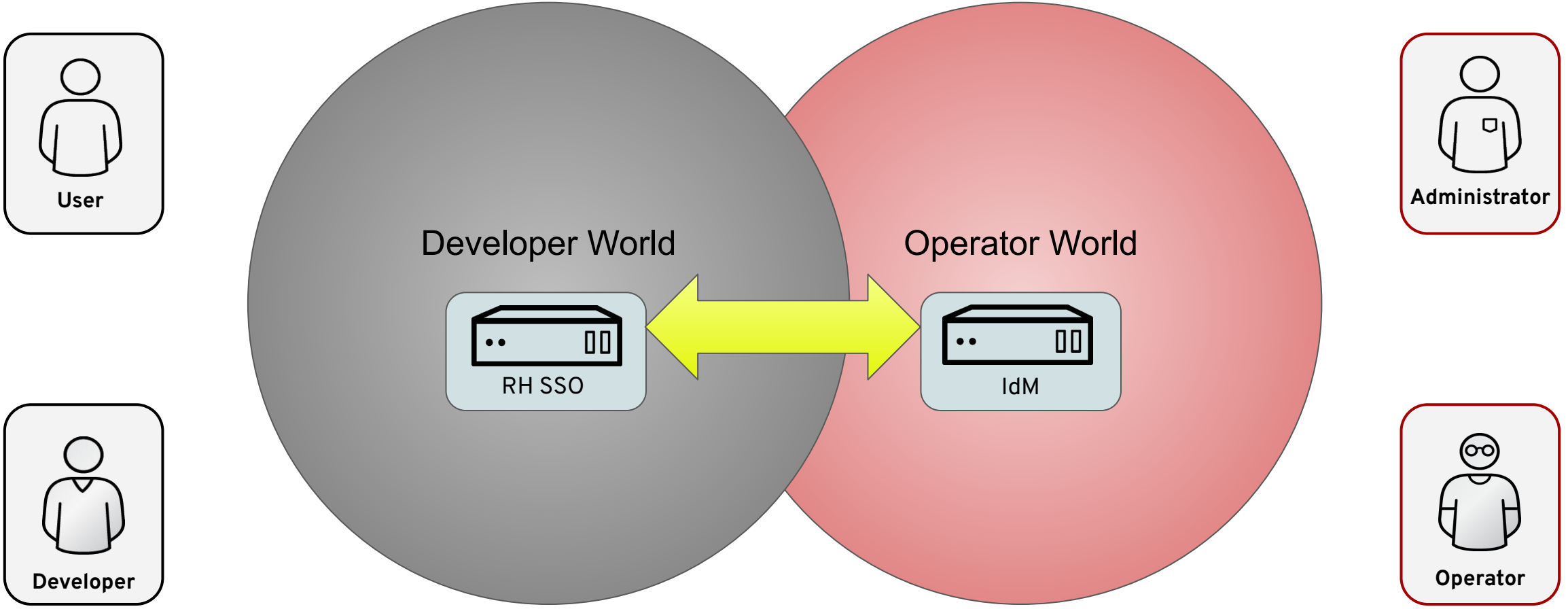
What is IdM?

- 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

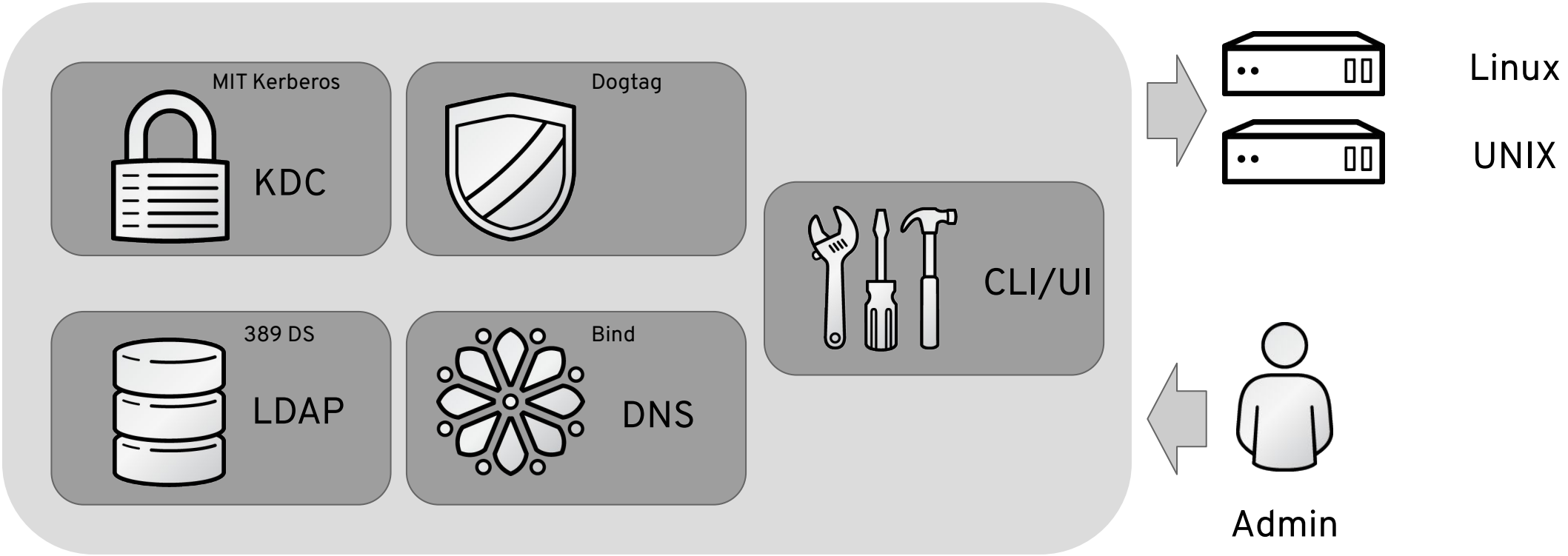
What Problems IdM Solves?

- 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)

RH SSO and IdM



IdM High Level Architecture



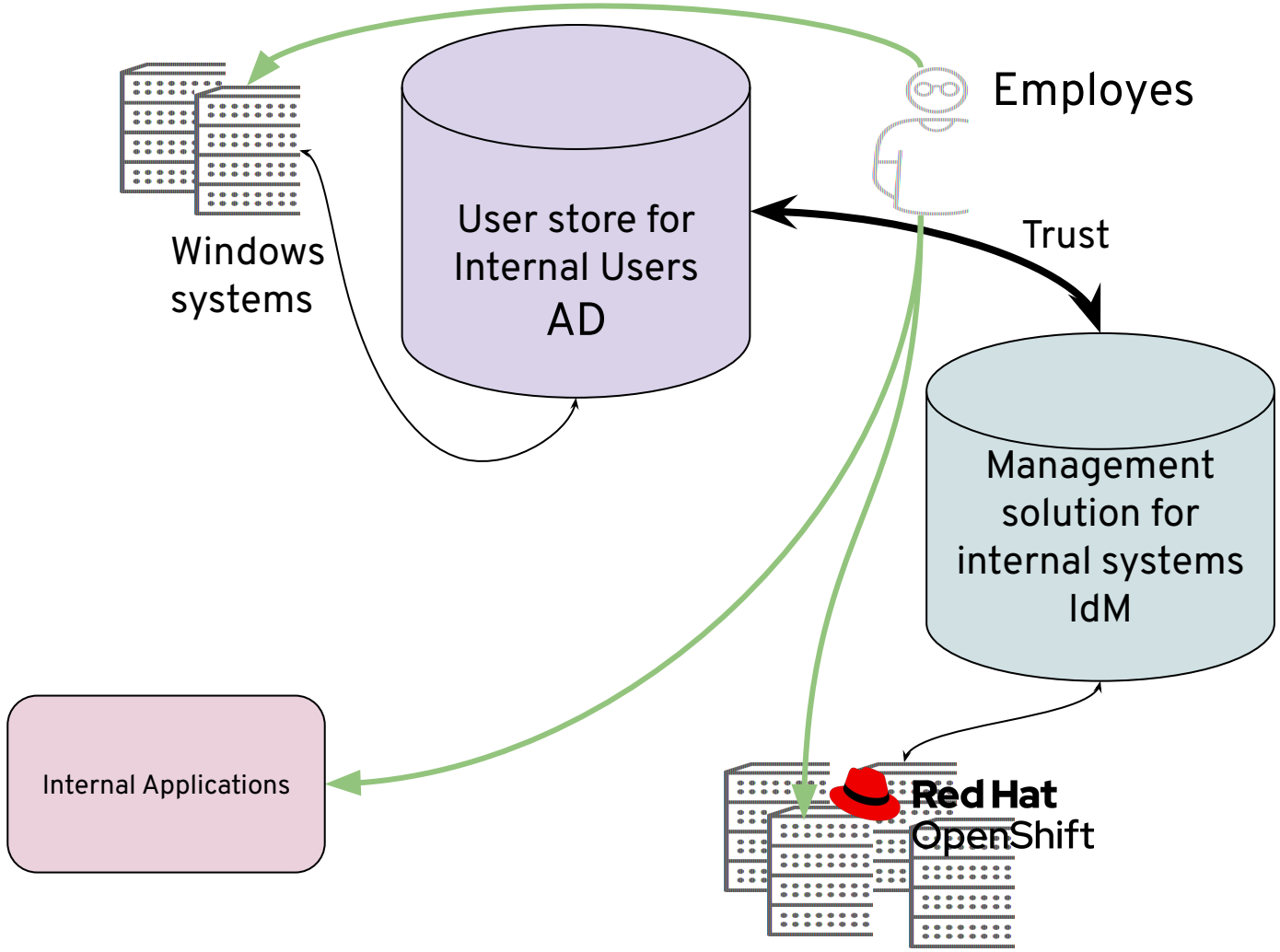
https://access.redhat.com/articles/1586893

Recommended Architecture

Employes

Recommended Architecture

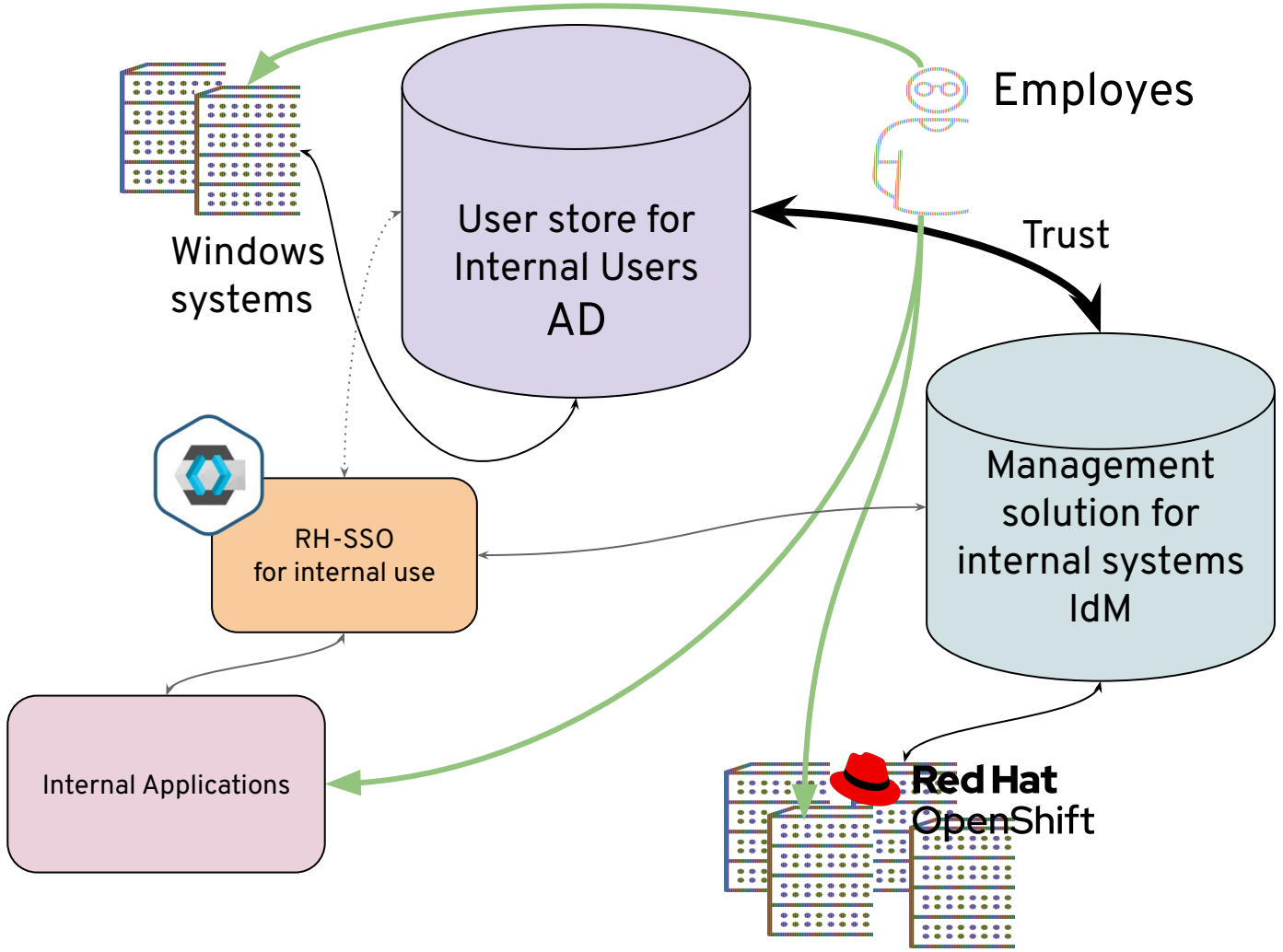
Recommended Architecture



Red Hat

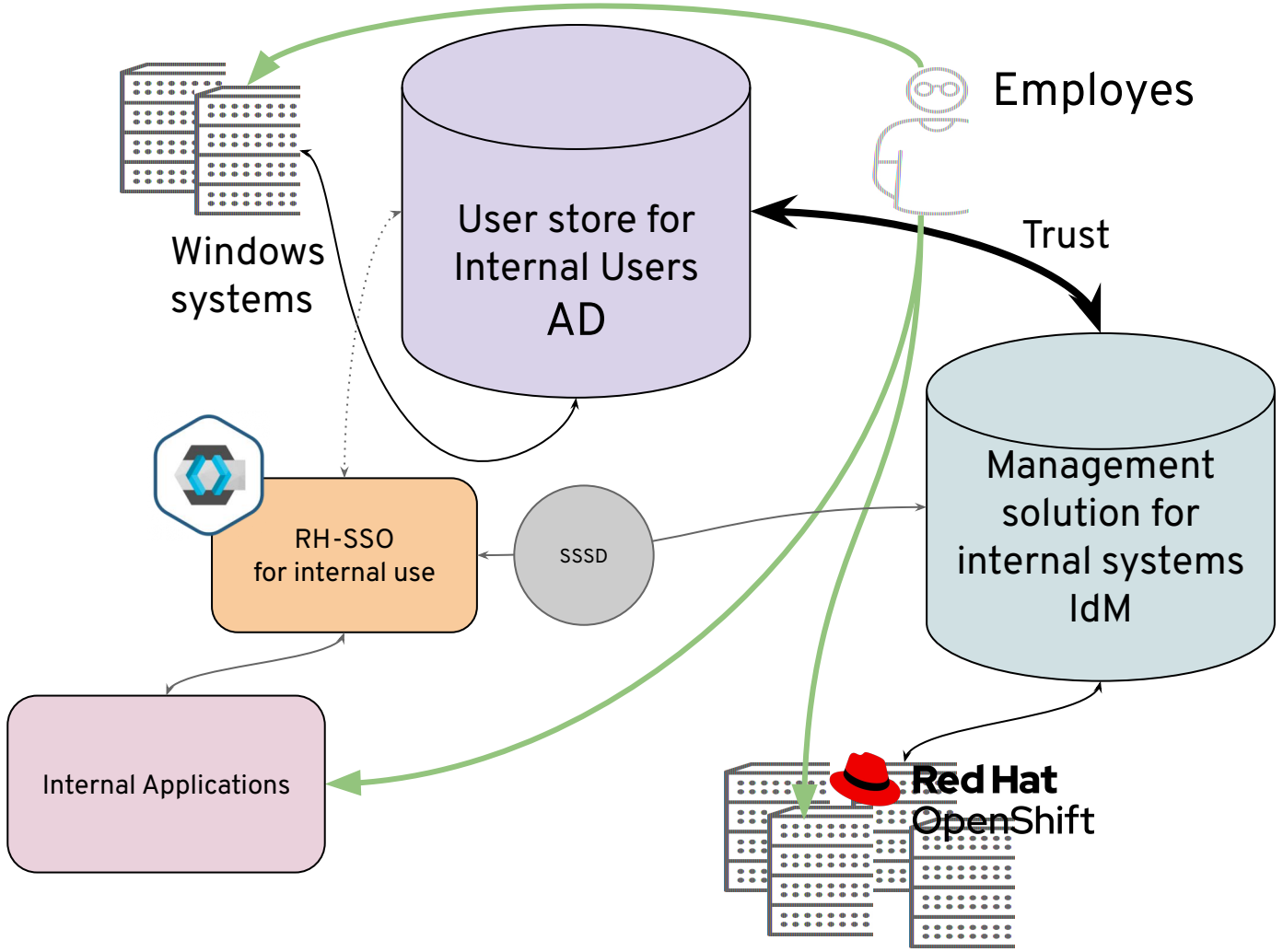
Single Sign-On / Keycloak

Recommended Architecture



Red Hat

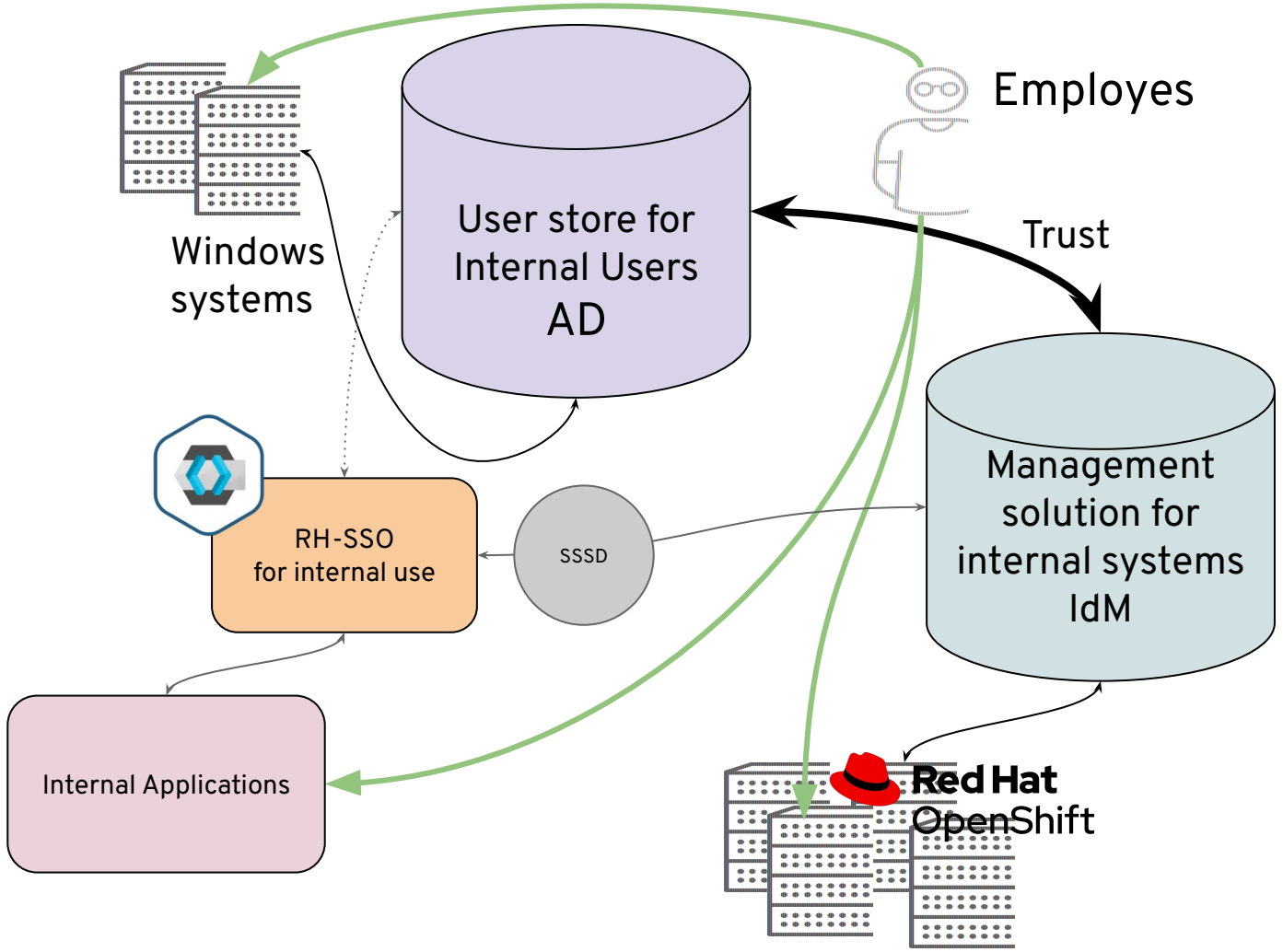
Recommended Architecture



Red Hat

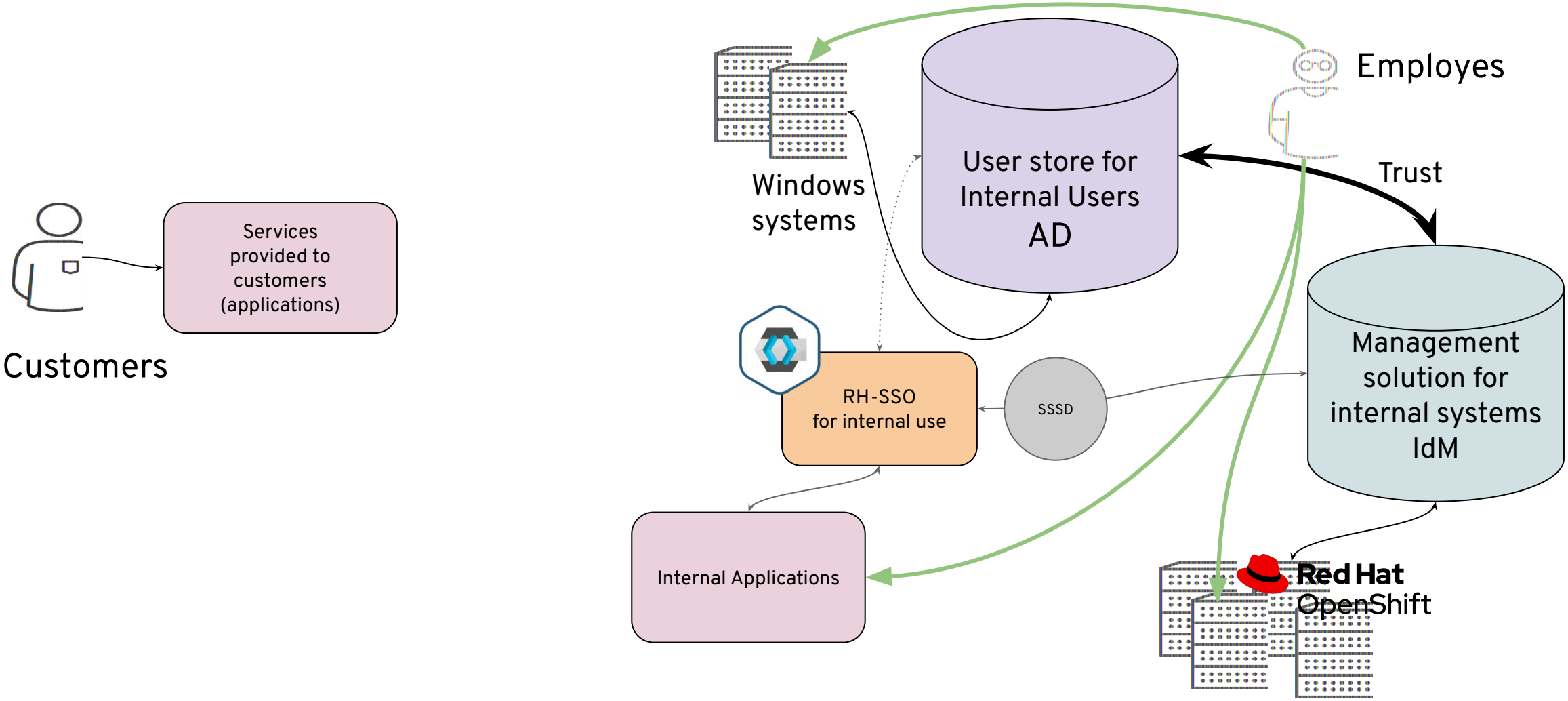
Recommended Architecture

Customers



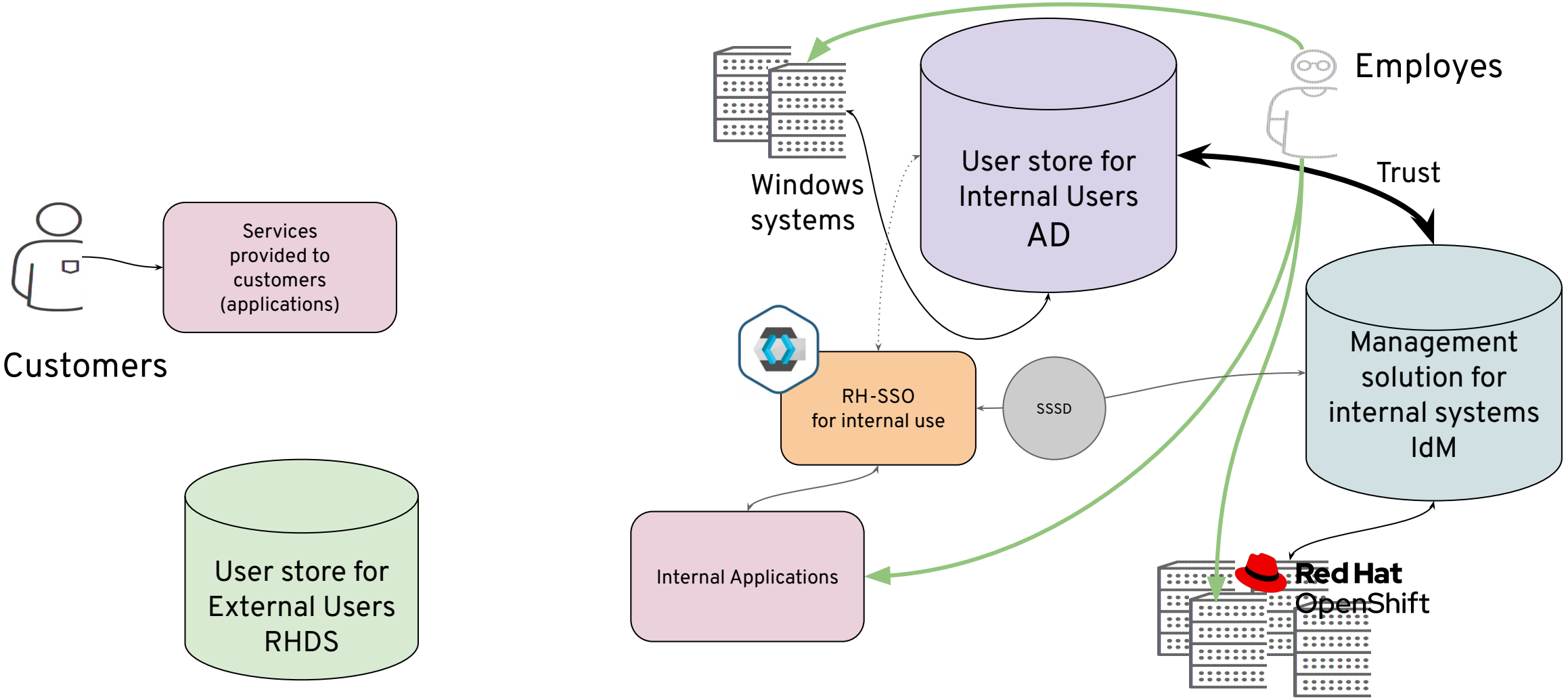
Red Hat

Recommended Architecture



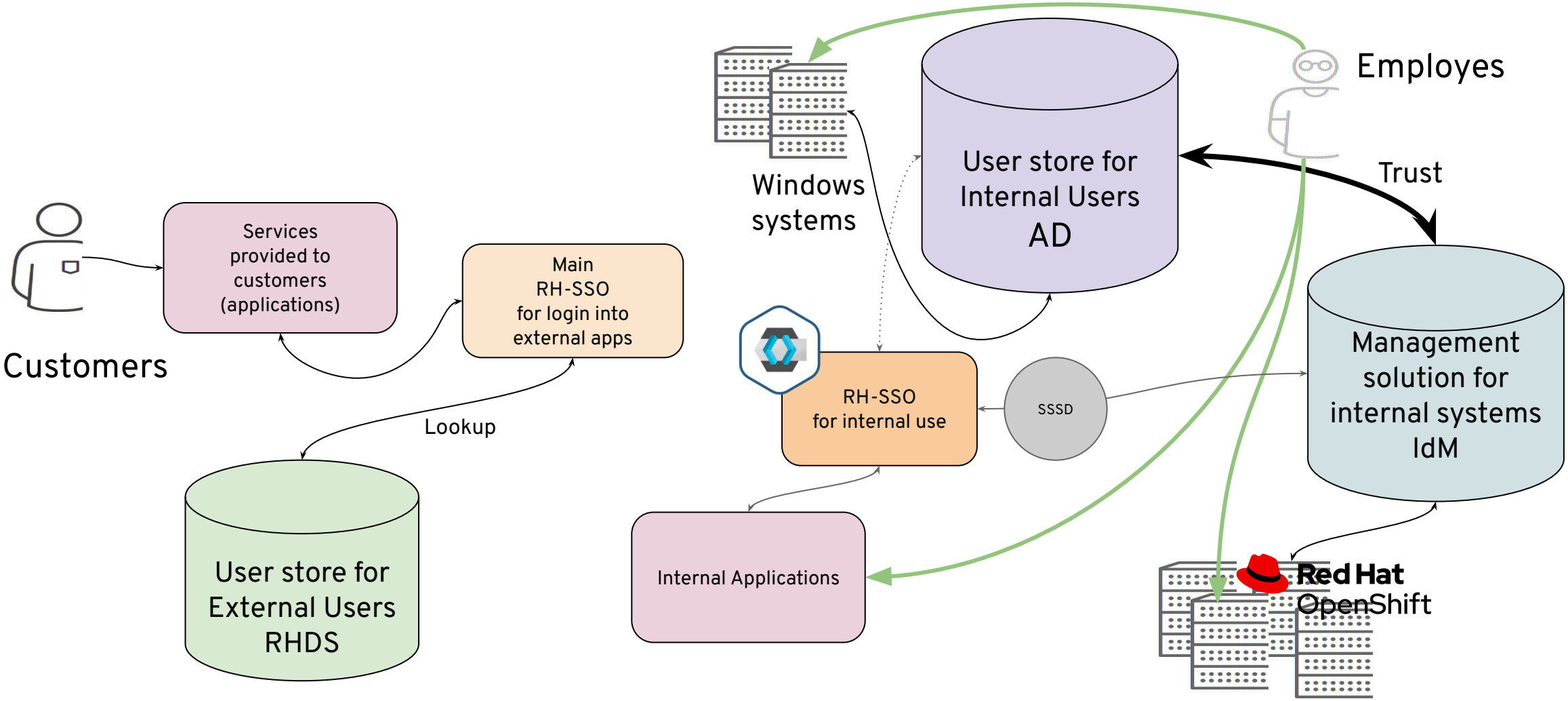
Red Hat

Recommended Architecture



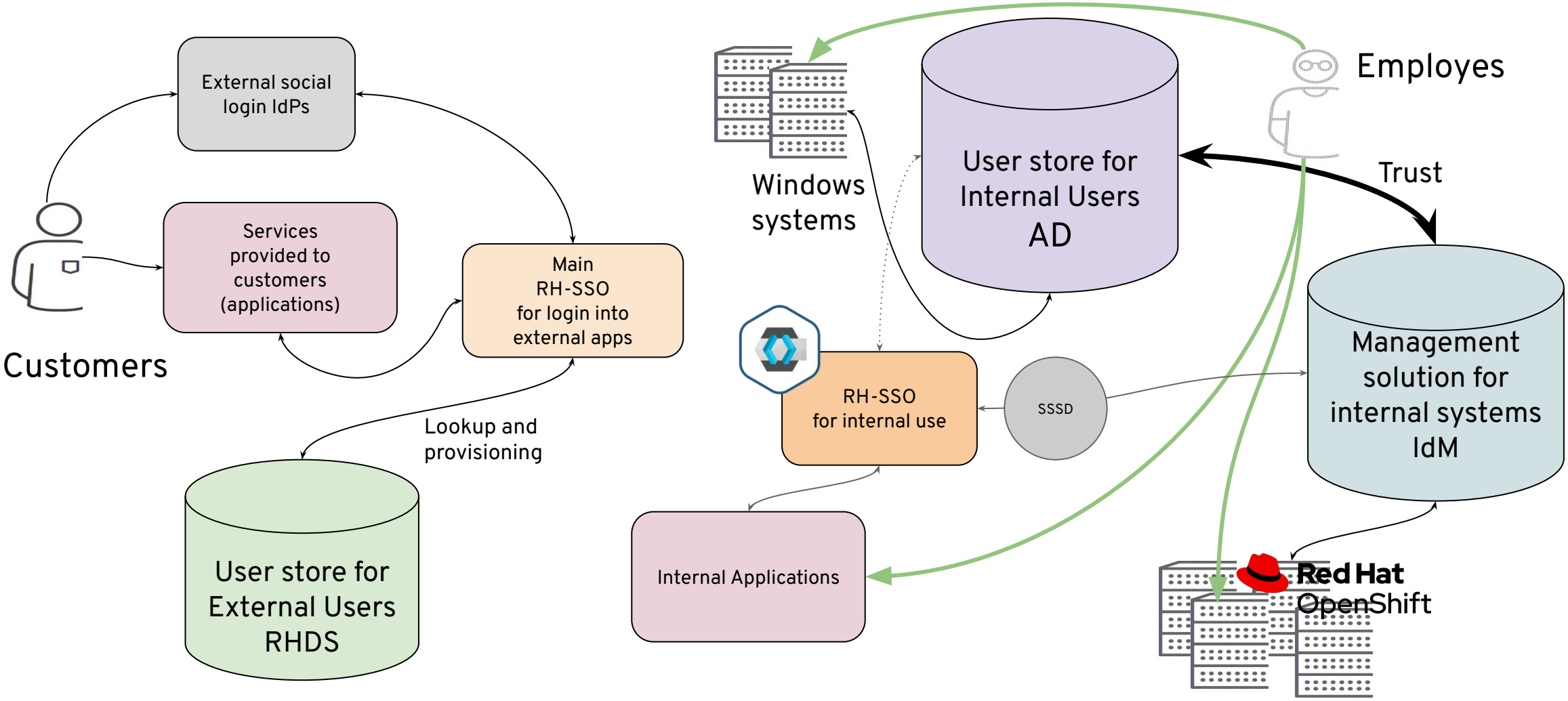
Red Hat

Recommended Architecture



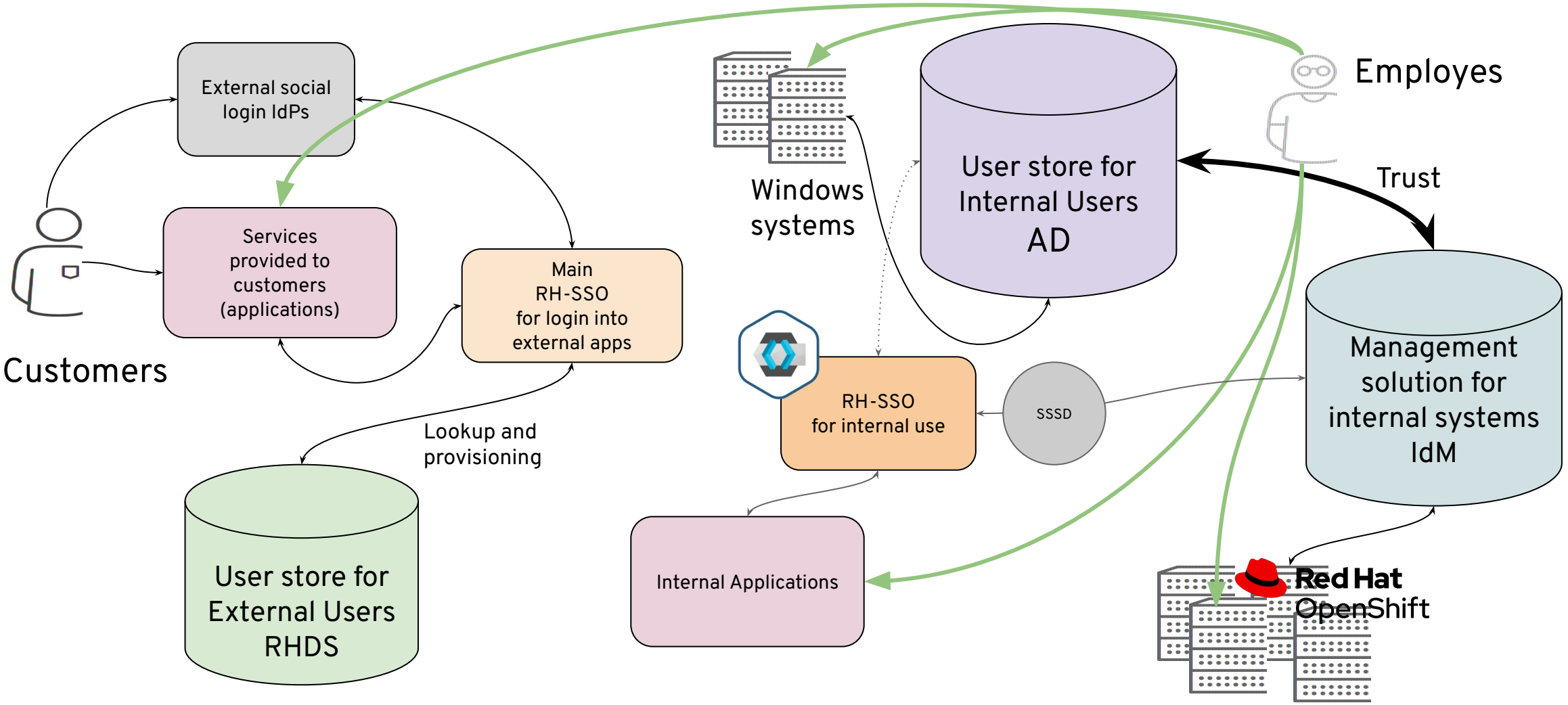
Red Hat

Recommended Architecture



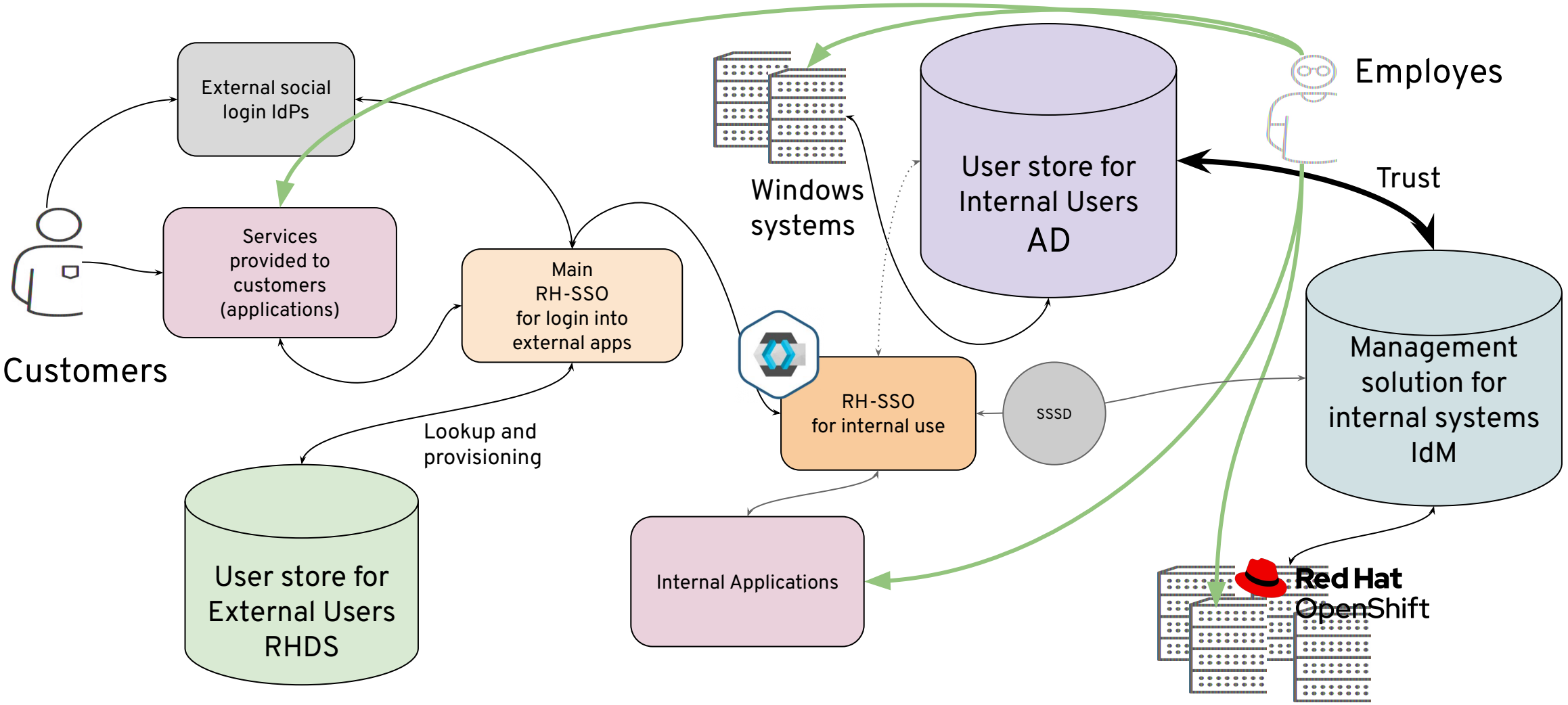
Red Hat

Recommended Architecture



Red Hat

Recommended Architecture



Red Hat

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat