Red Hat Identity Management(IdM) ご紹介

Red Hat K.K. Solution Architect
Kazuo Moriwaka <kmoriwak@redhat.com>
2017-10-16

redhat.

10秒で伝えるIdentity Management

RHELやUNIX環境むけのActive Directoryのようなドメイン管理システムです。
ホスト、ユーザー、グループの管理をしてシングルサインオンでき、ADと連携させることも可能です。
ssh、sudo、selinuxなどLinux/UNIXむけの機能が充実しており、アプリケーションからの利用もできます。

解決したい課題

- 多くの会社で……
  - WindowsはActive Directory(AD)でドメイン管理
- Linuxも同じように管理したい
  - LinuxそのものやLinux上のアプリケーションへ、シングルサインオンさせたい
  - ポリシーも集中して管理したい

どうやって統合しよう?

Red Hat Identity Management

- 「Red Hat Identity Management」はLinux/UNIX向けアイデンティティ管理基盤であるFreeIPAを製品化
- 主な機能
  - LDAPによるアイデンティティ情報保持
  - Kerberosによる認証
  - DNSによる名前解決
  - sudoer, HBAC, automountの集中管理
  - Active Directory との連携

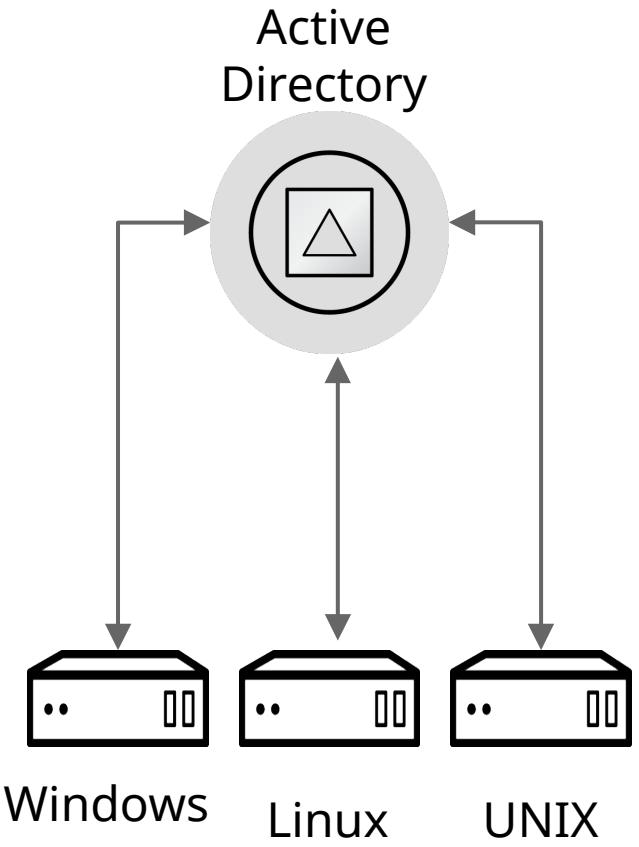
既存の他の選択肢

- Samba winbind
  - 現在よく使われている
  - セキュアに設定するのが難しい
  - sudoやsshなどLinux/UNIX独特の機能はサポートなし
- サードパーティSSO製品
  - Centrify, HPE IceWall, Tivoli Access Manager, OpenAM, Oracle Access Manager など
  - 追加コスト(2000〜10000円/アカウントくらい)

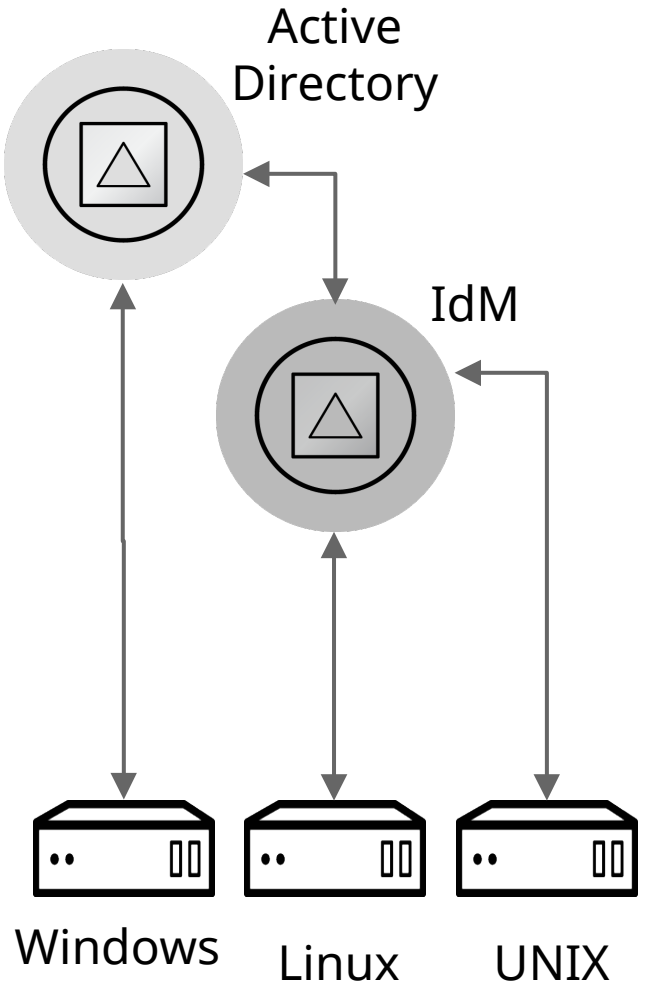
なぜRed Hat Identity Management?

- Samba winbindより機能が充実
  - HBAC管理、sudo, ssh対応等
- IdMはRHELに同梱で追加費用なし
  - RHEL最新バージョンへも追随
- RHELを“out of the box”の状態でAD環境へスムーズに統合
  → RHEL6からIdentity Managementを同梱

Active Directoryとの連携

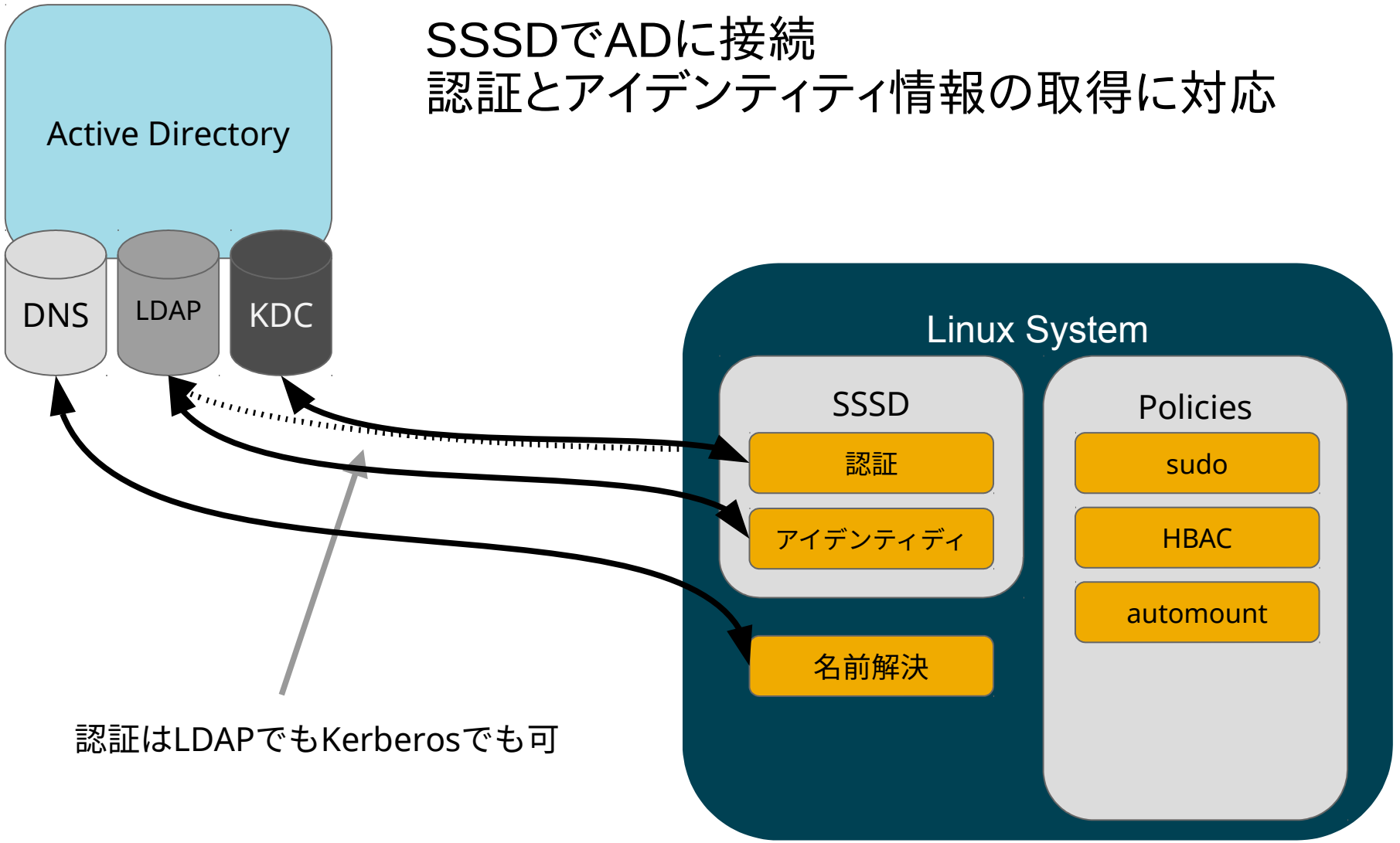


SSSDによる直接的な統合
Active Directoryで
Linux/UNIXの認証

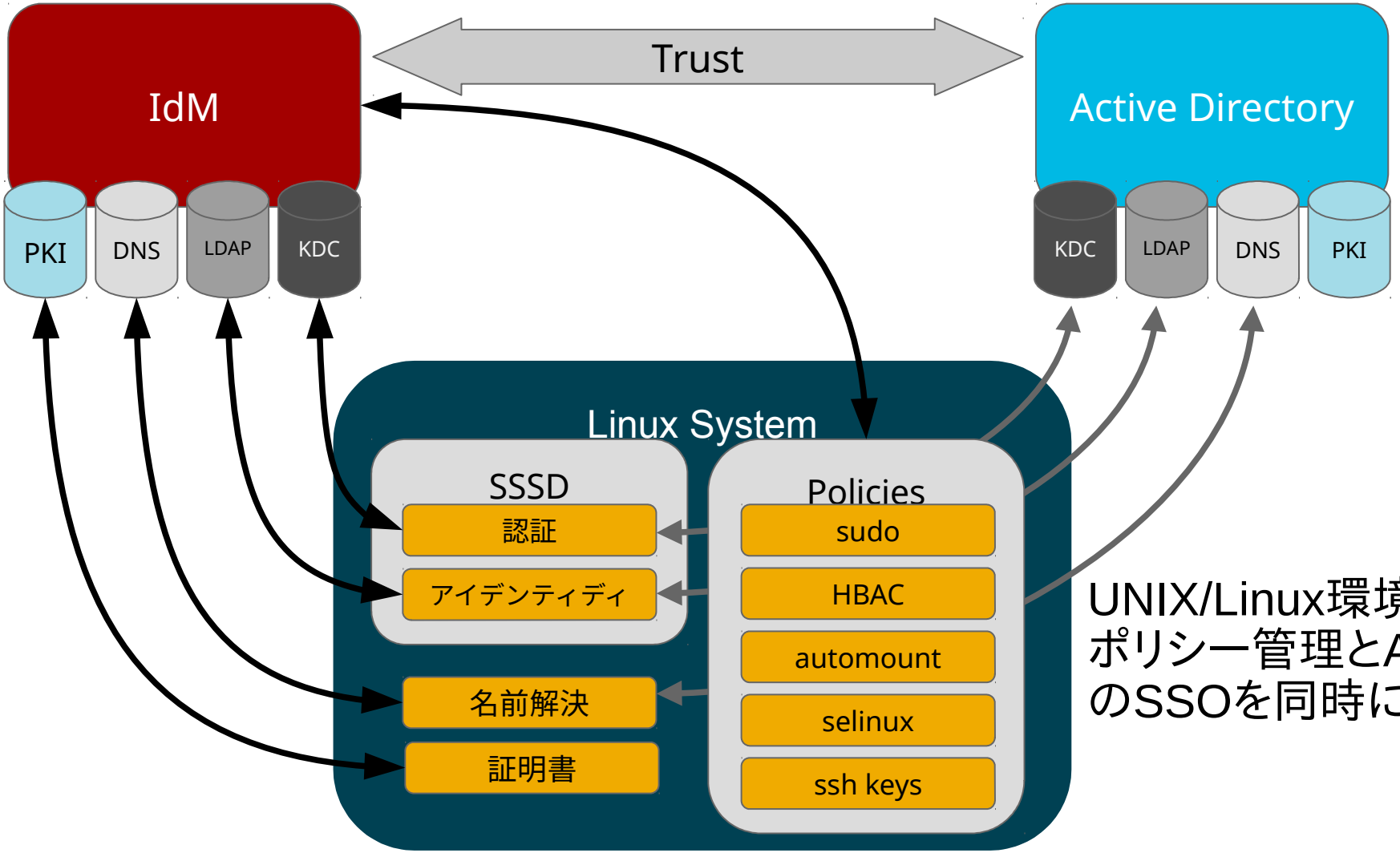


IdMによる間接的な統合
WindowsはActive Directory
Linux/UNIXはIdMで認証

SSSD による直接的な統合



信頼ベースのIdM - AD統合



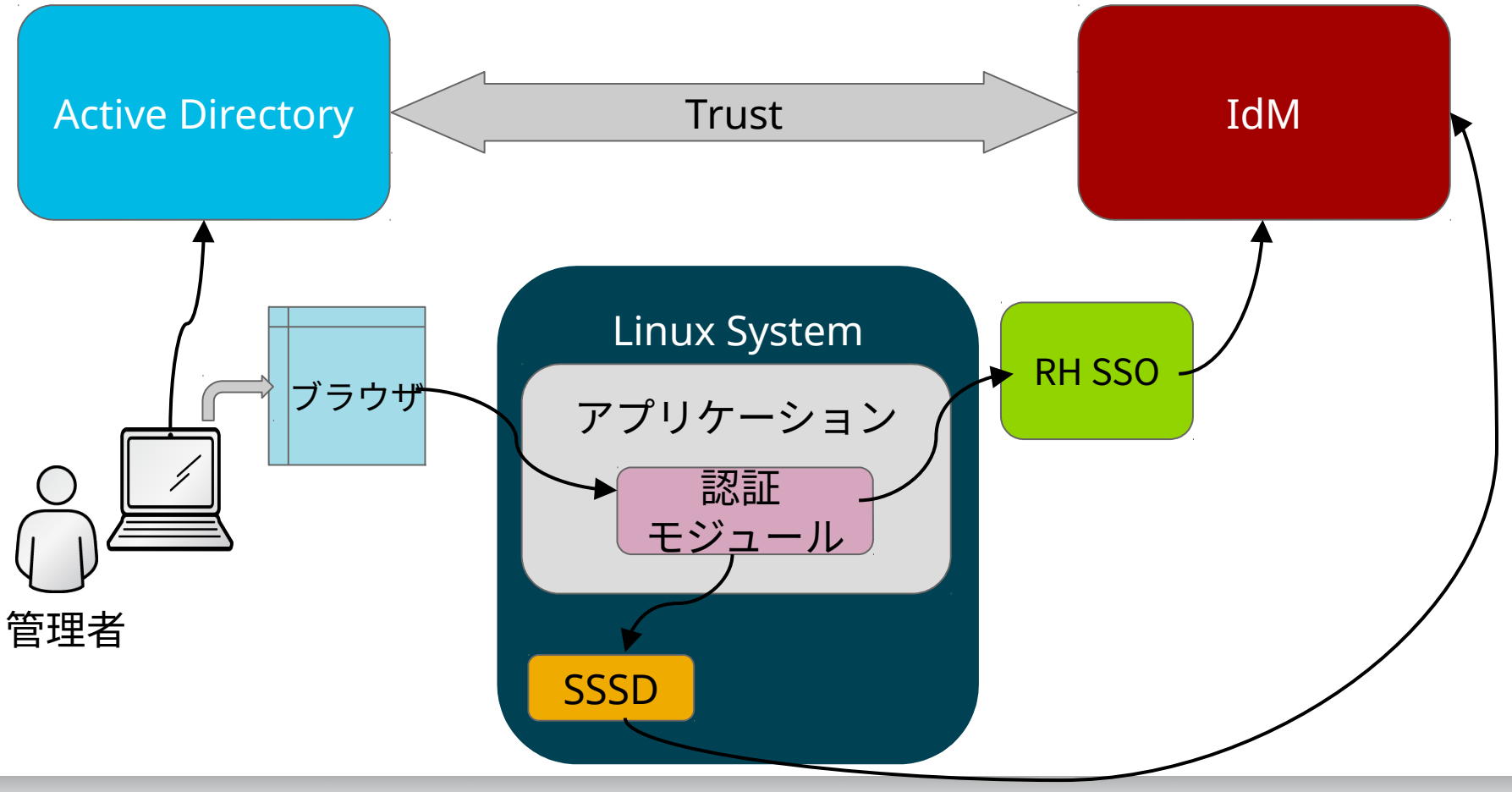
UNIX/Linux環境用のポリシー管理とADからのSSOを同時に実現。

他製品/サービスとの関連

- Red Hat製品との統合が徐々に進んでいます
  - 基本的なログインには全製品で適用可能
  - IdMとの統合作業が予定されている製品: CloudForms, Satellite, OpenShift, RHOSP, RH SSO
- アプリケーション連携はupsteramのhowtoが詳しい
  - http://www.freeipa.org/page/HowTos

アプリケーション認証統合のイメージ

LDAP, Kerberos, PAM対応app → IdMへ直接またはSSSD経由で認証
SAML, Open ID Connect対応app → RH SSO経由で認証



ユーザー事例

- アメリカ証券取引委員会(SEC)
  - 複数バージョンのRHEL、Solarisを含む1000台以上のシステムを利用
  - 数千アカウント、HBAC利用
  - ユーザ作成の待ち時間を短縮

まとめ

Red Hat Identity ManagementはRHELやUNIX環境むけのActive Directoryのようなドメイン管理システムです。
ホスト、ユーザー、グループの管理をしてシングルサインオンでき、ADと連携させることも可能です。
ssh、sudo、selinuxなどLinux/UNIXむけの機能が充実しており、アプリケーションからの利用もできます。