Red Hat Enterprise Linuxの認証基盤 Identity Management

Red Hat K.K. Solution Architect
Kazuo Moriwaka <kmoriwak@redhat.com>
2016-12-21

redhat.

このスライドの位置づけ

- 前提
  - RHELに同梱のIdentity Managementが割とよいのにあまり使われていなさそう……
- 対象
  - 「RHEL同梱の認証基盤って聞いたことないけどなにができるの?」という人
- 目的
  - 「RHEL IdMでだいたいこんなことができそう」というイメージを持ってもらう
  - 利用手順などは扱いません

Agenda

- 「Identity Management」で扱うもの
- Identity Managementの目標
- 主なコンポーネント
- Identity Managementの概要
  - Kerberosによる企業内ユーザへのSSO提供
  - Active Directoryとの連携
  - Host based Access Control
  - ユーザとホストのSSH鍵管理
  - sudo, SELinux ユーザマッピング、automountの集中管理
  - ユーザ、ホスト、デバイス、サービスの証明書管理
  - 二要素認証
  - SAMLによるシングルサインオン

「Identity Management」って何?

- Red Hat Enterprise Linuxに同梱されるアイデンティティ管理基盤
  - LDAPによるアイデンティティ情報管理
  - 認証
    - パスワード認証、スマートカード認証
    - ワンタイムパスワード対応
    - Active Directoryとのクロスレルム認証
  - 証明書発行
  - PAM/NSSとの統合
  - Apacheモジュールによるwebアプリケーションとの統合
  - Linux/UNIX環境用の機能
    - sudoer, automount, ssh鍵管理

    ……などをシンプルな操作で実現します

「Identity Management」で扱うもの (1/2)

- アイデンティティ
  - ユーザ情報がどこにあるか?
  - どのような属性をもっているか？
  - システムやアプリケーションからこれらのデータへどのようにアクセスするか？
- 認証
  - ユーザーは認証にどのようなクレデンシャルを利用するか?
    - パスワード? スマートカード? 特殊なデバイス?
  - シングルサインオンはあるか?
    - どうやって同じユーザがファイルサーバとwebアプリケーションに認証しなおしせずにアクセスするか?

「Identity Management」で扱うもの (2/2)

- アクセスコントロール/認可
  - どのユーザがどのシステム・サービス・アプリケーションにアクセスできるか?
  - sudoでどのコマンドを実行できるか?
  - ユーザはどのSELinuxのコンテキストに対応するか?
- ポリシー
  - パスワードの強度は?
  - automountのルールは?
  - Kerberos ticketのポリシーは?

Identity Managementの目標(1/2)

- アイデンティティ管理基盤をシンプルに提供する
- PCI DSS, USGCB, STIGなどの基準に合致する基盤を提供する
- 認可されないアクセスや認可されていない権限昇格のリスクを減らす
- ダイナミックでスケーラブルな基盤を提供する
  - 最大60ノードのマルチマスタまでサポート
- 新しいシステムのデプロイメントを自動化する

Identity Managementの目標(2/2)

- 日々の運用コストを削減する
- 基盤にかかるコストを削減する
- 企業の混在環境全体にわたるシングルサインオンを提供してユーザ体験を向上する
- アイデンティティ管理基盤とアプリケーションの緊密な統合を可能にする
- アイデンティティ情報とユーザ・サービス・システム・デバイスの認証情報を管理する

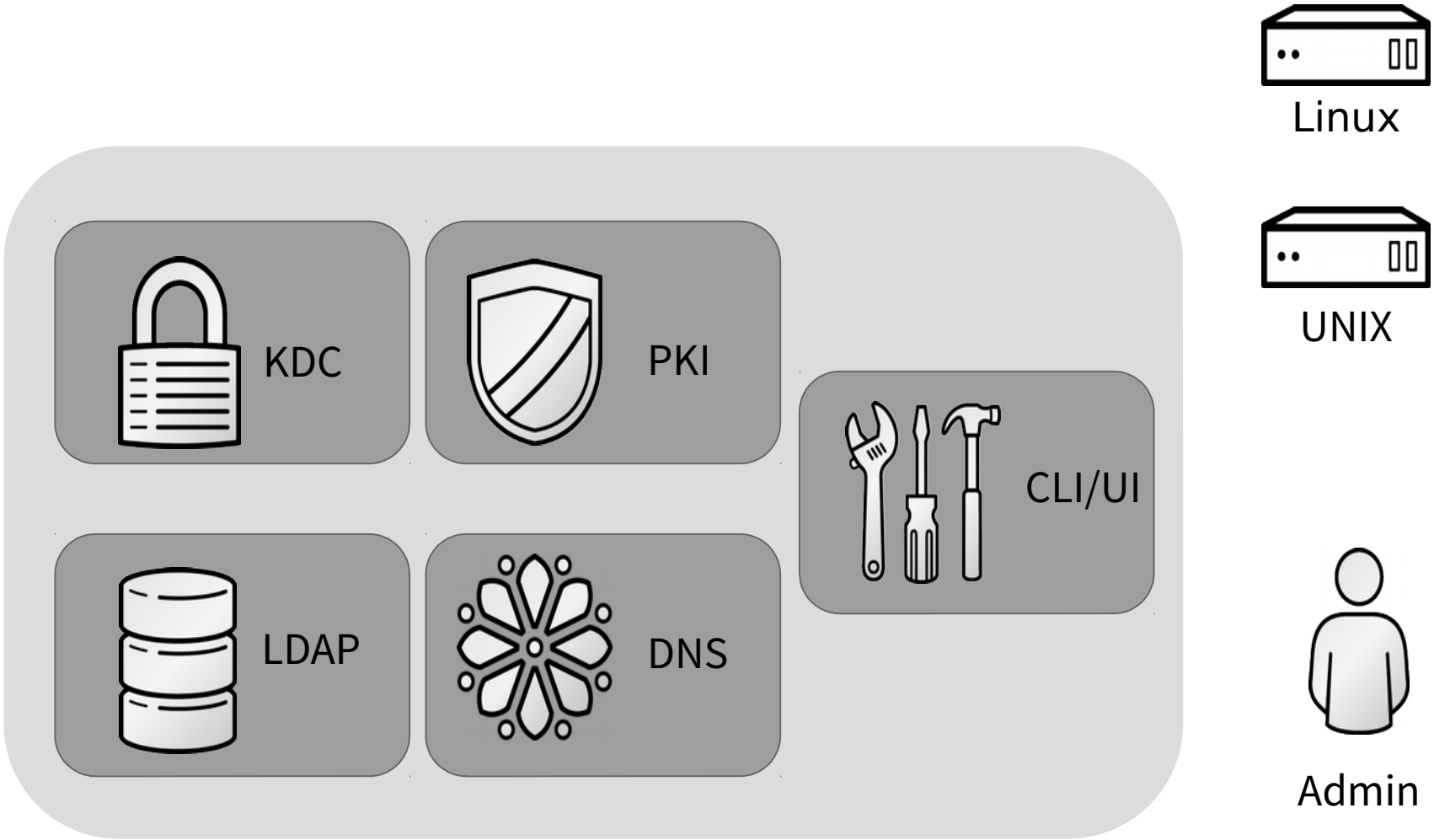
Identity Managementの主なコンポーネント

- Identity Management (FreeIPA/IdM)
  - 以下を統合
    - MIT Kerberos
    - 389 Directory Server
    - Dogtag Certificate System
    - BIND
- SSSD
- Certmonger
- Keycloak IdP (Red Hat SSO)
- Apacheモジュール

FreeIPA/IdM

- Linux/UNIX環境用のドメインコントローラ
  - 「Linuxドメイン」を作成・管理
- OSSプロジェクトFreeIPAがベース
- LDAP, Kerberos, DNS, 証明書管理を統合
- Linux/UNIX環境むけの認証、認可、アイデンティティ情報の集中管理
- ポリシーと権限昇格(sudo)の管理
- Active DirectoryサーバとIdMサーバでの連携
- Web UI, CLI, APIによる管理

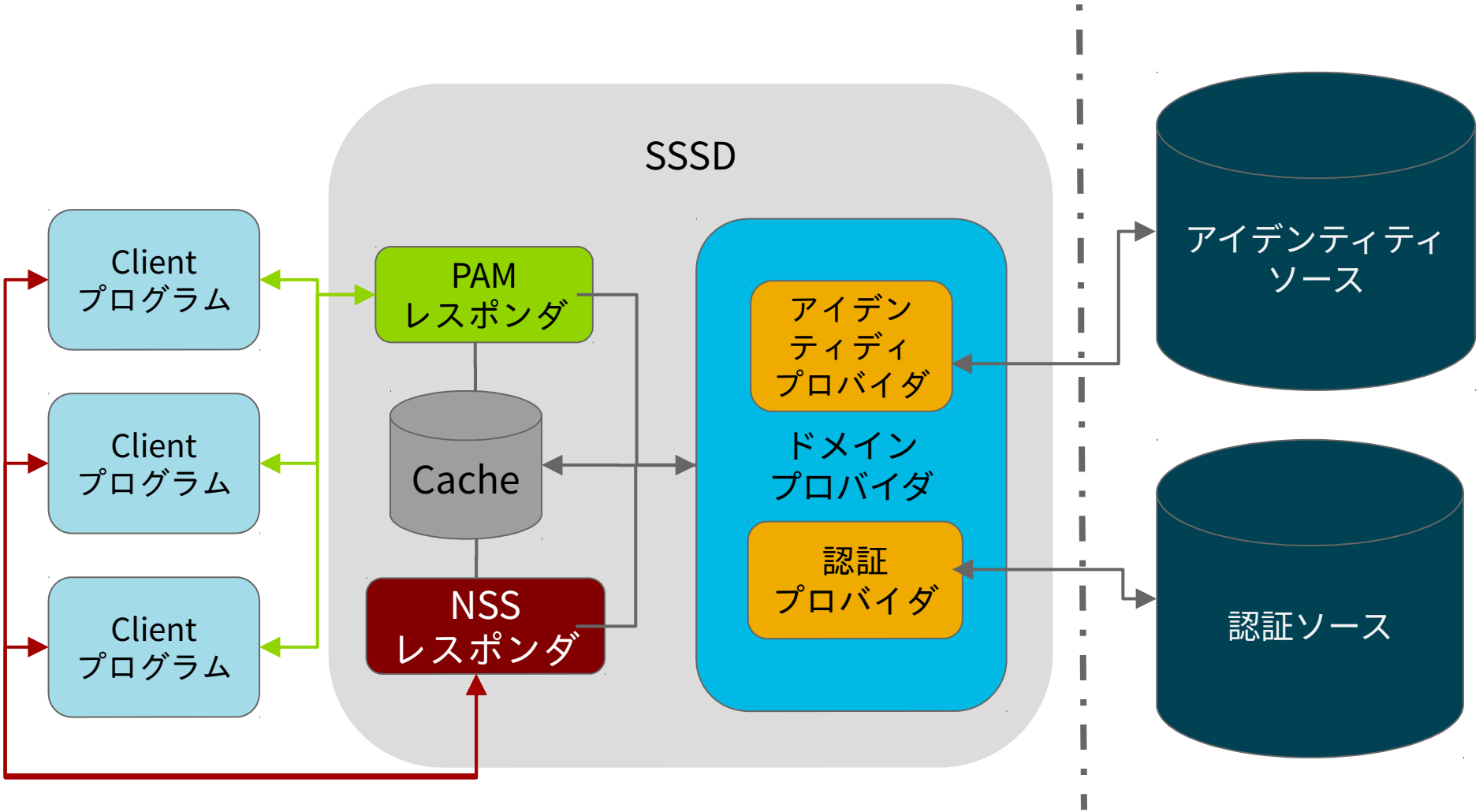
FreeIPA/IdM



SSSD (System Security Services Daemon)

- クライアント側のコンポーネント
- Red Hat Enterprise Linuxや他のLinuxディストリビューションに同梱
- アイデンティディソースおよび認証ソースとの接続を管理
- アイデンティティとポリシー情報のキャッシュ
- 複数のアイデンティティソースを同時に利用可能

SSSD 概要図



Certmonger

- クライアント側のコンポーネント
- 認証局サーバに接続して証明書をリクエストする
- 証明書を追跡して自動更新する

Keycloak IdP (Red Hat SSO)

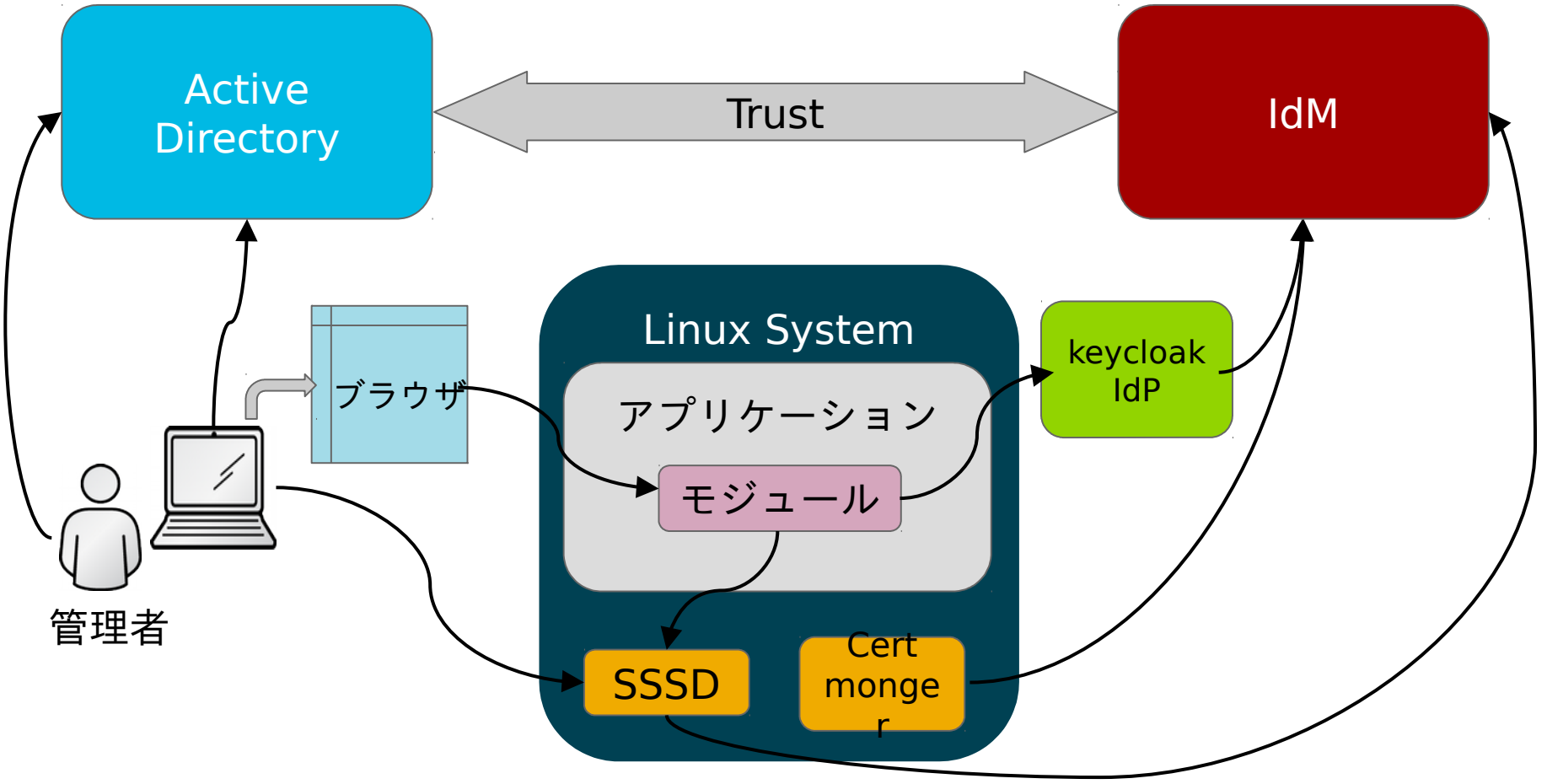
- アイデンティティプロバイダの実装
- 異なるWebアプリケーション間で SAML, OpenID Connect, OAuthベースのシングルサインオンとIDフェデレーションを提供

  ※Keycloak IdPはRHELではなくJBoss EAPに同梱

Apacheモジュール

- Apache httpdで利用されるモジュール
- フォームベース認証、Kerberos認証、証明書ベース認証、SAML認証をサポートするモジュールを提供
  - OpenID Connect認証については作業中
- 認可およびアイデンティティ情報の参照も対応するモジュールにより可能

アーキテクチャの例

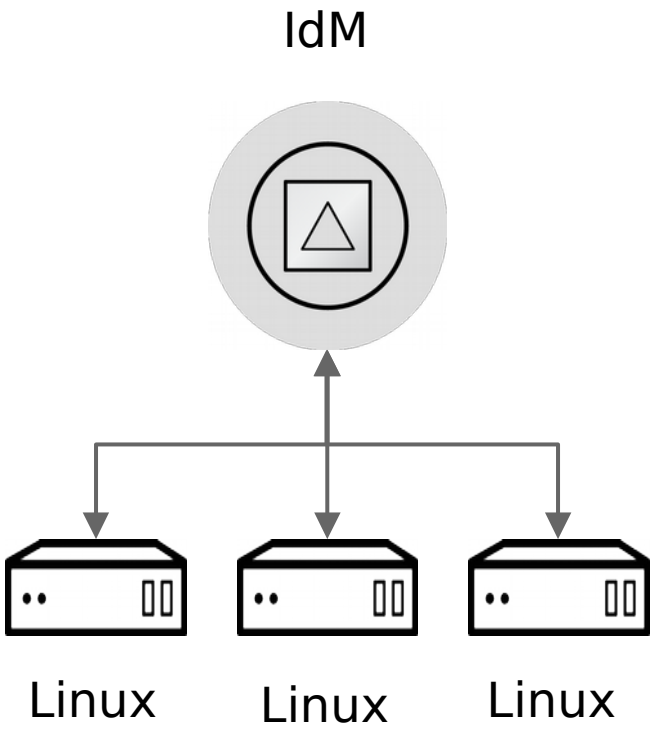


Identity Managementの概要

Identity Managementの概要

- Kerberosによる企業内ユーザへのSSO提供
- Active Directoryとの連携
  - SSSDによる直接的な連携
  - IdMを利用する間接的な連携
- Host based Access Control
- ユーザとホストのSSH鍵管理
- sudo, SELinux ユーザマッピング、automountの集中管理
- ユーザ、ホスト、デバイス、サービスの証明書管理
- 二要素認証
- SAMLによるシングルサインオン

認証



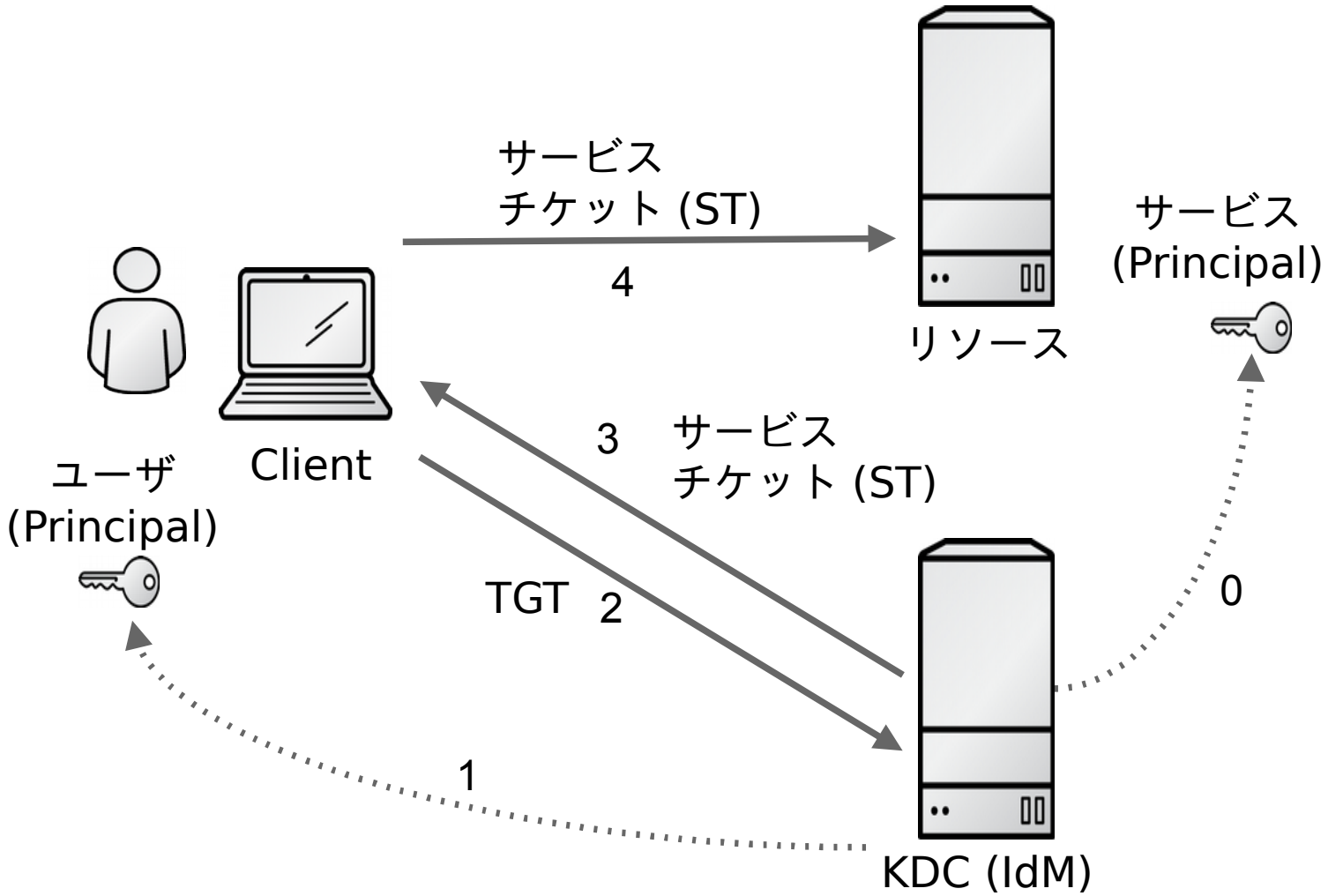
ステップ:

- ユーザアカウントを統合
- ユーザデータをIdMへロード
- Linux/UNIXシステムをIdMへ接続
  - ipa-client-install

なぜIdMか?

- 複数の認証方式をサポート:
  - LDAP, Kerberos, OTP, 証明書
- 統合されたソリューション
  - インストールと管理が容易
- Active Directoryとの統合
- Linuxホストのセキュリティ管理を強化

Kerberosによるシングルサインオン

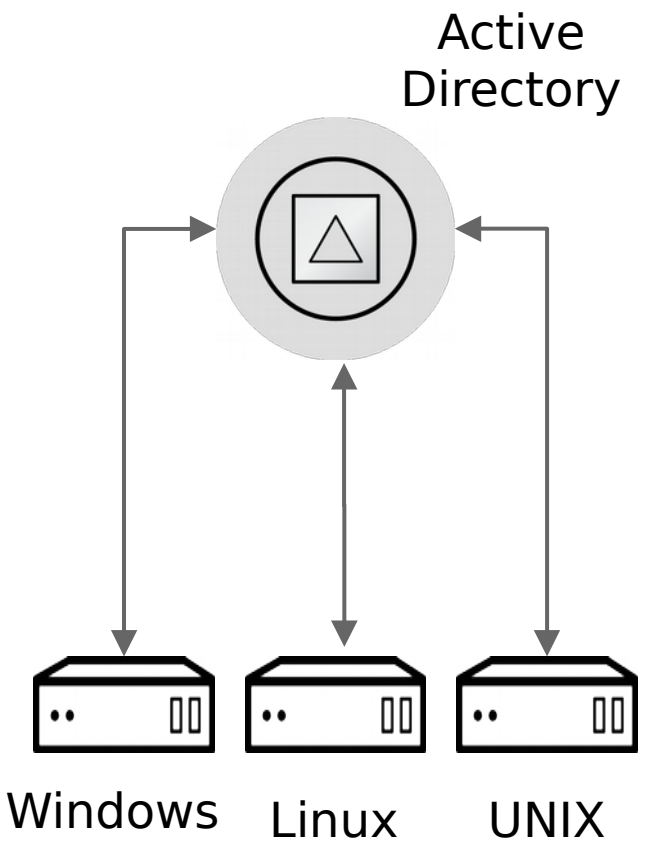


Kerberosによる認証のフロー

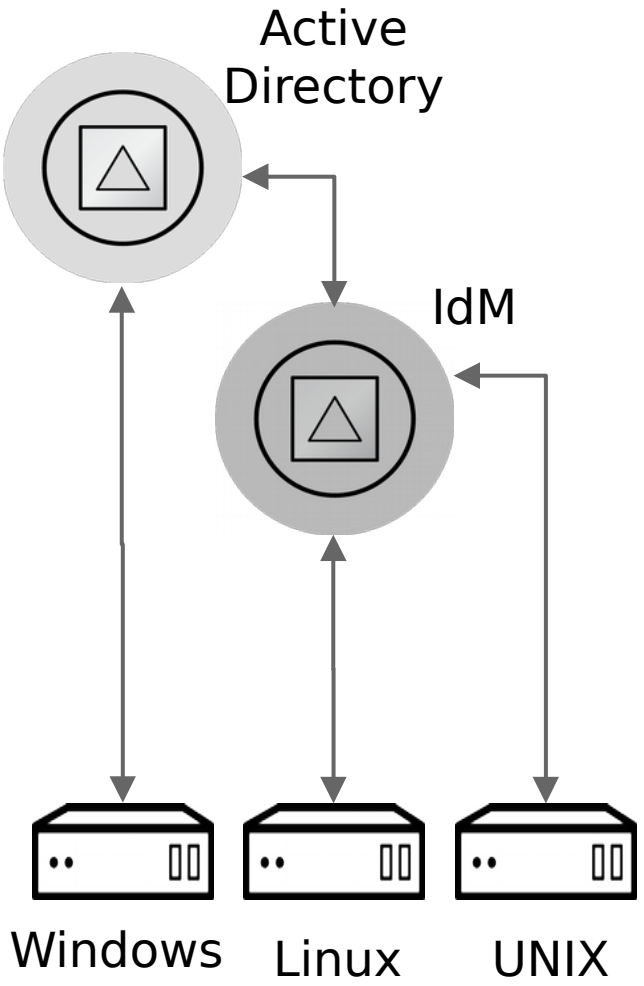
- あらかじめサービスの鍵を作成してkeytabへ登録(0)
- Kerberosに接続されたシステムにユーザがログイン(1)
  - Kerberos KDC, Active Directory, IdMのいずれも可
  - ユーザはこのとき ticket granting ticket (TGT) を取得
- ユーザ(例: NFSクライアント)がリソースにアクセス
- Kerberosライブラリがサービスチケットを KDCに要求(2 - 3)
- サービスチケットをサービス(例: NFSサーバ)へ提示 (4)
- サーバはkeytabに格納された鍵でチケットを復号

※鍵はインストール・設定時に配布され、必要に応じて更新される

Active Directoryとの連携

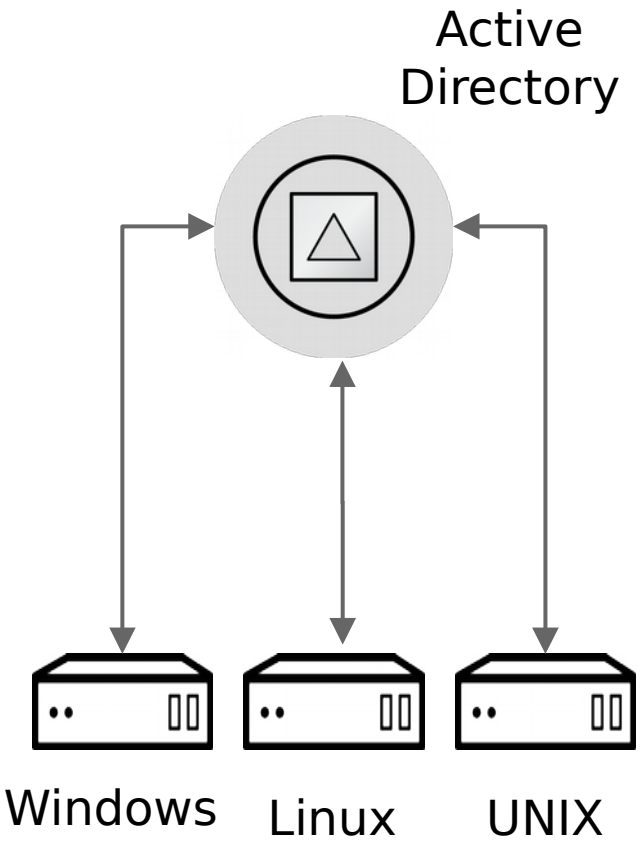


直接的な統合
Active Directory
でLinux/UNIXの認証



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

直接的な統合



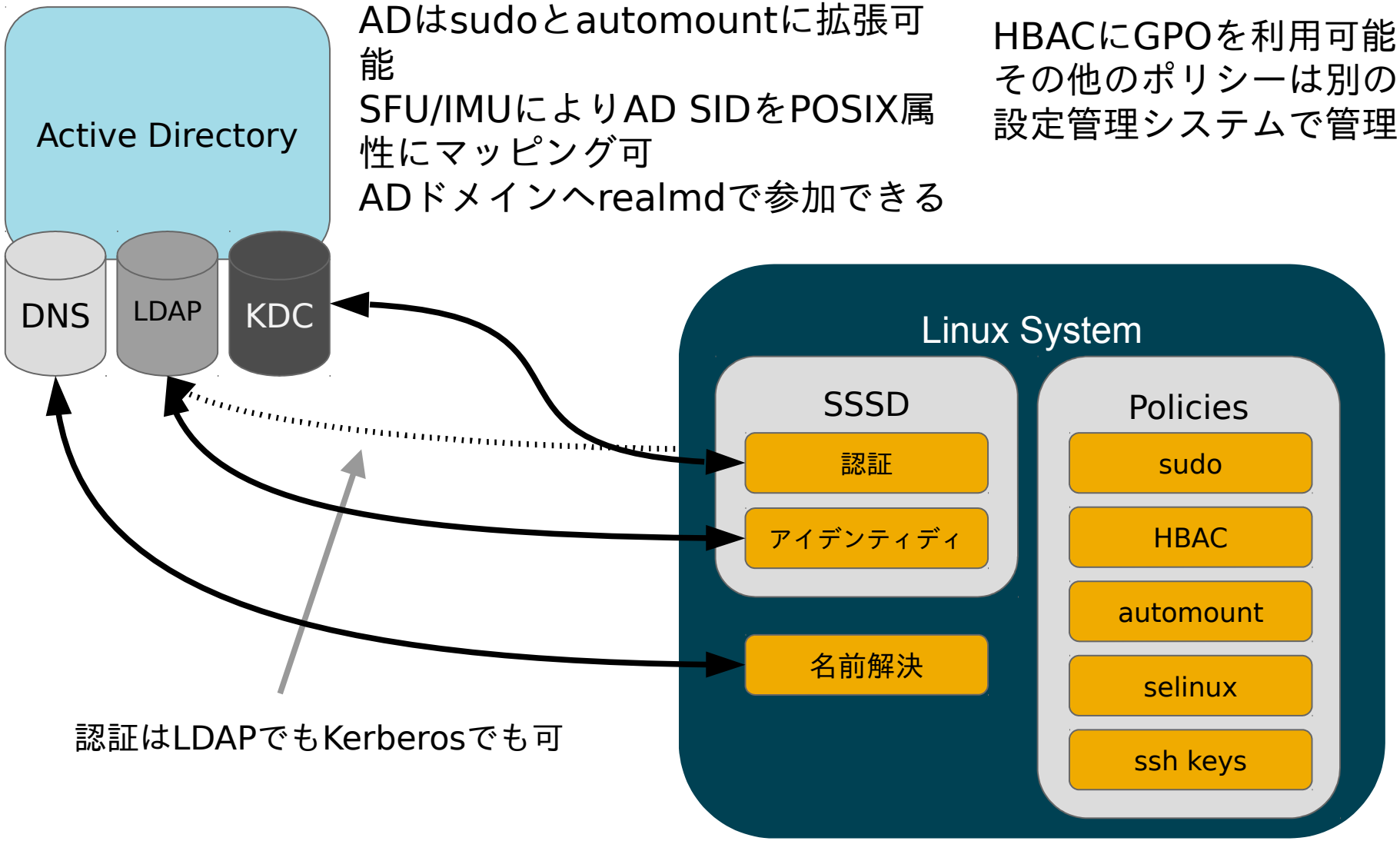
- Active Directoryドメインに Linux/UNIXを参加させる
- Linux/UNIXの台数が少ない場合には簡便な方法

ドキュメント:
- http://red.ht/2h4QGL6

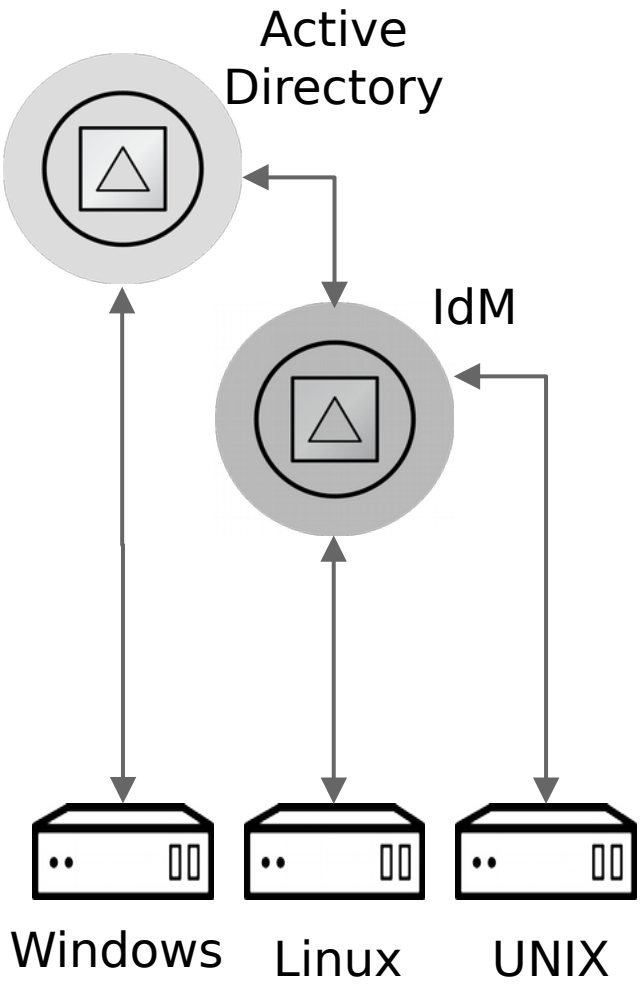
直接的な統合のオプション

- サードパーティ製品を利用する
- 以前からある方法
  - pam_krb5/pam_ldap, nss_ldap, nslcd
  - winbind
- 新しい方法
  - SSSD (with realmd)

SSSD による直接的な統合



間接的な統合



- Active DIrectoryと Identity Managerを連携
- IdMのLinuxドメインに Linux/UNIXを参加させる

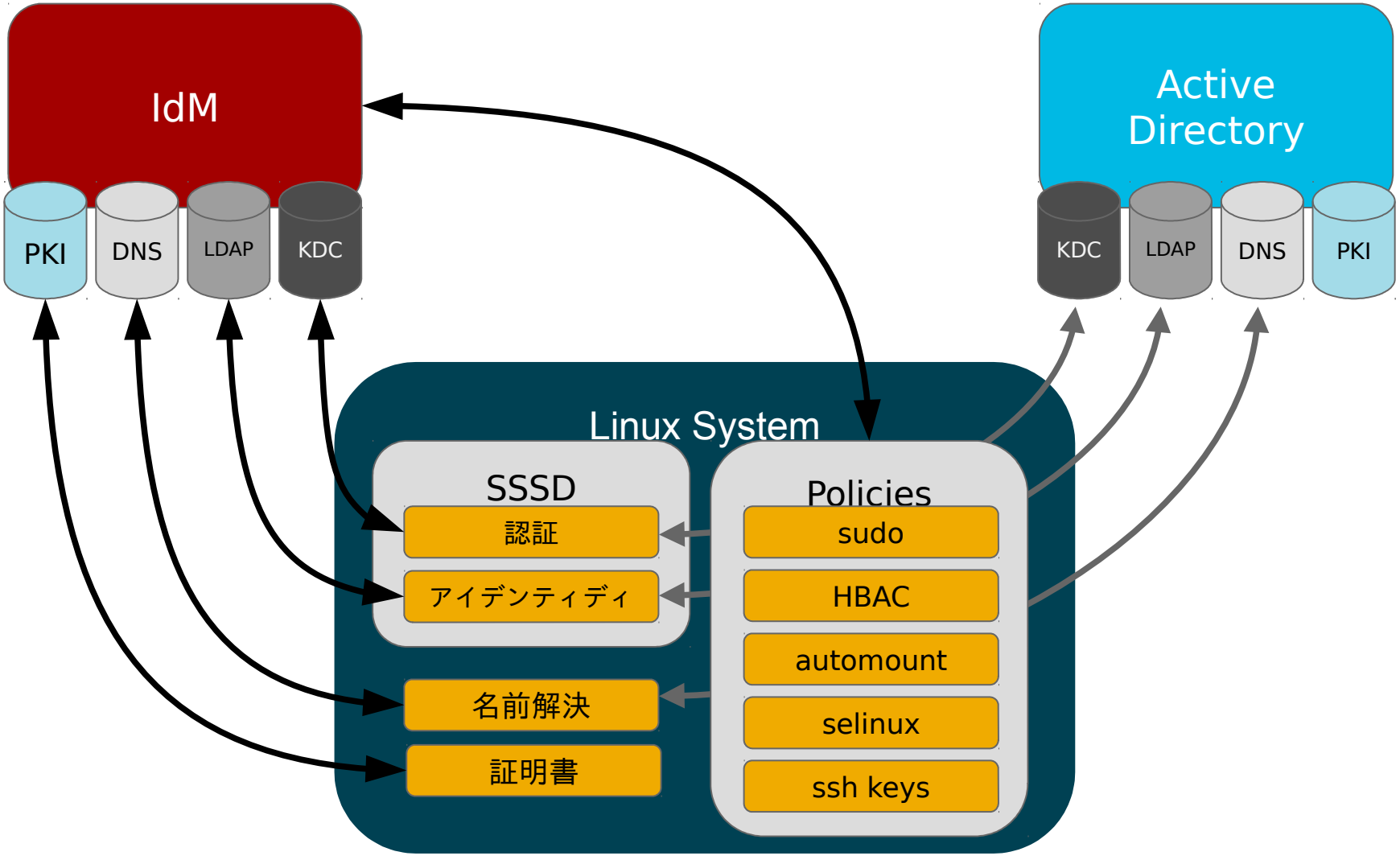
ドキュメント:

- http://red.ht/2hOdrSg

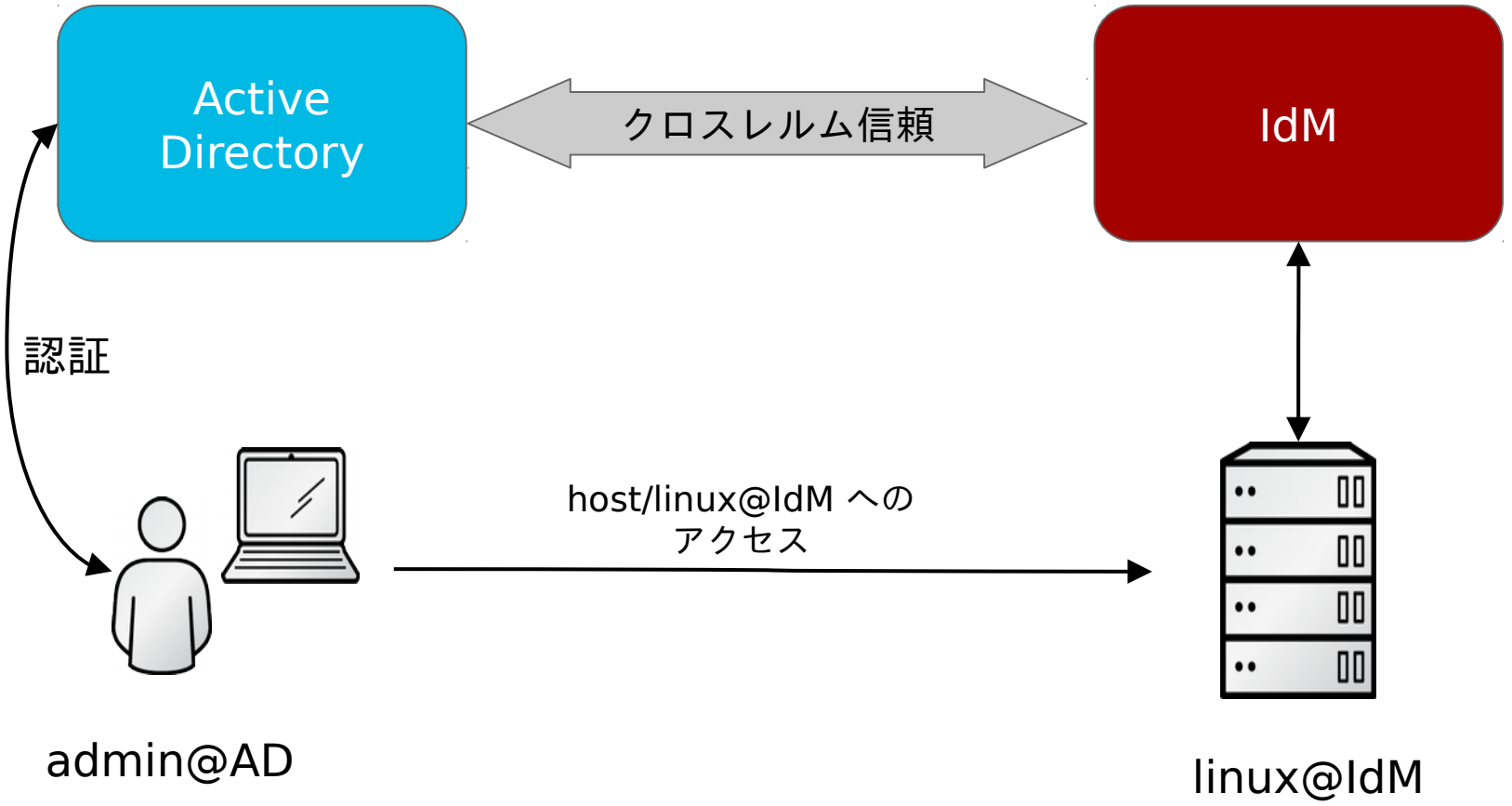
間接的な統合のオプション

- 信頼ベースのソリューション
  - ADとIdM間でクロスレルムKerberos信頼を設定
    - ADのユーザがLinuxシステムおよびリソースにアクセス可能
  - IdMに独自のDNSドメインが必要
- 同期ベースのソリューション
  - LDAPでユーザアカウントをADからIdMへ同期
  - パスワード同期のためADに追加コンポーネントが必要
  - 全ユーザはIdM利用時にパスワードを一度手動で変更する必要あり
  - 1ドメイン、ユーザのみ(グループは不可)サポート

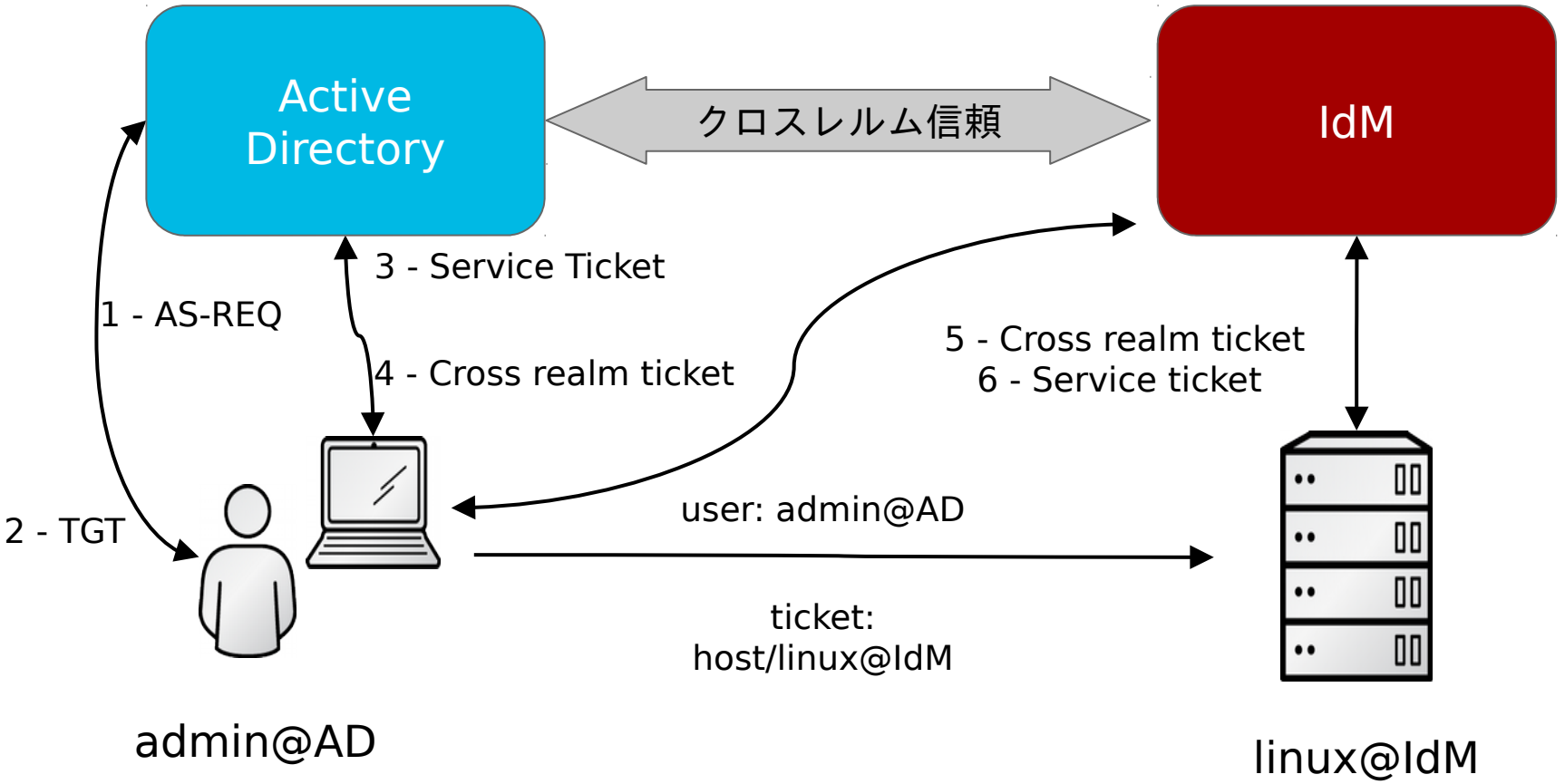
信頼ベースのIdM - AD統合



信頼関係によるシングルサインオン(1/2)



信頼関係によるシングルサインオン(2/2)



ADとIdMの信頼関係

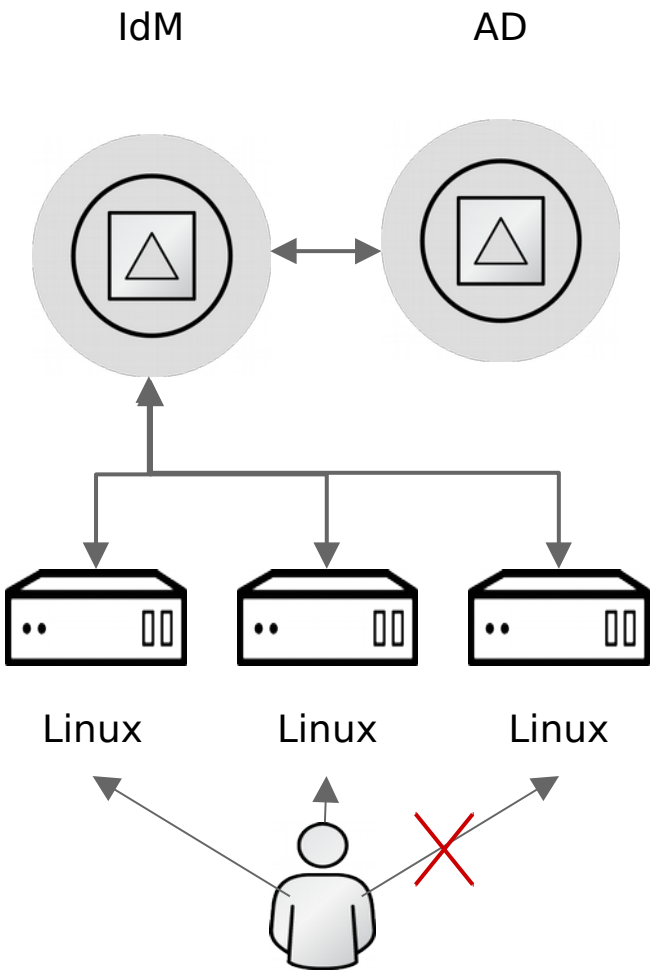
- あるフォレストのユーザが別のフォレストのリソースにアクセスできるようにする
- あらかじめ信頼関係を構成する
  - 2つのフォレスト間で暗号化鍵を共有する
- 現在サポートされる構成は
  - ADとIdMが双方向に信頼
  - IdMがADを信頼

    ※ADがIdMを信頼する信頼関係は現在構成できない

ADとIdMのユーザのマッピング

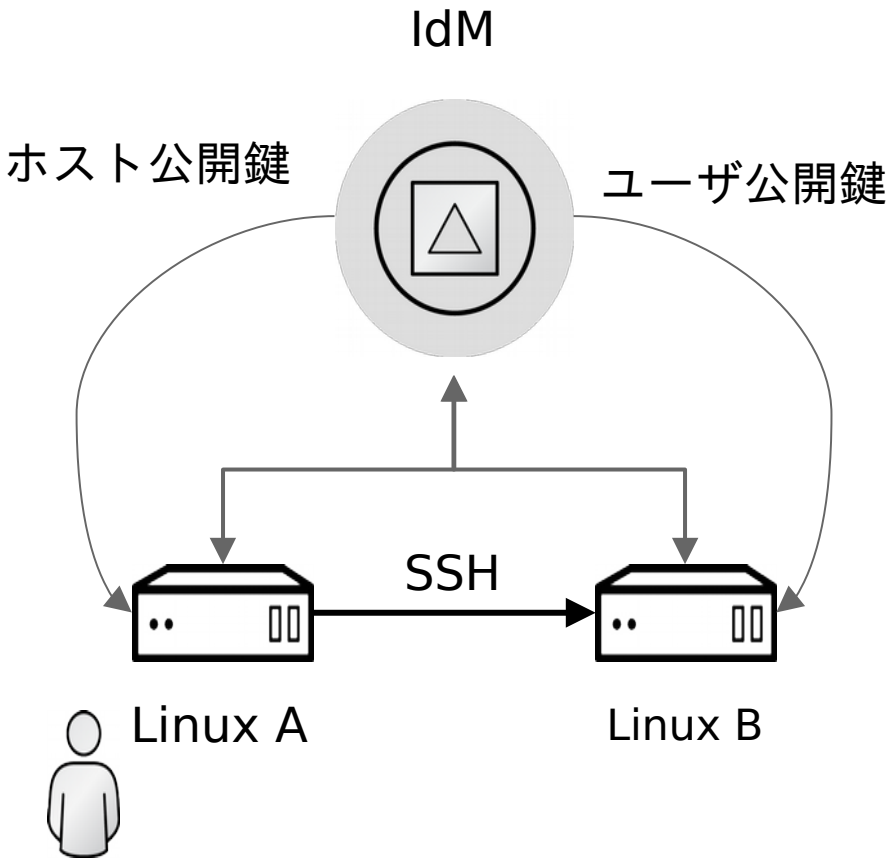
- SFU/IMUによるPOSIX属性対応
  - Windows 2012R2 Serverから deprecated
- IdMによるADのSIDからUID, GIDへのダイナミックマッピング
- ID viewによる静的なオーバーライド
  - ユーザとユーザ属性
  - ユーザ属性以外も対応
    - SSHキー
    - OTP および証明書 (予定)

Host Based Access Control(HBAC)



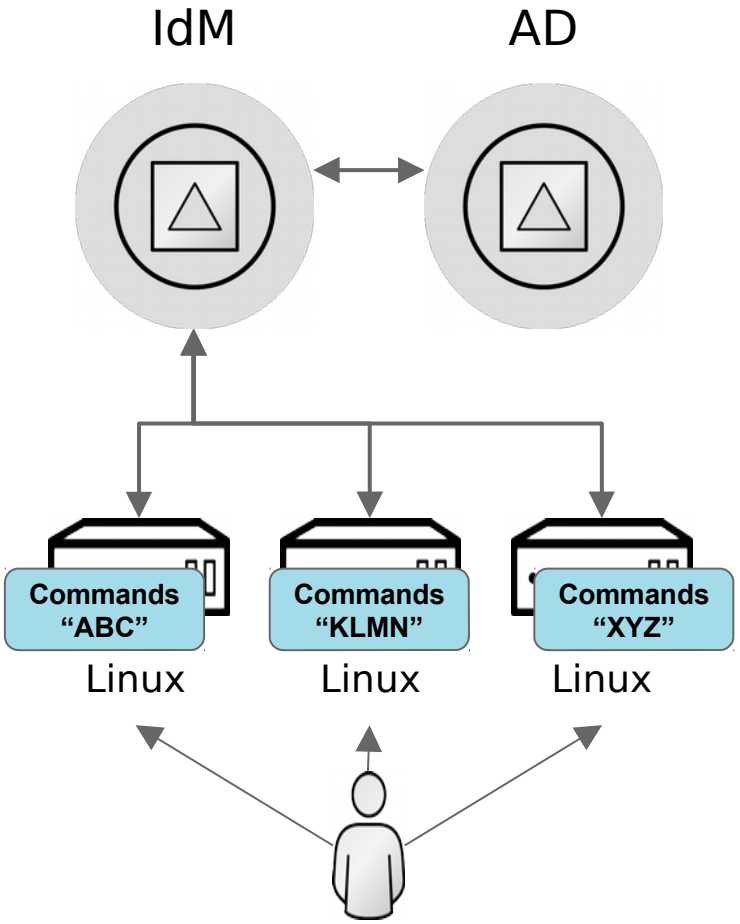
- ホストベースアクセス制御
  - どのユーザ(群)が
  - どのホスト(群)から
  - どのサービスへアクセスできるか
    - コンソール, ssh, sudo, ftp, sftp など
- ルールを集中的に定義
- 信頼したADのユーザにも適用

ユーザとホストのSSH 鍵管理



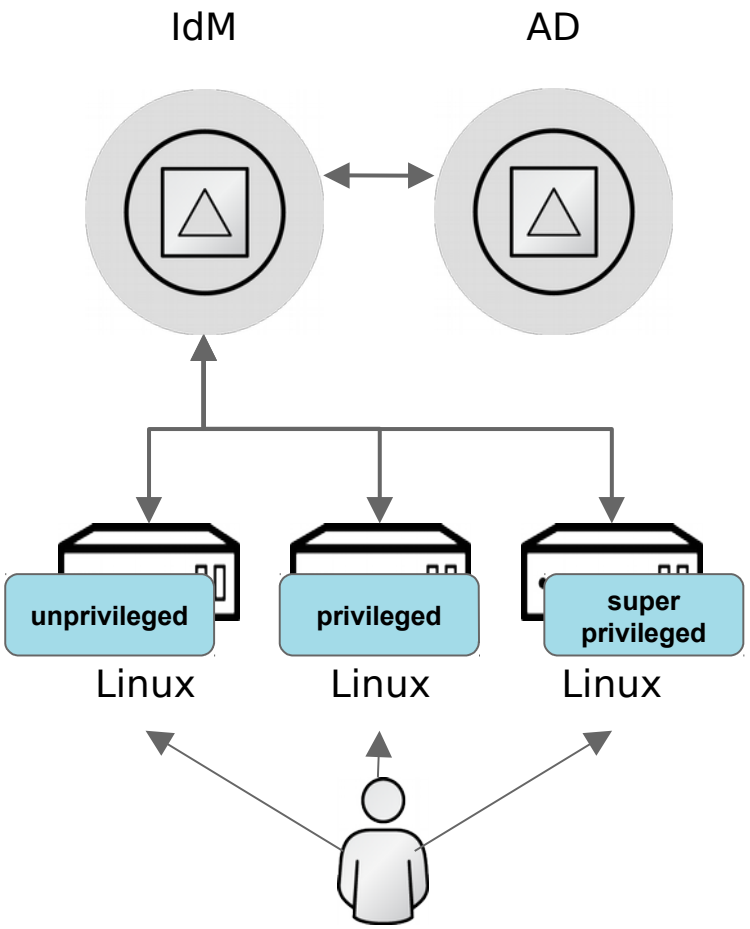
- ホストの公開鍵をクライアント導入時にアップロード
- ユーザの公開鍵をアップロード
- システムAからシステムBへsshするとき
  - Bの公開鍵をIdMがAへ配布(手動でのdigest確認は不要)
  - ユーザの公開鍵をIdMがBへ配布(手動でのコピー不要)
- 信頼したADのユーザにも適用

sudoの統合



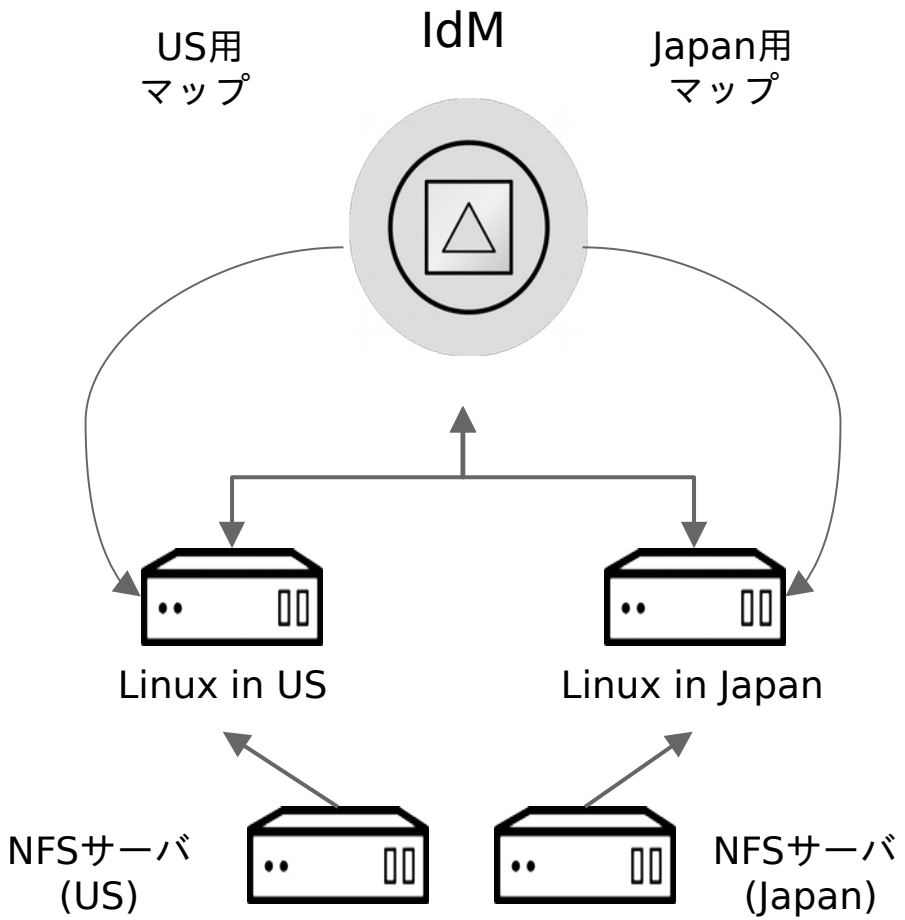
- sudoers管理
  - どのコマンド(群)を
  - どのユーザ(群)が
  - どのホスト(群)でsudo実行できるか
- ルールはクライアントで適用
  - SSSDでキャッシュ
  - sudoに統合
- 信頼したADのユーザにも適用

SELinux のユーザマッピング



- 集中的にマッピングを管理
- SELinuxのMLS/MCSポリシーで利用
- ユーザとホストの組み合わせ毎にコンテキストをマッピング
- デフォルトのラベルをIdMで設定可
- マッピングはクライアントで強制
- SSSDでキャッシュ
- 信頼したADのユーザにも適用

Automountのマッピング

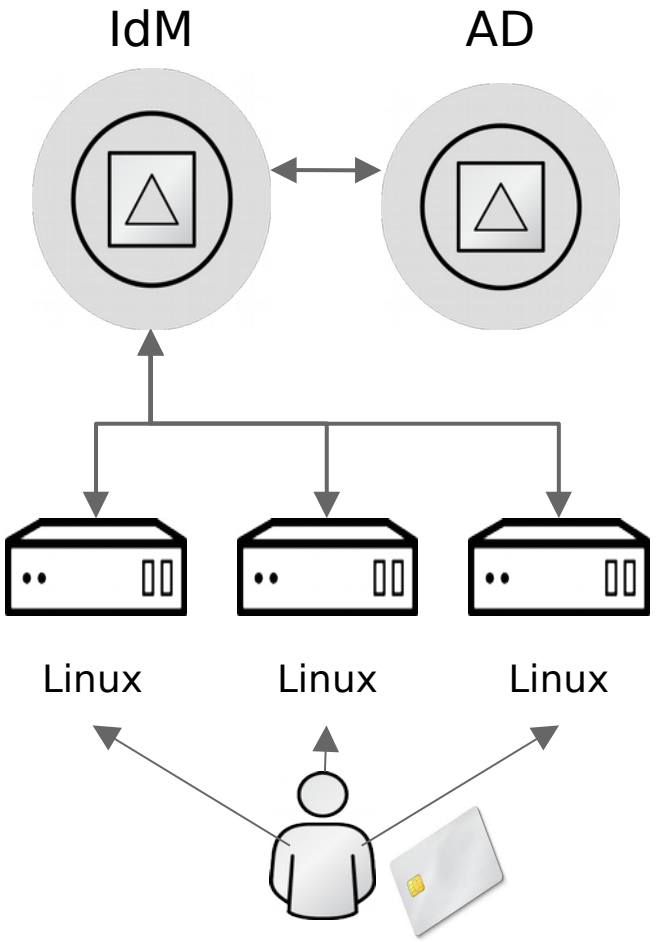


- 場所ごとにマップを定義
- direct map, indirect map
- autofsクライアントに統合
  - IdMはautofsサーバの設定はしません
- クライアントはその場所に対応したマップを取得するよう設定
- マップは集中管理
- マップはクライアントで適用される
- マップはSSSDでキャッシュ

証明書と認証局の管理

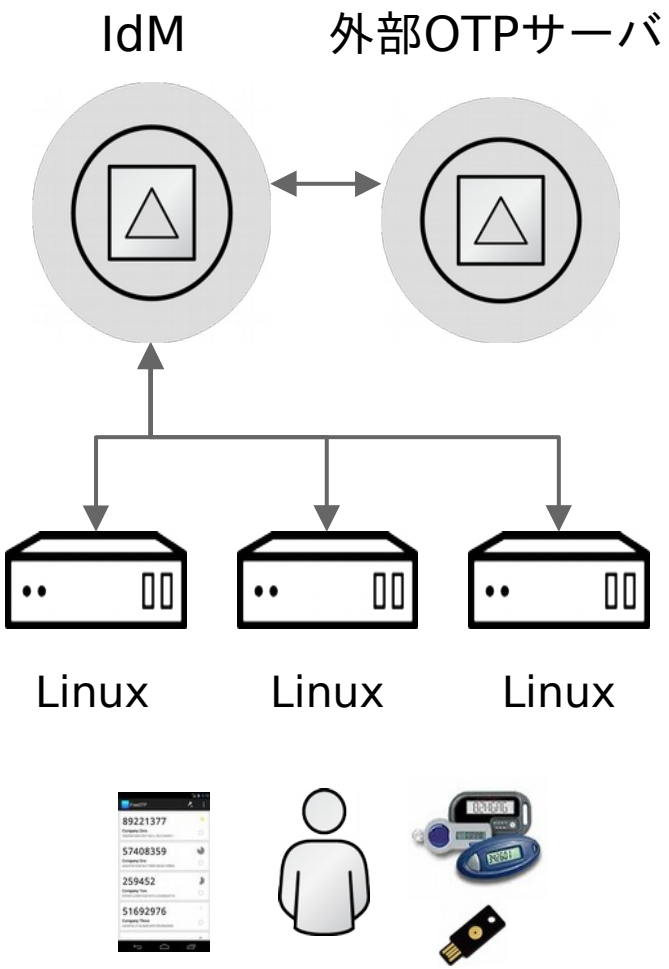
- Dogtag Certificate SystemによるPKI基盤
- Subjects
  - Users, hosts, devices, services
- Profiles
  - 目的毎のプロファイル
- Sub CA
  - 特定目的用のCA
- certmonger による証明書の追跡と更新

証明書による認証



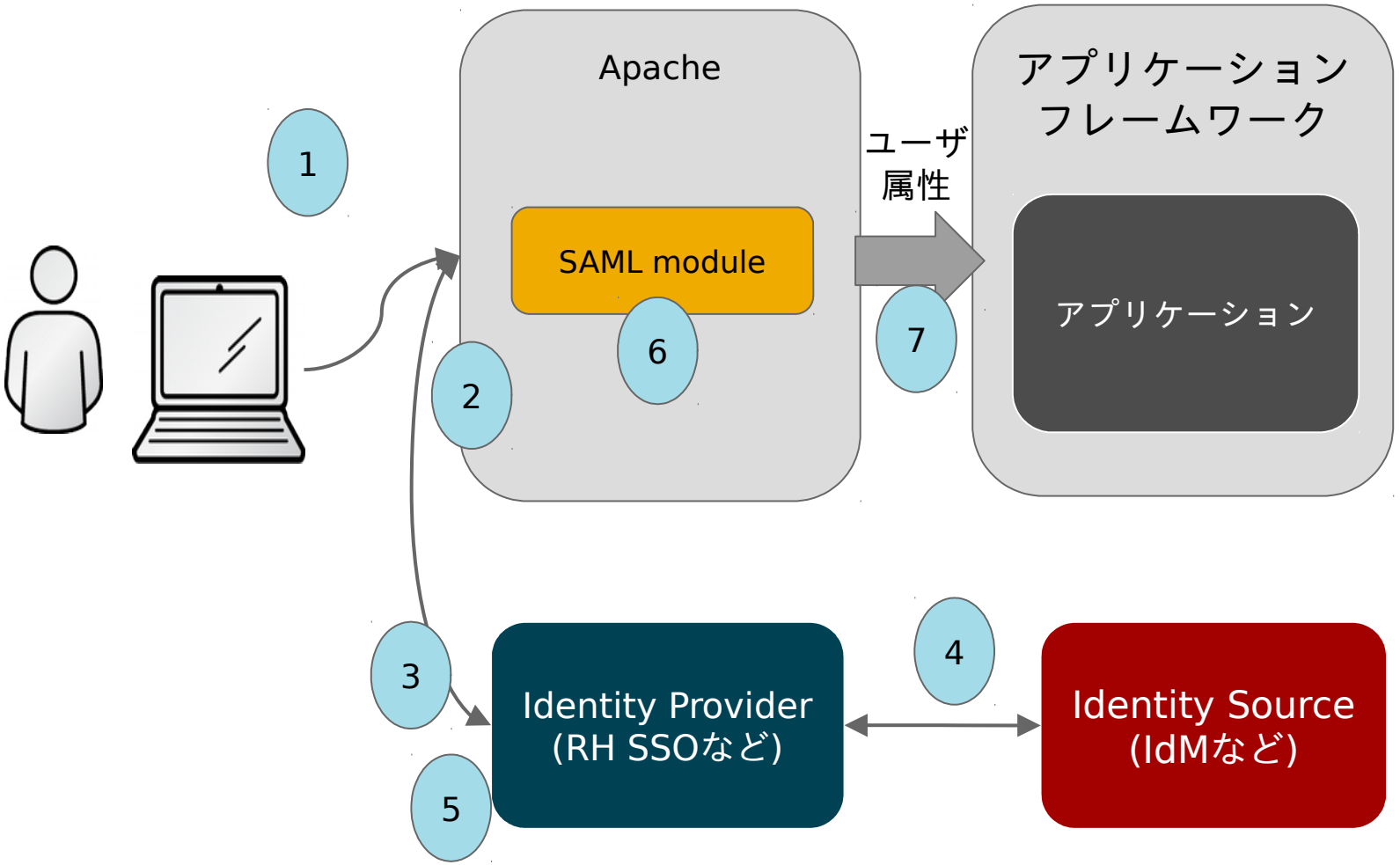
- ユーザ認証を証明書によって実施する
- 証明書またはスマートカードをもつIdMユーザ
- 証明書またはスマートカードをもつADユーザ
- IdM UI/CLI での証明書による認証(作業中)

二要素認証



- IdM内蔵の二要素認証
  - Yubikey, FreeOTP, Google authenticator
  - HOTP/TOTP互換
  - LDAPまたはKerberos経由で利用可
- RADIUSプロキシによる認証
  - RADIUSをサポートする任意のサードパーティ製品
  - Kerberos経由でのみ利用可

SAMLによるシングルサインオン



SAMLによるシングルサインオンの流れ

1. ユーザはブラウザでアプリケーションを開く
2. SAMLモジュールが適切なassertionがあるかチェックしてIdPにリダイレクト
3. IdPは必要に応じて認証(またはシングルサインオン)を実施
4. IdPは設定されたIdentity sourceで認証
5. IdPはSAML assertionを作成してリソースにリダイレクト
6. SAMLモジュールはassertionを確認しユーザデータを取得
7. ユーザデータがアプリケーションへ渡されて認証完了

SAMLによるシングルサインオン

- IdMだけではSAMLによるシングルサインオンはできません
  - IdMはIdentity Sourceとして利用
- Identity Provider(Red Hat SSOなど)が必要
  - RHEL 7.2でtechnology previewとして同梱されたIpsilon IdPはdeprecatedとなりました
- 必要なApache moduleは最新のRHELに同梱

まとめ

- 「Red Hat Identity Management」はRed Hat Enterprise Linuxに同梱されるアイデンティティ管理基盤
- アイデンティティ・認証・アクセスコントロール・ポリシーを管理します
  - LDAPによるアイデンティティ情報管理
  - DNSによる名前解決
  - 認証
  - 証明書発行
  - sudoer, HBAC, automountとの統合
- PAM/NSS, Apache module等の連携が充実していてアプリケーションとの連携も考慮されています

参考文献

- RHELドキュメント
  - Linux ドメイン ID、認証、およびポリシーガイド
    http://red.ht/2hYBk9h
  - Windows 統合ガイド
    http://red.ht/2h0oPsb