Linuxでの近代的な認証基盤を実現するFreeIPA

森若和雄

2017-12-12

このスライドの目的

- 目的 : OSS の認証基盤 FreeIPA が解決している課題とどうやって解決しているかをざっくり紹介します
- 背景 : FreeIPA はかなりよく作り込まれていて、使うために必要なドキュメント類もある。でも「ウチで使ってるよ」という人をあまり見かけない……

  → 布教活動が必要なのでは……？

Google trends で 'freeipa' を見ると

概要

- FreeIPA って何？
- FreeIPA のサーバー側
- FreeIPA のクライアント側
- くっつけると……？

FreeIPA って何？

FreeIPA とは……

- 多数の Linux システムのユーザ認証とポリシーを集中管理する仕組み
- うれしい機能
  - マルチマスターレプリケーションで冗長化する
  - シングルサインオン
    - AD との Cross realm trust
  - 2 要素認証、スマートカード認証
  - FreeIPA 未対応システムむけインタフェース提供 (LDAP の互換性用ツリー , NIS)
  - ssh, sudo, automount, SELinux 連携

FreeIPA のサーバー側

Linux でもドメイン管理したい

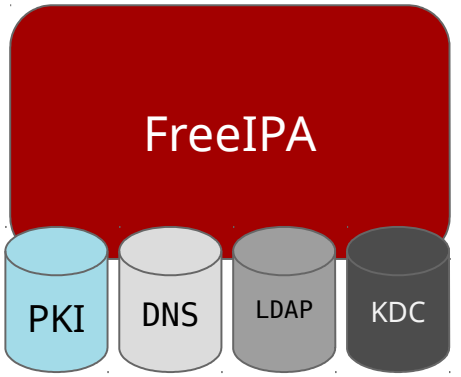
FreeIPA プロジェクトが始まったのは 2007 年ごろ

- Windows 世界は AD で統合されてきたのに UNIX 世界は……
  - NIS+, LDAP でアカウントまとめるくらい
  - samba で AD に直接繋ぐとログインやファイル共有はできるけど UNIX 世界のための拡張は期待できない
- ドメインコントローラの基本的な機能はもうある
  - ユーザ情報、ホスト情報などを保持→ LDAP
  - シングルサインオン→ Kerberos
  - ホスト登録するし、サービスの自動検出 → DNS
  - Kerberos で認証するから時計あわせるよね→ NTP
  - 証明書の発行と管理→ PKI

→ くっつければいいのでは……？

FreeIPA

- 各プロトコルの代表的なソフトを束ねよう
  - MIT Kerberos
  - 389 Directory Server
  - BIND
  - Dogtag (PKI 基盤)
  - これらを統合するのに必要なもの色々



- 基本的な方針
  - 汎用のディレクトリではない。企業内の ID 管理を行う。
  - UNIX/Linux 世界のための認証基盤を作る。
    - AD と同じものは作りませんが AD との相互運用性は気にします
  - FreeIPA 未対応のシステムからも利用できるように互換性のあるインタフェースを提供する。

くっつけただけなの？

- 「束ねよう」といっても簡単にはくっつかないのでいろいろ開発しています
  - FreeIPA 用 389DS 用プラグインたくさん
    - 2 要素認証
    - AD 連携 , DNS 連携
    - パスワード再発行 etc.
  - 2 要素認証による Kerberos 認証
  - クライアント側サービス SSSD
  - サーバとクライアントのインストーラ
  - XMLRPC API 、ライブラリ、コマンドラインクライアント
  - Web UI 一式

想定するターゲットは？

- Linux/UNIX が 10 台〜 10 万台くらいの企業内システム群の管理
  - 何かしらまとめて扱う仕組みがないとしんどい
  - セキュリティがそれなり (以上) に大事
- 既に Windows 環境では AD を使っている
  - AD と連携して SSO したい

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
  - 機能は十分 (以上)
  - 追加コスト (2000 ～ 10000 円 / アカウントくらい)

FreeIPA 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
  - (製品としては最大 60 ノード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
  - デプロイ用使い捨てパスワード発行

FreeIPA 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

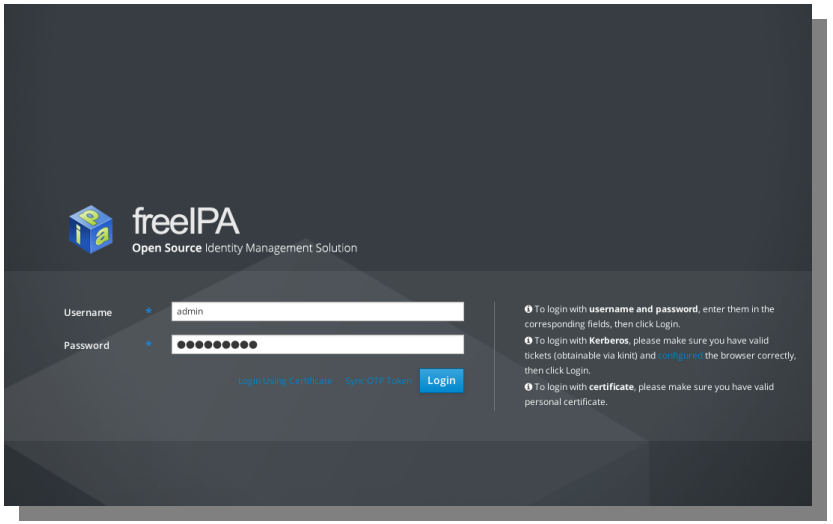
用語

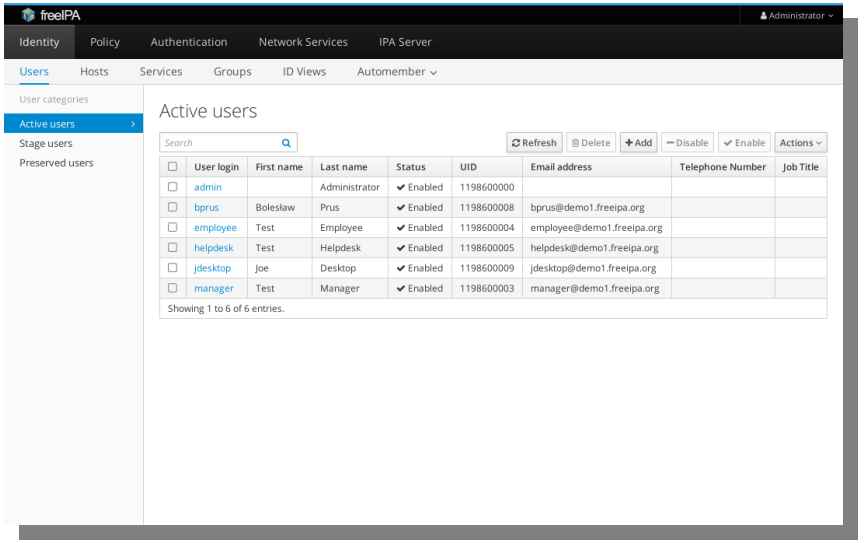
- Linux ドメイン : FreeIPA が管理するドメインのこと
- IPA: “Identity Policy Audit” の略なのですが Audit 機能はなくなってしまい、実態としては Identity と Policy 管理の仕組みになっています
- IdM: RHEL6 から FreeIPA が RHEL に同梱されるにあたって、当時 Policy も微妙だったので “ Identity Management” という名前がつきました。その略称が IdM です。

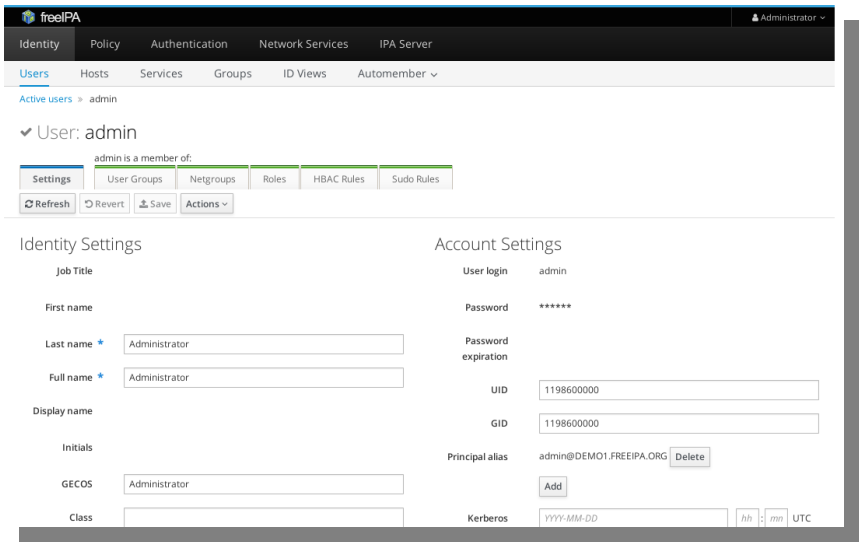
デモサイト

https://ipa.demo1.freeipa.org

パスワード等は以下ページ参照
http://www.freeipa.org/page/Demo

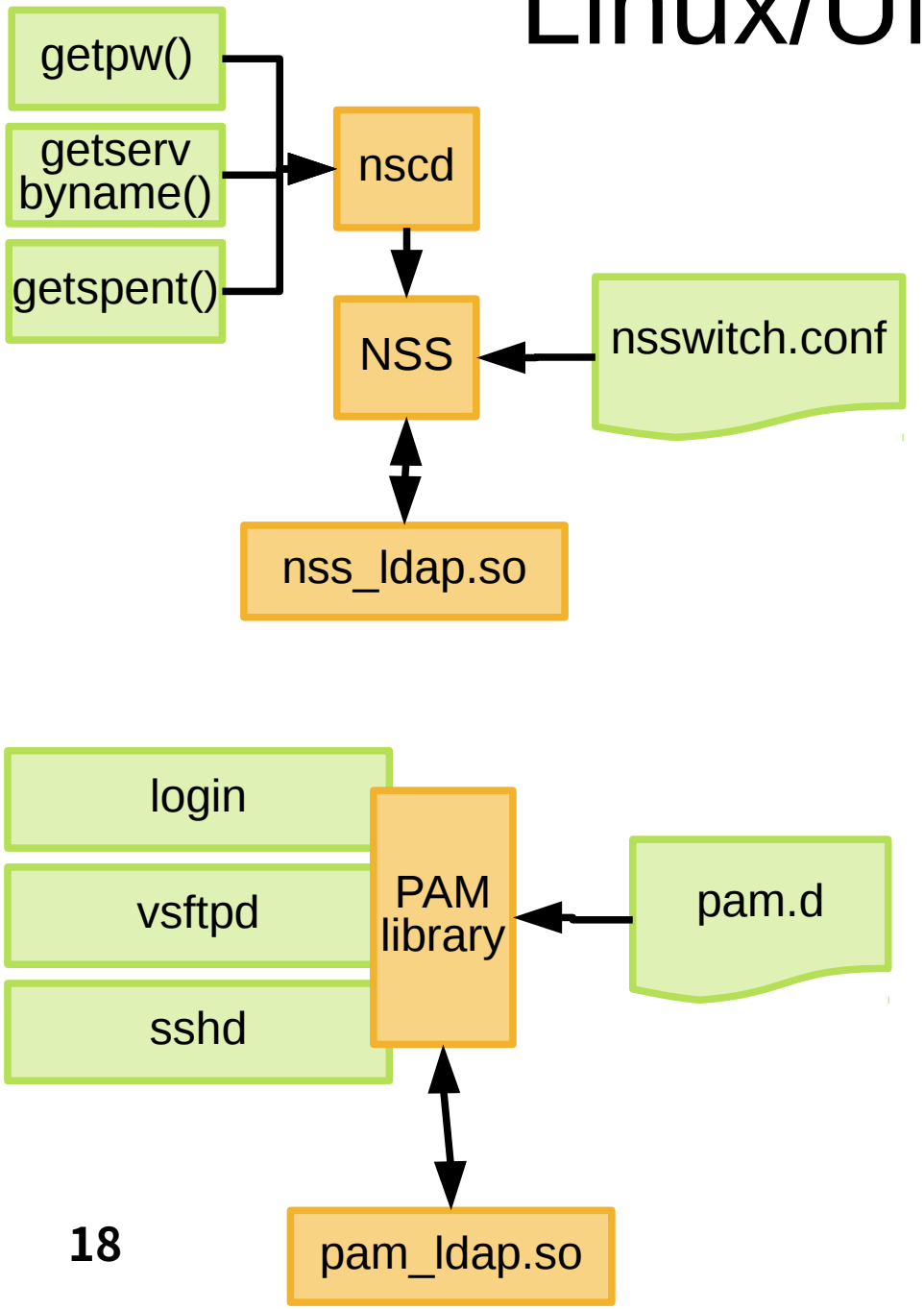






FreeIPA のクライアント側

Linux/UNIX の認証

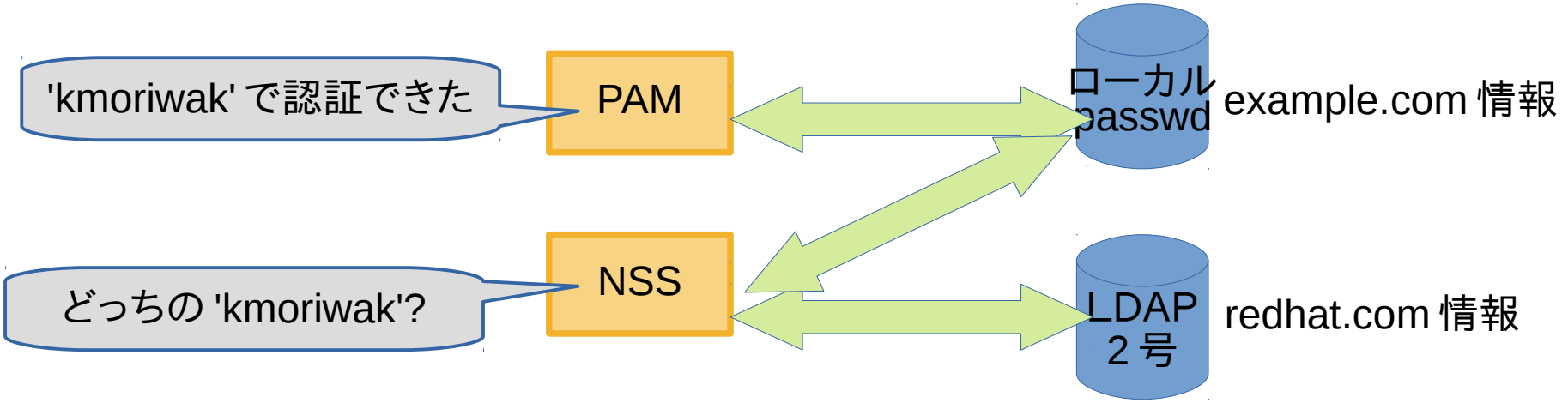


- Name Service Switch(NSS)
  - ユーザ ID やグループ ID、ホスト名と、それにひもづく情報を提供・更新する
  - libc の関数、getpw() や gespent() 等がインタフェースとなり、nsswitch.conf でバックエンドを指定
- Pluggable Authentication Module(PAM)
  - 認証サービスへのアクセス
  - PAM ライブラリを認証をおこなうアプリケーションが呼びだす

ドメイン修飾のある認証

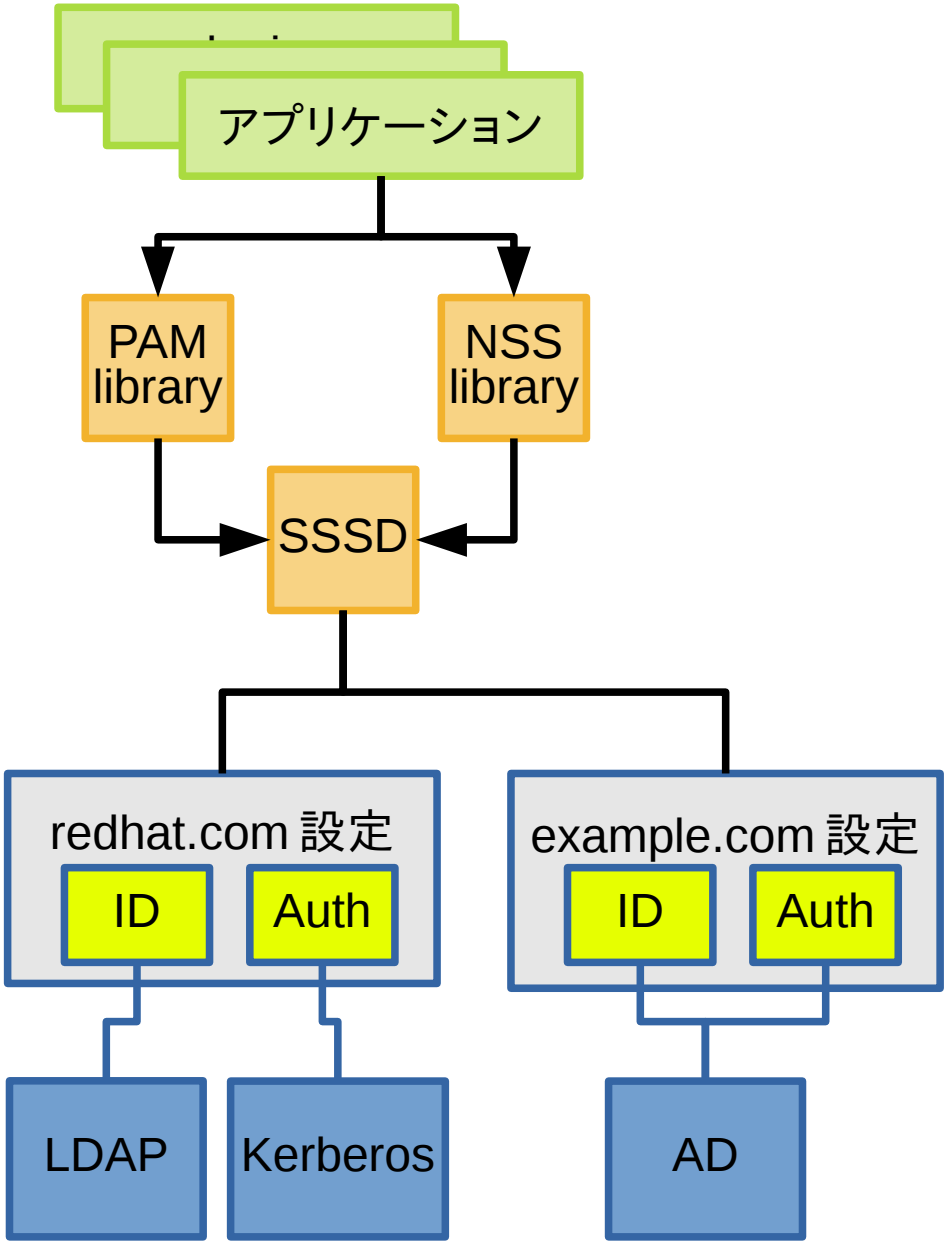
- 認証するときに複数の名前空間を扱いたい
  - 'kmoriwak@example.com' ユーザーと、'kmorwiak@redhat.com' ユーザーを区別したい
- 今までの PAM と NSS の仕組みで素直に設定すると、PAM と NSS が独立しているため破綻する
  - 認証されたユーザがどちらのドメインかわからないから

※ 実際に pam_ldap で複数のユーザにマッチすると認証を失敗させる



SSSD によるドメイン対応

- 複数ドメインに対応した認証と識別のサービス
  - PAM と NSS のバックエンドとして動作
  - キャッシュも SSSD が一元管理 (nscd は不要)
  - オフライン時の認証に利用するためにパスワードのハッシュも維持 (option)
  - 各ドメインに名前をつけ、'ユーザ名 @ ドメイン名 ' という名前を利用できる
- 各ドメイン毎に ID と Auth のバックエンドを指定



ドメインが複数なくても (きっと) 便利

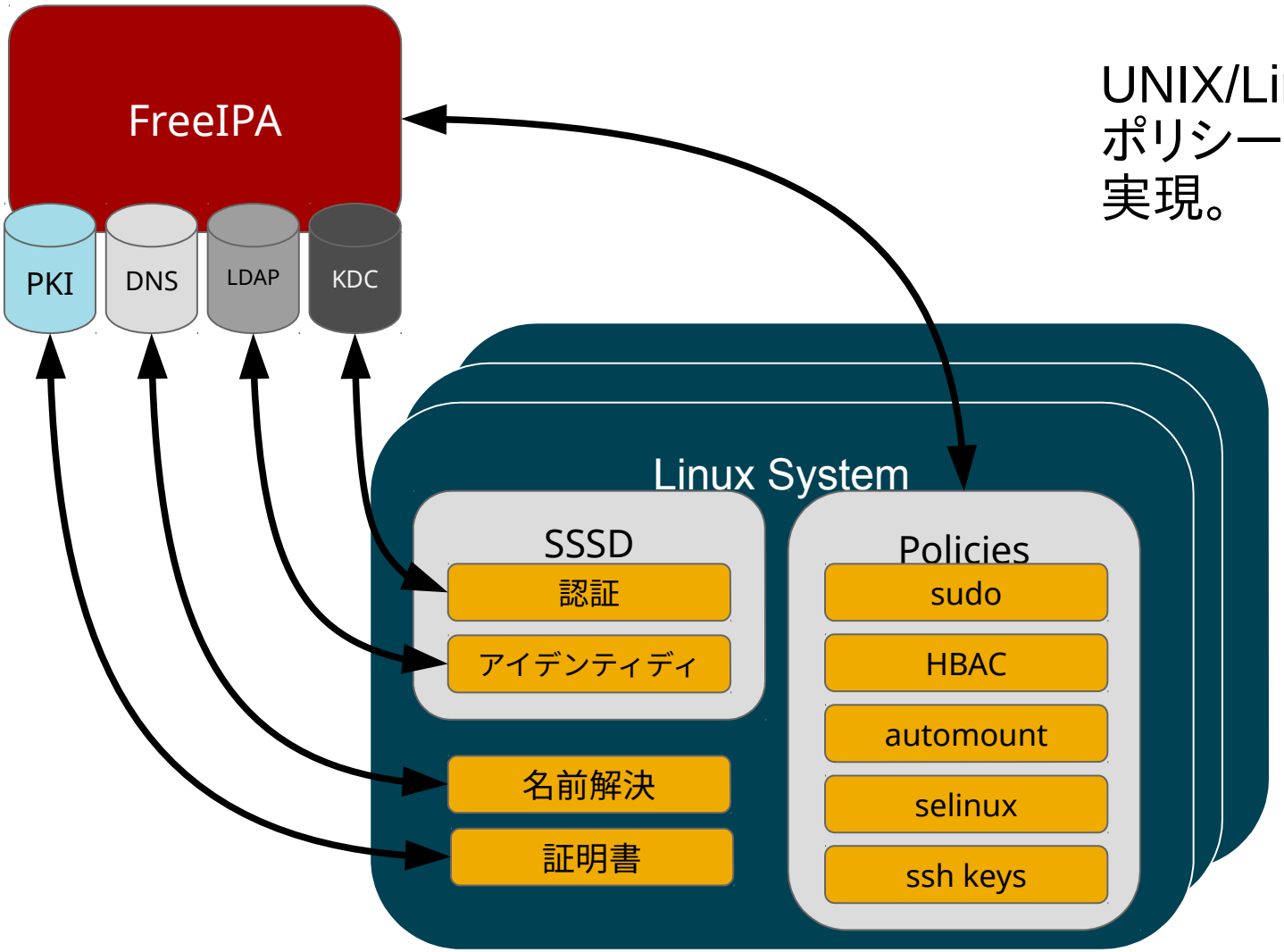
- local で既に定義してあるユーザ名と
  ドメイン内のユーザ名が一部重なっている
- 既存のパスワード管理から移行するとき、一時的に
  どちらでも利用できるようにしたい
- 普段はローカルに登録されているユーザだけを使
  うけど AD に登録されているユーザもたまに使いた
  い

簡単に設定したい……!!

- 課題 : 認証だけしたい時でも関連する設定が多い
  - Kerberos を認証サービスに、LDAP を ID サービスに設定した SSSD の設定
  - pam の設定に pam_sss を追加
  - nsswitch.conf に nss_sss を追加
- 解決 : realmd, realm コマンド
  - AD および FreeIPA で認証する設定を自動化
    - 上記設定を自動的に実施
  - DBus 経由で利用できるので GNOME とも統合
  - 認証以外の設定は行わないので注意 (必要な場合は後述の ipa-client-install を利用する)

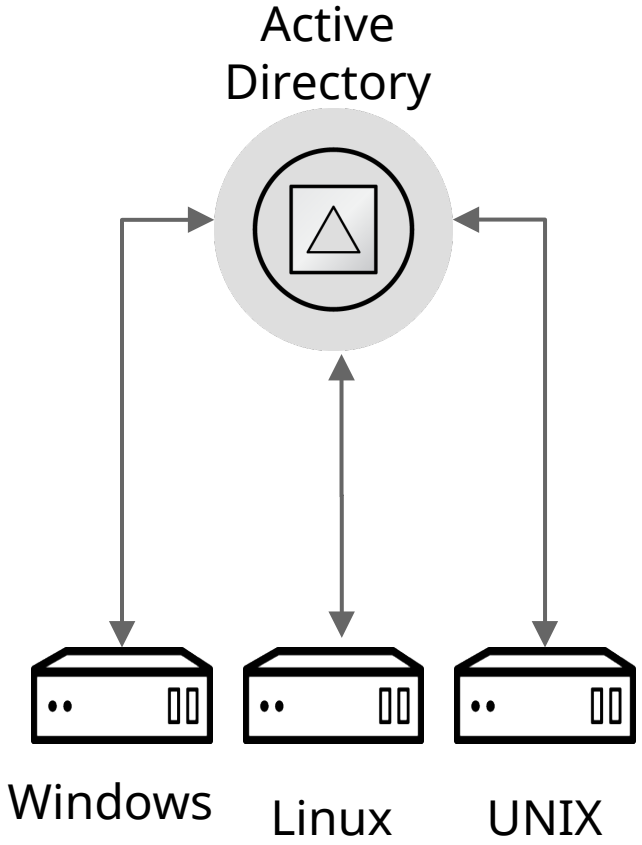
くっつけると……

FreeIPA によるポリシー管理と SSO

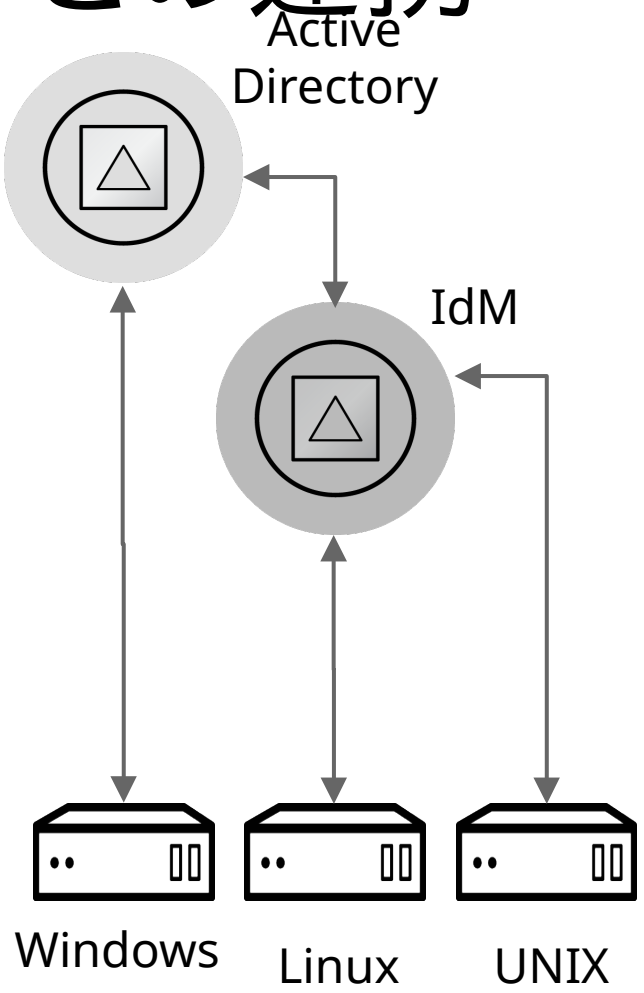


UNIX/Linux 環境用のポリシー管理と SSO を実現。

Active Directory との連携



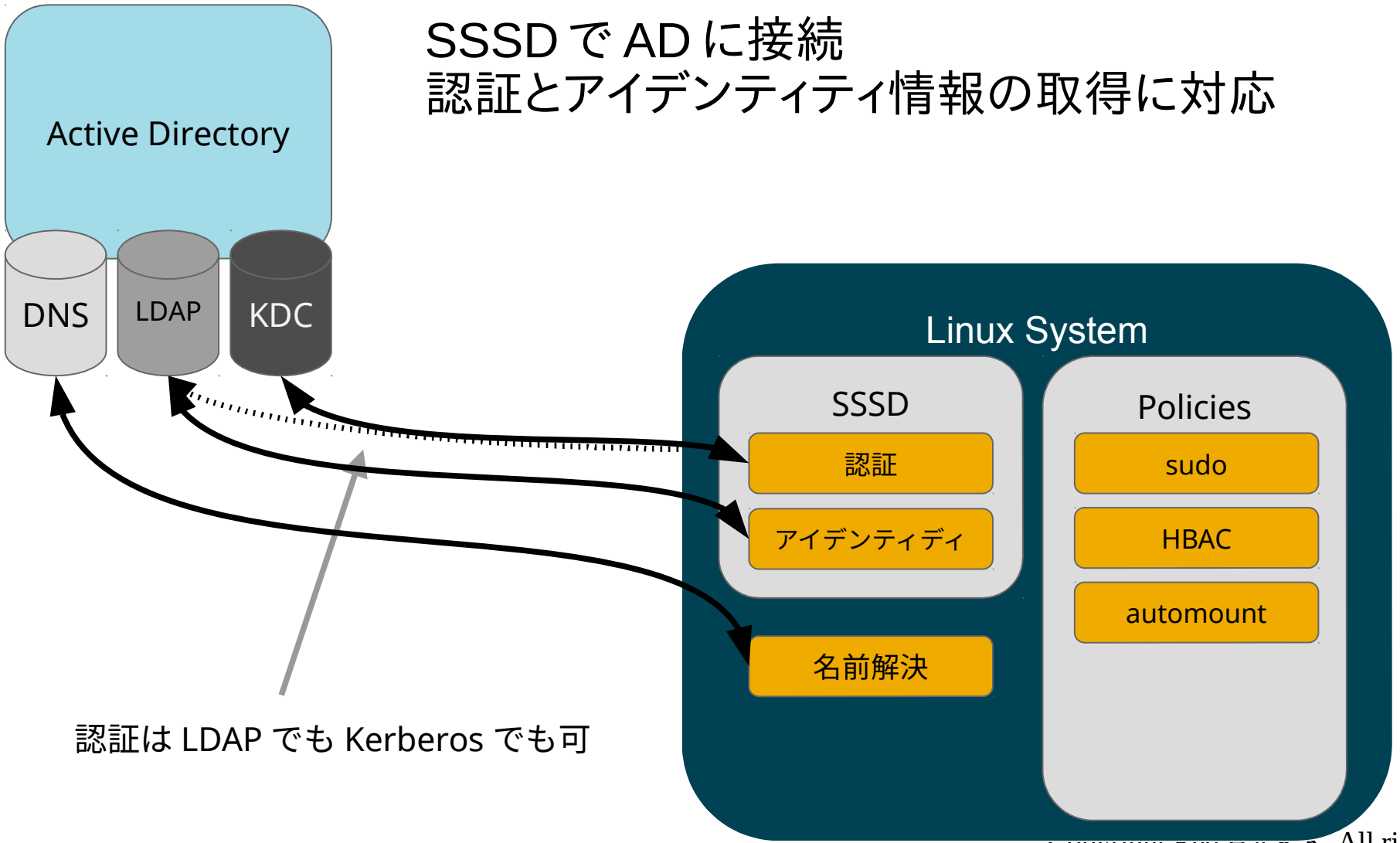
SSSD による直接的な統合
Active Directory で
Linux/UNIX の認証



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

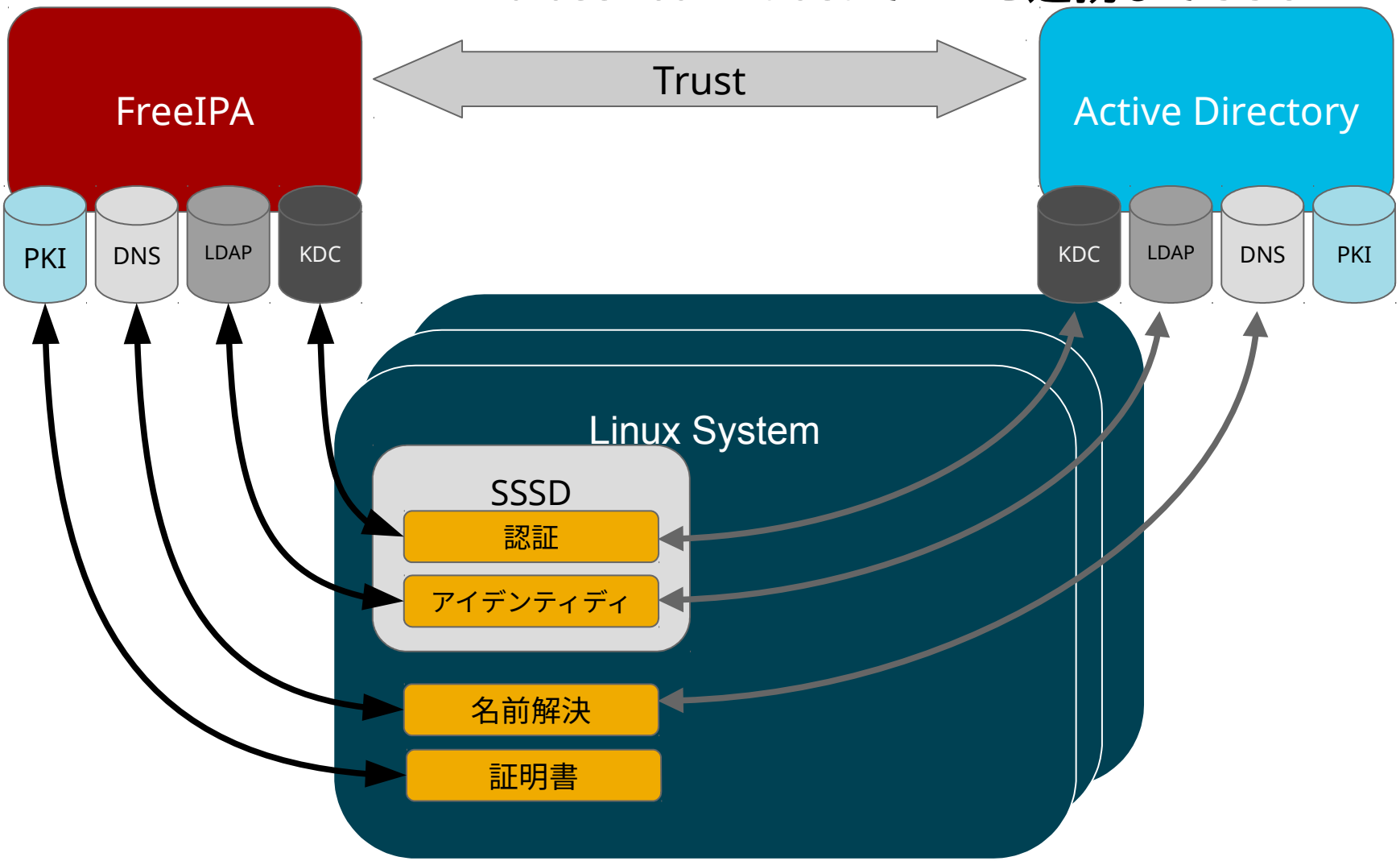
SSSD による直接的な統合

SSSD で AD に接続
認証とアイデンティティ情報の取得に対応



Active Directory と連携

Kerberosの cross realm trust で AD と連携して SSO



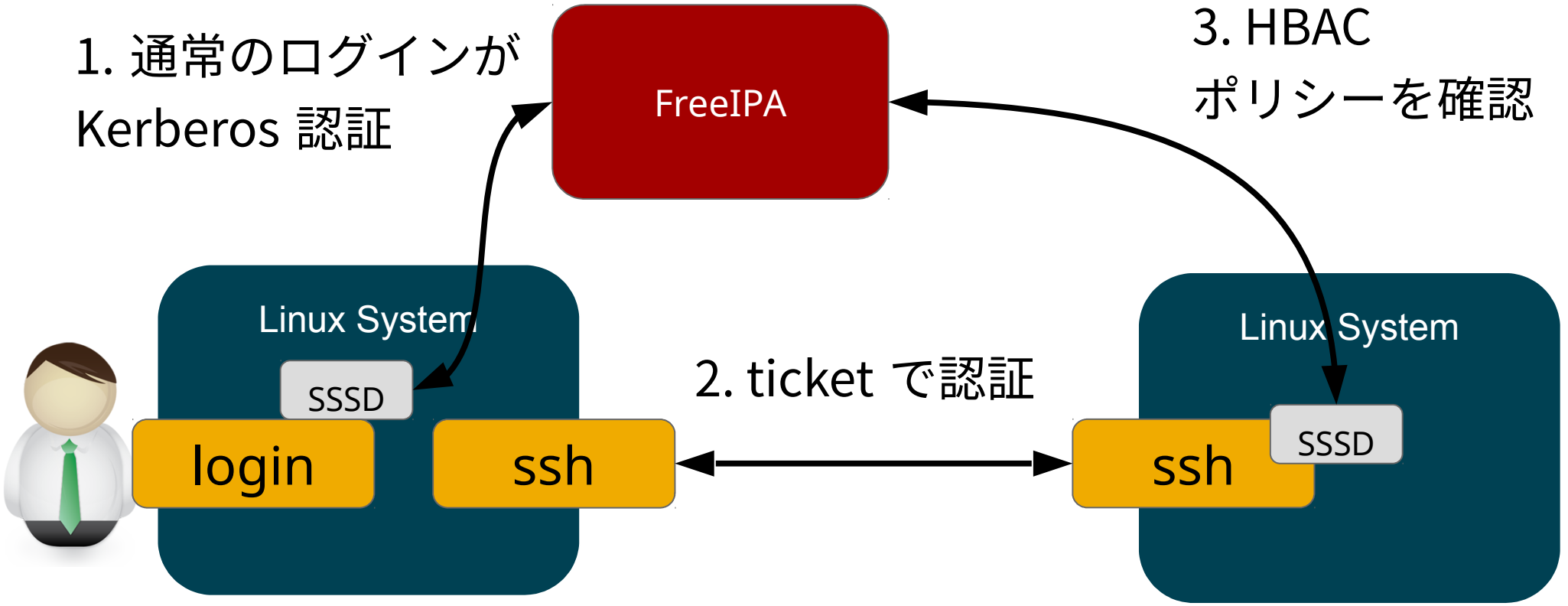
SSH

- ドメイン内で認証したいだけなら Kerberos で OK?
- でも配りたいデータもある
- ホストの fingerprint を配布したい
  - fingerprint、まじめにチェックしたことありますか？
  - ホスト再構築時に known_hosts を更新し忘れて怒られる

→ ドメイン参加時に FreeIPA に公開鍵を登録、DNS の SSHFP レコードで Fingerprint 配布

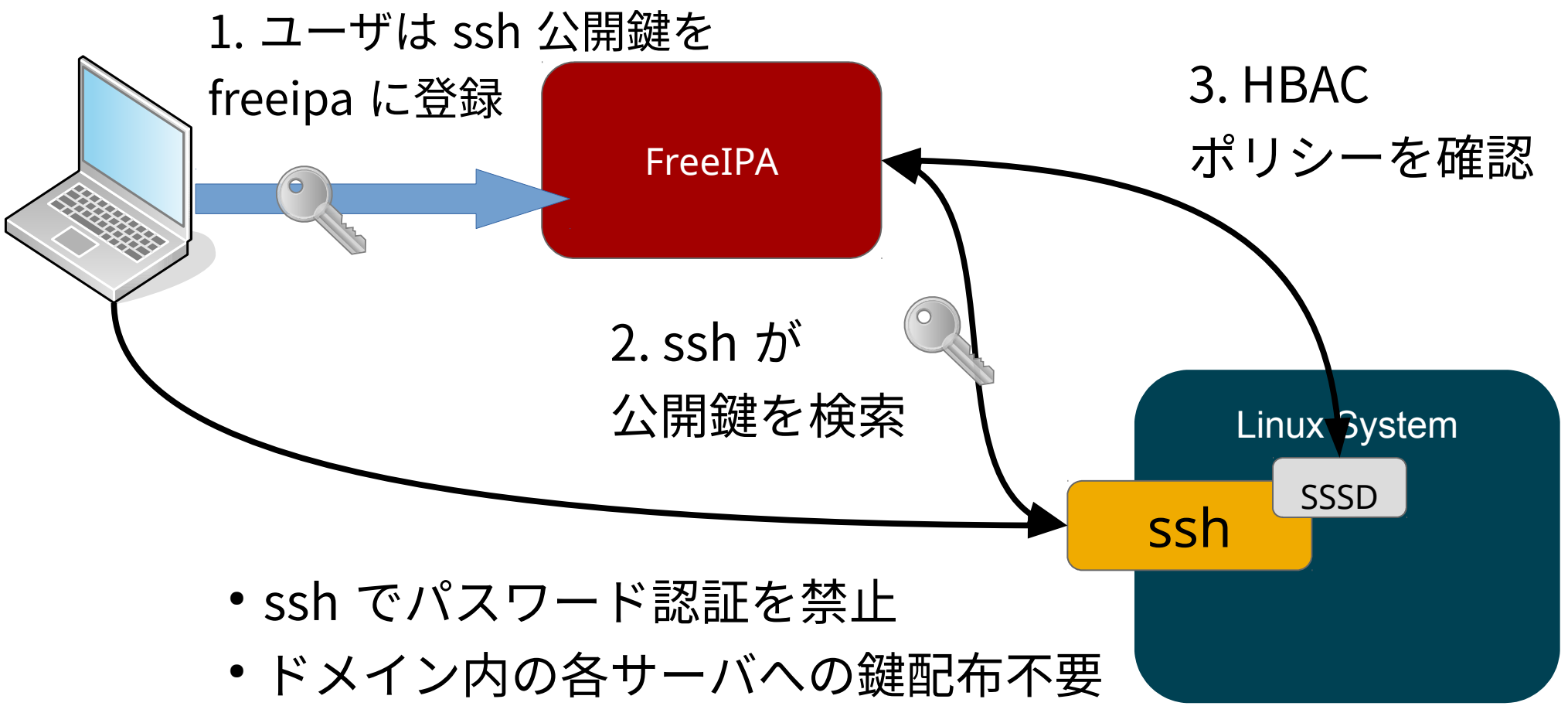
☐	ipa	A	52.57.162.88
		SSHFP	3 1 CA39FB815844D4123FDCF886F7FB472D3EF71CF7
		SSHFP	3 2 E99C5DDBEC6DD84694733FF8190739C1CABAA00C40E8D4ECEE07CB9F6E0F5F83
		SSHFP	1 1 802B025217151686EC64FB54D884886D74605D95
		SSHFP	1 2 3DB8258BE2A4EEFF114AB287B9E2CD0F3A8550295DE97FEB9BE5F2A3F3F31E9C
		SSHFP	4 1 6DC2CB89C8263403B472DA2F3FE835442B776589

ドメイン内での ssh



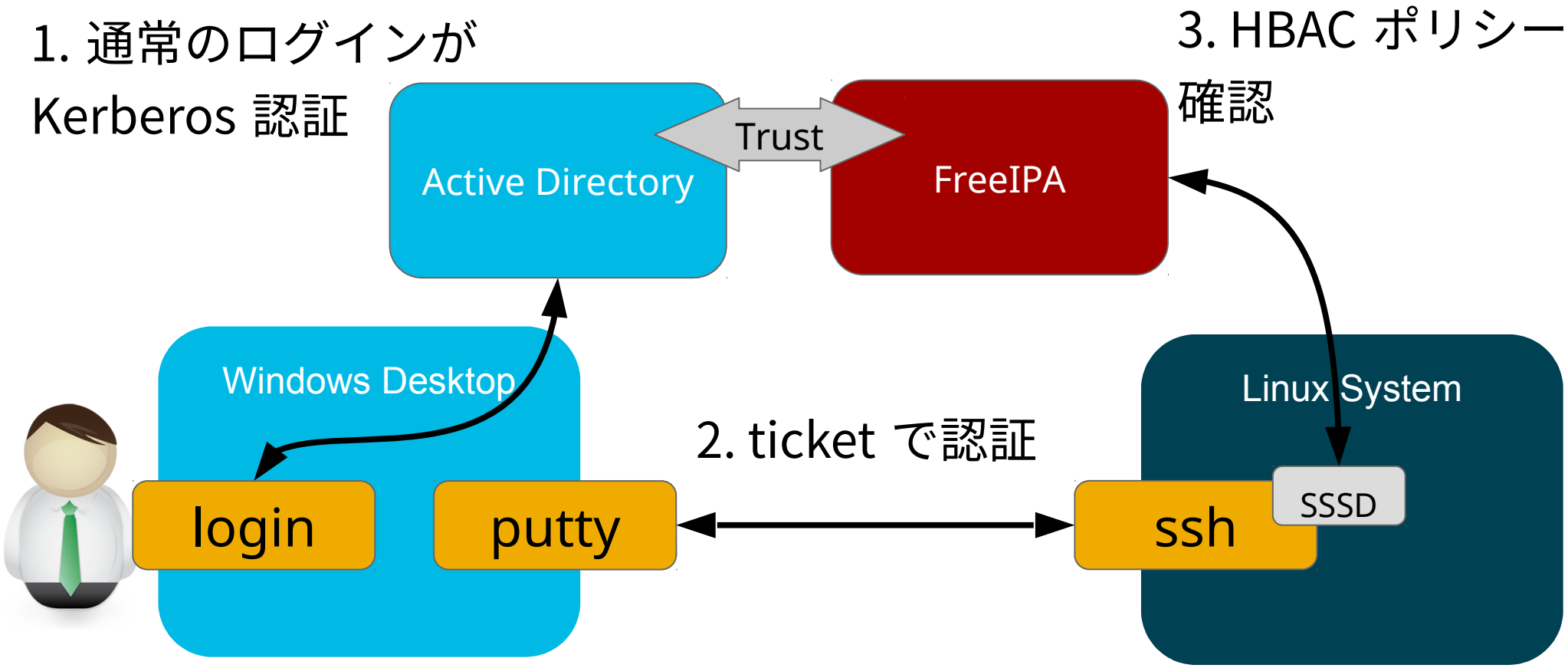
- パスワードを打つのは最初のログインだけ
- ドメイン内なら ssh の各ユーザの鍵配布不要
- HBAC ポリシーを設定可 (デフォルトは全員何でもできる)

FreeIPA による ssh 公開鍵配布



- ssh でパスワード認証を禁止
- ドメイン内の各サーバへの鍵配布不要
- 不要になった鍵の削除も簡単

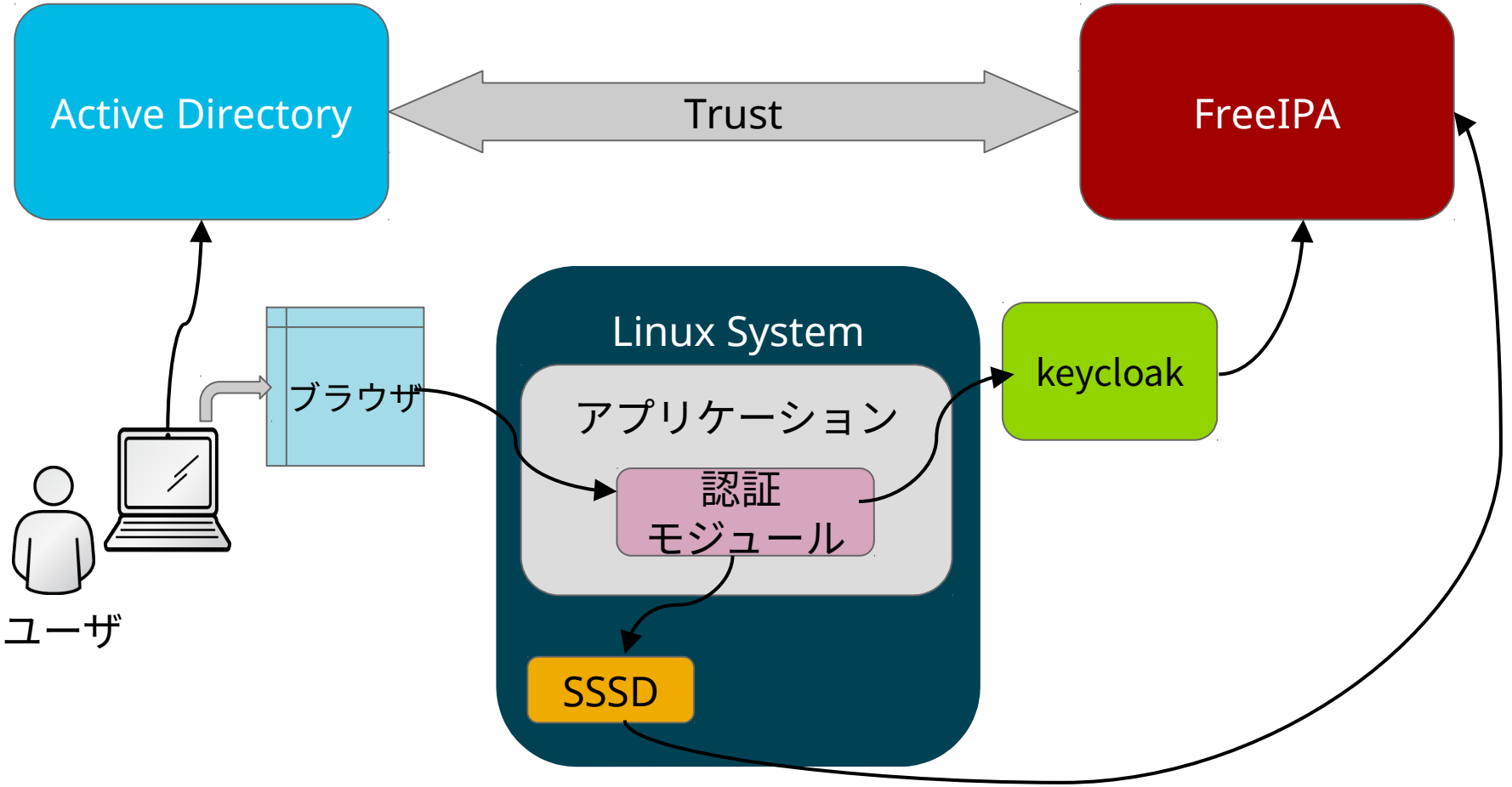
AD と連携した ssh



- パスワードを打つのは最初のログインだけ
- ドメイン内なら ssh の各ユーザの鍵配布不要
- HBAC などのポリシーを設定可 (デフォルトは全員何でもできるポリシー)

web アプリケーションの認証を統合

- SPNEGO(Kerberos) 対応 app　　→FreeIPA へ PAM 経由で認証
- SAML, Open ID Connect 対応 app → Keycloak 経由で認証
- 上記なし。LDAP, PAM 対応 app → SSO は不可。共通パスワードは利用可



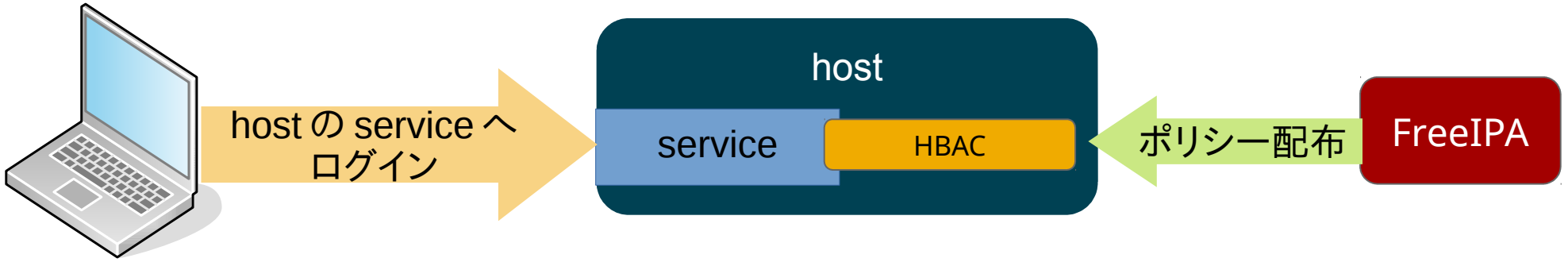
32

FreeIPA と SSSD の組み合わせにより実現する機能

HBAC

- 誰 (user, group) が
  どこ (host, host group) に
  どうやって (service, service group)
  アクセスするか許可する仕組み
- SSSD が通常の認証と同時にポリシーのチェックを実施

  ※ デフォルトでは全て許可



sudoers 管理

- FreeIPA の LDAP 上に sudoers エントリを保持
- SSSD で sudoers をキャッシュ
  - 素朴に毎回取得すると非常に遅くなる
  - 定期的にポリシーの更新を取得
  - sudo 実行時には該当ユーザのポリシーのみ更新

まとめ

- FreeIPA は多数の Linux システムのユーザ認証とポリシーを集中管理する仕組み
- うれしい機能
  - マルチマスターレプリケーションで冗長化する
  - シングルサインオン
    - AD との Cross realm trust
  - ssh, sudo
- ほかにも扱えなかったものいろいろ

ドキュメントは？

- FreeIPA 自体のドキュメントは以下。デザインドキュメントが調査時に有用
  - http://www.freeipa.org/page/Documentation
- ユーザー向けのドキュメント
  - RHEL のドキュメントの一部として提供 : http://red.ht/2iXUYDP
  - FreeIPA 3 以降のユーザー向けドキュメントはこちらに統合。和訳もある。

Q&A

- Q: なんで OpenLDAP じゃなくて 389DS なの？
  A: FreeIPA の開発チームが、ほぼ 389DS のチームと同じなので。
- Q: RHEL に入ってる ipa と freeipa って何か違うの？
  A: ソフトウェアとしてはほぼ一緒。ロゴがちがうくらい。
- Q: FreeIPA ってユーザいるの？
  A: サポートへの問い合わせベースで集計すると RHEL IdM のユーザーは順調に増えています。言える範囲だとアメリカの証券取引委員会 (SEC) とか使っています。

構築とか難しいんでしょ？

- 前提条件が厳しめ
  - 導入ホストは DNS で正引き、逆引きができてアドレスが一致することが必須 (/etc/hosts のみは不可)
  - FQDN が必須
  - NTP での時刻あわせを強く推奨
  - FreeIPA の DNS を使う場合は専用サブドメインを推奨
- ドキュメントにしっかり書いているので確認
  - http://www.freeipa.org/page/Deployment_Recommendations
  - http://www.freeipa.org/page/Quick_Start_Guide

主なインストール手順

主なインストール手順

- firewall の port あけて、パッケージをいれて以下を実行
- サーバ : ipa-server-install コマンド
  - DNS が必要なら forwarder, reverse DNS zone の指定
  - ドメイン名、realm 名、管理者パスワード指定
  - 外部 CA を使うなら証明書の指定
- クライアント : ipa-client-install コマンド
  - (自動で発見されない場合) サーバを指定
  - Kerberos realm に接続するための認証ユーザ
  - SSSD の設定の他、ホストの証明書発行、ssh キーの初期化、ipaUniqueID
- 詳しくはこちら : http://red.ht/2zKkKFu

スケーラビリティは？

- マルチマスタレプリケーション対応
  - 複数 DC，無停止アップデート可
  - 証明書発行のみシングルノード
- 10 万アカウント +5 万グループでサーバにメモリ 16GB くらい必要
  - 100 万アカウント必要とかだと速度が厳しい
  - 古いバージョンでは 5000 アカウントくらいで管理操作の反応が遅くなってきます。最新に近い版を使いましょう。