Identity Management und 2FA mit (Free)IPA

@Chemitzer Linuxtage 2015

Luc de Louw <ldelouw@redhat.com>
Senior Linux Consultant

Agenda

- Wieso eigenlich IdM einsetzen?
- Authentifizierung und Autorisierung
- Lokales Usermanagement
- Zentrales Usermanagement der alten Schule
- Zentrales vs. lokales Usermanagement
- IPA und die Features
- Architektur
- IPA Client

Agenda II

- Skalierung
- Zweifaktor Authentifizierung
- Architektur 2FA
- Unterstützte Clients
- Implementierung
- Und Windows?
- Integration von anderen Systemen
- Links

Wieso eigentlich IdM?

Abbildung von Prozessen einer Organisation

- Ein- und Austritte von Personen
- Abbilden von Berechtigungen von Personen und Teams
- ...
- ...

Authentifizierung/Autorisierung

Authentifizierung → Feststellen der Identität

- Autorisierung → Zugriffskontrolle/Access control

Lokales Usermanagement

useradd -m -d /home/tester tester → Alte Schule für einzelne Systeme, zentrales Benutzermanagement?

- Scripting: for i in serverliste; do ssh $i “useradd -m -d /home/tester tester”; done → Pseudo-zentralisiert, Skaliert bis zu dutzenden von Systemen, unflexibel, Zugriffskontrolle machbar aber komplex und fehleranfällig

Zentrales Usermanagement der alten Schule

NIS → Einigermaßen skalierbar, unflexibel, unsicher

- NIS+ → Sicherer Nachfolger von NIS, hat sich wegen der Komplexität nie durchgesetzt.
- LDAP → flexibel, komplex, skaliert gut. Zentral gesteuert
- Kerberos → Single-Sign-On, komplex, skaliert gut, nicht allzu breite Unterstützung.

IPA und die Features

Zentrales Management von Benutzern und Zugangsberechtigungen

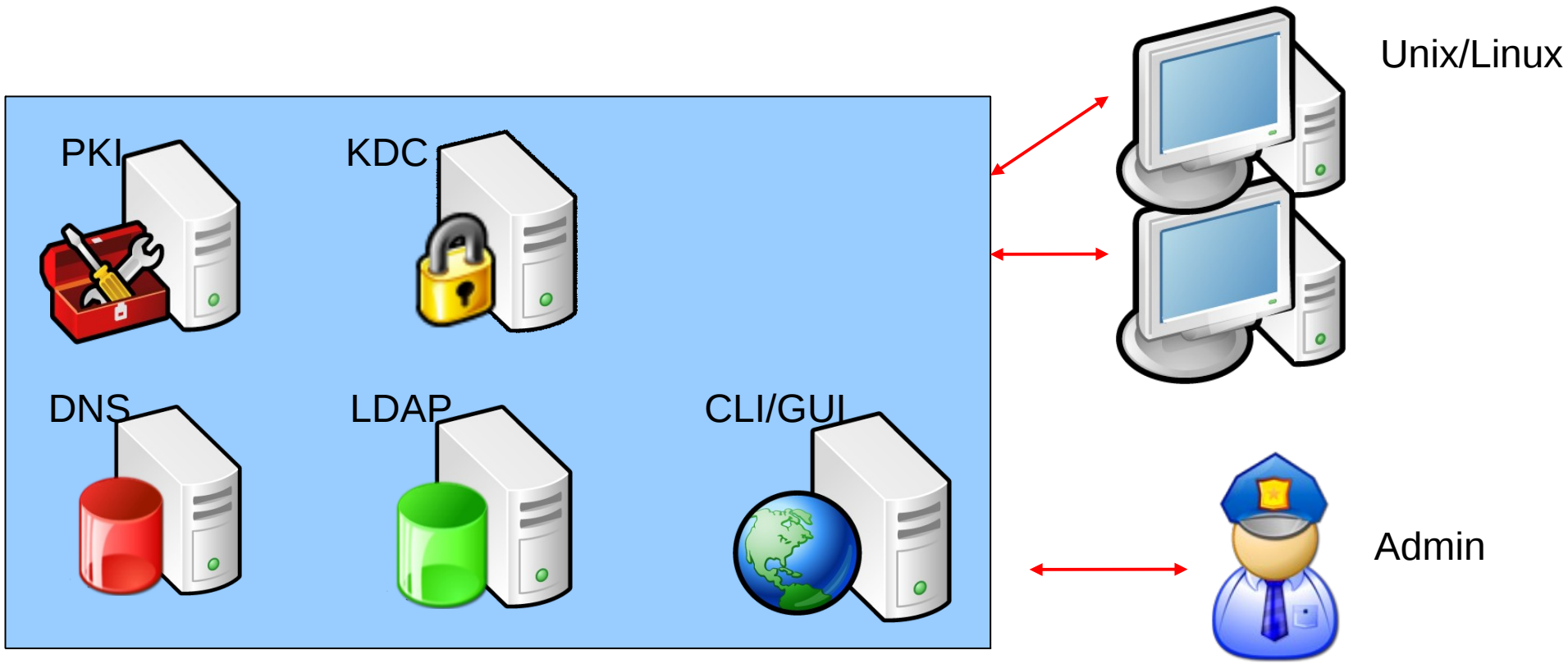
- Alle Komponenten sind offene Standards, “verheiratet” LDAP, Kerberos und weitere
- Versteckt die Komplexität → Benutzerfreundlich
- HBAC, Host Based Access Control. Regelt welche(r) User oder Usergruppe(n) auf welche(n) Host(s) oder Hostgruppe(n) Zugriff erhält.
- Multimaster Replikation, Hochverfügbarkeit by Design

IPA und die Features II

Zentrales Sudoers Management, welcher User darf welche Befehle* auf welchen hosts* als welcher user* ausführen (* oder Gruppen davon)

- Services autodiscovery (SRV Einträge im DNS)
- 2FA, Zweifaktor Authentifizierung
- DNS, erhöht den Grad an Automatisierung
- CLI
- WebUI
- Erweiterung von CLI/WebUI durch eigene Plugins

Architektur



Unterstützte Clients

Via SSSD

- RHEL 5.6+ (und EL clones wie CentOS 5.6+), sudoers via SSSD ab EL 5.9
- Fedora
- Ubuntu 14.04.2 LTS (Bug: Hostname nicht FQHN, `hostnamectl set-hostname $(hostname -f)` vor Enrollement repariert das Problem
- SLES 12 (manuelles Enrollment, kein ipa-client)
- Debian Stable (Wheezy) (manuelles Enrollment, kein ipa-client)
- Debian Unstable (Sid), selber Bug wie bei Ubuntu
- FreeBSD 10 (via 3rd Party repository, nicht getestet)

- Ohne SSSD, mit LDAP/Kerberos
  - RHEL (und EL clones) < 5.6 (kein Vendor-Support mehr → Upgrade!)
  - SLES <= 11
  - Unix Systeme wie AIX, Solaris, HPUX, BSD

IPA Client

IPA-client, ein Script zum problemlosen Enrolling

- Richtet alle benötigten Konfigurationsdateien ein:
  - /etc/sssd/sssd.conf
  - /etc/krb5.conf
  - /etc/nsswitch.conf
  - /etc/pam.d/*
- Upload der ssh public keys, Anpassungen ssh config
- Download Kerberos Keytab
- Erstellen Client Zertifikat
- Verfügbar für RHEL, Debian SID, Ubuntu 14.04 LTS

Skalierung

Mindestens zwei Replikas (multi-master) empfohlen.

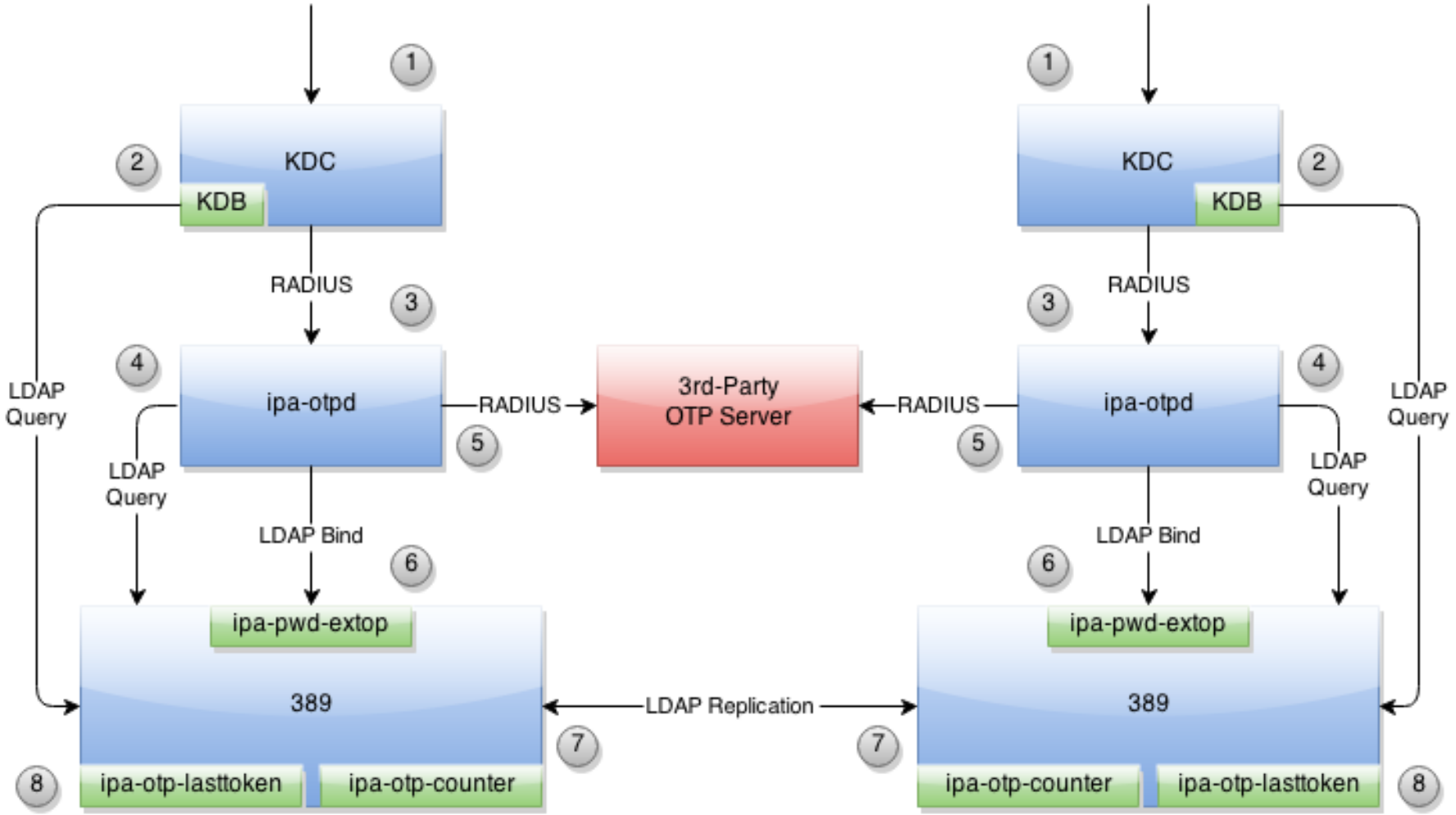
- 10'000 Server und tausende Benutzer sind null Problem
- Maximal vier “Replication Agreements” pro Server und maximal 20 IPA Server werden unterstützt, theoretisch sind mehr machbar aber selten sinnvoll
- Mehr Replikas erhöhen die Komplexität! Machmal ist weniger mehr.
- SSSD Cache nutzen, bei Legacy Systemen NSCD
- Enumeration sollte ausgeschalten werden (default)

Zweifaktor Authentifizierung

Neu ab (Free)IPA 4 (Fedora 21, RHEL 7.1)

- HOTP (Counter basierend, RFC 4226) und TOTP (Zeitbasierend, RFC 6238) mit eingebaut
- Funktioniert Out-of-the-box (und zwar schmerzlos)
- Unterstützte Tokens:
  - FreeIPA Android App
  - Google Authenticator App
  - Yubikeys und ähnliche
  - Proprietäre wie RSA via Radius Proxy (Nur Kerberos, kein LDAP)

Architektur 2FA



Implementierung

Zwei Replikas aufgesetzt, ein User plus ein Host enrolled in 10min

- Implementierungs- und/oder Migrationsprojekt umgesetzt in 10 Tagen bis zu 10 Monaten (je nach Komplexität und Grösse der Organisation)
- Die Organisation muss auf IPA abgebildet werden
- Konflikte mit Windows gibts fast immer (DNS SRV Records, Kerberos REALM)
- DNS Hoheit (externer DNS vs. IPA Managed DNS)

Und Windows?

Integration mit Samba z.Zt. nicht möglich, es ist aber was am “köcheln”. Zeitrahmen unbekannt.

- Einzelne Systeme können eingebunden werden, nicht empfohlen, IPA hat nicht die Features von AD
- Ein- oder Zweiwege Replikation mit MS Active Directory
- Crossdomain Trusts mit MS Active Directory
- “Single Source of Identity” von AD ist vielerorts ein Dogma, Replikation/Trusts bewahren dieses.
- Replikation/Trust mit AD technisch kein Problem, scheitert oft an organisatorischem

Integration von anderen Systemen

Postfix

- Zimbra
- Radius
- ...
- Alles was LDAP und/oder Kerberos unterstützt

-> http://www.freeipa.org/page/HowTos

Demo (falls es die Zeit erlaubt)

Links

http://www.freeipa.org/page/Main_Page

- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Linux_Domain_Identity_Authentication_and_Policy_Guide/index.html
- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/System-Level_Authentication_Guide/index.html