FreeIPA
Verzeichnisdienst und Authentifizierung leicht gemacht

Christian Stankowic
www.stankowic-development.net

Free and Open Source software Conference
21.08.2016

whoami

Christian Stankowic

Messer Information Services GmbH

Linux-/vSphere-Administrator

Blogger & Fachbuchautor

AGENDA

Agenda

Motivation

Installation

Client-Integration

Grundlegende Administration und Beispiele

MOTIVATION

Wozu zentrale Authentifizierung?

Benutzerinformationen werden an zentraler Stelle gesichert

kein Passwort-Wirrwarr

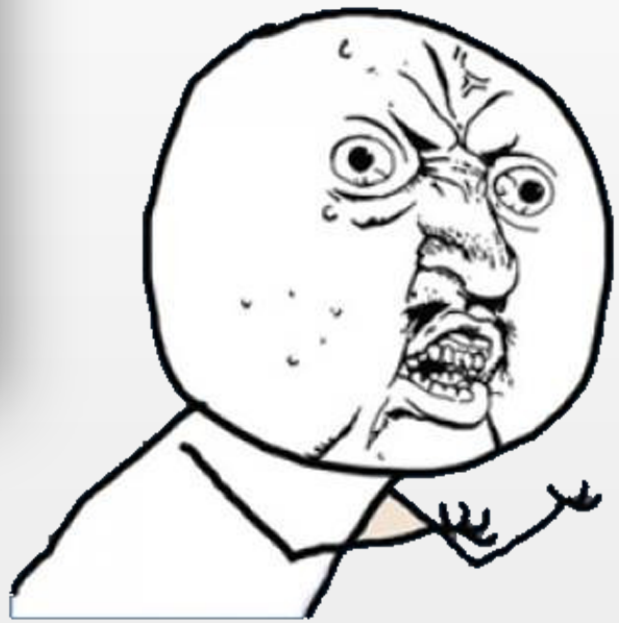
geringerer Aufwand nach Kündigungen

bei mehr als 2 Systemen absolut sinnvoll

1. bash

```
Christians-MacBook-Pro:~ christian$ ssh hmeis@10.22.2.2
hmeis@10.22.2.2's password:
Permission denied, please try again.
hmeis@10.22.2.2's password:
Permission denied, please try again.
hmeis@10.22.2.2's password:
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
Christians-MacBook-Pro:~ christian$ frhreuiorhfglre -.-
```

PASSWORDS



Y U NO CENTRALIZE

Was ist FreeIPA?

freie IPA-Lösung von Red Hat

Identify, **P**olicy, **A**udit

Unter RHEL auch als *Red Hat Identity Management (IdM)* bekannt

Vergleichbar mit Microsoft AD-DS und Novell eDirectory

Was ist FreeIPA?

Vereint in einer Web-Oberfläche:

- DNS-Server (**BIND9**)
- Verzeichnis-Dienst (**389ds**)
- Dogtag Zertifikatsystem
- MIT-Kerberos zur Authentifizierung und Single-Sign-On (**SSO**)

Features (1/2)

Verwaltung von DNS-Zonen

Pflege von Benutzer(*gruppe*)n, Hosts/Hostgruppen

sudo und **HBAC** (*Host Based Access Control*)-Regeln

rollenfähig (*z.B. Admins, Servicedesk,...*)

Features (2/2)

AD-DS-Trusts (*Version 3*+)

Mehrere Server/Replicas, Ausfallsicherheit / Lastverteilung

2FA (Zwei-Faktor-Authenfizierung) + **OTP** (*One-time password*)

zahlreiche APIs (*XML/JSONRPC, Python,...*)

INSTALLATION

System-Anforderungen

mindestens 2 CPUs

1 GB+ Arbeitsspeicher

10 GB+ Festplatte

Linux-Distributionen:

- Fedora
- Enterprise Linux (*RHEL, CentOS, SL*)
- Debian Sid / Ubuntu 16.04

Netzwerk-Anforderungen

IPv6 **sollte** deaktiviert werden

Uhrzeit per `ntpd` (*kein* `chronyd`)

Offene Ports:

- 80, 443, 8080 (*tcp, Web-Server*)
- 389, 636 (*tcp, ldap/ldaps*)
- 88, 464 (*tcp/udp, Kerberos*)
- 123 (*udp, NTP*)

Installation (1/3)

```
# yum install ipa-server{,-trust-ad}
# ipa-server-install
...
Do you want to configure integrated DNS (BIND)? [no]: yes
Server host name [st-ipa.stankowic.loc]:
Please confirm the domain name [stankowic.loc]:
Please provide a realm name [STANKOWIC.LOC]:
```

Listing 1: Paket-Installation, DNS und Realm konfigurieren

Installation (2/3)

```
Directory Manager password:
Password (confirm):
IPA admin password:
Password (confirm):
...
Do you want to configure the reverse zone? [yes]:
Please specify the reverse zone name [1.22.10.in-addr.arpa.]:
Using reverse zone(s) 1.22.10.in-addr.arpa.
```

Listing 2: Passwörter und Reverse Zones

Installation (3/3)

```
The IPA Master Server will be configured with:
Hostname: st-ipa.stankowic.loc
IP address(es): 10.22.1.3
Domain name: stankowic.loc
Realm name: STANKOWIC.LOC
BIND DNS server will be configured to serve IPA domain with:
Forwarders: 10.22.1.1, 10.22.0.2
Reverse zone(s): 1.22.10.in-addr.arpa.
Continue to configure the system with these values? [no]: yes
```

Listing 3: Zusammenfassung

freeIPA

Christian Stankowic

Identität | Regeln | Authentifizierung | Netzwerkdienste | IPA-Server

Benutzer | Benutzergruppen | Hosts | Host-Gruppen | Netgroups | Dienste | Automember

User categories

- Active users
- Stage users
- Preserved users

Active users

Suchen

Neu laden | Löschen | Hinzufügen | Deaktivieren | Aktivieren | Actions

Anmeldename	Vorname	Nachname	Status	UID	Email-Adresse	Telefonnummer	Tätigkeit
aadmi	Anton	Administrator	Aktiviert	35800005	aadmi@stankowic.loc		Administrator
admin		Administrator	Aktiviert	35800000			
cstan	Christian	Stankowic	Aktiviert	35800001	info@stankowic-development.net		IT-Administrator
hhelp	Helmut	Helpdesk	Aktiviert	35800009	hhelp@stankowic.loc		Helpdesk operator
max	Max	Mustermann	Aktiviert	35800006	max@stankowic.loc		
svc-cmdb	Calmund	Datenbank	Aktiviert	35800010	svc-cmdb@stankowic.loc		
svc-vro	Otto	Orchestrator	Aktiviert	35800008	svc-vro@stankowic.loc		

Zeige 1 bis 7 von 7 Einträgen.

INTEGRATION

Client-Anforderungen

`freeipa-client` registriert und konfiguriert automatisch:

- Kerberos
- LDAP-Client
- SSSD

Linux-Distributionen:

- Fedora
- Enterprise Linux (*RHEL, CentOS, SL*)
- Debian Sid / Ubuntu 16.04

Exkurs: SSSD

System **S**ecurity **S**ervices **D**aemon

zentrale Authentifizierung, lokaler Credentials-Cache

Integration in LDAP, IPA, AD-DS, Kerberos,...

Stellt **PAM**- und **NSS**-Module bereit

Client-Integration (1/4)

Paket `freeipa-client` installieren

FreeIPA-DNS gesetzt? (NS, SRV *records*)

Gültiger Hostname vergeben?

`ipa-client-install` aufrufen:

- `--mkhomedir` - Home-Ordner erstellen
- `--uninstall` - Registrierung aufheben
- `--domain` - Domäne manuell angeben

Client-Integration (2/4)

```
# yum install -y ipa-client
# hostnamectl set-hostname giertz.stankowic.loc
# ipa-client-install --mkhomedir
Discovery was successful!
Hostname: giertz.stankowic.loc
Realm: STANKOWIC.LOC
DNS Domain: stankowic.loc
IPA Server: st-ipa.stankowic.loc
BaseDN: dc=stankowic,dc=loc
Continue to configure the system with these
values? [no]: yes
```

Listing 4: Integration eines Clients

Client-Integration (3/4)

```
User authorized to enrole computers: cstan
Synchronizing time with KDC...
Password for cstan@STANKOWIC.LOC:
Successfully retrieved CA cert
...
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/sshd_config
Client configuration complete.
```

Listing 5: Integration eines Clients

Client-Integration (4/4)

```
# kinit cstan
Password for cstan@STANKOWIC.LOC:
# klist
Ticket cache: KEYRING:persistent:35800001:
krb_ccache_xTeMlYY
Default principal: cstan@STANKOWIC.LOC

Valid starting Expires Service principal
14.07.2016 23:03:25 15.07.2016 23:03:25 krbtgt/
STANKOWIC.LOC@STANKOWIC.LOC
# ssh st-ipa.stankowic.loc
```

Listing 6: Tests nach Integration

ADMINISTRATION

Benutzer(gruppen)

Definition typischer Benutzerinformation

LDAP-Schema erweiterbar

Benutzer lassen sich gruppieren

Beispiel: alle DB-Admins, alle FTP-Benutzer,...

freeIPA

Christian Stankowic

Identität | Regeln | Authentifizierung | Netzwerkdienste | IPA-Server

Benutzer | Benutzergruppen | Hosts | Host-Gruppen | Netgroups | Dienste | Automember

User categories

- Active users
- Stage users
- Preserved users

Active users

Suchen

Neu laden | Löschen | Hinzufügen | Deaktivieren | Aktivieren | Actions

Anmeldename	Vorname	Nachname	Status	UID	Email-Adresse	Telefonnummer	Tätigkeit
aadmi	Anton	Administrator	Aktiviert	35800005	aadmi@stankowic.loc		Administrator
admin		Administrator	Aktiviert	35800000			
cstan	Christian	Stankowic	Aktiviert	35800001	info@stankowic-development.net		IT-Administrator
hhelp	Helmut	Helpdesk	Aktiviert	35800009	hhelp@stankowic.loc		Helpdesk operator
max	Max	Mustermann	Aktiviert	35800006	max@stankowic.loc		
svc-cmdb	Calmund	Datenbank	Aktiviert	35800010	svc-cmdb@stankowic.loc		
svc-vro	Otto	Orchestrator	Aktiviert	35800008	svc-vro@stankowic.loc		

Zeige 1 bis 7 von 7 Einträgen.

freeIPA

Christian Stankowic

Identität | Regeln | Authentifizierung | Netzwerkdienste | IPA-Server

Benutzer | Benutzergruppen | Hosts | Host-Gruppen | Netgroups | Dienste | Automember

Benutzergruppen

Suchen

Neu laden | Löschen | Hinzufügen

Gruppenname	Gruppen-ID	Beschreibung
admins	35800000	Account administrators group
editors	35800002	Limited admins who can edit other users
icinga-users	35800012	Icinga user
ipausers		Default group for all users
service-users	35800011	Service users
spacewalk-admins	35800004	Spacewalk full administrators
spacewalk-readonly	35800007	Spacewalk read-only users
trust admins		Trusts administrators group

Zeige 1 bis 8 von 8 Einträgen.

Hosts/Hostgruppen

Hosts lassen sich in Gruppen zusammenfassen

Beispiel: alle Webserver, alle DB-Server,...

Hostgruppen lassen sich in sudo-/HBAC-Regeln verwenden

Immer Gruppen statt einzelne Hosts referenzieren!

freeIPA

Christian Stankowic

Identität | Regeln | Authentifizierung | Netzwerkdienste | IPA-Server

Benutzer | Benutzergruppen | Hosts | Host-Gruppen | Netgroups | Dienste | Automember

Hosts

Suchen

Neu laden | Löschen | Hinzufügen | Actions

Host name	Beschreibung	Enrolled
oprah6.kiez.loc	Chat host	
st-backup03.stankowic.loc	Backup appliance	
st-devel02.stankowic.loc	Gitlab and development system	True
st-esxi03.mgmt.stankowic.loc	ASUS-iKVM Management	
st-esxi03.stankowic.loc	ESXi-Host 1	
st-esxi04.mgmt.stankowic.loc	ASUS-iKVM Management	
st-esxi04.stankowic.loc	ESXi-Host 2	
st-htpc.stankowic.loc	HTPC	
st-ipa.stankowic.loc	IPA server	True
st-ipfire02.stankowic.loc	IPFire router	
st-katello01.stankowic.loc	Katello server	True
st-mail01.stankowic.loc	Mail server	True
st-mon02.stankowic.loc	Monitoring server	True
st-mon03.stankowic.loc	Monitoring server	True
st-power01.stankowic.loc	NETIO-230A rack PDU	
st-power02.stankowic.loc	NETIO-230B TV PDU	
st-power03.stankowic.loc	NETIO-230A office PDU	

freeIPA

Christian Stankowic

Identität | Regeln | Authentifizierung | Netzwerkdienste | IPA-Server

Benutzer | Benutzergruppen | Hosts | Host-Gruppen | Netgroups | Dienste | Automember

Host-Gruppen

Suchen

Neu laden | Löschen | Hinzufügen

Host-group	Beschreibung
devel	Development hosts
prod	Productive hosts

Zeige 1 bis 2 von 2 Einträgen.

HBAC-Regeln

Regeln *welche* Benutzer(*gruppen*) auf *welche* Hosts/Hostgruppen mit *welchem* Dienst zugreifen dürfen

Beispiel: alle DB-Admins auf alle DB-Server per SSH

Standard-Regel `allow_all` unbedingt **deaktivieren**!

kein Ersatz für Firewall-Regeln!

freeIPA

Anton Administrator

Identität | Regeln | Authentifizierung | Netzwerkdienste | IPA-Server

Host Based Access Control | Sudo | SELinux User Maps | Password Policies | Kerberos Ticket Policy

HBAC-Regeln » finch-users-TO-finch-hosts

HBAC-Regel: finch-users-TO-finch-hosts

Einstellungen

Neu laden | Revert | Save | Actions

General

Regelname: finch-users-TO-finch-hosts

Beschreibung: Allow finch users to access finch hosts over SSH/su

Wer

Benutzerkategorie, auf welche die Regel angewendet werden soll: ○ Jeder ◉ Spezifische Benutzer und Gruppen

Benutzer

Löschen + Hinzufügen

Benutzergruppen
finch-users

Löschen + Hinzufügen

Greift zu

Host-Kategorie, auf welche die Regel angewendet werden soll: ○ Jeder Host ◉ Spezifische Hosts und Gruppen

Hosts

Host-Gruppen
finch-hosts

Löschen + Hinzufügen

Benutzergruppe: finch-users

finch-users Mitglieder: Benutzer (2) | Benutzergruppen | External | Einstellungen

finch-users ist Mitglied von: Benutzergruppen | Netgroups

Neu laden | Löschen | + Hinzufügen

Anmeldename	UID	Email-Adresse
hmeis	1472800001	hmeis@kiez.loc
wwhin	1472800004	wwhin@kiez.loc

Zeige 1 bis 2 von 2 Einträgen.

Host Group: finch-hosts

finch-hosts Mitglieder: Hosts (1) | Host-Gruppen | Einstellungen

finch-hosts ist Mitglied von: Host-Gruppen | Netgroups | HBAC-Regeln (1)

Neu laden | Löschen | + Hinzufügen

Host name
oprah6.kiez.loc

Zeige 1 bis 1 von 1 Einträgen.

Mit Dienst

Service category the rule applies to: ○ Jeder Dienst ◉ Spezifische Dienste und Gruppen

Dienste
sshd
su
su-l

sudo-Regeln

Steuerung von Kommandos und Kommandogruppen

Definition von:

- Benutzer(*gruppen*)
- Hosts/Hostgruppen
- Kommandos/Kommandogruppen
- alternative Identitäten

Befehle ausführen

Befehlskategorie, auf die die Regel angewendet werden soll: ○ Jeder Befehl ◉ Spezifische Befehle und Gruppen

Erlauben

☐	**Sudo Allow Commands**

☐	**Sudo Allow Command Groups**
☐	delegating
☐	drivers
☐	editors
☐	filemgmt
☐	fileperm
☐	fileperm-acl
☐	ipa-client
☐	ipa-server
☐	locate
☐	monitoring
☐	networking
☐	processes
☐	selinux
☐	services
☐	software
☐	storage
☐	usermgmt
☐	rhn-client

Sudo-Befehle

Suchen

☐	**Sudo-Befehl**
☐	/bin/bash
☐	/bin/cat
☐	/bin/chgrp
☐	/bin/chmod
☐	/bin/chown
☐	/bin/cp
☐	/bin/csh
☐	/bin/dash
☐	/bin/df
☐	/bin/du
☐	/bin/echo
☐	/bin/find
☐	/bin/kill
☐	/bin/ksh
☐	/bin/ls
☐	/bin/mkdir
☐	/bin/mksh
☐	/bin/more
☐	/bin/mount
☐	/bin/mv

Zeige 1 bis 20 von 234 Einträgen.

Exkurs: ipa-sudo-basic-rules (1/2)

Gruppierung gängiger Administrationskommandos (*derzeit 250*)

Erstellt automatisch sudo-Kommandos und Kommandogruppen

Python-Skript, deploy’n’play

Download auf **github.com/stdevel/freeipa-stuff**

Exkurs: ipa-sudo-basic-rules (2/2)

```
$ ./ipa-sudo-basic-rules.py -i
INFO:ipa-sudo-basic-rules.py:This definition has version 0.1.9 and consists of 33 command groups and 255 commands.

$ ./ipa-sudo-basic-rules.py -n
INFO:ipa-sudo-basic-rules.py:I'd like to execute the following command: ipa sudocmdgroup-add firewall --desc='Managing firewall configuration'
...
```

Listing 7: Installation eines Katalogs simulieren

FRAGEN?

Links

FreeIPA-Webseite: **freeipa.org**

Deployment Recommendations

Quickstart Guide

Active Directory trust setup

freeipa-stuff-Repository auf GitHub

Vielen Dank für die Aufmerksamkeit!

http://www.stankowic-development.net

@stankowic_devel

Christian Stankowic

stankowicdevel