Free IPA on CentOS 7

Begin met een Clone van de CentOS7 minimal

zet ipv6 aan voor het loopback interface

Zet ipv6 aan voor het loopback interface, FreeIPA heeft dit nodig, maar we willen voorlopig eth0 geen ipv6 adress geven.

`vi vi /etc/sysctl.conf`

en voeg de volgende regels toe:

```
net.ipv6.conf.eth0.disable_ipv6=1
net.ipv6.conf.lo.disable_ipv6=0
```

Zorg dat de volgende regel in `/etc/hosts` staat:

```
::1         localhost localhost.localdomain localhost6
localhost6.localdomain6
```

Pseudo random generator

De IPA server gebruikt random om keys, passwords en certificaten te maken. Omdat hij op een VM wordt geïnstalleerd is het zaak om een pseudo random generator te gebruiken om te zorgen dat het systeem geen tekort aan entropy krijgt.

Installeer haveged:
```
yum install haveged
systemctl start haveged
systemctl enable haveged
```

Alternatief is om in KVM een RNG device toevoegen (server moet hier voor uit) in VMWare is deze optie er niet, en ben je toegewezen op haveged of de minder random `/dev/urandom`.

installeer de software

de installatie is eenvoudig:

`yum install ~~ipa-server-dns~~ ipa-server -y`

Configureer IPA

run het configuratie script:

```
ipa-server-install
```

of met DNS:
```
ipa-server-install --setup-dns
```

en beantwoord de vragen:

```
The log file for this installation can be found in /var/log/ipaserver-
install.log
==============================================================================
==
This program will set up the IPA Server.

This includes:
  * Configure a stand-alone CA (dogtag) for certificate management
  * Configure the Network Time Daemon (ntpd)
  * Create and configure an instance of Directory Server
  * Create and configure a Kerberos Key Distribution Center (KDC)
  * Configure Apache (httpd)
  * Configure the KDC to enable PKINIT

To accept the default shown in brackets, press the Enter key.

WARNING: conflicting time&date synchronization service 'chronyd' will be
disabled
in favor of ntpd

Do you want to configure integrated DNS (BIND)? [no]:

Enter the fully qualified domain name of the computer
on which you're setting up server software. Using the form
<hostname>.<domainname>
Example: master.example.com.


Server host name [ipaserver.domein.nl]:

The domain name has been determined based on the host name.

Please confirm the domain name [domein.nl]:

The kerberos protocol requires a Realm name to be defined.
This is typically the domain name converted to uppercase.

Please provide a realm name [DOMEIN.NL]:
```

```
Certain directory server operations require an administrative user.
This user is referred to as the Directory Manager and has full access
to the Directory for system management tasks and will be added to the
instance of directory server created for IPA.
The password must be at least 8 characters long.

Directory Manager password:Pa55w0rd
Password (confirm):Pa55w0rd

The IPA server requires an administrative user, named 'admin'.
This user is a regular system account used for IPA server administration.

IPA admin password:Pa55w0rd
Password (confirm):Pa55w0rd


The IPA Master Server will be configured with:
Hostname:       ipaserver.domein.nl
IP address(es): 192.168.1.207
Domain name:    domein.nl
Realm name:     DOMEIN.NL

Continue to configure the system with these values? [no]: yes

The following operations may take some minutes to complete.
Please wait until the prompt is returned.
```

Kerberos ticket maken

`kinit admin` geef het IPA admin password wat je eerder hebt opgegeven bij de configuratie.

list de tickets: `klist`

start de sssd

```
systemctl enable sssd
systemctl start sssd
```

open de firewall

```
firewall-cmd --permanent --add-
service={ntp,http,https,ldap,ldaps,kerberos,kpasswd,dns}
firewall-cmd --reload
```

inloggen

Op dit moment is de installatie voltooid.

log in op de webinterface met user ADMIN en het password wat je eerder voor `IPA admin password` hebt opgegeven.

Vanaf hier zijn de vogende stappen:

gebruikers aanmaken

Als eerste zorgen we er voor dat de default sheel van een nieuwe gebruiker de bash shell is;

```
ipa config-mod --defaultshell=/bin/bash
```

Zorg er voor dat homedirectories van nieuwe users kunnen worden aangemaakt:

```
authconfig --enablemkhomedir --update
```

cliënt koppelen

Om clients te kunnen koppelen is een kerberos ticket nodig. maak het admin ticket door:

Linux OS servers

Work in Progress

Microsoft OS werkstations

Work in Progress

Mac OSX werkstations

Work in Progress

KeyCloak applications IAM

Work in Progress

sssd to cach credentials from off-site IPA

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/identity_management_guide/setting_up_ipa_replicas#replica-topologies

Rather than using a server or replica, small offices can use SSSD to cache credentials and use an off-site IdM server as its data backend.

Bronnen

https://www.certdepot.net/rhel7-configure-freeipa-server/

https://holdmybeersecurity.com/2017/02/05/installsetup-freeipa-on-centos-7/

http://www.juliosblog.com/freeipa-server-on-centos-7/

https://www.globo.tech/learning-center/install-freeipa-centos-7/