https://www.youtube.com/watch?v=8wc4MO3LXQI
Red Hat Identity Management is now included in RHEL7.

- 2GB RAM - 12GB HD for Server with Graphic Int, default partitioning
- Turn off SELinux (setenforce=0 vim /etc/sysconfig/selinux/ set SELINUX=PERMISSIVE
192.168.4.200 and
192.168.4.2 GW
8.8.8.8 DNS
- yum repolist --to make sure you have access to the CentOS repos (of course you would in a fresh install!)
- vim /etc/hosts and put an entry in for name resolution of this machine the .200 IP to ipa.example.com and labipa.example.com
- yum -y install ipa-server bind-dyndb-ldap ipa-server-dns

IMPORTANT SIDENOTE- HE UPGRADED to 7.2 from 7.0 and it nuked his default route - temp fix: route add default via 192.168.4.2 - said upgrade is what nuked it. Better do /vim /etc/sysconfig/network-scripts/ifcfg-eth0 to make it permanent!! In this file, we found the right IP for the GW but it was called GATEWAY0= and CentOS needs this file to be GATEWAY=

ipa-server-install --setup-dns

Will use TLS CA, installs Directory Server (LDAP), Kerberos KDC, Apache and bind
Will try to use ntpd disabling local chrony
(asks for hostname with your hostname in parens- it needs to match - if it doesn't prompt it will break)
make sure the next prompts also match- "realm" is like domain in Windows. dns is fine
Directory Manager password (sets the password)
IPA admin password (sets the password)
Asks to overwrite existing bind configuration say yeah so it matches this package
DNS forwarders?- Yes since this is our s put 8.8.8.8
Another forwarder? no don't need
Reverse zone - will be the in-addr.arpa reverse version of our ip
It then verifies with overview, say yes and it goies.

Note- cert server install says pki-tomcatd
Directory server install is called dirsrv
Kerberos KDC called krb5kdc - this step you need entropy to make keys/certs
Certs are stored in /root/cacert.p12 (in the example) and we are advised to back them up (it tells us the location) when the program install concludes. It turns out that is for admin access- user CAs are stored in /etc/ipa/ca.crt - he contradicts and says a few minutes later this is the kerb server CA. He says for LDAP this is going to be wrong and need fixing later (in another lesson)

run kinit admin as instructed by installer upon completion to make kerberos ticket and add users with ipa user-add. It wil prompt for password and give no response, but grant access to run ipa user-add
klist to show kerberos credentials
Because we just set up bind, cat /etc/resolve.conf should show the loopback instead of 8.8.8.8

Firefox should now be able to go to localhost and it will resolve to something like labipa.example.com/ipa/ui/

Web interface lets you add other servers you have (NFS) Go to network services> DNS Resource Records, and click "add"
That was all from https://www.youtube.com/watch?v=8wc4MO3LXQI
I was able to download the new appendix and other file in folder called sander-dwnlds

Red Hat Enterprise Linux IdM
https://www.freeipa.org/

Based on FreeIPA - Identity Policy Audit

- Provides 369 Dir Server (main LDAPv3-based data store- replaces OpenLDAP)
- SSO provided by MIT Kerberos KDC

- Integrated certificate system based on TLS
- Integrated NTPd (local Chrony will be disabled when using!)
- Integrated optional DNS server based on ISC Bind Service

IdM needs to be on a dedicated server not running NTP, DNS, LDAP
- IdM needs hostname resolution for itself, either through DNS or /etc/hosts. (do before install)
- ipa-client and ipa-server for those components.

We will be using AuthConfig instead of Client, and "ipa-server-install" for a scripted server installation
The ipa tool is a generic client interface
- ipa user-add username
- ipa passwd username
- ipa user-find username
- ipa-xxx to locate other tasks, use ipa-<tab> for others (tab completion)

Preinstall:
- fix hostname resolution
- disable nscd and any LDAP or Kerberos services, NTP, DNS/BIND
- Open ports: LDAP, Kerberos, DNS,

yum -y install ipa-server bind nds-ldap
ipa-server-install guided install
[Long version command-line install with options (for scripting):
ipa-server-install --hostname=server.example.com -n example.com -r EXAMPLE.COM -p password -a password -U --no-ntp]
Restart SSH **systemctl restart sshd** to obttain kerberos credentials
Verify for default admin user: **kinit admin**
Many problems crop up when there simply in not longer a valid kerberos ticket

Before managing the IdM server you need to log into the domain for an admin ticket:
Generate ticket: **kinit admin**
Show ticket validity: **klist**

ipa help commands and **ipa help user-add** for a specific command
Browser administration: load https://myserver.example.com for the IPA management interface

<u>User account creation</u>
- ipa user-add username
- ipa passwd username
- ipa user-find username

AuthConfig Setup -
yum install authconfig-gtk
Run **authconfig-gtk** and it brings up an Authentication Configuration window (looks like many systems settings windows)

Panel1 - Identity and Authentication
User Account DB: Choices of Local Accounts Only, LDAP, IPAv2, FreeIPA, NIS, Winbind
[LDAP for kerberos Auth will tell you to install addl packages. Fill in LDAP Search Base DN and LDAP Server field.
- Checkbox offers TLS option and button to DL a CA certificate for that option]
- Here we install addl packages it mentions, provided by nss.pam.ldapd. It gives us an install button so its easy.

Then it wants to install pam_kbr5, do so. Then it's done.

At the bottom of the same panel for LDAP is also Authentication Method section asking for Realm, KDCs, Admin Servers, option checkboxes to use DNS to resolve hosts to realms (unchecked) and Use DNS to locate KDCs for realms (checked). Diff options for non-Kerberos

Window supposedly will populate after installing the requirements- doesn't, he says because of a low-screen resolution bug). Closed window and rean authconfig-tui instead

in the TUI, authentication Config brings up "use LDAP" checked, and auth options, which have LDAP auth unchecked- but options "kerberos, local auth is sufficient, and use shadow passwords" all checked

authconfig --help   Many options! Great for scripting.

<u>Client:</u>
Ensure /etc/hosts has lines for the machines.

    192.168.x.x server.example.com   server1

Make sure /etc/resolve.conf has the IP address of the kerberos server in a line like this:
nameserver 192.168.x.x

Run authconfig-tui
Check Use LDAP for user config, and kerberos for authentication
Next window is LDAP settings: use TLS? yes, and change server to server1.example.com
    Make sure Base DN has the right domain components: dc=example, dc=com
Next window: Kerberos settings. Realm- EXAMPLE.COM (our DNS domain)
    KDC leave blank, same with admin server. Check BOTH "Use DNS to locate KDCs for realms" and "resolve hosts to realm" for that stuff

A window pops up saying TLS on LDAP needs a CA cert signed by server's cert. Copy in PEM format to /etc/openldap/cacerts directory and press ok.
    If you get this on the exam, you will be provided an FTP link to get the CA- says this isn't an exam objective so it shouldn't come up.
    Just hit "ok" and go to the directory, then **ssh server2** to log in.
Login landed us in server2's root directory. LS lists anaconda-ks.cfg, ca-agent.pl2, cacert.pl2, initial-setup-ks.cfg
We only needed the pathname here so exit the ssh connection
    Run "**scp server2:/root/cacert.pl2**"

There is a quicker way to do this: Open authconfig-gtk - the LDAP Server info is populated from what we did in the TUI. Check "Use SSL" and the "Download CA Certificate" button will ask us where to look.
It should be noted that in the example, the Kerberos settings that also were put in are blank in the GUI. This is blamed on the GUI having bugs as described previously

If you get authentication errors here is a fix:
vim /etc/nslcd.conf
Comment out the line that says "tls_reqcert never" which allows TLS without certificates, which is sometimes ok in a production environment, here it might be interfering with our setup
If it doesn't use nslcd.conf, try telling sssd.conf to not be too critical about certificates. Add this line if that's the case "ldap_tls_required_cert=never"

--- THIS SAYS TUI IS DEPRECATED!!
https://www.certdepot.net/rhel7-configure-system-use-existing-ldap-directory-service-user-group-information/
<u>LDAP Client configuration</u>

As the authconfig-tui is deprecated, to configure the LDAP client side, there are two available options: nslcd and sssd. In this tutorial, the nslcd option will be used, see the authconfig tutorial for the sssd option.

Install the following packages:

```
# yum install -y openldap-clients nss-pam-ldapd
```

Note: Just to mention that Sander van Vugt advises to install the Directory Client group package: # yum group install “Directory Client”

Then, type:

```
# authconfig --enableforcelegacy --update
# authconfig --enableldap --enableldapauth --ldapserver="instructor.example.com" \
--ldapbasedn="dc=example,dc=com" --update
```

Note1: According to your requirements, you can need to specify the –enablemkhomedir option after the installation of the oddjob-mkhomedir package. The option creates a local user home directory at the first connection if none exists.
Note2: Type # authconfig –help | grep ldap to remember the necessary options.

Put the LDAP server certificate into the /etc/openldap/cacerts directory:

```
# scp root@instructor.example.com:/etc/openldap/certs/cert.pem \
/etc/openldap/cacerts/cert.pem
```

Apply the correct SELinux context to the certificate:

```
# restorecon /etc/openldap/cacerts/cert.pem
```

Activate the TLS option

```
# authconfig --enableldaptls --update
```

Test the configuration:

```
# getent passwd ldapuser02
ldapuser02:*:1001:1001:ldapuser02:/home/guests/ldapuser02:/bin/bash
```

NFS server configuration
To get the home directory mounted, you need to configure a NFS server.
The NFS server is called instructor.example.com in the procedure.
Note: It’s not required to have the LDAP server and the NFS server on the same machine, it’s only easier.
Automounter Client configuration

Install the following packages:

```
# yum install -y autofs nfs-utils
```

Create a new indirect /etc/auto.guests map and paste the following line:

```
* -rw,nfs4 instructor.example.com:/home/guests/&
```

Add the following line at the beginning of the /etc/auto.master file:

```
/home/guests /etc/auto.guests
```

Start the Automounter daemon and enable it at boot:

```
# systemctl enable autofs && systemctl start autofs
```

Test the configuration:

```
# su - ldapuser02
```

Continuing with lesson conclusion (despite "issues" with curriculum)

Configuration files: Things to know
cd /etc/sysconfig/
vim authconfig
(paste file contents here - didn't find with Goggle)
Has stuff like USELDAP=yes, USEKERBEROS=yes

/etc/sssd/sssd.conf
This is arguably the most important file here
This file contains variable showing the server names, the domain components, other stuff for LDAP and Kerberos
Tells which directory to look for CACERTs and all that. It specifies the kerberos information matched in the krb5 file

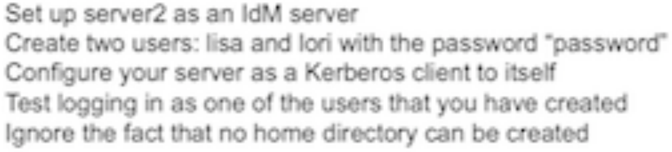
/etc/krb5.conf
All the server info for kerberos, DNS mapping, realms, ticket lifetime and other values, and where the logs live.

/etc/nsswitch.conf
Has the lines passwd, shadow and group, and for each is specified the order to look for authentication info
passwd: files   sss

/etc/nslcd.conf
This is the old LDAP config file, which existed in early versions of RHEL7
It is superceded by sssd.conf

If the tui etc are different it doesn't matter does it? You see this is where that stuff is stored!

Exercise 1 - RHCE Video part07.mp4


Set up server2 as an IdM server
Create two users: lisa and lori with the password "password"
Configure your server as a Kerberos client to itself
Test logging in as one of the users that you have created
Ignore the fact that no home directory can be created

systemctl stop firewalld
BE CAREFUL WITH THIS BECAUSE YOU CAN GET POINTS COUNTED OFF IF YOU HAVE THE FIREWALL OFF

Add these to your /etc/hosts file (your equivalents)
192.168.1.4   server1.example.com   server1
192.168.1.5   server2.example.com   server2

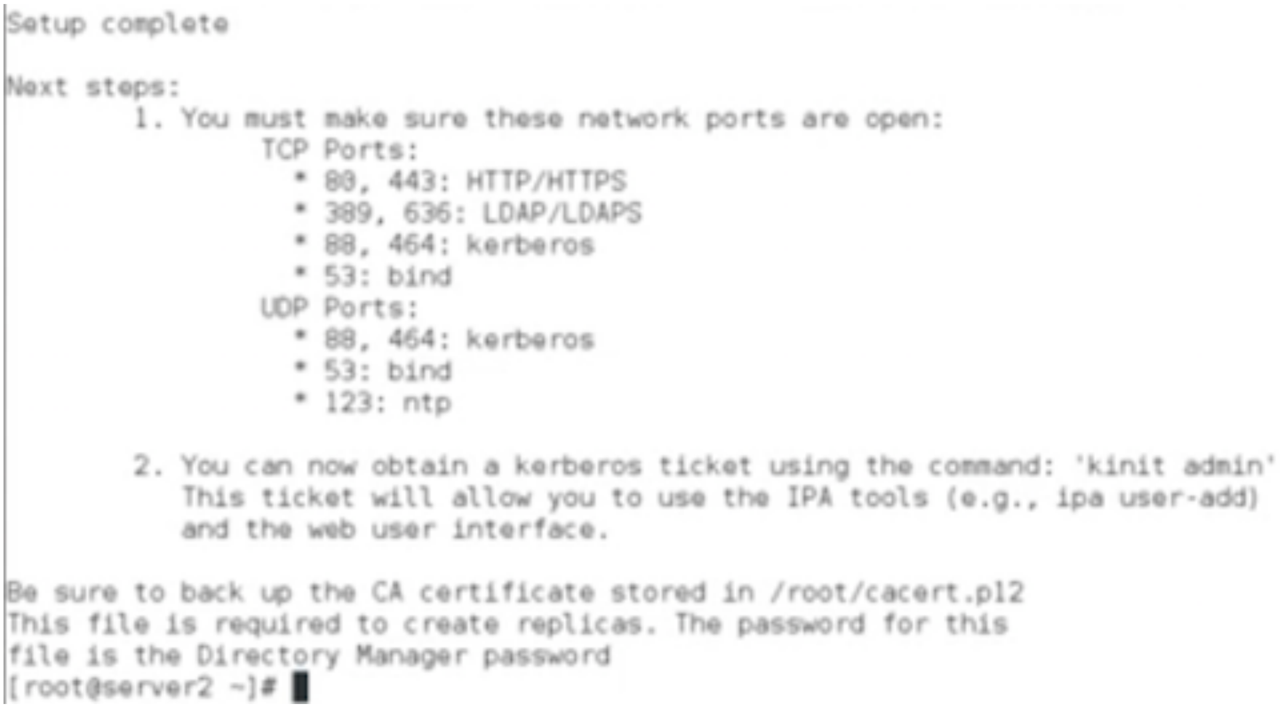
Turn off any services having to do wi nslcd, kerberos, ldap. Since they weren't turned on yet and these are fresh systems, check, but they should be on.

yum -y install ipa-server bind nds-ldap
ipa-server-install
- it tells us chronyd is going to be disabled in favor of ntpd
- it asks if we want to configure intergrated DNS (BIND) YES
- STOP it complains we need a plugin installed, do it

yum -y install bind-dyndb-ldap
- DONE ok continuing where it left off (start again)
- Existing BIND configuration. Overwrite?   YES
- Server host names: Confirm domain name: realm name: These should be grabbed automatically from the hosts file. If it doesn't, there is a problem with the host file. The defaults should be (more or less) correct.

- Directory Manager password: (set it, then confirm)
- IPA "admin" user- same thing.
- Do you want to configure DNS forwarders? YES (for external hosts)
- It asks for an IP address - 8.8.8.8
- Do you want to configure a reverse zone? YES Please specify: default is something like 1.168.192.in-addr.arpa You can just accept it unless it is obviously weird. It should just look like your subnet in reverse order
- Do you want to configure the system with this stuff (YES)

DONE.



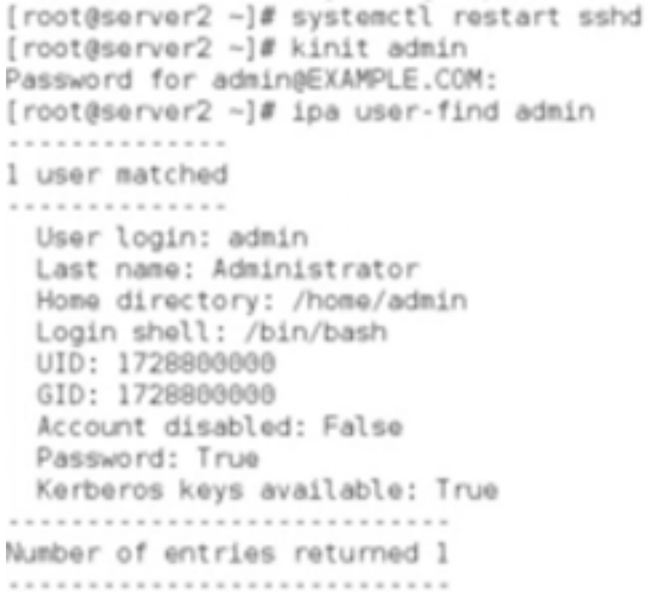
```
Setup complete

Next steps:
        1. You must make sure these network ports are open:
                TCP Ports:
                  * 80, 443: HTTP/HTTPS
                  * 389, 636: LDAP/LDAPS
                  * 88, 464: kerberos
                  * 53: bind
                UDP Ports:
                  * 88, 464: kerberos
                  * 53: bind
                  * 123: ntp

        2. You can now obtain a kerberos ticket using the command: 'kinit admin'
           This ticket will allow you to use the IPA tools (e.g., ipa user-add)
           and the web user interface.

Be sure to back up the CA certificate stored in /root/cacert.p12
This file is required to create replicas. The password for this
file is the Directory Manager password
[root@server2 ~]# 
```

Restart sshd - systemctl restart sshd
kinit admin - log in
ipa user-find admin



```
[root@server2 ~]# systemctl restart sshd
[root@server2 ~]# kinit admin
Password for admin@EXAMPLE.COM:
[root@server2 ~]# ipa user-find admin
--------------
1 user matched
--------------
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  UID: 1728800000
  GID: 1728800000
  Account disabled: False
  Password: True
  Kerberos keys available: True
----------------------------
Number of entries returned 1
----------------------------
```

ipa user-add lisa   -will ask for first, last name
ipa passwd lisa --set a password
ipa user-find lisa   --check it out

ssh server1
fix up it's /etc/hosts file
authconfig-tui
Choose LDAP for auth make sure LDAP is off, kerberos is on
Use TLS? yeah.
Kerberos settings - make sure realm matches, KDC and admin server can be blank.
This time example only checked use DNS to LOCATE KDCs, and not to resolve hosts (not both)

What is on the exam and what isn't? Exam covers setting up client to autoconfig with kerberos. Does not need you to know how to set up IdM.